DUMPSBOSS.

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

Cisco 300-715

Version Demo

Total Demo Questions: 37

Total Premium Questions: 379

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, ISE Architecture and Deployment	45
Topic 2, ISE Policy Administration and Management	16
Topic 3, ISE Profiling	50
Topic 4, ISE Authentication and Authorization	134
Topic 5, ISE Guest Services	42
Topic 6, ISE Posture	30
Topic 7, ISE Compliance and Remediation	5
Topic 8, ISE BYOD	34
Topic 9, ISE pxGrid	3
Topic 10, ISE Troubleshooting	15
Topic 11, Mix Questions	5
Total	379

QUESTION NO: 1

An organization has a fully distributed Cisco ISE deployment. When implementing probes, an administrator must scan for unknown endpoints to learn the IP-to-MAC address bindings The scan is complete on one PSN, but the information is not available on the others.

What must be done to make the information available?

A. Cisco ISE must be configured to learn the IP-MAC binding of unknown endpoints via RADIUS authentication, not via scanning.

B. Cisco ISE must learn the IP-MAC binding of unknown endpoints via DHCP profiling, not via scanning.

C. Scanning must be initiated from the MnT node to centrally gather the information.

D. Scanning must be initiated from the PSN that last authenticated the endpoint.

E. Configure centralized profiling so probe/scan-learned IP-to-MAC bindings are collected on the profiling node and replicated/available to all PSNs.

ANSWER: E

Explanation:

In a fully distributed Cisco ISE deployment, endpoint profiling data (including IP-to-MAC bindings learned by probes) is not automatically shared between Policy Service Nodes unless profiling is centralized. To make scan-learned IP-to-MAC bindings available to all PSNs, profiling must be configured to use a centralized node that collects and distributes profiling attributes across the deployment. This is done by enabling a dedicated Profiling Service on a single node (commonly the PAN/Monitoring persona depending on design) and configuring the other PSNs to forward profiling data to that central profiling node, so all PSNs can consume the same endpoint identity and profiling attributes. Without centralized profiling, a scan performed by one PSN can remain local to that node's profiling database view, which is why other PSNs do not see the learned bindings. Cisco's profiling guidance describes the need for centralized profiling in distributed designs to ensure consistent endpoint visibility and attribute sharing across PSNs.

References: Cisco Community – ISE Profiling Design Guide, Cisco ISE Install & Config Guides

QUESTION NO: 2

A company manager is hosting a conference. Conference participants must connect to an open guest SSID and only use a preassigned code that they enter into the guest portal prior to gaining access to the network.

How should the manager configure Cisco ISE to accomplish this goal?

A. Create logins for each participant to give them sponsored access.

B. Create entries in the guest identity group for all participants.

C. Create an access code to be entered in the AUP mode.

D. Create a registration code to be entered on the portal splash page.

ANSWER: D

Explanation:

Creating a registration code to be entered on the portal splash page is the right approach because it matches the requirement for an open guest SSID where users are not issued individual usernames/passwords, but instead must enter a preassigned code in the guest portal before being granted access. In Cisco ISE Guest, a registration (or “guest”) code workflow is designed for events like conferences where you want a simple shared code that gates access through the portal. The user connects to the open SSID, is redirected to the guest portal, and enters the provided code; ISE then authorizes the session according to the guest access policy without needing per-user account creation or sponsorship. This is commonly implemented using a Guest portal flow that supports self-registration with a registration code (or a hotspot/guest access flow depending on the portal type) and an authorization rule that permits network access after successful portal completion.

References: Cisco ISE Admin Guide – Guest Access, Cisco ISE Install & Config Guides

QUESTION NO: 3

What is a difference between RADIUS versus TACACS+ with regards to packet encryption?

A. TACACS+ encrypts the entire body of the packet, and RADIUS encrypts the username and password in the access-request packet.

B. RADIUS encrypts the entire body of the packet, and TACACS+ encrypts the username and password in the access-request packet.

C. RADIUS encrypts the entire body of the packet, and TACACS+ encrypts only the password in the access-request packet.

D. TACACS+ encrypts the entire body of the packet, and RADIUS encrypts only the password in the access-request packet.

ANSWER: D

Explanation:

TACACS+ encrypts the entire body of the packet, and RADIUS encrypts only the password in the access-request packet.

This is the key encryption distinction between the two AAA protocols. TACACS+ uses TCP and encrypts the full payload (the TACACS+ packet body), which includes the authentication and authorization content, leaving only a small header in cleartext. This provides better confidentiality for AAA attributes exchanged between the network device (NAS) and the TACACS+ server. In contrast, classic RADIUS uses UDP and does not encrypt the entire packet; it protects only the User-Password attribute in an Access-Request by obfuscating it using a shared secret and an MD5-based mechanism. Other RADIUS attributes (including the username and many authorization-related attributes) are not encrypted, which is why RADIUS is often paired with additional protections such as IPsec or run in environments where transport security is otherwise addressed. This difference is commonly tested because it impacts how much sensitive authorization/accounting data is exposed on the wire when comparing RADIUS to TACACS+.

References: Cisco - RADIUS and TACACS+ Overview, RFC 2865 (RADIUS Authentication)

QUESTION NO: 4

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:

To validate that a host-based firewall is present without tying the posture policy to a specific vendor's firewall product, Cisco ISE posture provides a built-in firewall posture condition. This condition is designed to evaluate the endpoint's firewall state (enabled/disabled) in a vendor-agnostic way, which is exactly what you need when endpoints may run different third-party firewall products across Windows and macOS. In practice, you enable and use the default firewall condition in the posture policy so the posture agent can report firewall status and ISE can enforce access based on whether a firewall is active. This approach avoids brittle checks like looking for a particular application name, file, or registry key, which vary widely by vendor and can be bypassed or change across versions. Using the default firewall condition also aligns with best practice: check the security control's state rather than the presence of a specific executable. For more detail on ISE posture conditions and how posture evaluates endpoint security controls, see Cisco ISE Posture documentation: Cisco ISE Install and Configure Guides and the ISE posture overview resources: Cisco Identity Services Engine (ISE).

QUESTION NO: 5

An administrator is configuring a Cisco ISE posture agent in the client provisioning policy and needs to ensure that the posture policies that interact with clients are monitored, and end users are required to comply with network usage rules Which two resources must be added in Cisco ISE to accomplish this goal? (Choose two)

A. AnyConnect

B. Supplicant

C. Cisco ISE NAC

D. PEAP

E. Posture Agent

ANSWER: A E

Explanation:

To monitor posture policies on endpoints and enforce that users comply with network usage rules, Cisco ISE relies on the Cisco AnyConnect Secure Mobility Client with the ISE Posture module. In ISE Client Provisioning, you must add the AnyConnect resource so endpoints can download/install the AnyConnect client package, and you must also add the Posture

Agent resource (the posture module/profile delivered via AnyConnect) so the endpoint can perform posture assessment and report compliance status back to ISE. Together, these resources enable ISE to run posture checks (such as AV/AS status, firewall, disk encryption, etc.), continuously monitor compliance, and trigger authorization changes (for example, quarantine/remediation vs. full access) based on posture results. This is the standard Cisco ISE posture workflow: ISE provisions AnyConnect, AnyConnect hosts the posture module, and ISE evaluates posture results to enforce policy. See Cisco AnyConnect Posture configuration guidance and ISE client provisioning documentation for how posture is delivered and used for compliance enforcement: Cisco AnyConnect Administrator Guide – Configure Posture and Cisco ISE Admin Guide – Configure Client Provisioning.

QUESTION NO: 6

An engineer tests Cisco ISE posture services on the network and must configure the compliance module to automatically download and install on endpoints.

Which action accomplishes this task for VPN users?

A. Push the compliance module from Cisco FTD prior to attempting posture.

B. Use a compound posture condition to check for the compliance module and download, if needed.

C. Configure the compliance module to be downloaded from within the posture policy.

D. Create a Cisco AnyConnect configuration and Client Provisioning policy within Cisco ISE.

ANSWER: D

Explanation:

Creating a Cisco AnyConnect configuration and Client Provisioning policy within Cisco ISE is the correct way to automatically download and install the posture compliance module for VPN users. In an ISE posture deployment, the “compliance module” is delivered as part of the AnyConnect Posture module, and ISE handles distribution using Client Provisioning (often via the Client Provisioning Portal and/or the AnyConnect ISE Posture agent workflow). For remote-access VPN, endpoints typically already run AnyConnect, and ISE can be configured with an AnyConnect configuration (including the posture module package and profile) and a Client Provisioning policy that targets the VPN user session so the required module is installed when missing or outdated. This approach aligns with Cisco’s design where posture assessment depends on the AnyConnect posture components being present, and ISE’s Client Provisioning is the supported mechanism to automate that installation rather than trying to “push” it from a firewall or embedding downloads directly inside posture policy logic. See Cisco ISE Client Provisioning configuration guidance and AnyConnect posture module behavior in the ISE admin documentation: Cisco ISE Admin Guide – Configure Client Provisioning and AnyConnect posture module overview: Cisco AnyConnect Secure Mobility Client guides.

QUESTION NO: 7

An administrator connects an HP printer to a dot1x enable port, but the printer in not accessible Which feature must the administrator enable to access the printer?

A. MAC authentication bypass

B. change of authorization

C. TACACS authentication

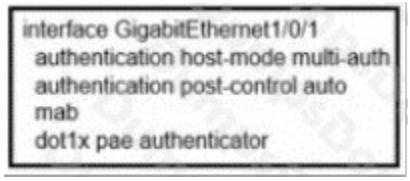
D. RADIUS authentication

ANSWER: A

Explanation:

MAC authentication bypass is the feature to enable when a device like a printer is connected to an 802.1X-enabled switchport but cannot complete 802.1X authentication. Many printers either do not support 802.1X supplicant functionality at all, or they are not configured with the required EAP method and credentials. In those cases, the switch can fall back to MAB, where the endpoint's MAC address is used as the identity in a RADIUS Access-Request to Cisco ISE. ISE can then match that MAC address against an internal endpoint identity store, an endpoint group, or profiling results, and return an authorization policy that permits the printer's required network access (often with a restricted ACL or a printer VLAN). This is a common best-practice approach for "headless" or non-user devices on 802.1X ports: keep 802.1X enabled for capable endpoints, and use MAB as a fallback for devices like printers, cameras, and IoT. See Cisco ISE guidance on MAB and wired access deployments: https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html and an overview of MAB behavior on Cisco switches: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/116291-configure-mab-00.html.

QUESTION NO: 8



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-domain authentication is the switch feature designed to permit exactly two authenticated "domains" on the same access port: one data device (typically a PC) and one voice device (typically an IP phone). In Cisco access-layer designs using 802.1X/MAB, this is implemented by setting the host mode to multi-domain, which allows one authenticated MAC/identity in the data VLAN and one authenticated MAC/identity in the voice VLAN. This directly matches the requirement to allow only one voice and one data endpoint on each port, while preventing additional endpoints from authenticating on either domain. In contrast, multi-auth host mode is intended to allow multiple authenticated endpoints on the same port (commonly used behind an IP phone or hub), which does not enforce the "one-and-one" limit. Therefore, changing from multi-auth to multi-domain is the correct configuration change to meet the stated endpoint limit per port.

References: Cisco ISE 802.1X/MAB configuration examples, Cisco 802.1X host modes and deployment guidance

QUESTION NO: 9

An engineer is configuring the remote access VPN to use Cisco ISE for AAA and needs to conduct posture checks on the connecting endpoints After the endpoint connects, it receives its initial authorization result and continues onto the compliance scan What must be done for this AAA configuration to allow compliant access to the network?

A. Configure the posture authorization so it defaults to unknown status

B. Fix the CoA port number

C. Ensure that authorization only mode is not enabled

D. Enable dynamic authorization within the AAA server group

ANSWER: D

Explanation:

Enable dynamic authorization within the AAA server group is required because posture assessment is not a one-time decision at initial authentication; the endpoint's authorization must be able to change after the posture agent completes its compliance scan. In Cisco ISE posture flows, the user/device typically authenticates first and is placed into a limited/redirected authorization state while posture is evaluated. Once the endpoint becomes compliant, ISE must signal the network access device (the VPN headend) to reauthorize the session so the new, more permissive authorization result can be applied without forcing the user to disconnect and reconnect. That change is accomplished using Dynamic Authorization (CoA/Reauth), which requires the NAD to be configured to accept and process ISE's dynamic authorization requests. On Cisco VPN headends integrated with ISE via RADIUS, this is commonly done by enabling dynamic authorization (Change of Authorization) for the AAA server group so the device can receive CoA/Disconnect messages from ISE and trigger a reauthentication/reauthorization of the session to transition from "posture unknown/noncompliant" to "compliant" access. References: Cisco ISE Admin Guide (Dynamic Authorization/CoA concepts), Cisco ISE CoA configuration overview.

QUESTION NO: 10

What does the dot1x system-auth-control command do?

A. globally enables 802.1x

B. causes a network access switch not to track 802.1x sessions

C. enables 802.1x on a network access device interface

D. causes a network access switch to track 802.1x sessions

ANSWER: A

Explanation:

The dot1x system-auth-control command is the global "master switch" that turns on IEEE 802.1X authentication processing on the device. On Cisco switches, 802.1X has both global and per-interface components: you can configure interface-level 802.1X settings, but the switch will not actually run 802.1X until it is globally enabled. When dot1x system-auth-control is present, the switch begins acting as an 802.1X authenticator and will start 802.1X state machines on ports where 802.1X is configured, allowing EAPOL exchanges and RADIUS authentication to occur. Without this global command, 802.1X remains administratively disabled regardless of interface configuration, so endpoints will not be authenticated via 802.1X. This

behavior is consistent across many Cisco Catalyst platforms and is a common prerequisite step in wired 802.1X deployments alongside configuring AAA/RADIUS and enabling 802.1X on the relevant interfaces.

References: Cisco 802.1X configuration guidance, Cisco IOS XE IEEE 802.1X configuration guide.

QUESTION NO: 11

Which portal is used to customize the settings for a user to log in and download the compliance module?

A. Client Provisioning

B. Client Endpoint

C. Client Profiling

D. Client Guest

ANSWER: A

Explanation:

The portal used to customize the end-user experience for logging in and downloading the compliance module is the Client Provisioning portal. In Cisco ISE, Client Provisioning is the web portal that delivers posture-related components to endpoints, including the Cisco Compliance Module (and, depending on design, other posture/agent components). Administrators use this portal to control how users are presented with installation instructions, what packages are offered, and the overall look-and-feel and behavior of the provisioning flow. This aligns with ISE posture workflows where endpoints that are not yet posture-capable are redirected to a provisioning page to obtain the required compliance/posture module before they can be assessed and granted appropriate network access.

In contrast, guest portals focus on guest account access and onboarding, and profiling/endpoint concepts relate to device identification and endpoint records rather than delivering posture modules. For posture enablement and compliance module download, the configuration point is the Client Provisioning portal within ISE.

References: Cisco Identity Services Engine Configuration Guides, Cisco ISE Administrator Guide (portal configuration and posture/provisioning)

QUESTION NO: 12

What are two differences of TACACS+ compared to RADIUS? (Choose two.)

A. TACACS+ uses a connectionless transport protocol, whereas RADIUS uses a connection-oriented transport protocol.

B. TACACS+ encrypts the full packet payload, whereas RADIUS only encrypts the password.

C. TACACS+ only encrypts the password, whereas RADIUS encrypts the full packet payload.

D. TACACS+ uses a connection-oriented transport protocol, whereas RADIUS uses a connectionless transport protocol.

E. TACACS+ supports multiple sessions per user, whereas RADIUS supports one session per user.

ANSWER: B D

Explanation:

TACACS+ and RADIUS differ in both transport behavior and what they protect on the wire. TACACS+ uses TCP, which is connection-oriented, providing reliable delivery and session-based communication between the network device (client) and the AAA server. In contrast, traditional RADIUS uses UDP, which is connectionless and does not establish a session before sending requests. Another key difference is encryption scope: TACACS+ encrypts the entire packet body (payload) so that most AAA attributes are protected in transit, while leaving only the header in cleartext. With classic RADIUS, only the user password is encrypted (with other attributes typically visible), which is why additional protections like IPsec or RadSec/TLS are often considered when confidentiality is required. These two characteristics—TCP vs UDP transport and full-payload vs password-only encryption—are commonly cited in Cisco guidance when comparing TACACS+ and RADIUS for device administration and network access use cases.

References: Cisco TACACS+ and RADIUS Comparison, RFC 2865 (RADIUS)

QUESTION NO: 13

An administrator is configuring Cisco ISE to authenticate users logging into network devices using TACACS+. The administrator is not seeing any of the authentication in the TACACS+ live logs.

Which action ensures the users are able to log into the network devices?

A. Enable the device administration service in the PSN persona.

B. Enable the device administration service in the Administration persona.

C. Enable the session services in the Administration persona.

D. Enable the service sessions in the PSN persona.

ANSWER: A

Explanation:

To process TACACS+ authentications (Device Administration) in Cisco ISE, the Policy Service Node must have the Device Administration service enabled. TACACS+ requests from network devices are sent to a PSN (the node providing policy services), and ISE will only accept and process those TACACS+ packets—and generate TACACS+ Live Logs—if the PSN is explicitly configured to run the Device Administration service. If that service is not enabled on the PSN, TACACS+ authentications will not be handled as expected, which commonly results in no TACACS+ activity appearing in Live Logs and failed/absent authentication processing. Enabling Device Administration on the PSN ensures the node listens for TACACS+ (TCP/49), evaluates the device admin policy set, and returns the appropriate TACACS+ responses so users can log into the network devices. This is a core deployment requirement for TACACS+ in ISE and aligns with Cisco's guidance on configuring TACACS+ device administration services on policy nodes.

References: Cisco Identity Services Engine Install and Upgrade Guides, Cisco ISE Admin Guide – Device Administration (TACACS+)

QUESTION NO: 14

Which two VMware features are supported on a Cisco ISE virtual appliance? (Choose two.)

A. multivendor integration

B. VM hardware version 7+

C. VM snapshots

D. OVF support

E. VM cold migration

ANSWER: B D E

Explanation:

Cisco ISE virtual appliances are deployed as VMware virtual machines using Cisco-provided installation media and/or an OVF/OVA-based workflow depending on the ISE release and distribution method. OVF support is therefore a supported VMware feature for deploying and provisioning the ISE VM with the correct virtual hardware settings (vCPU, RAM, NIC type, disk layout) as defined by Cisco's virtual appliance requirements. In addition, Cisco specifies a minimum supported VMware virtual hardware level for ISE VMs; using a supported VM hardware version (such as "VM hardware version 7+" in older compatibility matrices) is part of the supported virtualization baseline and ensures the VM can run with the required guest OS and device capabilities.

These supported items align with Cisco's guidance that ISE must be deployed only on supported hypervisor versions and configurations, and that the VM must meet the documented virtual hardware requirements. For authoritative requirements and supported virtualization details, see Cisco ISE Virtual Appliance documentation and compatibility guidance such as Cisco ISE Install and Upgrade Guides and the Cisco ISE compatibility/virtualization information available from Cisco documentation portals like Cisco Identity Services Engine (ISE) documentation.

QUESTION NO: 15

A network engineer has been tasked with enabling a switch to support standard web authentication for Cisco ISE. This must include the ability to provision for URL redirection on authentication Which two commands must be entered to meet this requirement? (Choose two)

A. Ip http secure-authentication

B. Ip http server

C. Ip http redirection

D. Ip http secure-server

E. Ip http authentication

ANSWER: B D

Explanation:

For Cisco ISE standard web authentication (central web auth) with URL redirection, the switch must be able to host the embedded HTTP/HTTPS services used to intercept HTTP requests and issue the redirect to the ISE portal. On Catalyst switches, this is enabled by turning on the HTTP server and/or the secure HTTP server. Enabling *ip http server* allows the switch to process HTTP-based redirection flows, while enabling *ip http secure-server* allows the same capability over HTTPS, which is commonly required in modern deployments and aligns with best practice to use TLS for web interactions. These commands are foundational prerequisites for web authentication and redirection features because the switch needs an active web service to generate the redirect response and support the webauth exchange with the client and ISE. In

practice, many deployments enable both to cover HTTP and HTTPS client behavior and to support secure redirection where applicable. See Cisco's web authentication configuration guidance for Catalyst switches and the broader Cisco ISE web authentication/redirection concepts: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/118978-config-ise-00.html and https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/consolidated_guide/b_consolidated_3850_3se_cg.html.

QUESTION NO: 16

The Cisco Wireless LAN Controller and guest portal must be set up in Cisco ISE. These configurations were performed:

configured all the required Cisco Wireless LAN Controller configurations added the wireless controller to Cisco ISE network devices

created an endpoint identity group configured credentials to be sent by email configured the SMTP server

configured an authorization profile with redirection to the guest portal and redirected the access control list

configured an authentication policy for MAB users created an authorization policy

Which two components would be required to complete the configuration? (Choose two.)

A. sponsor group

B. hotspot guest portal

C. sponsor portal

D. self-registered guest portal

E. guest type

ANSWER: C E

Explanation:

To complete a typical Cisco ISE guest workflow where credentials are generated and delivered (for example, via email using the configured SMTP server), you must define both the guest account "container" and the portal used to create/manage those accounts. A guest type is required because it defines the guest account policy (lifetime/expiration, password/credential format, sponsor approval requirements, and other account settings) that ISE applies when creating guest users. Without a guest type, ISE has no rule set for how to generate and manage the guest credentials you intend to send by email.

A sponsor portal is also required because it provides the interface for sponsors (internal users) to create guest accounts, assign the appropriate guest type, and trigger credential delivery (including email). In many deployments, the sponsor portal is the operational component that ties together the guest type, SMTP delivery, and the guest user creation process, while the authorization profile handles the redirection to the guest portal for network access.

References: Cisco Identity Services Engine configuration guides, Cisco ISE technical documentation

QUESTION NO: 17

Which two ports do network devices typically use for CoA? (Choose two.)

A. 19005

B. 443

C. 3799

D. 8080

E. 1700

ANSWER: C E

Explanation:

Change of Authorization (CoA) is part of the RADIUS Dynamic Authorization Extensions defined in RFC 5176. In practice, network access devices (NADs) listen for CoA and Disconnect messages from a RADIUS server (such as Cisco ISE) on UDP port 3799. This is the de-facto standard “RADIUS CoA” port used across many vendors and is the one most commonly referenced in Cisco ISE NAD configurations and documentation for dynamic authorization.

Some platforms also support (or historically used) UDP port 1700 for CoA/DM (dynamic authorization) in certain implementations, so you will see 1700 referenced as an alternate CoA port on some network devices and wireless platforms. When integrating ISE with a NAD, you must ensure the NAD is configured to accept CoA on the expected UDP port and that any intervening firewalls permit the traffic from the ISE PSN to the NAD on that port.

References: https://www.rfc-editor.org/rfc/rfc5176, https://documentation.meraki.com/MR/Encryption_and_Authentication/Change_of_Authorization_with_RADIUS_(CoA)_on_MR_Access_Points

QUESTION NO: 18

A Cisco ISE administrator needs to ensure that guest endpoint registrations are only valid for 1 day. When testing the guest policy flow, the administrator sees that the Cisco ISE does not delete the endpoint in the Guest Endpoints identity store after one day and allows access to the guest network after that period. Which configuration is causing this problem?

A. The RADIUS policy set for guest access is set to allow repeated authentication of the same device.

B. The length of access is set to 7 days in the Guest Portal Settings.

C. The Endpoint Purge Policy is set to 30 days for guest devices.

D. The Guest Account Purge Policy is set to 15 days.

ANSWER: C

Explanation:

The configuration causing this behavior is that the Endpoint Purge Policy is set to 30 days for guest devices. In Cisco ISE, “guest endpoint registrations” are stored as endpoint identity records (for example, MAC addresses) in the Guest Endpoints/Endpoints identity store. The lifetime of those endpoint records is not controlled by the guest account’s expiration or by portal “length of access” settings; instead, endpoint records remain until they are explicitly purged based on the endpoint purge settings. If the Endpoint Purge Policy is configured to purge guest endpoints after 30 days, the endpoint object will still exist well beyond the intended 1-day validity window. As a result, if your authorization policy allows access based on the presence of that endpoint record (or a prior registration state), the device can continue to authenticate and be

authorized after one day because the endpoint record was never removed. To enforce a 1-day validity for registered guest endpoints, you must align the endpoint purge/cleanup policy (and any authorization conditions relying on endpoint identity) with the desired timeframe.

References: Cisco Identity Services Engine Configuration Guides, Cisco ISE product documentation

QUESTION NO: 19

An engineer wants to learn more about Cisco ISE and deployed a new lab with two nodes. Which two persona configurations allow the engineer to successfully test redundancy of a failed node? (Choose two.)

A. Configure one of the Cisco ISE nodes as the Health Check node.

B. Configure both nodes with the PAN and MnT personas only.

C. Configure one of the Cisco ISE nodes as the primary PAN and MnT personas and the other as the secondary.

D. Configure both nodes with the PAN, MnT, and PSN personas.

E. Configure one of the Cisco ISE nodes as the primary PAN and PSN personas and the other as the secondary.

ANSWER: C D

Explanation:

To test redundancy with only two Cisco ISE nodes, you need personas that actually support high availability/failover behavior between nodes. The Administration persona (PAN) supports primary/secondary roles so that if the primary PAN fails, the secondary PAN can be promoted to become the active administrator node. Similarly, the Monitoring persona (MnT) supports primary/secondary roles for monitoring and reporting continuity. Therefore, configuring one node as the primary PAN and MnT and the other as the secondary PAN and MnT allows you to simulate a node failure and validate that administrative access and monitoring services can continue after promotion.

In addition, redundancy testing can include the Policy Service persona (PSN) by deploying PSN services on both nodes so authentications/authorizations can continue if one PSN goes down (clients can fail over to the remaining PSN). In a small lab, combining PAN with PSN on each node and using primary/secondary for PAN provides a practical way to test both administrative failover and policy service continuity. These align with Cisco ISE node personas and high-availability concepts described in Cisco ISE documentation. See Cisco ISE Install and Upgrade Guides and Cisco Identity Services Engine (ISE) documentation.

QUESTION NO: 20

In which two ways can users and endpoints be classified for TrustSec? (Choose two.)

A. VLAN

B. dynamic

C. QoS

D. SGACL

E. SXP

ANSWER: B D

Explanation:

TrustSec classifies users and endpoints primarily by assigning them a Security Group Tag (SGT), which represents the endpoint's role or identity (for example, employee, contractor, guest, or a specific device type). That SGT is then used to enforce policy based on group-to-group relationships rather than IP addressing. The enforcement mechanism for those classifications is the Security Group Access Control List (SGACL), which defines what traffic is permitted or denied between source and destination security groups. In other words, SGT provides the classification label and SGACL provides the policy construct that applies to those classified groups across the network fabric.

While technologies like VLANs and QoS can segment or treat traffic, they are not the core TrustSec classification methods; TrustSec's intent is to decouple access policy from topology and IP/VLAN constructs by using security group-based policy. Cisco ISE is commonly used to assign SGTs dynamically during authentication/authorization, and network devices enforce access using SGACLs derived from those group assignments.

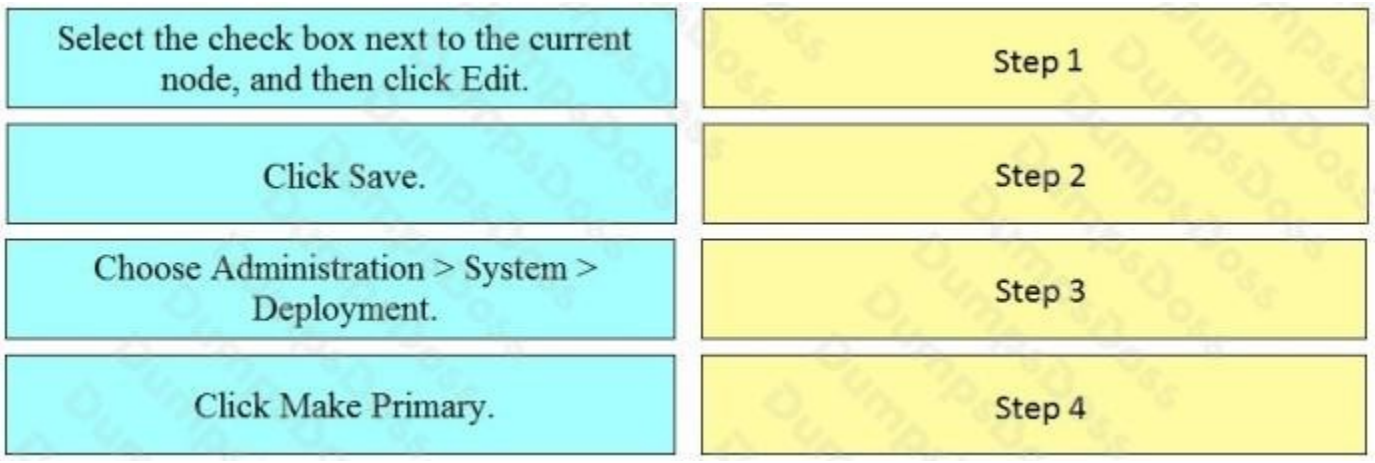
References: Cisco TrustSec overview, Cisco ISE Admin Guide – TrustSec

QUESTION NO: 21 - (DRAG DROP)

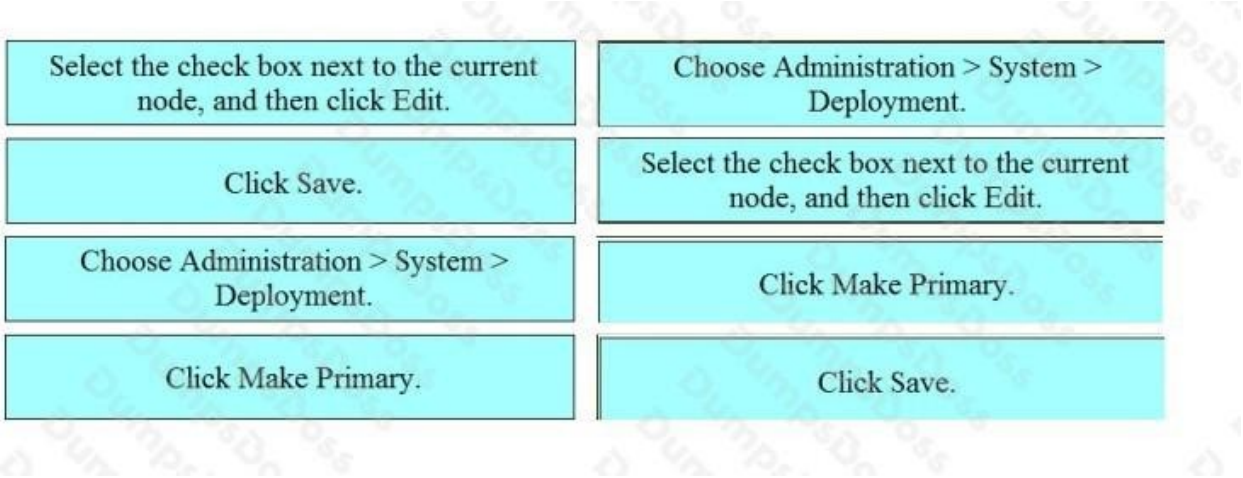
DRAG DROP

Drag the steps to configure a Cisco ISE node as a primary administration node from the left into the correct order on the right.

Select and Place:



ANSWER:



Explanation:

To configure a Cisco ISE node as the primary administration node, you perform the change from the Deployment view because that's where ISE manages node personas and primary/secondary roles. The correct flow starts by navigating in the GUI to **Administration > System > Deployment**, which lists all nodes and their roles. From there, you must **select the check box next to the current node and click Edit** so you can modify that node's deployment settings. Inside the edit workflow, you then use **Make Primary** to designate that node as the Primary Administration Node (PAN). Finally, you must **click Save** to commit the change; without saving, the role change is not applied to the deployment configuration.

This sequence reflects how ISE enforces configuration changes: you first enter the correct administrative context (Deployment), then open the node's editable configuration, then perform the role change action (Make Primary), and then persist the configuration (Save). This is the standard operational order for promoting a node to primary within the ISE deployment model. For additional background on ISE deployments and node roles, see Cisco's ISE documentation landing page at Cisco Identity Services Engine Install and Configure Guides and the ISE Admin Guide index at Cisco ISE Administrator Guide (3.3) (deployment concepts and node role management are consistent across versions).

QUESTION NO: 22

An engineer is configuring a guest password policy and needs to ensure that the password complexity requirements are set to mitigate brute force attacks. Which two requirement complete this policy? (Choose two)

A. minimum password length

B. active username limit

C. access code control

D. gpassword expiration period

E. username expiration date

ANSWER: A D

Explanation:

To mitigate brute-force attacks in a guest password policy, you focus on controls that directly increase the search space and reduce the useful lifetime of a guessed credential. Setting a minimum password length is a core complexity control because longer passwords exponentially increase the number of possible combinations an attacker must try, making online guessing

far less effective. In Cisco ISE Guest access, password policy settings commonly include length and other complexity elements (such as character classes), and length is one of the most impactful baseline requirements.

In addition, enforcing a guest password expiration period limits how long a password remains valid. Even if an attacker can attempt guesses over time, shortening the credential lifetime reduces the window in which a successful guess can be used and encourages frequent rotation for temporary accounts. This aligns with typical guest lifecycle management in ISE, where guest credentials are intended to be time-bound and automatically expire.

These two requirements together address both dimensions of brute-force risk: making guessing harder (complexity/length) and making any guessed password less valuable (expiration). For more on Cisco ISE guest services and policy concepts, see Cisco ISE Install and Configure Guides and the Cisco Identity Services Engine (ISE) product documentation.

QUESTION NO: 23

An administrator is configuring sponsored guest access using Cisco ISE Access must be restricted to the sponsor portal to ensure that only necessary employees can issue sponsored accounts and employees must be classified to do so What must be done to accomplish this task?

A. Configure an identity-based access list in Cisco ISE to restrict the users allowed to login

B. Edit the sponsor portal to only accept members from the selected groups

C. Modify the sponsor groups assigned to reflect the desired user groups

D. Create an authorization rule using the Guest Flow condition to authorize the administrators

ANSWER: C

Explanation:

Modify the sponsor groups assigned to reflect the desired user groups is the correct approach because Cisco ISE controls who can access the Sponsor Portal and what sponsor actions they can perform through Sponsor Groups. A sponsor group is effectively a role definition for sponsor users, and it is mapped to specific identity store groups (for example, AD groups) so that only employees who are members of those mapped groups are classified as sponsors and allowed to log in to the Sponsor Portal. By adjusting the sponsor group mappings (or creating a new sponsor group and mapping it to the appropriate AD/security groups), you ensure that only the necessary employees can issue sponsored guest accounts, meeting the requirement to “classify” employees before they can sponsor. This is the standard, built-in mechanism for restricting sponsor access and delegating sponsor capabilities, rather than trying to enforce it via network authorization rules or portal UI constraints alone. Cisco documents sponsor group configuration and mapping as the method to define sponsor access and privileges for sponsored guest workflows.

References: Cisco Identity Services Engine Install and Upgrade Guides (ISE configuration guides index), Cisco Identity Services Engine (ISE) product documentation

QUESTION NO: 24

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 ships with several built-in (default) endpoint identity groups that are used to classify endpoints for policy decisions without requiring you to manually create those groups. The default groups commonly referenced in ISE policy and endpoint workflows are *unknown*, *profiled*, and *block list*. The *unknown* group is used for endpoints that ISE has not yet identified or profiled, which is especially important early in an endpoint's lifecycle or when profiling data is insufficient. The *profiled* group is used once ISE's profiling services have determined an endpoint type (based on probes, DHCP, RADIUS, SNMP, etc.), enabling you to apply differentiated authorization based on device category. The *block list* group is a built-in mechanism to explicitly classify endpoints that should be denied or restricted, and it is frequently leveraged in authorization policies to quarantine or reject known-bad devices. These defaults are visible under the Endpoints/Identity Groups areas in the ISE administrative UI and are intended to accelerate common NAC policy designs.

References: Cisco ISE User Guide (Identity Management), Cisco ISE Admin Guide (Endpoints and Identity Groups)

QUESTION NO: 25

An administrator has added a new Cisco ISE PSN to their distributed deployment. Which two features must the administrator enable to accept authentication requests and profile the endpoints correctly, and add them to their respective endpoint identity groups? (Choose two)

A. Session Services

B. Endpoint Attribute Filter

C. Posture Services

D. Profiling Services

E. Radius Service

ANSWER: D E

Explanation:

On a newly added Policy Service Node, the node must be enabled to handle RADIUS authentications and to perform endpoint profiling so that endpoints can be classified and placed into the appropriate endpoint identity groups. Enabling

Radius Service

allows the PSN to accept and process network access authentication requests (for example, 802.1X and MAB) from NADs. Enabling

Profiling Services

allows the PSN to collect and evaluate profiling probes (such as DHCP, HTTP, RADIUS, SNMP, and others depending on your design) and then assign endpoints to the correct endpoint identity groups based on the profiling policy and collected attributes. In distributed ISE deployments, these are node-level persona/service settings that must be turned on for the PSN to actively participate in authentication and profiling workflows; otherwise, the PSN will not process those request types or

generate the profiling classifications needed for group assignment. This aligns with Cisco ISE's separation of services by node and the requirement to explicitly enable the relevant services on each PSN that will provide them.

References: Cisco Identity Services Engine Install and Configure Guides, Cisco Identity Services Engine (ISE) product documentation

QUESTION NO: 26

An administrator made changes in Cisco ISE and needs to apply new permissions for endpoints that have already been authenticated by sending a CoA packet to the network devices. Which IOS command must be configured on the devices to accomplish this goal?

A. aaa server radius dynamic-author

B. authentication command bounce-port

C. authentication command disable-port

D. aaa nas port extended

ANSWER: A

Explanation:

To allow Cisco ISE to push new authorization to endpoints that are already authenticated, the network device must be configured to accept RADIUS Change of Authorization (CoA), also known as Dynamic Authorization. On Cisco IOS/IOS-XE, this is enabled by configuring a RADIUS dynamic-author server block using the command

aaa server radius dynamic-author

. This configuration opens the device to receive CoA/Disconnect-Request packets from the policy server (ISE) and defines parameters such as the client IP address and shared secret, which are required for ISE to successfully send CoA. Without Dynamic Authorization enabled, ISE can change policy centrally, but it cannot force the network access device to reapply authorization (for example, to change a dACL, VLAN, or SGT) for an active session. CoA is the standard mechanism used in ISE deployments to reauthorize sessions after policy changes, posture changes, or endpoint profiling updates, and it is supported across common access platforms when RADIUS is used for AAA. See Cisco ISE CoA concepts and NAD configuration guidance in Cisco documentation: Cisco Identity Services Engine Install and Upgrade Guides and RADIUS CoA/Dynamic Authorization overview: Understanding RADIUS Change of Authorization (CoA).

QUESTION NO: 27

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 C E

Explanation:

In Cisco ISE, a Native Supplicant Profile is used to push 802.1X supplicant settings to endpoints (commonly via the ISE Posture/Compliance module) so the endpoint can authenticate on the network. When validating or "testing" a wired 802.1X connection, the key profile elements that determine what settings are available and how the supplicant will behave are the EAP method selection and the certificate parameters used by certificate-based EAP methods. The "allowed protocol" setting is central because it defines which EAP types (for example, PEAP, EAP-TLS, EAP-FAST) the native supplicant is permitted to negotiate on wired 802.1X, which directly impacts whether the endpoint can authenticate and what configuration fields become relevant. The "certificate template" setting is also essential in environments using EAP-TLS (or other certificate-based flows) because it ties the endpoint's certificate enrollment/selection expectations to the authentication method, ensuring the client presents an appropriate certificate for wired authentication testing. Together, these two settings are the most directly applicable to determining available profile behaviors for wired devices when using ISE posture agents.

References: Cisco Identity Services Engine Configuration Guides, Cisco ISE Native Supplicant Provisioning (Cisco Doc)

QUESTION NO: 28

Which two external identity stores are supported by Cisco ISE for password types? (Choose two.)

A. LDAP

B. OBDC

C. RADIUS Token Server

D. TACACS+ Token Server

E. SOL

ANSWER: A C

Explanation:

Cisco ISE supports using external identity stores to validate username/password-based authentications. For password types, LDAP-based directories are supported, which includes generic LDAP and commonly Microsoft Active Directory (via its LDAP/AD integration). This allows ISE to perform password validation against the directory and use directory attributes for authorization decisions. In addition, Cisco ISE supports token-based password validation through external token servers using the RADIUS protocol, commonly used for one-time password (OTP) systems. In this model, ISE proxies the authentication request to the external RADIUS token server, which performs the OTP/password validation and returns accept/reject to ISE. These two store types map directly to "LDAP" and "RADIUS Token Server" as supported external identity stores for password handling in ISE policy flows. This is consistent with ISE's external identity source options and how ISE integrates with LDAP directories and RADIUS-based token servers for password/OTP verification.

References: Cisco Identity Services Engine Administrator Guide, Cisco ISE Install and Configuration Guides

QUESTION NO: 29

Which two ports must be open between Cisco ISE and the client when you configure posture on Cisco ISE? (Choose two.)

A. TCP 80

B. TCP 8905

C. TCP 8443

D. TCP 8906

E. TCP 443

ANSWER: B C

Explanation:

For Cisco ISE posture, the client (typically the Cisco Secure Client/AnyConnect posture module or ISE Posture Agent components) must be able to communicate with ISE over specific TCP ports used for posture assessment and remediation workflows. TCP 8905 is used by ISE posture services for agent communications during posture discovery/assessment (for example, exchanging posture requirements, status, and related posture control messages). In addition, TCP 8443 is commonly used for ISE's client-facing web services involved in posture flows, such as agent provisioning/redirect and posture-related HTTPS interactions when the client is directed to ISE for posture resources. Ensuring these two ports are permitted end-to-end (no firewall blocks between endpoints and the ISE Policy Service Node handling posture) is a baseline requirement for successful posture operation, alongside any additional ports required by your specific remediation actions (for example, OS update sites, AV update servers, or internal patch repositories). Cisco documents these posture-related port requirements in ISE port reference and posture deployment guidance.

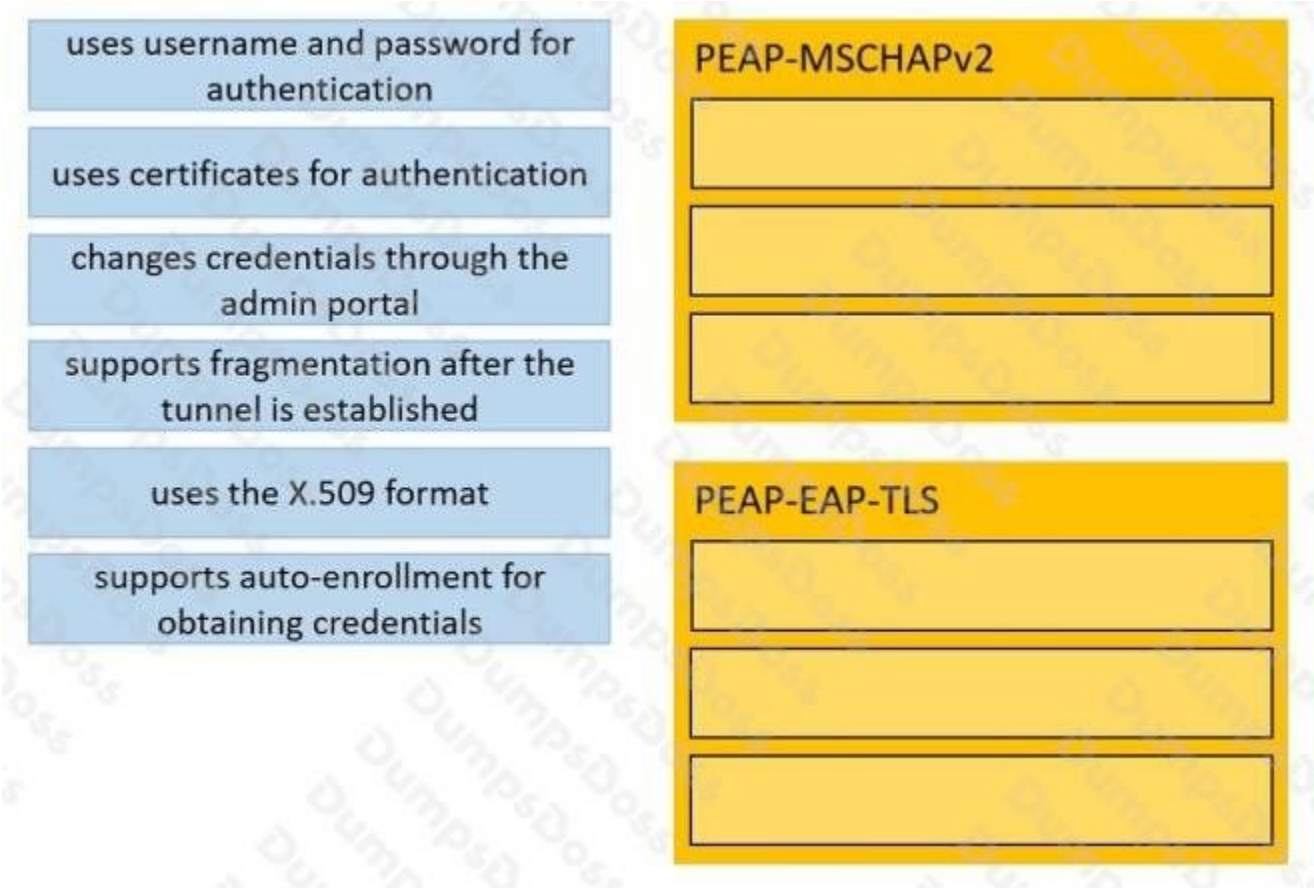
References: Cisco Identity Services Engine Install & Upgrade Guides, Cisco ISE Admin Guide (Posture section)

QUESTION NO: 30 - (DRAG DROP)

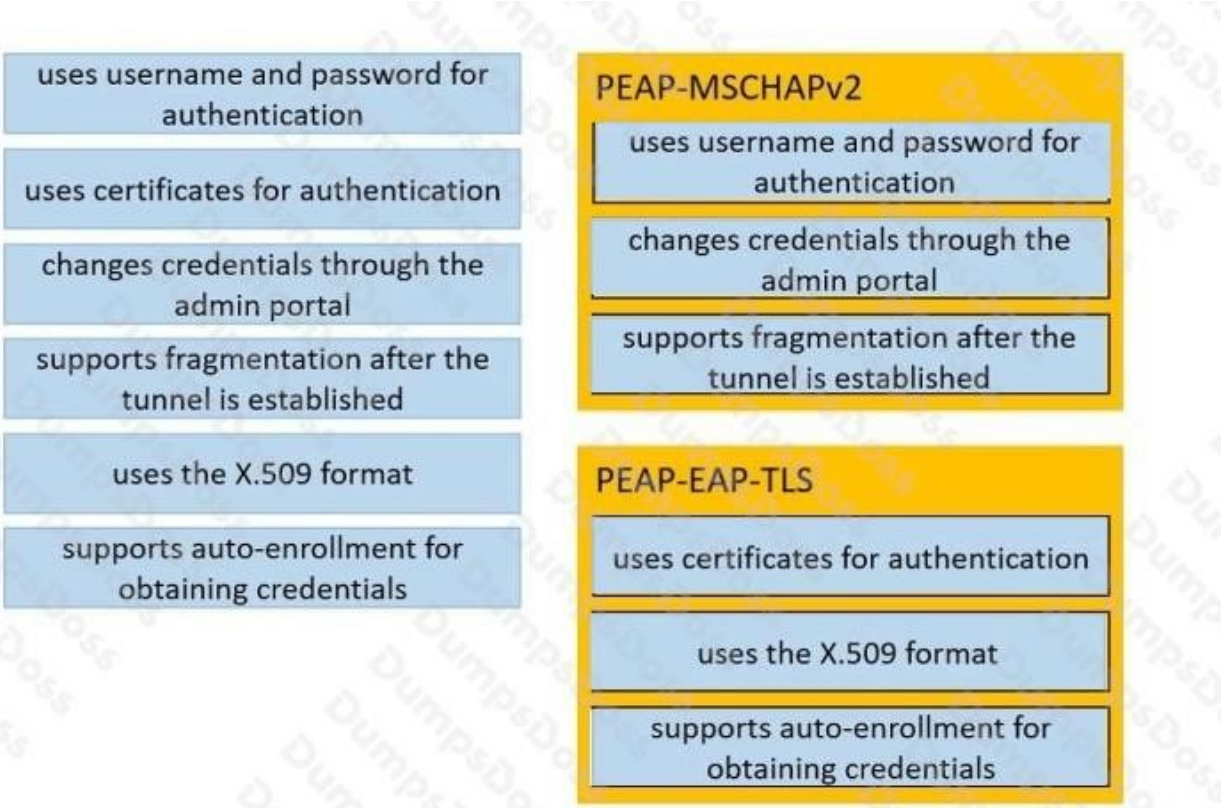
DRAG DROP

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:


uses username and password for authentication
uses certificates for authentication
changes credentials through the admin portal
supports fragmentation after the tunnel is established
uses the X.509 format
supports auto-enrollment for obtaining credentials
PEAP-MSCHAPv2
PEAP-EAP-TLS

ANSWER:



Explanation:

PEAP-MSCHAPv2 and PEAP-EAP-TLS are both commonly used with 802.1X, but they differ mainly in what the client presents as its “credential” inside the protected PEAP (TLS) tunnel. With PEAP-MSCHAPv2, the inner authentication is MSCHAPv2, which is fundamentally a username-and-password challenge/response exchange. That’s why it aligns with characteristics like using a username and password for authentication and fitting naturally into environments where user passwords are managed and changed through an administrative identity portal or directory-driven workflows.

PEAP-EAP-TLS, on the other hand, uses certificates for client authentication. In practice that means the endpoint must have a client certificate, and those certificates are typically X.509. Because managing certificates at scale is a major operational consideration, PEAP-EAP-TLS deployments often rely on auto-enrollment mechanisms (for example, enterprise PKI with automated certificate issuance) so endpoints can obtain and renew their certificates without manual handling.

Finally, PEAP itself is a TLS-based tunnel that encapsulates the inner EAP method and includes support for fragmenting EAP messages when needed (commonly discussed as part of PEAP/TLS encapsulation behavior). In this question’s framing, associating fragmentation support with the PEAP-MSCHAPv2 side is consistent with describing the PEAP tunneled method behavior used in that authentication flow.

References: RFC 5216 (EAP-TLS), Microsoft documentation on EAP methods (EAP-TLS and PEAP-MS-CHAP v2).

QUESTION NO: 31

Which action must be taken before configuring the Secure Client Agent profile when creating the Secure Client configuration for ISE posture services?

A. Create a posture remediation condition policy for the Agent profile.

B. Configure the posture policy for Secure Client posturing module.

C. Create a posture condition that references the Secure Client package.

D. Upload the Secure Client packages and the Secure Client compliance modules.

ANSWER: D

Explanation:

Uploading the Secure Client packages and the Secure Client compliance modules must be done first because the Secure Client Agent profile in ISE is built by selecting from software artifacts that ISE already has in its repository. In ISE posture, the “agent profile” (and the broader Secure Client configuration) references specific Secure Client installers (per OS) and the posture/compliance modules that the endpoint will download and run. If those packages are not uploaded into ISE ahead of time, there is nothing to attach to the profile, and ISE cannot stage or distribute the required components during posture assessment and remediation. This prerequisite step ensures ISE can present the correct installers/modules to endpoints, support version control, and properly deliver posture capabilities as part of the posture flow. After the packages/modules exist in ISE, you can then proceed to define agent profiles and later tie them into posture policies and authorization results for compliant/noncompliant handling. See Cisco ISE Posture and Secure Client integration guidance in the ISE admin documentation and Secure Client posture module references: Cisco Identity Services Engine Install and Configure Guides and Cisco Secure Client documentation.

QUESTION NO: 32

Which two external identity stores support EAP-TLS and PEAP-TLS? (Choose two.)

A. Active Directory

B. RADIUS Token

C. Internal Database

D. RSA SecurID

E. LDAP

ANSWER: A E

Explanation:

EAP-TLS and PEAP-TLS are certificate-based 802.1X methods where Cisco ISE performs the EAP exchange and validates the client certificate during the TLS handshake. After the certificate is validated, ISE can optionally perform authorization using identity attributes sourced from an external identity store. In practice, the external stores commonly used with these EAP methods are Active Directory and LDAP directories, because they can provide user/computer identity and group/attribute lookups that ISE can use in authorization policies (for example, AD security group membership or LDAP attributes). Active Directory is also tightly integrated with ISE for machine/user identity use cases common in EAP-TLS deployments. LDAP is likewise supported as an external directory for identity lookups that can complement certificate-based authentication flows. Token servers such as RSA SecurID or generic RADIUS token servers are typically used for one-time-password style authentications (for example, PEAP/MSCHAPv2 with token chaining) rather than certificate-based EAP-TLS/PEAP-TLS identity sourcing. For more details on ISE external identity sources and EAP methods, see Cisco ISE Admin guidance and 802.1X/EAP overviews: Cisco Identity Services Engine configuration guides and Cisco EAP authentication overview.

QUESTION NO: 33

An organization wants to enable web-based guest access for both employees and visitors The goal is to use a single portal for both user types Which two authentication methods should be used to meet this requirement? (Choose two)

A. LDAP

B. 802 1X

C. Certificate-based

D. LOCAL

E. MAC based

ANSWER: A D

Explanation:

To use a single web-based guest access portal for both employees and visitors in Cisco ISE, the portal must support authenticating “known” users (employees) against an enterprise identity store and “guest” users against an internal guest user database. Using LDAP enables employee authentication via an external directory such as Microsoft Active Directory/LDAP, which is the common approach for corporate users accessing a guest/BYOD-style web portal. Using LOCAL enables visitor (guest) authentication using ISE’s internal guest user accounts created via the Guest portal workflows (self-registered, sponsored, etc.). In practice, ISE guest portals can be configured to present multiple identity sources so employees can log in with directory credentials while visitors use guest accounts, all through the same portal experience. Methods like 802.1X and certificate-based authentication are not the typical mechanisms for a web-based guest portal login flow, and MAC-based authentication is a network access technique (MAB) rather than a web portal user authentication method. See Cisco ISE Guest Access and identity store concepts for how guest users and external directories are used together: Cisco ISE Install and Configure Guides and Cisco ISE Admin Guide.

QUESTION NO: 34

Which protocol must be allowed for a BYOD device to access the BYOD portal?

A. HTTPS

B. HTTP

C. SSH

D. SMTP

ANSWER: A

Explanation:

HTTPS must be allowed because the Cisco ISE BYOD portal is a web-based portal that is designed to be accessed securely over TLS. In typical ISE BYOD flows, the endpoint is redirected to a portal (often via a redirect ACL or pre-auth ACL) to perform onboarding actions such as device registration, certificate/profile provisioning, and posture-related steps. These portal interactions involve user credentials and device identity material, so Cisco’s best practice is to use encrypted transport. As a result, network access controls (WLC ACLs, switch dACLs, firewall rules, etc.) must permit TCP/443 from the

BYOD device to the ISE node hosting the BYOD portal (or the PSN/portal FQDN VIP) so the browser can load the portal and complete onboarding. While some deployments may optionally support HTTP-to-HTTPS redirection, the portal itself is fundamentally intended to be reached via HTTPS for confidentiality and integrity. This aligns with Cisco ISE portal behavior and the general requirement to allow secure web access to ISE guest/BYOD portals.

References: Cisco Identity Services Engine Configuration Guides, Cisco ISE Technical Documentation

QUESTION NO: 35

A network security administrator wants to integrate Cisco ISE with Active Directory. Which configuration action must the security administrator take to accomplish the task?

A. Remove Cisco ISE user account from the domain.

B. Remove the ISE machine account from the domain.

C. Join Cisco ISE to the Active Directory domain.

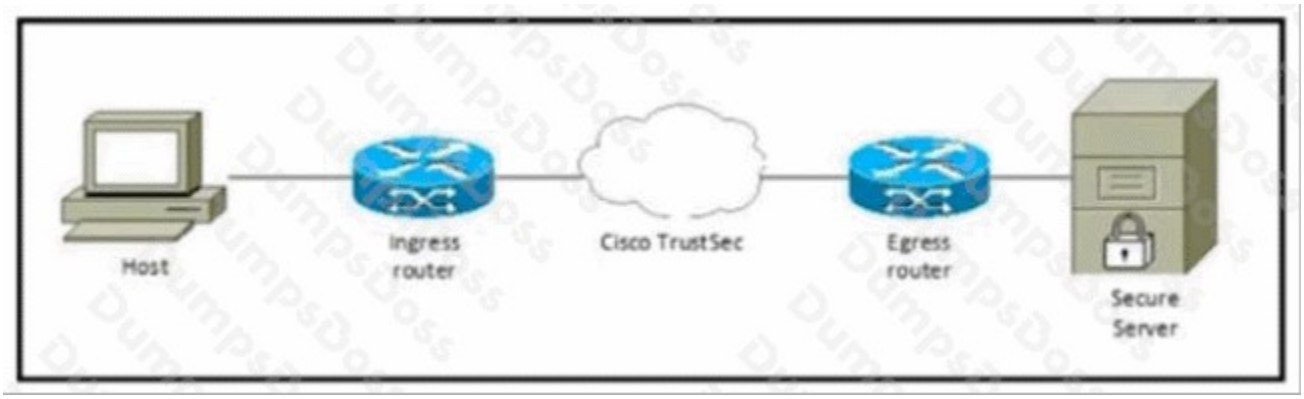
D. Search Active Directory to see if admin user account exists.

ANSWER: C

Explanation:

To integrate Cisco ISE with Microsoft Active Directory for user/computer authentication and group-based authorization, Cisco ISE must be joined to the Active Directory domain. Joining the domain creates (or uses) an AD machine account for the ISE node, establishes the secure trust relationship needed for AD queries, and enables ISE to use AD as an external identity source (including retrieving group membership for policy decisions). This is a required configuration step performed under the Active Directory identity source in ISE, where you specify the domain and provide credentials with rights to join computers to the domain. After the join succeeds, you can select AD groups, enable the domain for authentication, and use AD-based conditions in authentication/authorization policies. Without joining the domain, ISE cannot perform the necessary Kerberos/LDAP operations in the supported manner for AD integration and group resolution. See Cisco ISE Admin Guide sections on integrating with Active Directory and joining ISE nodes to an AD domain: Cisco Identity Services Engine Configuration Guides and the ISE 3.x/4.x AD integration overview: Cisco ISE Technical Documentation.

QUESTION NO: 36



Refer to the exhibit Which component must be configured to apply the SGACL?

A. egress router

B. host

C. secure server

D. ingress router

ANSWER: A

Explanation:

In Cisco TrustSec, a Security Group ACL (SGACL) is enforced at the policy enforcement point on the network device that is making the forwarding decision for the traffic. Practically, this means the device where traffic leaves the TrustSec domain toward its destination (or where the destination is attached) must be capable of enforcing the SGACL based on the source and destination Security Group Tags (SGTs). This is commonly described as enforcement on the egress device/interface: the switch/router receiving the packet, determining the destination, and applying the SGACL before transmitting it out toward the destination. The ingress device's primary role is often to classify/tag the traffic (assign an SGT via authentication, SGT mapping, or propagation), while the egress device applies the actual authorization policy (the SGACL) to permit/deny specific flows between SGTs. Therefore, the correct component to configure to apply the SGACL is the egress router (or egress enforcement device) that supports TrustSec SGACL enforcement.

References: Cisco TrustSec Architecture Overview, Cisco TrustSec Overview

QUESTION NO: 37

An employee logs on to the My Devices portal and marks a currently on-boarded device as "Lost".

Which two actions occur within Cisco ISE as a result of this action? (Choose two.)

A. BYOD Registration status is updated to No.

B. BYOD Registration status is updated to Unknown.

C. The device access has been denied.

D. Certificates provisioned to the device are not revoked.

E. The device status is updated to Stolen.

ANSWER: A C D

Explanation:

When a user marks an onboarded endpoint as "Lost" in the My Devices (MyDevices) portal, Cisco ISE updates the endpoint's registration state so it is no longer considered an actively registered BYOD device. In practice, this is reflected by changing the BYOD Registration status to "No", which indicates the endpoint is not currently registered/managed as a valid BYOD device in ISE's endpoint repository. This status change is what downstream policy conditions typically key off of (for example, BYOD-registered vs. not registered) to drive authorization outcomes.

Also, marking a device as "Lost" in MyDevices does not automatically revoke the client certificate that was provisioned during onboarding. Certificate revocation is a separate PKI lifecycle action (for example, revoking a certificate on the CA/RA

or via an explicit administrative workflow). Therefore, the certificates provisioned to the device are not revoked simply because the device is flagged as lost in the portal. This distinction is important because many deployments rely on additional controls (authorization policy, MDM actions, or manual certificate revocation) to fully disable access for a lost device.

References: Cisco Identity Services Engine Install and Upgrade Guides, Cisco ISE Admin Guide