

## Exam Questions 300-715

Implementing and Configuring Cisco Identity Services Engine (ISE)

<https://www.2passeasy.com/dumps/300-715/>



#### NEW QUESTION 1

Which port does Cisco ISE use for native supplicant provisioning of a Windows laptop?

- A. TCP 8909
- B. TCP 8905
- C. UDP 1812
- D. TCP 443

**Answer:** B

#### NEW QUESTION 2

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 Administration persona
- B. Enable the session services in the administration persona
- C. Enable the service sessions in the PSN persona.
- D. Enable the device administration service in the PSN persona.

**Answer:** D

#### Explanation:

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin\\_guide/b\\_ISE\\_admin\\_guide\\_24/m\\_ise\\_tacacs\\_dev](https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_ise_tacacs_dev)

#### NEW QUESTION 3

What is a restriction of a standalone Cisco ISE node deployment?

- A. Only the Policy Service persona can be disabled on the node.
- B. The domain name of the node cannot be changed after installation.
- C. Personas are enabled by default and cannot be edited on the node.
- D. The hostname of the node cannot be changed after installation.

**Answer:** C

#### NEW QUESTION 4

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

- A. VLAN
- B. SXP
- C. dynamic
- D. QoS
- E. SGACL

**Answer:** AE

#### NEW QUESTION 5

What is a characteristic of the UDP protocol?

- A. UDP can detect when a server is down.
- B. UDP offers best-effort delivery
- C. UDP can detect when a server is slow
- D. UDP offers information about a non-existent server

**Answer:** B

#### Explanation:

<https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838>

#### NEW QUESTION 6

An engineer is configuring web authentication and needs to allow specific protocols to permit DNS traffic. Which type of access list should be used for this configuration?

- A. reflexive ACL
- B. extended ACL
- C. standard ACL
- D. numbered ACL

**Answer:** B

#### NEW QUESTION 7

What is a valid status of an endpoint attribute during the device registration process?

- A. block listed
- B. pending

- C. unknown
- D. DenyAccess

**Answer:** B

#### NEW QUESTION 8

An engineer is configuring Cisco ISE to reprofile endpoints based only on new requests of INIT-REBOOT and SELECTING message types. Which probe should be used to accomplish this task?

- A. MMAP
- B. DNS
- C. DHCP
- D. RADIUS

**Answer:** C

#### NEW QUESTION 9

An engineer is working with a distributed deployment of Cisco ISE and needs to configure various network probes to collect a set of attributes from the endpoints on the network. Which node should be used to accomplish this task?

- A. PSN
- B. primary PAN
- C. pxGrid
- D. MnT

**Answer:** A

#### NEW QUESTION 10

A user reports that the RADIUS accounting packets are not being seen on the Cisco ISE server. Which command is the user missing in the switch's configuration?

- A. radius-server vsa send accounting
- B. aaa accounting network default start-stop group radius
- C. aaa accounting resource default start-stop group radius
- D. aaa accounting exec default start-stop group radios

**Answer:** A

#### NEW QUESTION 10

An administrator is configuring new probes to use with Cisco ISE and wants to use metadata to help profile the endpoints. The metadata must contain traffic information relating to the endpoints instead of industry-standard protocol information Which probe should be enabled to meet these requirements?

- A. NetFlow probe
- B. DNS probe
- C. DHCP probe
- D. SNMP query probe

**Answer:** C

#### Explanation:

<http://www.network-node.com/blog/2016/1/2/ise-20-profiling>

#### NEW QUESTION 15

A Cisco device has a port configured in multi-authentication mode and is accepting connections only from hosts assigned the SGT of SGT\_0422048549 The VLAN trunk link supports a maximum of 8 VLANS What is the reason for these restrictions?

- A. The device is performing inline tagging without acting as a SXP speaker
- B. The device is performing mime tagging while acting as a SXP speaker
- C. The IP subnet addresses are dynamically mapped to an SGT.
- D. The IP subnet addresses are statically mapped to an SGT

**Answer:** C

#### NEW QUESTION 20

Which two task types are included in the Cisco ISE common tasks support for TACACS+ profiles? (Choose two.)

- A. Firepower
- B. WLC
- C. IOS
- D. ASA
- E. Shell

**Answer:** BE

#### Explanation:

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin\\_guide/b\\_ise\\_admin\\_guide\\_21/b\\_ise\\_admin\\_guide\\_TACACS+ Profile](https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_TACACS+_Profile)

TACACS+ profiles control the initial login session of the device administrator. A session refers to each individual authentication, authorization, or accounting request. A session authorization request to a network device elicits an ISE response. The response includes a token that is interpreted by the network device, which limits the commands that may be executed for the duration of a session. The authorization policy for a device administration access service can contain a single shell profile and multiple command sets. The TACACS+ profile definitions are split into two components:

- > Common tasks
- > Custom attributes

There are two views in the TACACS+ Profiles page (Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles)—Task Attribute View and Raw View. Common tasks can be entered using the Task Attribute View and custom attributes can be created in the Task Attribute View as well as the Raw View.

The Common Tasks section allows you to select and configure the frequently used attributes for a profile. The attributes that are included here are those defined by the TACACS+ protocol draft specifications. However, the values can be used in the authorization of requests from other services. In the Task Attribute View, the ISE administrator can set the privileges that will be assigned to the device administrator. The common task types are:

- > Shell
- > WLC
- > Nexus
- > Generic

The Custom Attributes section allows you to configure additional attributes. It provides a list of attributes that are not recognized by the Common Tasks section. Each definition consists of the attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute. In the Raw View, you can enter the mandatory attributes using an equal to (=) sign between the attribute name and its value and optional attributes are entered using an asterisk (\*) between the attribute name and its value. The attributes entered in the Raw View are reflected in the Custom Attributes section in the Task Attribute View and vice versa. The Raw View is also used to copy paste the attribute list (for example, another product's attribute list) from the clipboard onto ISE. Custom attributes can be defined for nonshell services.

#### NEW QUESTION 22

An administrator is configuring posture with Cisco ISE and wants to check that specific services are present on the workstations that are attempting to access the network. What must be configured to accomplish this goal?

- A. Create a registry posture condition using a non-OPSWAT API version.
- B. Create an application posture condition using a OPSWAT API version.
- C. Create a compound posture condition using a OPSWAT API version.
- D. Create a service posture condition using a non-OPSWAT API version.

**Answer: D**

#### NEW QUESTION 25

A user changes the status of a device to stolen in the My Devices Portal of Cisco ISE. The device was originally onboarded in the BYOD wireless Portal without a certificate. The device is found later, but the user cannot re-onboard the device because Cisco ISE assigned the device to the Blocklist endpoint identity group. What must the user do in the My Devices Portal to resolve this issue?

- A. Manually remove the device from the Blocklist endpoint identity group.
- B. Change the device state from Stolen to Not Registered.
- C. Change the BYOD registration attribute of the device to None.
- D. Delete the device, and then re-add the device.

**Answer: B**

#### NEW QUESTION 30

An organization wants to standardize the 802.1X configuration on their switches and remove static ACLs on the switch ports while allowing Cisco ISE to communicate to the switch what access to provide. What must be configured to accomplish this task?

- A. security group tag within the authorization policy
- B. extended access-list on the switch for the client
- C. port security on the switch based on the client's information
- D. dynamic access list within the authorization profile

**Answer: A**

#### Explanation:

[https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user\\_guide/ise\\_user\\_guide/ise\\_sga\\_pol.html#](https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_sga_pol.html#)

#### NEW QUESTION 34

Refer to the exhibit.

```
Switch(config)# gigabitEthernet 1/0/2

Switch(config)# authentication port-control auto

Switch(config)# authentication host-mode multi-auth
```

In which scenario does this switch configuration apply?

- A. when allowing a hub with multiple clients connected
- B. when passing IP phone authentication
- C. when allowing multiple IP phones to be connected

D. when preventing users with hypervisor

**Answer:** A

**Explanation:**

[https://www.linkedin.com/pulse/mac-authentication-bypass-priyanka-kumari#:~:text=Multi%2Dauthentication%](https://www.linkedin.com/pulse/mac-authentication-bypass-priyanka-kumari#:~:text=Multi%2Dauthentication%2D)

#### NEW QUESTION 36

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:** CE

#### NEW QUESTION 41

An engineer is designing a new distributed deployment for Cisco ISE in the network and is considering failover options for the admin nodes. There is a need to ensure that an admin node is available for configuration of policies at all times. What is the requirement to enable this feature?

- A. one primary admin and one secondary admin node in the deployment
- B. one policy services node and one secondary admin node
- C. one policy services node and one monitoring and troubleshooting node
- D. one primary admin node and one monitoring and troubleshooting node

**Answer:** A

#### NEW QUESTION 42

A user is attempting to register a BYOD device to the Cisco ISE deployment, but needs to use the onboarding policy to request a digital certificate and provision the endpoint. What must be configured to accomplish this task?

- A. A native supplicant provisioning policy to redirect them to the BYOD portal for onboarding
- B. The Cisco AnyConnect provisioning policy to provision the endpoint for onboarding
- C. The BYOD flow to ensure that the endpoint will be provisioned prior to registering
- D. The posture provisioning policy to give the endpoint all necessary components prior to registering

**Answer:** A

#### NEW QUESTION 44

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

- A. HTTP
- B. SMTP
- C. HTTPS
- D. SSH

**Answer:** C

#### NEW QUESTION 49

An administrator is configuring a new profiling policy within Cisco ISE. The organization has several endpoints that are the same device type and all have the same Block ID in their MAC address. The profiler does not currently have a profiling policy created to categorize these endpoints. Therefore a custom profiling policy must be created. Which condition must the administrator use in order to properly profile an ACME AI Connector endpoint for network access with MAC address <MAC ADDRESS>?

- A. MAC\_OUI\_STARTSWITH\_<MACADDRESS>
- B. CDP\_cdpCacheDeviceID\_CONTAINS\_<MACADDRESS>
- C. MAC\_MACAddress\_CONTAINS\_<MACADDRESS>
- D. Radius Called Station-ID STARTSWITH <MACADDRESS>

**Answer:** D

#### NEW QUESTION 52

An administrator enables the profiling service for Cisco ISE to use for authorization policies while in closed mode. When the endpoints connect, they receive limited access so that the profiling probes can gather information and Cisco ISE can assign the correct profiles. They are using the default values within Cisco ISE. But the devices do not change their access due to the new profile. What is the problem?

- A. In closed mode, profiling does not work unless CDP is enabled.
- B. The profiling probes are not able to collect enough information to change the device profile.
- C. The profiler feed is not downloading new information so the profiler is inactive.
- D. The default profiler configuration is set to No CoA for the reauthentication setting.

**Answer:** D



#### NEW QUESTION 54

What must be configured on the WLC to configure Central Web Authentication using Cisco ISE and a WLC?

- A. Set the NAC State option to SNMP NAC.
- B. Set the NAC State option to RADIUS NAC.
- C. Use the radius-server vsa send authentication command.
- D. Use the ip access-group webauth in command.

**Answer:** B

#### NEW QUESTION 56

What is a requirement for Feed Service to work?

- A. TCP port 3080 must be opened between Cisco ISE and the feed server
- B. Cisco ISE has a base license.
- C. Cisco ISE has access to an internal server to download feed update
- D. Cisco ISE has Internet access to download feed update

**Answer:** C

#### NEW QUESTION 57

When configuring an authorization policy, an administrator cannot see specific Active Directory groups present in their domain to be used as a policy condition. However, other groups that are in the same domain are seen What is causing this issue?

- A. Cisco ISE only sees the built-in groups, not user created ones
- B. The groups are present but need to be manually typed as conditions
- C. Cisco ISE's connection to the AD join point is failing
- D. The groups are not added to Cisco ISE under the AD join point

**Answer:** D

#### Explanation:

[https://www.youtube.com/watch?v=0kuEZEo564s&ab\\_channel=CiscoISE-IdentityServicesEngine](https://www.youtube.com/watch?v=0kuEZEo564s&ab_channel=CiscoISE-IdentityServicesEngine)

#### NEW QUESTION 60

A security administrator is using Cisco ISE to create a BYOD onboarding solution for all employees who use personal devices on the corporate network. The administrator generates a Certificate Signing Request and signs the request using an external Certificate Authority server. Which certificate usage option must be selected when importing the certificate into ISE?

- A. RADIUS
- B. DLTS
- C. Portal
- D. Admin

**Answer:** C

#### NEW QUESTION 61

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:** BD

#### NEW QUESTION 63

An engineer is using Cisco ISE and configuring guest services to allow wireless devices to access the network. Which action should accomplish this task?

- A. Create the redirect ACL on the WLC and add it to the WLC policy
- B. Create the redirect ACL on the WLC and add it to the Cisco ISE policy.
- C. Create the redirect ACL on Cisco ISE and add it to the WLC policy
- D. Create the redirect ACL on Cisco ISE and add it to the Cisco ISE Policy

**Answer:** B

#### NEW QUESTION 68

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. LDAP 389
- C. HTTP 80
- D. HTTPS 443
- E. MSRPC 445

**Answer:** BE

#### NEW QUESTION 70

What is the deployment mode when two Cisco ISE nodes are configured in an environment?

- A. distributed
- B. active
- C. standalone
- D. standard

**Answer:** A

#### NEW QUESTION 71

What are two components of the posture requirement when configuring Cisco ISE posture? (Choose two)

- A. updates
- B. remediation actions
- C. Client Provisioning portal
- D. conditions
- E. access policy

**Answer:** BD

#### NEW QUESTION 74

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:** CD

#### NEW QUESTION 78

Which Cisco ISE deployment model is recommended for an enterprise that has over 50,000 concurrent active endpoints?

- A. large deployment with fully distributed nodes running all personas
- B. medium deployment with primary and secondary PAN/MnT/pxGrid nodes with shared PSNs
- C. medium deployment with primary and secondary PAN/MnT/pxGrid nodes with dedicated PSNs
- D. small deployment with one primary and one secondary node running all personas

**Answer:** C

#### NEW QUESTION 80

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-PEAP-MSCHAPv2
- B. EAP-TTLS
- C. EAP-FAST
- D. EAP-TLS

**Answer:** D

#### Explanation:

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/certificate-requirements-eap-tls-peap> about EAP FAST  
<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/eap-fast/200322-Understanding-EAP-FAST-and->

#### NEW QUESTION 82

An engineer is configuring Cisco ISE for guest services. They would like to have any unregistered guests redirected to the guest portal for authentication, then have a CoA provide them with full access to the network that is segmented via firewalls. Why is the given configuration failing to accomplish this goal?

- A. The Guest Flow condition is not in the line that gives access to the guest portal.
- B. The Network\_Access\_Authentication\_Passed condition will not work with guest services for portal access.
- C. The Permit Access result is not set to restricted access in its policy line.
- D. The Guest Portal and Guest Access policy lines are in the wrong order.

**Answer:** D

#### NEW QUESTION 83

What service can be enabled on the Cisco ISE node to identify the types of devices connecting to a network?

- A. MAB
- B. profiling
- C. posture
- D. central web authentication

**Answer:** B

#### NEW QUESTION 84

An engineer deploys Cisco ISE and must configure Active Directory to then use information from Active Directory in an authorization policy. Which two components must be configured, in addition to Active Directory groups, to achieve this goal? (Choose two )

- A. Active Directory External Identity Sources
- B. Library Condition for External Identit
- C. External Groups
- D. Identity Source Sequences
- E. LDAP External Identity SourcesE Library Condition for Identity Group: User Identity Group

**Answer:** AB

#### NEW QUESTION 87

An engineer needs to export a file in CSV format, encrypted with the password C1\$c0438563935, and contains users currently configured in Cisco ISE. Drag and drop the steps from the left into the sequence on the right to complete this task.

Click Export Selected, click Key, and enter the password.	1
Click Administration, and then click Identity Management.	2
Click Start Export, and then click OK.	3
Click Identities, click Users, and then select the list of users.	4

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Graphical user interface, text, application Description automatically generated

#### NEW QUESTION 89

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

#### NEW QUESTION 94

Which Cisco ISE solution ensures endpoints have the latest version of antivirus updates installed before being allowed access to the corporate network?

- A. Threat Services
- B. Profiling Services
- C. Provisioning Services
- D. Posture Services

**Answer:** D

#### NEW QUESTION 98

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:** DE

**Explanation:**

Cisco ISE implements an ARP cache in the profiling service, so that you can reliably map the IP addresses and the MAC addresses of endpoints. For the ARP cache to function, you must enable either the DHCP probe or the RADIUS probe. The DHCP and RADIUS probes carry the IP addresses and the MAC addresses of endpoints in the payload data. The dhcp-requested address attribute in the DHCP probe and the Framed-IP-address attribute in the RADIUS probe carry the IP addresses of endpoints, along with their MAC addresses, which can be mapped and stored in the ARP cache.  
[https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin\\_guide/b\\_ise\\_admin\\_guide\\_21/b\\_ise\\_admin\\_guide](https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide)

**NEW QUESTION 101**

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

- A. causes a network access switch not to track 802.1x sessions
- B. globally enables 802.1x
- C. enables 802.1x on a network access device interface
- D. causes a network access switch to track 802.1x sessions

**Answer:** B

**Explanation:**

<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-8-0E/15-24E/configuration/guide/xe-380>

**NEW QUESTION 106**

An engineer needs to configure a compliance policy on Cisco ISE to ensure that the latest encryption software is running on the C drive of all endpoints. Drag and drop the configuration steps from the left into the sequence on the right to accomplish this task.

**Answer Area**

select Posture and Disk Encryption Condition	step 1
access the Disk Encryption Condition window	step 2
select the Encryption settings	step 3
access Policy Elements and Conditions	step 4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Diagram Description automatically generated

**NEW QUESTION 108**

A laptop was stolen and a network engineer added it to the block list endpoint identity group What must be done on a new Cisco ISE deployment to redirect the laptop and restrict access?

- A. Select DenyAccess within the authorization policy.
- B. Ensure that access to port 8443 is allowed within the ACL.
- C. Ensure that access to port 8444 is allowed within the ACL.
- D. Select DROP under If Auth fail within the authentication policy.

**Answer:** C

**Explanation:**

[https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin\\_guide/b\\_ise\\_admin\\_guide\\_13/b\\_ise\\_admin\\_guide](https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide)

**NEW QUESTION 109**

An engineer is enabling a newly configured wireless SSID for tablets and needs visibility into which other types of devices are connecting to it. What must be done on the Cisco WLC to provide this information to Cisco ISE9

- A. enable IP Device Tracking
- B. enable MAC filtering

- C. enable Fast Transition
- D. enable mDNS snooping

**Answer:** B

#### NEW QUESTION 114

An engineer needs to configure a new certificate template in the Cisco ISE Internal Certificate Authority to prevent BYOD devices from needing to re-enroll when their MAC address changes. Which option must be selected in the Subject Alternative Name field?

- A. Common Name and GUID
- B. MAC Address and GUID
- C. Distinguished Name
- D. Common Name

**Answer:** B

#### Explanation:

The engineer needs to select the option of MAC Address and GUID in the Subject Alternative Name field when configuring a new certificate template in the Cisco ISE Internal Certificate Authority to prevent BYOD devices from needing to re-enroll when their MAC address changes.

#### NEW QUESTION 117

What is a valid guest portal type?

- A. Sponsored-Guest
- B. My Devices
- C. Sponsor
- D. Captive-Guest

**Answer:** A

#### NEW QUESTION 122

An administrator must block access to BYOD endpoints that were onboarded without a certificate and have been reported as stolen in the Cisco ISE My Devices Portal. Which condition must be used when configuring an authorization policy that sets DenyAccess permission?

- A. Endpoint Identity Group is Blocklist, and the BYOD state is Registered.
- B. Endpoint Identify Group is Blocklist, and the BYOD state is Pending.
- C. Endpoint Identity Group is Blocklist, and the BYOD state is Lost.
- D. Endpoint Identity Group is Blocklist, and the BYOD state is Reinstate.

**Answer:** A

#### Explanation:

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin\\_guide/b\\_ISE\\_26\\_admin\\_guide/b\\_ISE\\_admin\\_26\\_](https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ISE_26_admin_guide/b_ISE_admin_26_)

#### NEW QUESTION 127

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. Create a Cisco AnyConnect configuration and Client Provisioning policy within Cisco ISE.
- B. Configure the compliance module to be downloaded from within the posture policy.
- C. Push the compliance module from Cisco FTD prior to attempting posture.
- D. Use a compound posture condition to check for the compliance module and download if needed.

**Answer:** A

#### NEW QUESTION 128

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

- A. Device Administration License
- B. Server Sequence
- C. Command Sets
- D. Enable Device Admin Service
- E. External TACACS Servers

**Answer:** AD

#### NEW QUESTION 130

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:** AB

#### NEW QUESTION 135

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 properly 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 verify 1`
- D. EAP-FAST is not enabled

**Answer:** B

#### NEW QUESTION 136

An engineer is configuring static SGT classification. Which configuration should be used when authentication is disabled and third-party switches are in use?

- A. VLAN to SGT mapping
- B. IP Address to SGT mapping
- C. L3IF to SGT mapping
- D. Subnet to SGT mapping

**Answer:** B

#### Explanation:

<https://community.cisco.com/t5/security-knowledge-base/segmentation-strategy/ta-p/3757424>: "The method of sending out IP to SGT mappings from ISE is particularly useful if the access switch does not support TrustSec"

#### NEW QUESTION 139

An administrator for a small network is configuring Cisco ISE to provide dynamic network access to users. Management needs Cisco ISE to not automatically trigger a CoA whenever a profile change is detected. Instead, the administrator needs to verify the new profile and manually trigger a CoA. What must be configuring in the profiler to accomplish this goal?

- A. Port Bounce
- B. No CoA
- C. Session Query
- D. Reauth

**Answer:** B

#### Explanation:

<https://ciscocustomer.lookbookhq.com/iseguidedjourney/ISE-profiling-policies>

#### NEW QUESTION 140

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. Use the file registry condition to ensure that the firewal is installed and running appropriately.
- B. Use a compound condition to look for the Windows or Mac native firewall applications.
- C. Enable the default rewall condition to check for any vendor rewall application.
- D. Enable the default application condition to identify the applications installed and validade the rewall app.

**Answer:** C

#### Explanation:

[https://www.youtube.com/watch?v=6Kj8P8Hn7dY&t=109s&ab\\_channel=CiscoISE-IdentityServicesEngine](https://www.youtube.com/watch?v=6Kj8P8Hn7dY&t=109s&ab_channel=CiscoISE-IdentityServicesEngine)

#### NEW QUESTION 142

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

- A. 443
- B. 19005
- C. 8080
- D. 3799
- E. 1700

**Answer:** DE

#### NEW QUESTION 147

If a user reports a device lost or stolen, which portal should be used to prevent the device from accessing the network while still providing information about why the device is blocked?

- A. Client Provisioning
- B. Guest
- C. BYOD

D. Blacklist

**Answer:** D

**Explanation:**

[https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless\\_Networks/Unified\\_Access/BYOD\\_Desi](https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Desi) The Blacklist identity group is system generated and maintained by ISE to prevent access to lost or stolen devices. In this design guide, two authorization profiles are used to enforce the permissions for wireless and wired devices within the Blacklist:

- Blackhole WiFi Access
- Blackhole Wired Access

**NEW QUESTION 149**

An engineer is designing a BYOD environment utilizing Cisco ISE for devices that do not support native supplicants Which portal must the security engineer configure to accomplish this task?

- A. MDM
- B. Client provisioning
- C. My devices
- D. BYOD

**Answer:** C

**Explanation:**

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin\\_guide/b\\_ise\\_admin\\_guide\\_22/b\\_ise\\_admin\\_guide](https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide)

**NEW QUESTION 152**

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:** AD

**NEW QUESTION 157**

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

- A. Client Profiling
- B. Client Endpoint
- C. Client Provisioning
- D. Client Guest

**Answer:** C

**NEW QUESTION 158**

What sends the redirect ACL that is configured in the authorization profile back to the Cisco WLC?

- A. Cisco-av-pair
- B. Class attribute
- C. Event
- D. State attribute

**Answer:** A

**NEW QUESTION 163**

An organization is adding new profiling probes to the system to improve profiling on Oseo ISE The probes must support a common network management protocol to receive information about the endpoints and the ports to which they are connected What must be configured on the network device to accomplish this goal?

- A. ARP
- B. SNMP
- C. WCCP
- D. ICMP

**Answer:** B

**Explanation:**

<https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456#toc-hId-79034313>

**NEW QUESTION 168**

Which interface-level command is needed to turn on 802 1X authentication?

- A. Dofl1x pae authenticator
- B. dot1x system-auth-control

- C. authentication host-mode single-host
- D. aaa server radius dynamic-author

**Answer:** A

#### NEW QUESTION 172

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:** CD

#### NEW QUESTION 174

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

- A. Location the CSV file for the device MAC
- B. Select the certificate template
- C. Choose the hashing method
- D. Enter the common name
- E. Enter the IP address of the device

**Answer:** BD

#### Explanation:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200534-ISE-2-0-Certificate-Provi>

#### NEW QUESTION 178

Refer to the exhibit.

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 )

```
radius server ISE1
 address ipv4 192.168.255.17 auth-port 1645 acct-port 1646
 key 7 0607542D5F4A0213034C1E0A1F0F2E2122733F3429000D12055A5A52

tacacs server ISE1
 address ipv4 192.168.255.15 auth-port 1645 acct-port 1646
 key 7 0607542D5F4A0213034C1E0A1F0F2E2122733F3429000D12055A5A52

radius server ISE1
 address ipv4 192.168.255.19 auth-port 1645 acct-port 1646
 key 7 0607542D5F4A0213034C1E0A1F0F2E2122733F3429000D12055A5A52

radius server ISE1
 address ipv4 192.168.255.16 auth-port 1645 acct-port 1646
 key 7 0607542D5F4A0213034C1E0A1F0F2E2122733F3429000D12055A5A52

tacacs server ISE1
 address ipv4 192.168.255.18 auth-port 1645 acct-port 1646
 key 7 0607542D5F4A0213034C1E0A1F0F2E2122733F3429000D12055A5A52
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D
- E. Option E

**Answer:** AC

#### NEW QUESTION 183

An administrator wants to configure network device administration and is trying to decide whether to use TACACS\* or RADIUS. A reliable protocol must be used that can check command authorization Which protocol meets these requirements and why?

- A. TACACS+ because it runs over TCP
- B. RADIUS because it runs over UDP
- C. RADIUS because it runs over TCP.
- D. TACACS+ because it runs over UDP



**Answer:** A

#### NEW QUESTION 184

An engineer is configuring 802.1X and wants it to be transparent from the users' point of view. The implementation should provide open authentication on the switch ports while providing strong levels of security for non-authenticated devices. Which deployment mode should be used to achieve this?

- A. closed
- B. low-impact
- C. open
- D. high-impact

**Answer:** B

#### Explanation:

<https://www.lookingpoint.com/blog/cisco-ise-wired-802.1x-deployment-monitormode#:~:text=Low%20im>

#### NEW QUESTION 189

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

- A. Unknown
- B. whitelist
- C. end point
- D. profiled
- E. blacklist

**Answer:** ADE

#### Explanation:

Default Endpoint Identity Groups Created for Endpoints

Cisco ISE creates the following five endpoint identity groups by default: Blacklist, GuestEndpoints, Profiled, RegisteredDevices, and Unknown. In addition, it creates two more identity groups, such as Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group. A parent group is the default identity group that exists in the system.

[https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin\\_guide/b\\_ise\\_admin\\_guide\\_24/b\\_ise\\_admin\\_guide](https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide)

#### NEW QUESTION 192

What is a function of client provisioning?

- A. It ensures an application process is running on the endpoint.
- B. It checks a dictionary' attribute with a value.
- C. It ensures that endpoints receive the appropriate posture agents
- D. It checks the existence date and versions of the file on a client.

**Answer:** C

#### NEW QUESTION 197

MacOS users are complaining about having to read through wordy instructions when remediating their workstations to gain access to the network Which alternate method should be used to tell users how to remediate?

- A. URL link
- B. message text
- C. executable
- D. file distribution

**Answer:** A

#### Explanation:

<https://www.sciencedirect.com/topics/computer-science/remediation-action>

#### NEW QUESTION 202

A network engineer is configuring guest access and notices that when a guest user registers a second device for access, the first device loses access What must be done to ensure that both devices for a particular user are able to access the guest network simultaneously?

- A. Configure the sponsor group to increase the number of logins.
- B. Use a custom portal to increase the number of logins
- C. Modify the guest type to increase the number of maximum devices
- D. Create an Adaptive Network Control policy to increase the number of devices

**Answer:** C

#### Explanation:

[https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/security/ise/2-7/admin\\_guide](https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/security/ise/2-7/admin_guide)

#### NEW QUESTION 206

An engineer is using the low-impact mode for a phased deployment of Cisco ISE and is trying to connect to the network prior to authentication. Which access will be denied in this?

- A. HTTP
- B. DNS
- C. EAP
- D. DHCP

Answer: A

NEW QUESTION 207

An engineer has been tasked with standing up a new guest portal for customers that are waiting in the lobby. There is a requirement to allow guests to use their social media logins to access the guest network to appeal to more customers What must be done to accomplish this task?

- A. Create a sponsor portal to allow guests to create accounts using their social media logins.
- B. Create a sponsored guest portal and enable social media in the external identity sources.
- C. Create a self-registered guest portal and enable the feature for social media logins
- D. Create a hotspot portal and enable social media login for network access

Answer: C

NEW QUESTION 209

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.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

PEAP-MSCHAPv2

uses username and password for authentication

changes credentials through the admin portal

supports fragmentation after the tunnel is established

PEAP-EAP-TLS

uses certificates for authentication

uses the X.509 format

supports auto-enrollment for obtaining credentials

NEW QUESTION 214

A network administrator must configure Cisco SE Personas in the company to share session information via syslog. Which Cisco ISE personas must be added to syslog receivers to accomplish this goal?

- A. pxGrid

- B. admin
- C. policy services
- D. monitor

**Answer:** D

#### NEW QUESTION 215

What is a difference between TACACS+ and RADIUS in regards to encryption?

- A. TACACS+ encrypts only the password, whereas RADIUS encrypts the username and password.
- B. TACACS+ encrypts the username and password, whereas RADIUS encrypts only the password.
- C. TACACS+ encrypts the password, whereas RADIUS sends the entire packet in clear text.
- D. TACACS+ encrypts the entire packet, whereas RADIUS encrypts only the password.

**Answer:** D

#### NEW QUESTION 219

A network administrator is setting up wireless guest access and has been unsuccessful in testing client access. The endpoint is able to connect to the SSID but is unable to grant access to the guest network through the guest portal. What must be done to identify the problem?

- A. Use context visibility to verify posture status.
- B. Use the endpoint ID to execute a session trace.
- C. Use the identity group to validate the authorization rules.
- D. Use traceroute to ensure connectivity.

**Answer:** B

#### Explanation:

[https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin\\_guide/b\\_ise\\_admin\\_guide\\_13/b\\_ise\\_admin\\_guide](https://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide)

#### NEW QUESTION 221

Which two Cisco ISE deployment models require two nodes configured with dedicated PAN and MnT personas? (Choose two.)

- A. three PSN nodes
- B. seven PSN nodes with one PxGrid node
- C. five PSN nodes with one PxGrid node
- D. two PSN nodes with one PxGrid node
- E. six PSN nodes

**Answer:** CD

#### NEW QUESTION 223

Which default endpoint identity group does an endpoint that does not match any profile in Cisco ISE become a member of?

- A. Endpoint
- B. unknown
- C. blacklist
- D. white list
- E. profiled

**Answer:** B

#### Explanation:

If you do not have a matching profiling policy, you can assign an unknown profiling policy. The endpoint is therefore profiled as Unknown. The endpoint that does not match any profile is grouped within the Unknown identity group. The endpoint profiled to the Unknown profile requires that you create a profile with an attribute or a set of attributes collected for that endpoint.

[https://www.cisco.com/en/US/docs/security/ise/1.0/user\\_guide/ise10\\_man\\_identities.html](https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_man_identities.html)

#### NEW QUESTION 227

An administrator is trying to collect metadata information about the traffic going across the network to gain added visibility into the hosts. This information will be used to create profiling policies for devices using Cisco ISE so that network access policies can be used. What must be done to accomplish this task?

- A. Configure the RADIUS profiling probe within Cisco ISE
- B. Configure NetFlow to be sent to the Cisco ISE appliance.
- C. Configure SNMP to be used with the Cisco ISE appliance
- D. Configure the DHCP probe within Cisco ISE

**Answer:** D

#### NEW QUESTION 231

What gives Cisco ISE an option to scan endpoints for vulnerabilities?

- A. authorization policy
- B. authentication policy
- C. authentication profile
- D. authorization profile

**Answer:** A

**NEW QUESTION 233**

An administrator adds a new network device to the Cisco ISE configuration to authenticate endpoints to the network. The RADIUS test fails after the administrator configures all of the settings in Cisco ISE and adds the proper configurations to the switch. What is the issue"?

- A. The endpoint profile is showing as "unknown."
- B. The endpoint does not have the appropriate credentials for network access.
- C. The shared secret is incorrect on the switch or on Cisco ISE.
- D. The certificate on the switch is self-signed not a CA-provided certificate.

**Answer:** B

**NEW QUESTION 236**

What are the minimum requirements for deploying the Automatic Failover feature on Administration nodes in a distributed Cisco ISE deployment?

- A. a primary and secondary PAN and a health check node for the Secondary PAN
- B. a primary and secondary PAN and no health check nodes
- C. a primary and secondary PAN and a pair of health check nodes
- D. a primary and secondary PAN and a health check node for the Primary PAN

**Answer:** D

**NEW QUESTION 241**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 300-715 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-715 Product From:

<https://www.2passeasy.com/dumps/300-715/>

## Money Back Guarantee

### 300-715 Practice Exam Features:

- \* 300-715 Questions and Answers Updated Frequently
- \* 300-715 Practice Questions Verified by Expert Senior Certified Staff
- \* 300-715 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 300-715 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year