Cisco

Exam Questions 300-715

Implementing and Configuring Cisco Identity Services Engine (SISE)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

　　All examinations will be up to date.

* 24/7 Quality Support

　　We will provide service round the clock.

* 100% Pass Rate

　　Our guarantee that you will pass the exam.

* Unique Gurantee

　　If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
An engineer is migrating users from MAB to 802.1X on the network. This must be done during normal business hours with minimal impact to users. Which CoA method should be used?

A. Port Bounce
B. Port Shutdown
C. Session Termination
D. Session Reauthentication

Answer: D

NEW QUESTION 2
What should be considered when configuring certificates for BYOD?

A. An endpoint certificate is mandatory for the Cisco ISE BYOD
B. An Android endpoint uses EST whereas other operation systems use SCEP for enrollment
C. The CN field is populated with the endpoint host name.
D. The SAN field is populated with the end user name

Answer: A

NEW QUESTION 3
A Cisco ISE administrator must restrict specific endpoints from accessing the network while in closed mode. The requirement is to have Cisco ISE centrally store the endpoints to restrict access from. What must be done to accomplish this task''

A. Add each MAC address manually to a blocklist identity group and create a policy denying access
B. Create a logical profile for each device's profile policy and block that via authorization policies.
C. Create a profiling policy for each endpoint with the cdpCacheDeviceld attribute.
D. Add each IP address to a policy denying access.

Answer: B

NEW QUESTION 4
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%

NEW QUESTION 5
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 6
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 7
Which term refers to an endpoint agent that tries to join an 802 1X-enabled network?

A. EAP server
B. supplicant
C. client
D. authenticator

Answer: B

Explanation:
https://www.oreilly.com/library/view/cisco-ise-for/9780133103632/ch16.html#:~:text=What%20is%20a%
&text=The%20802.1X%20transactions%20are,Identity%20Services%20Engine%20(ISE).

NEW QUESTION 8
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 9
In a Cisco ISE split deployment model, which load is split between the nodes?

A. AAA
B. network admission
C. log collection
D. device admission

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/install_guide/b_ise_InstallationGuide26.pdf

NEW QUESTION 10
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 10
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 13
During a 802 1X deployment, an engineer must identify failed authentications without causing problems for the connected endpoint. Which command will successfully achieve this"

A. dot1x system-auth-control
B. dot1x pae authenticator
C. authentication open
D. authentication port-control auto

Answer: C

NEW QUESTION 14

What is the minimum certainty factor when creating a profiler policy?

A. the minimum number that a predefined condition provides
B. the maximum number that a predefined condition provides
C. the minimum number that a device certainty factor must reach to become a member of the profile
D. the maximum number that a device certainty factor must reach to become a member of the profile

Answer: C

NEW QUESTION 19
Which supplicant(s) and server(s) are capable of supporting EAP-CHAINING?

A. Cisco AnyConnect NAM and Cisco Identity Service Engine
B. Cisco AnyConnect NAM and Cisco Access Control Server
C. Cisco Secure Services Client and Cisco Access Control Server
D. Windows Native Supplicant and Cisco Identity Service Engine

Answer: A

NEW QUESTION 23
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 27
Which two components are required for creating a Native Supplicant Profile within a BYOD flow? (Choose two)

A. Windows Settings
B. Connection Type
C. iOS Settings
D. Redirect ACL
E. Operating System

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_

NEW QUESTION 30
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

NEW QUESTION 34
An administrator needs to give the same level of access to the network devices when users are logging into them using TACACS+ However, the administrator must restrict certain commands based on one of three user roles that require different commands How is this accomplished without creating too many objects using Cisco ISE?

A. Create one shell profile and multiple command sets.
B. Create multiple shell profiles and multiple command sets.
C. Create one shell profile and one command set.
D. Create multiple shell profiles and one command set

Answer: A

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
https://www.youtube.com/watch?v=IlZwB71Szog&ab_channel=JasonMaynard

NEW QUESTION 37
Which Cisco ISE service allows an engineer to check the compliance of endpoints before connecting to the network?

A. personas
B. qualys
C. nexpose
D. posture

Answer: D

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 Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control clients to access protected areas of a network.

NEW QUESTION 40
Which two fields are available when creating an endpoint on the context visibility page of Cisco IS? (Choose two)

A. Policy Assignment
B. Endpoint Family
C. Identity Group Assignment
D. Security Group Tag
E. IP Address

Answer: AC

NEW QUESTION 43
An engineer is configuring ISE for network device administration and has devices that support both protocols. What are two benefits of choosing TACACS+ over RADUs for these devices? (Choose two.)

A. TACACS+ is FIPS compliant while RADIUS is not
B. TACACS+ is designed for network access control while RADIUS is designed for role-based access.
C. TACACS+ uses secure EAP-TLS while RADIUS does not.
D. TACACS+ provides the ability to authorize specific commands while RADIUS does not
E. TACACS+ encrypts the entire payload being sent while RADIUS only encrypts the password.

Answer: DE

NEW QUESTION 44
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 quest 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 45
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 48
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

NEW QUESTION 53
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

NEW QUESTION 58
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 59
An ISE administrator must change the inactivity timer for MAB endpoints to terminate the authentication session whenever a switch port that is connected to an IP phone does not detect packets from the device for 30 minutes. Which action must be taken to accomplish this task?

A. Add the authentication timer reauthenticate server command to the switchport.
B. Add the authentication timer inactivity 3600 command to the switchport.
C. Change the idle-timeout on the Radius server to 3600 seconds for IP Phone endpoints.
D. Configure the session-timeout to be 3600 seconds on Cisco ISE.

Answer: B

NEW QUESTION 60
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 goat? (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 62
When setting up profiling in an environment using Cisco ISE for network access control, an organization must use non-proprietary protocols for collecting the information at layer 2. Which two probes will provide this information without forwarding SPAN packets to Cisco ISE? {Choose two.)

A. DHCP SPAN probe
B. SNMP query probe
C. NetFlow probe
D. RADIUS probe
E. DNS probe

Answer: BD

Explanation:
https://ciscocustomer.lookbookhq.com/iseguidedjourney/ISE-profiling-design

NEW QUESTION 66
What service can be enabled on the Cisco ISE node to identity the types of devices connecting to a network?

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

Answer: B

NEW QUESTION 68
Refer to the exhibit.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1xdefault group radius
Switch(config)# aaa authorization network default group radius
```

A network engineers configuring the switch to accept downloadable ACLs from a Cisco ISC server Which two commands should be run to complete the

configuration? (Choose two)

A. aaa authorization auth-proxy default group radius
B. radius server vsa sand authentication
C. radius-server attribute 8 include-in-access-req
D. ip device tracking
E. dot1x system-auth-control

Answer: BC

NEW QUESTION 69
Refer to the exhibit:

```
Interface: GigabitEthernet2/0/36
MAC Address: 000e.84af.59af
Status: Authz Success
Domain: DATA
Oper host mode: single-host
Authorized By: Authentication Server
Vlan Policy: 10
Handle: 0xE0000000
Runnable methods list:
Method State
dot1x Authc Success
```

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

A. show authentication sessions mac 000e.84af.59af details
B. show authentication registrations
C. show authentication interface gigabitethemet2/0/36
D. show authentication sessions method

Answer: A

NEW QUESTION 72
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

NEW QUESTION 73
What is a valid guest portal type?

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

Answer: A

NEW QUESTION 76
An engineer is configuring Cisco ISE policies to support MAB for devices that do not have 802.1X capabilities. The engineer is configuring new endpoint identity groups as conditions to be used in the AuthZ policies, but noticed that the endpoints are not hitting the correct policies. What must be done in order to get the devices into the right policies?

A. Manually add the MAC addresses of the devices to endpoint ID groups in the context visibility database.
B. Create an AuthZ policy to identify Unknown devices and provide partial network access prior to profiling.
C. Add an identity policy to dynamically add the IP address of the devices to their endpoint identity groups.
D. Identify the non 802.1X supported device types and create custom profiles for them to profile into.

Answer: D

NEW QUESTION 77
Which two responses from the RADIUS server to NAS are valid during the authentication process? (Choose two)

A. access-response
B. access-request
C. access-reserved

D. access-accept
E. access-challenge

Answer: BD

NEW QUESTION 79
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 entries in the guest identity group for all participants.
B. Create an access code to be entered in the AUP page.
C. Create logins for each participant to give them sponsored access.
D. Create a registration code to be entered on the portal splash page.

Answer: B

NEW QUESTION 84
A network administrator has just added a front desk receptionist account to the Cisco ISE Guest Service sponsor group. Using the Cisco ISE Guest Sponsor Portal, which guest services can the receptionist provide?

A. Keep track of guest user activities
B. Configure authorization settings for guest users
C. Create and manage guest user accounts
D. Authenticate guest users to Cisco ISE

Answer: C

NEW QUESTION 88
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 92
A network administrator is configuring client provisioning resource policies for client machines and must ensure that an agent pop-up is presented to the client when attempting to connect to the network Which configuration item needs to be added to allow for this'?

A. the client provisioning URL in the authorization policy
B. a temporal agent that gets installed onto the system
C. a remote posture agent proxying the network connection
D. an API connection back to the client

Answer: C

NEW QUESTION 95
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

NEW QUESTION 97
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 101
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 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 103
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 firewall 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

NEW QUESTION 107
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 110
An organization wants to improve their BYOD processes to have Cisco ISE issue certificates to the BYOD endpoints. Currently, they have an active certificate authority and do not want to replace it with Cisco ISE. What must be configured within Cisco ISE to accomplish this goal?

A. Create a certificate signing request and have the root certificate authority sign it.
B. Add the root certificate authority to the trust store and enable it for authentication.
C. Create an SCEP profile to link Cisco ISE with the root certificate authority.
D. Add an OCSP profile and configure the root certificate authority as secondary.

Answer: C

Explanation:
Ref:https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/116068-configure-pr

NEW QUESTION 111
Which profiling probe collects the user-agent string?

A. DHCP
B. AD
C. HTTP
D. NMAP

Answer: C

NEW QUESTION 116
Refer to the exhibit. An engineer is creating a new TACACS* command set and cannot use any show commands after togging into the device with this command set authorization Which configuration is causing this issue?

A. Question marks are not allowed as wildcards for command sets.
B. The command set is allowing all commands that are not in the command list

C. The wildcard command listed is in the wrong format
D. The command set is working like an ACL and denying every command.

Answer: A

NEW QUESTION 118
A network administrator is currently using Cisco ISE to authenticate devices and users via 802 1X There is now a need to also authorize devices and users using EAP-TLS. Which two additional components must be configured in Cisco ISE to accomplish this'? (Choose two.)

A. Network Device Group
B. Serial Number attribute that maps to a CA Server
C. Common Name attribute that maps to an identity store
D. Certificate Authentication Profile
E. EAP Authorization Profile

Answer: CD

NEW QUESTION 119
What are two benefits of TACACS+ versus RADIUS for device administration? (Choose two)

A. TACACS+ supports 802.1X, and RADIUS supports MAB
B. TACACS+ uses UDP, and RADIUS uses TCP
C. TACACS+ has command authorization, and RADIUS does not.
D. TACACS+ provides the service type, and RADIUS does not
E. TACACS+ encrypts the whole payload, and RADIUS encrypts only the password.

Answer: CE

NEW QUESTION 120
An engineer is configuring 802.1X and is testing out their policy sets. After authentication, some endpoints are given an access-reject message but are still allowed onto the network. What is causing this issue to occur?

A. The switch port is configured with authentication event server dead action authorize vlan.
B. The authorization results for the endpoints include a dACL allowing access.
C. The authorization results for the endpoints include the Trusted security group tag.
D. The switch port is configured with authentication open.

Answer: D

NEW QUESTION 125
A network engineer is configuring Cisco TrustSec and needs to ensure that the Security Group Tag is being transmitted between two devices Where in the Layer 2 frame should this be verified?

A. CMD filed
B. 802.1Q filed
C. Payload
D. 802.1 AE header

Answer: A

Explanation:
https://www.cisco.com/c/dam/global/en_ca/assets/ciscoconnect/2014/pdfs/policy_defined_segmentation_with_tr (slide 25)

NEW QUESTION 128
Which two actions must be verified to confirm that the internet is accessible via guest access when configuring a guest portal? (Choose two.)

A. The guest device successfully associates with the correct SSID.
B. The guest user gets redirected to the authentication page when opening a browser.
C. The guest device has internal network access on the WLAN.
D. The guest device can connect to network file shares.
E. Cisco ISE sends a CoA upon successful guest authentication.

Answer: BE

NEW QUESTION 129
A customer wants to set up the Sponsor portal and delegate the authentication flow to a third party for added security while using Kerberos Which database should be used to accomplish this goal?

A. RSA Token Server
B. Active Directory
C. Local Database
D. LDAP

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide

NEW QUESTION 130
What must be configured on the Cisco ISE authentication policy for unknown MAC addresses/identities for successful authentication?

A. pass
B. reject
C. drop
D. continue

Answer: D

Explanation:
https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_man_id_stores.html

NEW QUESTION 132
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 135
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 138
What happens when an internal user is configured with an external identity store for authentication, but an engineer uses the Cisco ISE admin portal to select an internal identity store as the identity source?

A. Authentication is redirected to the internal identity source.
B. Authentication is redirected to the external identity source.
C. Authentication is granted.
D. Authentication fails.

Answer: D

NEW QUESTION 141
An administrator is attempting to replace the built-in self-signed certificates on a Cisco ISE appliance. The CA is requesting some information about the appliance in order to sign the new certificate. What must be done in order to provide the CA this information?

A. Install the Root CA and intermediate CA.
B. Generate the CSR.
C. Download the intermediate server certificate.
D. Download the CA server certificate.

Answer: B

NEW QUESTION 144
What is the purpose of the ip http server command on a switch?

A. It enables the https server for users for web authentication
B. It enables MAB authentication on the switch
C. It enables the switch to redirect users for web authentication.
D. It enables dot1x authentication on the switch.

Answer: C

NEW QUESTION 149
MacOS users are complaining about having to read through wordy instructions when remediating their workstations to gam 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 150
Which advanced option within a WLAN must be enabled to trigger Central Web Authentication for Wireless users on AireOS controller?

A. DHCP server
B. static IP tunneling
C. override Interface ACL
D. AAA override

Answer: D

NEW QUESTION 154
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:
https://community.cisco.com/t5/network-access-control/ise-for-printer-security/m-p/3933216

NEW QUESTION 158
What is the maximum number of PSN nodes supported in a medium-sized deployment?

A. three
B. five
C. two
D. eight

Answer: B

NEW QUESTION 160
An engineer is configuring TACACS+ within Cisco ISE for use with a non-Cisco network device. They need to send special attributes in the Access-Accept response to ensure that the users are given the appropriate access. What must be configured to accomplish this'?

A. dACLs to enforce the various access policies for the users
B. custom access conditions for defining the different roles
C. shell profiles with custom attributes that define the various roles
D. TACACS+ command sets to provide appropriate access
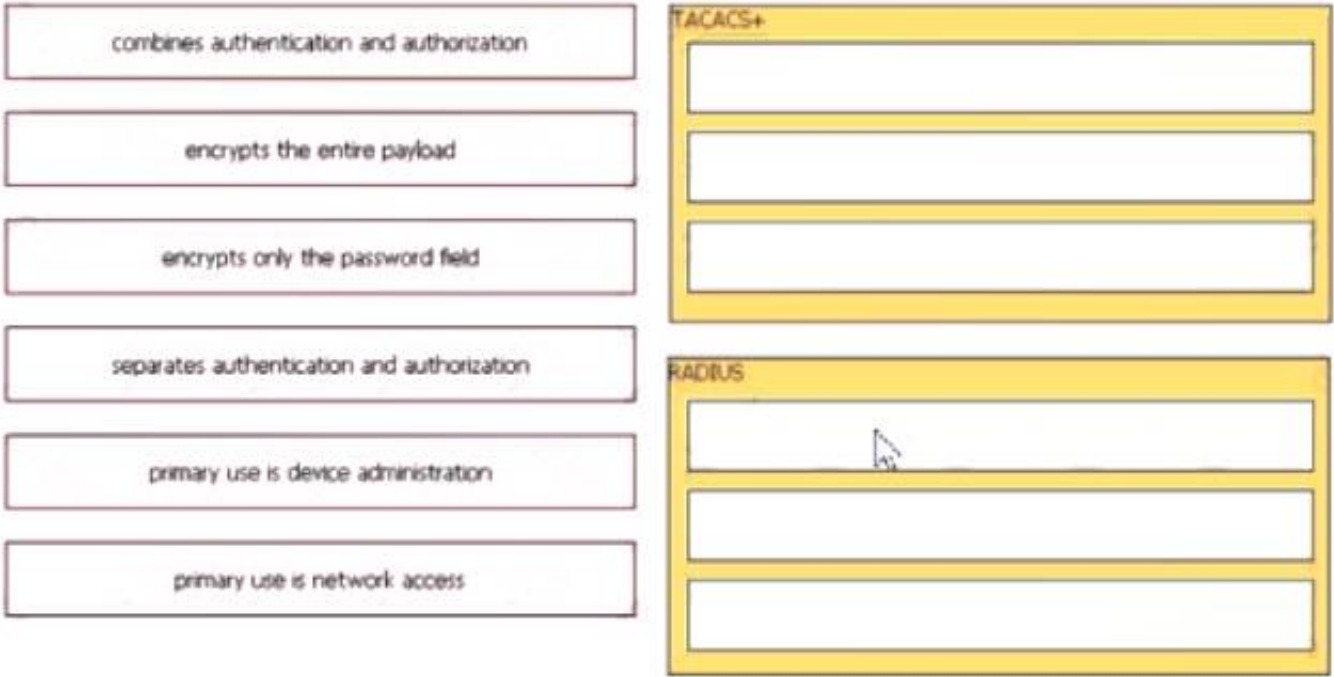
Answer: C

NEW QUESTION 161
Which Cisco ISE deployment model provides redundancy by having every node in the deployment configured with the Administration. Policy Service, and Monitoring personas to protect from a complete node failure?

A. distributed
B. dispersed
C. two-node
D. hybrid

Answer: C

NEW QUESTION 164
Drag and drop the description from the left onto the protocol on the right that is used to carry out system authentication, authentication, and accounting.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, chart, application Description automatically generated
https://www.mbne.net/tech-notes/aaa-tacacs-radius

NEW QUESTION 166
What is an advantage of using EAP-TLS over EAP-MS-CHAPv2 for client authentication?

A. EAP-TLS uses a username and password for authentication to enhance security, while EAP-MS-CHAPv2 does not.
B. EAP-TLS secures the exchange of credentials, while EAP-MS-CHAPv2 does not.
C. EAP-TLS uses a device certificate for authentication to enhance security, while EAP-MS-CHAPv2 does not.
D. EAP-TLS uses multiple forms of authentication, while EAP-MS-CHAPv2 only uses one.

Answer: C

NEW QUESTION 168
An engineer is tasked with placing a guest access anchor controller in the DMZ. Which two ports or port sets must be opened up on the firewall to accomplish this task? (Choose two.)

A. UDP port 1812 RADIUS
B. TCP port 161
C. TCP port 514
D. UDP port 79
E. UDP port 16666

Answer: BC

NEW QUESTION 172
Refer to the exhibit.

An engineer is configuring a client but cannot authenticate to Cisco ISE During troubleshooting, the show authentication sessions command was issued to display the authentication status of each port Which command gives additional information to help identify the problem with the authentication?

A. show authentication sessions
B. show authentication sessions Interface Gil/0/1 output
C. show authentication sessions interface Gi1/0/1 details
D. show authentication sessions output

Answer: C

NEW QUESTION 175
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 180
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 183
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

NEW QUESTION 188
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: DE

NEW QUESTION 190
An administrator is migrating device administration access to Cisco ISE from the legacy TACACS+ solution that used only privilege 1 and 15 access levels. The organization requires more granular controls of the privileges and wants to customize access levels 2-5 to correspond with different roles and access needs. Besides defining a new shell profile in Cisco ISE. what must be done to accomplish this configuration?

A. Enable the privilege levels in Cisco ISE
B. Enable the privilege levels in the IOS devices.
C. Define the command privileges for levels 2-5 in the IOS devices
D. Define the command privileges for levels 2-5 in Cisco ISE

Answer: B

Explanation:
https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels

NEW QUESTION 192
An administrator is configuring a new profiling policy in Cisco ISE for a printer type that is missing from the profiler feed The logical profile Printers must be used in the authorization rule and the rule must be hit. What must be done to ensure that this configuration will be successful^

A. Create a new logical profile for the new printer policy
B. Enable the EndPoints:EndPointPolicy condition in the authorization policy.
C. Add the new profiling policy to the logical profile Printers.
D. Modify the profiler conditions to ensure that it goes into the correct logical profile

Answer: B

NEW QUESTION 195
What occurs when a Cisco ISE distributed deployment has two nodes and the secondary node is deregistered?

A. The primary node restarts
B. The secondary node restarts.
C. The primary node becomes standalone
D. Both nodes restart.

Answer: D

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-1-1/installation_guide/ise_install_guide/ise_deploy.html if your deployment has two nodes and you deregister

the secondary node, both nodes in this
primary-secondary pair are restarted. (The former primary and secondary nodes become standalone.)

NEW QUESTION 197
Refer to the exhibit

```
interface GigabitEthernet1/0/1
authentication host-mode multi-auth
authentication post-control auto
mab
dot1x pae authenticator
```

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:
https://community.cisco.com/t5/network-access-control/cisco-ise-multi-auth-or-multi-host/m-p/3750907

NEW QUESTION 199
What is a function of client provisioning?

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

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_client_prov.html#:~:text=After%20

NEW QUESTION 204
An engineer is configuring posture assessment for their network access control and needs to use an agent that supports using service conditions as conditions for the assessment. The agent should be run as a background process to avoid user interruption but when it is run. the user can see it. What is the problem?

A. The engineer is using the "Anyconnect" posture agent but should be using the "Stealth Anyconnect posture agent
B. The posture module was deployed using the headend instead of installing it with SCCM
C. The user was in need of remediation so the agent appeared m the notifications
D. The proper permissions were no! given to the temporal agent to conduct the assessment

Answer: A

NEW QUESTION 209
Which compliance status is set when a matching posture policy has been defined for that endpomt. but all the mandatory requirements during posture assessment are not met?

A. unauthorized
B. untrusted
C. non-compliant
D. unknown

Answer: C

NEW QUESTION 214
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 215
An engineer is configuring a posture policy for Windows 10 endpoints and wants to ensure that users in each AD group have different conditions to meet to be compliant. What must be done to accomplish this task?

A. identify The users groups needed for different policies and create service conditions to map each one to its posture requirement
B. Configure a simple condition for each AD group and use it in the posture policy for each use case
C. Use the authorization policy within the policy set to group each AD group with their respective posture policy
D. Change the posture requirements to use an AD group lor each use case then use those requirements in the posture policy

Answer: C

NEW QUESTION 218
When planning for the deployment of Cisco ISE, an organization's security policy dictates that they must use network access authentication via RADIUS. It also states that the deployment provide an adequate amount of security and visibility for the hosts on the network. Why should the engineer configure MAB in this situation?

A. The Cisco switches only support MAB.
B. MAB provides the strongest form of authentication available.
C. The devices in the network do not have a supplicant.
D. MAB provides user authentication.

Answer: C

NEW QUESTION 222
An administrator is configuring cisco ISE lo authenticate users logging into network devices using TACACS+ The administrator is not seeing any oí 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

NEW QUESTION 225
Select and Place

A. Mastered
B. Not Mastered

Answer: A

Explanation:

uses username and password for authentication	**PEAP-MSCHAPv2**
uses certificates for authentication	uses username and password for authentication
changes credentials through the admin portal	changes credentials through the admin portal
supports fragmentation after the tunnel is established	supports fragmentation after the tunnel is established
uses the X.509 format	**PEAP-EAP-TLS**
supports auto-enrollment for obtaining credentials	uses certificates for authentication
	uses the X.509 format
	supports auto-enrollment for obtaining credentials
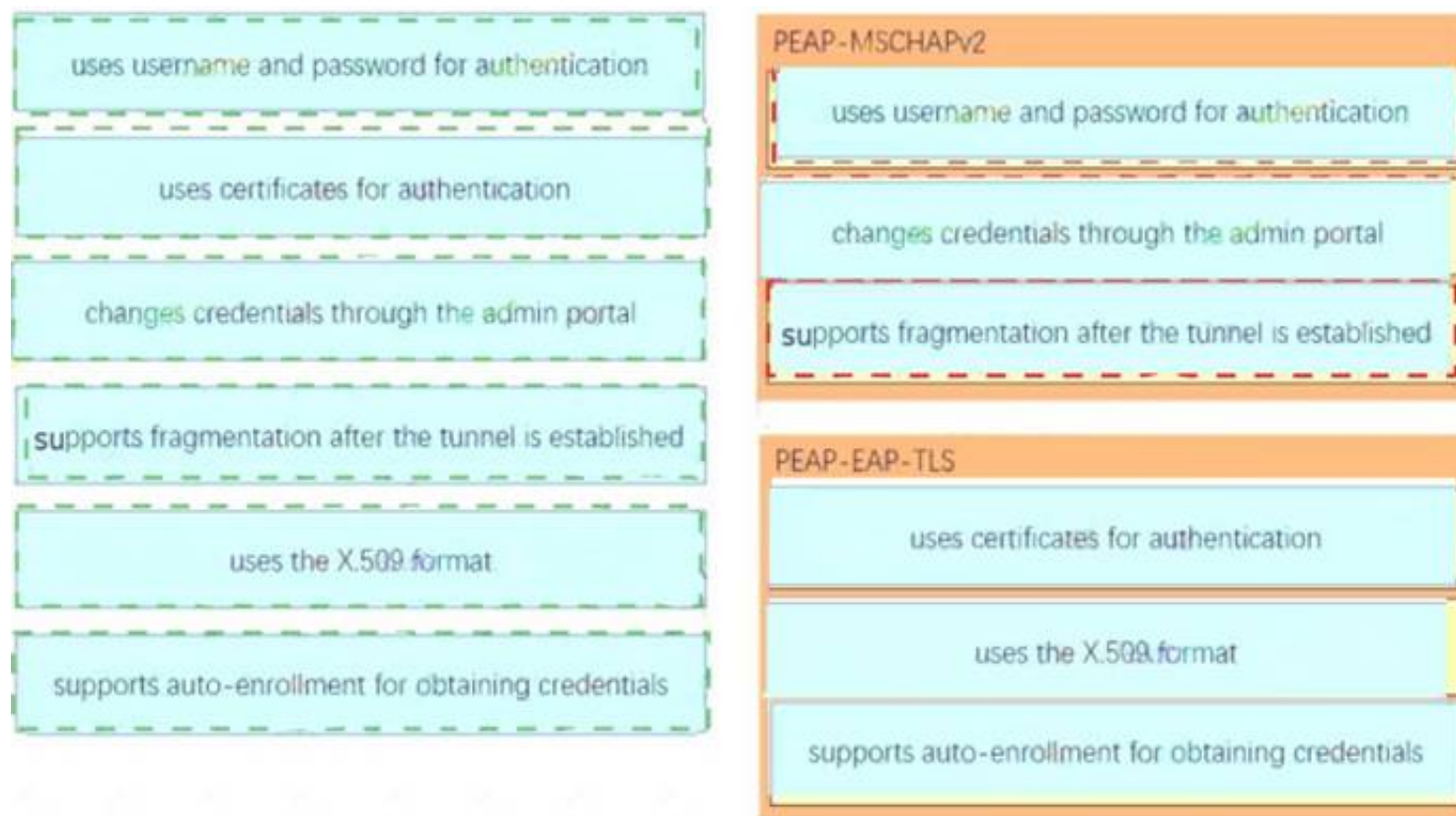
NEW QUESTION 229
Which statement about configuring certificates for BYOD is true?

A. An Android endpoint uses EST, whereas other operating systems use SCEP for enrollment
B. The SAN field is populated with the end user name.
C. An endpoint certificate is mandatory for the Cisco ISE BYOD
D. The CN field is populated with the endpoint host name

Answer: C

NEW QUESTION 230
Which two features should be used on Cisco ISE to enable the TACACS+ feature? (Choose two)

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

Answer: BC

NEW QUESTION 234
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: AE

NEW QUESTION 236
An administrator is adding a switch to a network that is running Cisco ISE and is only for IP Phones The phones do not have the ability to authenticate via 802 1X
Which command is needed on each switch port for authentication?

A. dot1x system-auth-control
B. enable bypass-mac
C. enable network-authentication
D. mab

Answer: D

Explanation:
https://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_aaa/configuration/15-2mt/sec-config-mab.html

NEW QUESTION 241
An engineer is configuring a virtual Cisco ISE deployment and needs each persona to be on a different node. Which persona should be configured with the largest amount of storage in this environment?

A. policy Services
B. Primary Administration

C. Monitoring and Troubleshooting
D. Platform Exchange Grid

Answer: C

NEW QUESTION 246
An engineer is implementing Cisco ISE and needs to configure 802.1X. The port settings are configured for port-based authentication. Which command should be used to complete this configuration?

A. dot1x pae authenticator
B. dot1x system-auth-control
C. authentication port-control auto
D. aaa authentication dot1x default group radius

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/31sg/configuration/guide/conf/dot1x.

NEW QUESTION 248
A network administrator notices that after a company-wide shut down, many users cannot connect their laptops to the corporate SSID. What must be done to permit access in a timely manner?

A. Authenticate the user's system to the secondary Cisco ISE node and move this user to the primary with the renewed certificate.
B. Connect this system as a guest user and then redirect the web auth protocol to log in to the network.
C. Add a certificate issue from the CA server, revoke the expired certificate, and add the new certificate in system.
D. Allow authentication for expired certificates within the EAP-TLS section under the allowed protocols.

Answer: A

NEW QUESTION 253
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 258
An engineer is configuring a dedicated SSID for onboarding devices. Which SSID type accomplishes this configuration?

A. dual
B. hidden
C. broadcast
D. guest

Answer: A

Explanation:
https://community.cisco.com/t5/security-documents/ise-byod-dual-vs-single-ssid-onboarding/ta-p/3641422
https://www.youtube.com/watch?v=HH_Xasqd9k4&ab_channel=CiscoISE-IdentityServicesEngine
http://www.labminutes.com/sec0053_ise_1_1_byod_wireless_onboarding_dual_ssid

NEW QUESTION 262
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 267
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 271
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
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 a 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 274
A policy is being created in order to provide device administration access to the switches on a network. There is a requirement to ensure that if the session is not actively being used, after 10 minutes, it will be disconnected. Which task must be configured in order to meet this requirement?

A. session timeout
B. idle time
C. monitor
D. set attribute as

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_admin_ac

NEW QUESTION 277
An engineer is configuring Cisco ISE and needs to dynamically identify the network endpoints and ensure that endpoint access is protected. Which service should be used to accomplish this task?

A. Profiling
B. Guest access
C. Client provisioning
D. Posture

Answer: A

NEW QUESTION 279
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 281
......

Relate Links

100% Pass Your 300-715 Exam with Exambible Prep Materials

https://www.exambible.com/300-715-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/