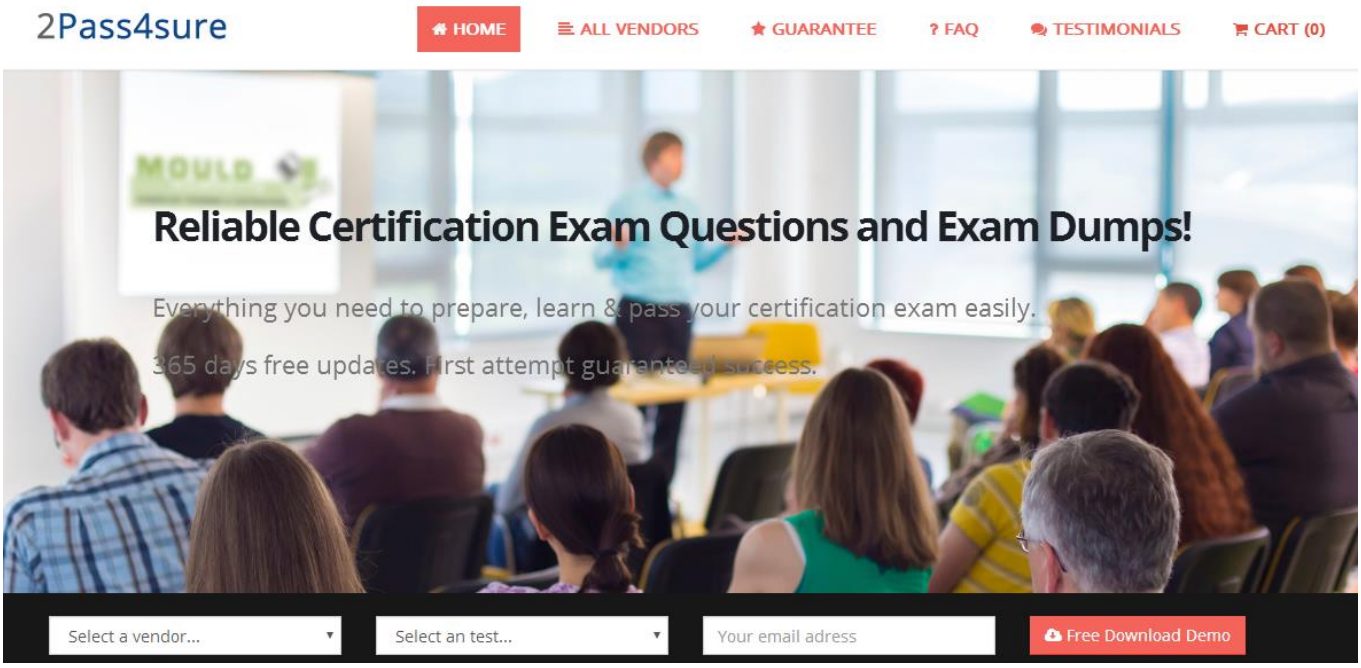
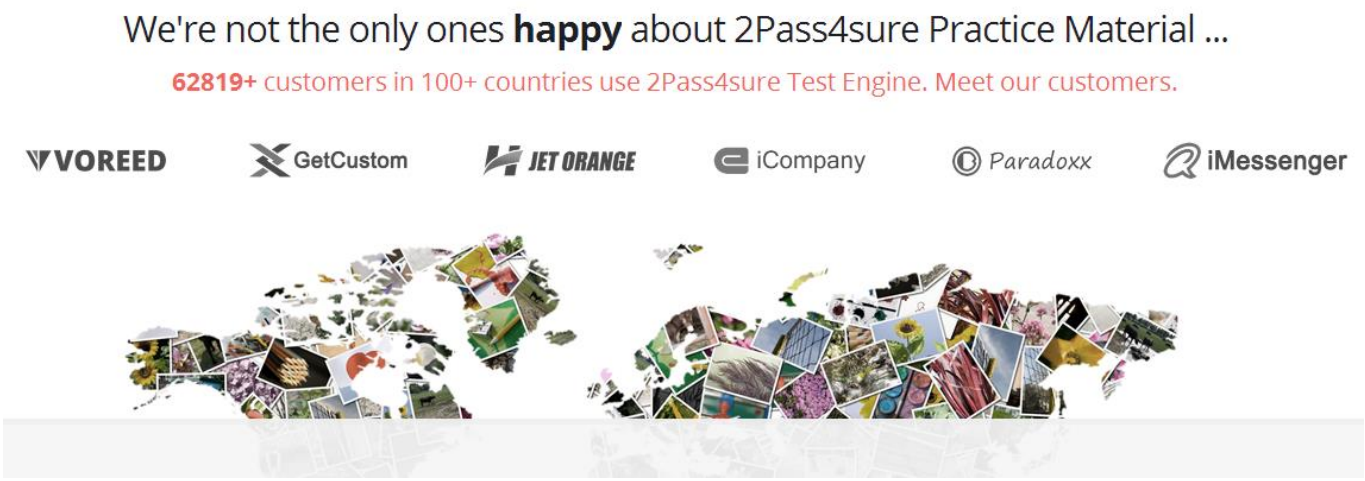
2Pass4sure





http://www.2pass4sure.com/

Reliable Certification Exam Questions and Exam Dumps - 2Pass4sure

Exam : **NSE5_FNC_AD_7.6**

Title : Fortinet NSE 5 - FortiNAC-F 7.6 Administrator

Vendor : Fortinet

Version : DEMO

NO.1 In which three ways would deploying a FortiNAC-F Manager into a large environment consisting of several FortiNAC-F CAs simplify management? (Choose three.)

A. Global infrastructure device inventory

B. Global version control

C. Global authentication security policies

D. Pooled licenses

E. Global visibility

Answer: B D E

Explanation:

TheFortiNAC-F Manager (FortiNAC-M)is designed as a centralized management platform for large-scale distributed environments where multiple FortiNAC-F Control and Application (CA) appliances are deployed across different sites. According to theFortiNAC-F Manager Administration Guide, the deployment of a Manager simplifies administrative overhead in three specific ways:

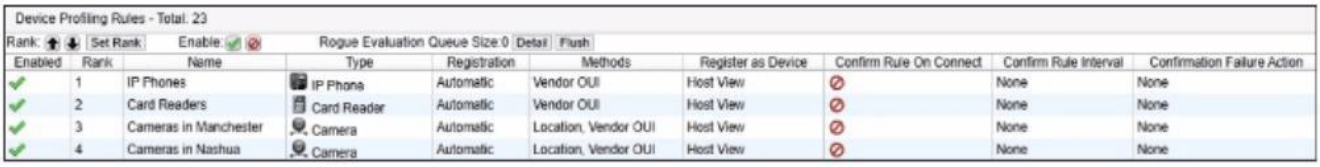
First, it providesGlobal Version Control (B). The Manager serves as a central repository for firmware and software updates, allowing administrators to push specific versions to all managed CAs simultaneously, ensuring consistency across the entire fabric. Second, it enablesPooled Licenses (D). Instead of purchasing and managing individual licenses for every CA, licenses are centralized on the Manager. The Manager then distributes these licenses to the CAs as needed based on their host counts. This " floating " license model optimizes cost and prevents individual sites from running out of capacity while others have excess. Third, it offersGlobal Visibility (E). The Manager aggregates host and device data from every managed CA into a single console. This " single pane of glass " allows an administrator to search for a specific MAC address or user across the entire global organization without logging into individual servers.

While the Manager can assist with configuration templates, authentication security policies (C) and infrastructure modeling (A) are still predominantly managed at the local CA level to ensure site-specific logic and performance.

" The FortiNAC Manager provides a central management console for multiple FortiNAC-F servers (CAs).

Key benefits include: *License Management: Licenses are pooled on the Manager and allocated to managed CAs as needed. *Software Management: Firmware updates can be centrally managed and pushed to all CAs from the Manager. *Centralized Monitoring: Provides a global view of all hosts, adapters, and events across the entire managed environment. " -FortiNAC-F Manager Administration Guide: Overview and Benefits.

NO.2 Refer to the exhibit.


Device Profiling Rules - Total: 23

Rank: Set Rank Enable: Rogue Evaluation Queue Size: 0 Detail Flush

Enabled	Rank	Name	Type	Registration	Methods	Register as Device	Confirm Rule On Connect	Confirm Rule Interval	Confirmation Failure Action
✓	1	IP Phones	IP Phone	Automatic	Vendor OUI	Host View	⊘	None	None
✓	2	Card Readers	Card Reader	Automatic	Vendor OUI	Host View	⊘	None	None
✓	3	Cameras in Manchester	Camera	Automatic	Location, Vendor OUI	Host View	⊘	None	None
✓	4	Cameras in Nashua	Camera	Automatic	Location, Vendor OUI	Host View	⊘	None	None

Which devices are automatically evaluated by these device profiling rules?

A. Rogue devices, only when they are initially added to the database

B. Known trusted devices, each time they connect

C. All hosts, each time they connect

D. Rogue devices, each time they change location

Answer: A

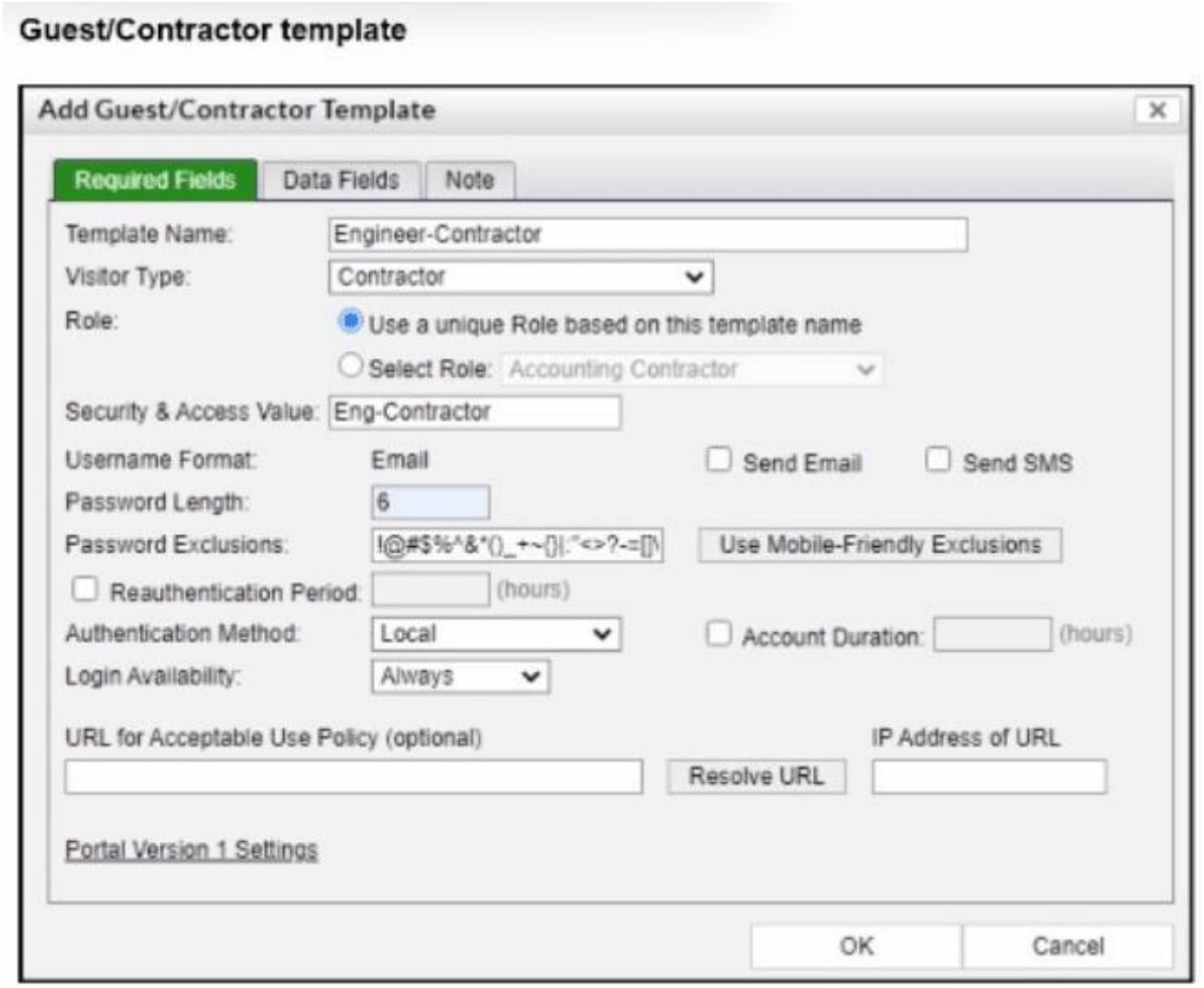
Explanation:
The correct answer is A . In FortiNAC-F, device profiling rules are used primarily to classify unknown or untrusted devices when they are first discovered. The study guide explains that when a device does not already exist in the database, FortiNAC-F adds it, treats it as a rogue, and evaluates it against enabled device profiling rules. It also states that devices are initially evaluated against device profiling rules only if they do not already exist in the database, because this avoids unnecessary repeated evaluation of known devices.
The exhibit also matters: the rules are enabled and set to Automatic registration, but Confirm Rule On Connect is not enabled and Confirm Rule Interval is set to None . That means FortiNAC-F will not automatically revalidate already-profiled or trusted devices every time they connect. Option B is wrong because trusted devices are not repeatedly evaluated unless rule confirmation is configured. Option C is too broad because all hosts are not processed through profiling rules on every connection. Option D is also wrong because changing location does not by itself force automatic device profiling; location can be used as a rule method, but the automatic evaluation described here applies when the rogue device is initially added to the database.

NO.3 While discovering network infrastructure devices, a switch appears in the inventory topology with a question mark (?) on the icon. What would cause this?
A. The wrong SNMP community string was entered during discovery.
B. The SNMP ObjectID is not recognized by FortiNAC-F.
C. A read-only SNMP community siring was used.
D. SNMP is not enabled on the switch.
Answer: B
Explanation:
In FortiNAC-F, theInventory topologyuses specific icons to represent the status and model of discovered network infrastructure. When a switch or other network device is discovered via SNMP, FortiNAC-F retrieves itsSystem ObjectID (sysObjectID)to identify the specific make and model. This OID is then compared against the internal database of supported device mappings.
Aquestion mark (?)icon appearing on a discovered switch indicates that while the discovery process successfully communicated with the device (meaning SNMP credentials were correct), theSNMP ObjectID is not recognizedor mapped in the current version of FortiNAC-F. This essentially means the device is " unsupported " by the current software out-of-the-box. Because the OID is unknown, FortiNAC-F does not know which CLI or SNMP command set to use for critical functions like L2 polling (host visibility) or VLAN switching (enforcement). To resolve this, an administrator can manually " Set Device Mapping " to a similar existing model or a " Generic SNMP Device " if only basic L3 visibility is required.
" Discovered devices displaying a ' ? ' iconindicate the currently running version does not have a mapping for that device ' sSystem OID(device is not supported). Device mappings are used to manage the device by performing functions such as L2/L3 Polling, Reading, and Switching VLANs. " -Fortinet Technical Tip:
Options for devices unable to be modeled in Inventory.

NO.4 An administrator manages a corporate environment where all users log into the corporate domain each time they connect to the network. The administrator wants to leverage login scripts to use a FortiNAC-F agent to enhance endpoint visibility Which agent can be deployed as part of a login script?

A. Persistent
B. Dissolvable
C. Mobile
D. Passive
Answer: A
Explanation:
In a corporate domain environment where " enhanced endpoint visibility " is required, thePersistent Agentis the recommended choice. Unlike the Dissolvable Agent, which is temporary and intended for one-time compliance scans during registration, the Persistent Agent is an " install-and-stay-resident " application.
The Persistent Agent is specifically designed to be distributed through automated enterprise methods, includinglogin scripts, Group Policy Objects (GPO), or third-party software management tools. When deployed via a login script, the agent can be configured to silently install and immediately begin communicating with the FortiNAC-F service interface. Once active, it provides continuous visibility by reporting host details such as logged-on users, installed applications, and adapter information. It also listens for Windows session events (logon/logoff) to trigger automatic single-sign-on (SSO) registration in FortiNAC- F, ensuring that as soon as a user connects to the domain, their device is identified and assigned the correct network access policy.
" The Persistent Agent can be distributed to Windows domain machines vialogin scriptor by any other software distribution method your organization might use. The Persistent Agent remains installed on the host at all times. Once the agent is installed it runs in the background and communicates with FortiNAC at intervals established by the FortiNAC administrator. " -FortiNAC-F Administration Guide: Persistent Agent Overview.

NO.5 Refer to the exhibit.



When a contractor account is created using this template, which value is set in the accounts Role field?

A. Engineer-Contractor

B. Eng-Contractor

C. Contractor

D. Accounting Contractor

Answer: A

Explanation:

The correct answer is A . In the exhibit, the Template Name is Engineer-Contractor , and the selected Role option is Use a unique Role based on this template name . That means FortiNAC-F uses the template name itself as the role value for any account created from this guest/contractor template. The study guide confirms this behavior: by default, the Role field is populated with the template name, although the administrator can alternatively select from an existing role list. It also states that the role value in the guest and contractor template populates the Role field of any account created from that template.

Option B , Eng-Contractor , is wrong because that value is entered in the Security and Access Value field, not the Role field. That value can still be used in user/host profiles or policies, but it does not populate the account Role field. Option C , Contractor , is only the Visitor Type , which controls the kind of guest

/contractor account and associated icon behavior. Option D , Accounting Contractor , is visible in the disabled Select Role dropdown, but that option is not selected because the template is configured to use a unique role based on the template name.

NO.6 An administrator wants to build device profiling rules based on network traffic, but the network session view is not populated with any records.
Which two settings can be enabled to gather network session information? (Choose two.)
A. Network traffic polling on any modeled infrastructure device
B. Firewall session polling on modeled FortiGate devices
C. Netflow setting on the FortiNAC-F interfaces
D. Layer 3 polling on the infrastructure devices
Answer: B C
Explanation:
In FortiNAC-F, theNetwork Sessionsview provides a real-time and historical log of traffic flows, including source/destination IP addresses, ports, and protocols. This data is essential for buildingDevice Profiling Rulesthat rely on " Traffic Patterns " or " Network Footprints " to identify devices (e.g., an IP camera communicating with its specific NVR). If the network session view is empty, the system is not receiving the necessary flow or session data from the network infrastructure.
According to theFortiNAC-F Administration Guide, there are two primary methods to populate this view:
NetFlow/sFlow/IPFIX (C):FortiNAC-F can act as a flow collector. By enablingNetFlowsettings on the FortiNAC-F service interface (port2/eth1) and configuring your switches or routers to export flow data to the FortiNAC IP, the system can parse these packets and record sessions.
Firewall Session Polling (B):For environments with FortiGate firewalls, FortiNAC-F can proactively poll the FortiGate via theREST APIto retrieve its current session table. This is particularly useful as it provides session visibility without requiring the overhead of configuring NetFlow on every access layer switch.
Settings likeLayer 3 Polling(D) only provide ARP table mappings (IP to MAC correlation) and do not provide the detailed flow information required for the session view.
" TheNetwork Sessionsview displays information regarding active and inactive network traffic sessions... To populate this view, FortiNAC must receive data through one of the following methods: *NetFlow/sFlow Support: Configure network devices to send flow data to the FortiNAC service interface. *Firewall Session Polling: Enable session polling on modeled FortiGate devices to retrieve session information via API. These records are then used by the Device Profiler to match rules based on traffic patterns. " -FortiNAC-F Administration Guide: Network Sessions and Flow Data Collection.