

IoT Connected Safety and Security Account Manager

Cisco 700-803

Version Demo

Total Demo Questions: 5

Total Premium Questions: 56

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, IoT Market and Business Outcomes	5
Topic 2, Cisco IoT Connected Safety and Security Solutions	50
Topic 3, Cisco IoT Sales Strategies	1
Total	56

QUESTION NO: 1

What is a benefit of using Power over Ethernet for an IP camera deployment?

- A. power and network connectivity can be delivered through one Ethernet cable
- B. video can be transmitted without an IP network
- C. cameras no longer require access controls
- D. all camera footage is automatically retained indefinitely

ANSWER: A

Explanation:

power and network connectivity can be delivered through one Ethernet cable is correct because Power over Ethernet enables compatible switches to provide electrical power and data connectivity over the same Ethernet cable. This simplifies installation where a separate power outlet would otherwise be required near each camera.

For connected safety and security deployments, PoE can reduce cabling complexity and provide a centrally managed power source for cameras and other supported endpoints. The switch and connected devices must support the appropriate PoE standard and available power budget. Cisco explains PoE capabilities and deployment considerations at [Cisco Power over Ethernet](#).

QUESTION NO: 2

Lack of interoperability is a common roadblock to implementing new IoT technologies. Which option best describes this roadblock?

- A. Implementing new technologies requires new management techniques.
- B. Information transfer leaves users open to physical and legal vulnerabilities.
- C. Purchasing, deploying, and integrating new solutions involves significant costs.
- D. BYOD and IoT solutions must work with existing and future infrastructure.
- E. New technology must follow standard operating procedures.

ANSWER: D

Explanation:

BYOD and IoT solutions must work with existing and future infrastructure. best describes the interoperability roadblock because an IoT deployment is rarely a self-contained, greenfield system. Connected safety and security solutions need to exchange usable data and operate reliably across a customer's installed network, devices, applications, operational technologies, and identity or management platforms. They must also remain compatible as the environment evolves, including when endpoints, protocols, software, and network services are upgraded or added. If the new solution cannot communicate with those systems through supported interfaces, common standards, or appropriate gateways, the organization can face integration delays, limited functionality, fragmented visibility, and added operational complexity. This is especially important in BYOD environments, where device types, operating systems, and ownership models vary, and in IoT environments, where devices may have long lifecycles and constrained capabilities. Designing for interoperability therefore means assessing existing infrastructure and ensuring the architecture can accommodate future technologies rather than creating an isolated deployment. Cisco identifies interoperability and integration across connected devices, networks, and applications as central considerations for IoT solutions; see [Cisco's Internet of Things overview](#). The importance of interoperable IoT architectures and standards is also addressed by [NIST's Internet of Things program](#).

QUESTION NO: 3

Effective public safety requires a positive feedback loop that includes which three options? (Choose three.)

- A. growing economies
- B. better roads
- C. protected citizens
- D. faster subways
- E. stronger communities

ANSWER: A C E

Explanation:

Effective public safety creates a reinforcing cycle among protected citizens, stronger communities, and growing economies. When citizens are protected, they can participate more confidently in everyday life, including working, attending school, using public spaces, and engaging with local institutions. This safety and trust supports stronger communities through greater civic participation, resilience, and cooperation between residents and public-safety organizations. Stronger communities can in turn improve prevention, reporting, preparedness, and coordinated responses to incidents, helping sustain protection for citizens.

That stability also enables growing economies. Businesses are more willing to invest where people, assets, and operations are secure; reliable public services and a perception of safety support commerce, employment, and long-term development. Economic growth can provide communities and public agencies with additional resources to maintain services, adopt safety technology, and improve resilience, completing the positive feedback loop. Cisco describes public-safety technology as helping agencies and communities improve safety, response, and resilience: [Cisco Public Safety](#). The World Bank likewise identifies safety, security, and violence prevention as important foundations for sustainable development and economic opportunity: [World Bank Violence Prevention](#).

QUESTION NO: 4

Which four of these Cisco Connected Safety and Security solutions can address smart city challenges? (Choose four.)

- A. create safer streets and neighborhoods
- B. increase the productivity and efficiency of city services
- C. promote sustainable city growth
- D. maximize reliability and performance by reducing breakdowns
- E. increase city revenue
- F. enable the flow of goods and services

ANSWER: A B C F

Explanation:

Cisco Connected Safety and Security supports smart-city outcomes that make communities safer, more responsive, and more sustainable. “create safer streets and neighborhoods” is a core outcome because connected video, sensors, analytics, and coordinated communications can help city teams gain situational awareness and respond more effectively to incidents. “increase the productivity and efficiency of city services” is also central: networked systems allow public-safety, transportation, utilities, and municipal operations to share actionable information and streamline service delivery. “promote sustainable city growth” reflects the ability to use connected infrastructure and data to manage resources, plan for changing demand, and improve long-term urban resilience. Finally, “enable the flow of goods and services” aligns with smart-city transportation and operational capabilities that help improve mobility, logistics, and access to essential services. These outcomes are consistent with Cisco’s smart-city approach, which connects city infrastructure, people, processes, and data to improve quality of life and operational effectiveness. See Cisco’s [Smart Connected Communities](#) overview and its [Smart Cities](#) resources.

QUESTION NO: 5

Which customer concern is best addressed by integrating physical-security systems with the enterprise network?

- A. limited visibility across disconnected safety and security systems
- B. the need to eliminate all network connectivity
- C. the requirement to prevent information sharing among responders
- D. the preference for separate management tools at every location

ANSWER: A

Explanation:

Limited visibility across disconnected safety and security systems. When video, access control, sensors, and communications are managed as separate systems, operators can have difficulty obtaining a complete view of an event. Integrating these capabilities with a secure enterprise network helps authorized teams share information, correlate events, and manage distributed operations more effectively.

The network serves as the foundation for connecting physical-security devices and applications while applying appropriate controls for access, segmentation, and management. This supports a more unified operational model than separate, standalone security environments. Cisco describes physical security as an integrated approach to protecting people, property, and assets; see [Cisco: What Is Physical Security?](#).