

IoT Manufacturing Account Manager

Cisco 700-802

Version Demo

Total Demo Questions: 5

Total Premium Questions: 56

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

QUESTION NO: 1

What does Cisco Connected Factory Wireless primarily help customers to do?

- A. Budget money.
- B. Save money.
- C. Make money.
- D. Be safer.

ANSWER: B

Explanation:

Save money. Cisco Connected Factory Wireless is designed to reduce the cost and operational burden of connecting people, assets, and industrial processes across manufacturing environments. A reliable industrial wireless network can reduce the expense and disruption associated with running or modifying physical cabling, particularly where production equipment, layouts, or workflows change frequently. It also enables more efficient access to production data and supports mobile workers, connected machines, and wireless applications on a common networking foundation. These capabilities help organizations improve operational efficiency, reduce downtime-related costs, and simplify the deployment and management of connectivity in harsh or complex factory settings. Cisco positions industrial wireless as a way to securely connect industrial assets and operations while supporting digitalization initiatives that improve productivity and operational outcomes. This cost-efficiency focus aligns with the primary customer benefit expressed by “Save money.” See Cisco’s [manufacturing solutions overview](#) and its [industrial wireless solutions](#) for details on using wireless networking to connect industrial operations and improve efficiency.

QUESTION NO: 2

Specific company characteristics signal opportunities to sell the Cisco Internet of Things. Which three characteristics indicate such an opportunity? (Choose three.)

- A. security concerns
- B. a slow-moving company
- C. an IT preference for Cisco
- D. a focus on green energy_____
- E. a move to wireless manufacturing, Ethernet I/O, predictive maintenance, or other new models

ANSWER: A D E

Explanation:

Security concerns are a strong IoT sales indicator because connecting operational technology, industrial assets, sensors, and remote users expands the attack surface. Cisco IoT solutions address this need through network segmentation, identity-based access, visibility, secure remote access, and threat detection across IT and operational environments. A focus on green energy also signals opportunity because IoT connectivity and analytics can measure energy use, monitor distributed assets, reduce waste, and support sustainability and efficiency goals. These outcomes are particularly relevant in manufacturing, utilities, and other asset-intensive environments. A move to wireless manufacturing, Ethernet I/O, predictive maintenance, or other new models is likewise an important signal: these initiatives require reliable industrial connectivity, collection of machine and sensor data, and integration of operational systems with enterprise applications. Cisco positions Industrial IoT around securely connecting industrial assets and extracting data that supports operational efficiency, uptime, and business innovation. Together, these characteristics indicate a customer with identifiable operational requirements that Cisco IoT networking, security, and edge capabilities can help address. See Cisco’s [Internet of Things overview](#) and [manufacturing solutions](#).

QUESTION NO: 3

What does Cisco Connected Factory Security primarily help customers to do?

- A. Make money.
- B. Save money.
- C. Be safer.
- D. Budget money.

ANSWER: C

Explanation:

Be safer. Cisco Connected Factory Security is primarily intended to reduce cyber and operational risk in manufacturing environments. Connected factories bring together industrial control systems, operational technology, enterprise networks, cloud services, remote users, and connected devices. Securing those connections helps manufacturers maintain safe, reliable production while protecting people, processes, equipment, and intellectual property.

Cisco's industrial-security approach provides visibility into industrial assets and communications, network segmentation to limit the reach of threats, secure remote access for authorized personnel, and threat detection and response capabilities. These controls are especially important because a cyber incident affecting operational technology can disrupt physical processes and potentially create safety consequences for workers and facilities. By applying security across the converged IT and OT environment, manufacturers can operate with greater confidence that production systems are protected and resilient.

Cisco describes industrial networking and security as a way to protect critical infrastructure and enable secure IT/OT convergence. Additional details are available in Cisco's [manufacturing solutions](#) and its [industrial security](#) overview.

QUESTION NO: 4

Secure production access is an important success metric for Plant IT Directors. In the Internet of Things, which four options achieve secure production access? (Choose four.)

- A. increased uptime
- B. reduced IP theft
- C. risk reduction
- D. reduced downtime
- E. increased safety
- F. faster new product introduction

ANSWER: B C D E

Explanation:

Secure production access in an industrial IoT environment means that only authorized users, devices, and applications can reach production systems, and that access is controlled, monitored, and protected from misuse. This directly supports **reduced IP theft** because segmentation, identity-based access control, and secure remote access limit exposure of proprietary process information, designs, recipes, and operational data. It also delivers **risk reduction** by reducing the attack surface and helping prevent unauthorized changes to operational technology assets. **Reduced downtime** is achieved when access controls and network protections help prevent cyber incidents, accidental configuration changes, and unauthorized activity from interrupting plant operations. Finally, **increased safety** follows from protecting industrial control systems against inappropriate commands or access that could place people, equipment, or processes at risk. Cisco describes industrial security as a way to protect connected operational environments while maintaining resilient operations, and NIST

emphasizes that industrial control system security must account for safety, reliability, and availability. See [Cisco Manufacturing solutions](#) and [NIST SP 800-82 Rev. 3](#).

QUESTION NO: 5

In addition to devices, hardware, software, and services, what are additional sales opportunities for Cisco partners?

- A. maintenance
- B. buildings
- C. sensors
- D. construction equipment

ANSWER: A

Explanation:

maintenance is correct because connected-manufacturing solutions create a continuing opportunity across the operational life of plant assets. Cisco partners can help manufacturers use securely connected industrial networks, operational data, and visibility tools to support condition monitoring and predictive-maintenance practices. This shifts customer engagement beyond the initial sale of infrastructure and applications into recurring lifecycle work, such as monitoring network and asset health, identifying potential failures before they disrupt production, providing support contracts, and helping integrate maintenance workflows with operational systems.

For manufacturers, unplanned downtime can directly affect throughput, quality, delivery schedules, and operating cost. A maintenance-focused offer therefore has measurable business value and enables partners to build longer-term customer relationships around ongoing optimization and support. Cisco describes manufacturing as an industry in which secure connectivity and data-driven operations help improve resilience and efficiency, while its IoT portfolio emphasizes connecting, securing, and managing distributed operational assets. These capabilities provide the technical foundation for maintenance-related solutions and associated recurring partner services. See Cisco's [Manufacturing solutions](#) and [Internet of Things overview](#).