Engineering Cisco Meraki Solutions 2

Duration: 3 Days **Course Code: ECMS2**

Overview:

Elevate your Cisco Meraki technical knowledge and skills with this three-day, instructor-led training! In this advanced technical training course, you'll gain the knowledge and skills to plan, design, implement, and operate complex Cisco Meraki solutions. This is the second of two courses that will prepare you to take the upcoming Cisco Meraki Solutions Specialist certification exam.

This course:Provides hands-on experience with Cisco Meraki equipment via innovative technical presentations and lab exercisesDelivers expert instruction by senior members of the Meraki technical teamEquips you with the knowledge and skills to confidently plan, design, implement, and operate complex Cisco Meraki solutionsPrepares you to take the upcoming Cisco Meraki Solutions Specialist certification exam

Target Audience:

This course is ideal for those who regularly deploy or manage Meraki networks and want to deepen their technical expertise and understanding of the full Meraki product suite and features.
Before taking the ECMS2 course, you should:Have taken ECMS1 or CMNO, or possess equivalent Meraki knowledge and experienceBe CCNA-certified or have an equivalent level of technical expertiseBe employed by Cisco Systems, a Meraki partner, or a Meraki customer

Objectives:

- After attending an ECMS2 session, you should be able to:
- Plan for network deployments and integrations using the Meraki platform
- Design Meraki architectures for redundancy, high-density, and scalability
- Implement comprehensive Meraki product features to meet design objectives
- Operate Meraki networks and troubleshoot complex network incidents using the Meraki Dashboard and analytics

Prerequisites:

Before taking the ECMS2 course, learners should have the following skills and knowledge:

General networking:

- Be actively engaged in the design, deployment, scaling, and management of enterprise networks
- Be experienced with hierarchical network segmentation (access, distribution, and core layer) design and best practices
- Strong fundamental knowledge of IP addressing and subnetting schemas necessary to build local area networks
- A foundational understanding of network authentication, authorization, and accounting services
- Strong fundamental knowledge of dynamic routing protocols (focus/emphasis on OSPF and BGP)
- A foundational understanding of wired and wireless quality of service (QoS) mechanisms, packet queue operations, and practical implementations
- Be experienced with the design and configuration of IPsec and associated VPN technologies
- A foundational understanding of threat modeling concepts/methodologies and apply them to identify, analyze and

respond to cybersecurity threats
- A foundational understanding of network security controls/protocols, network management best practices, and data security
- Intermediate fundamental knowledge of RF concepts and terminology as they apply to wireless networking and current 802.11 wireless standards
- A foundational understanding of best practice RF design principles and practical implementations
- A foundational understanding of wireless security best practices centered around access control (802.1x) and spectrum security through wireless intrusion detection and prevention (WIDS/WIPS)
- A foundational understanding of standard logging/monitoring protocols (focus/emphasis on SNMP, syslog, and webhooks) and related implementation components or tools
- Be familiar with and have basic knowledge of application programming interfaces (API's) and related languages/formats (REST, JSON)

Meraki knowledge:

- Be able to describe the security, reliability, and scalability of the Dashboard cloud architecture and its out-of-band control plane
- Fundamental understanding of Dashboard's organizational structure, delineation of privileges, and overarching administrative processes
- Be able to outline the key components of Meraki licensing (co-termination model and expiration grace period)
- Have the knowledge and ability to deploy advanced security features on MX security appliances (intrusion detection/prevention, Advanced Malware Protection (AMP), layer 3 & 7 firewall rules)
- Fundamental understanding of Auto VPN and its purpose when utilized in an SD-WAN deployment
- Be experienced at navigating, configuring, and applying configurations to MS switches through the virtual stack interface in Dashboard
- Be able to describe the concepts behind a cloud-based WLAN solution and the features that can be delivered including layer 7 traffic shaping and various guest access authentication methods
- Fundamental understanding of device profile containerization and remote management capabilities as managed through the Systems Manager platform
- Fundamental understanding of the edge architecture as implemented by MV security cameras and its implications on video retention through various configurable options
- Be able to effectively leverage the live tools and monitoring capabilities of the Meraki Dashboard when troubleshooting device or application performance issues

Content:

The ECMS2 curriculum is comprised of 15 lessons and supplemental lab exercises. Attendees will be familiar with the topics listed below after attending an ECMS2 session.

- Identify optimal Meraki networks architectures (organization/network sizing and limitations)
- Plan for and complete license renewals through the Dashboard
- Design Meraki organization administrative structure using tags (network and device tags)
- Design highly available and redundant networks through the use of MX warm-spare and MS physical stacking technology
- Design high density wireless networks (access point calculations and SSID configurations)
- Utilize SAML for scalable role-based access control
- Explain the capabilities and limitations of Templates and Network Cloning
- Explain and identify ideal use cases for the Dashboard API
- Design proper static and dynamic routing topologies based on network needs
- Explain dynamic routing capabilities on the MX appliance platform
- Explain dynamic routing capabilities on the MS switch platform
- Configure OSPF across the network as the dynamic routing protocol
- Leverage BGP to expand networks and improve WAN performance
- Identify the configurable quality of service (QoS) mechanisms across the LAN and WLAN
- Prepare for VoIP and video traffic using class of service (CoS), DSCP tags, and wireless traffic shaping
- Configure policy and performance-based routing on the MX appliance platform
- Design highly scalable VPN architectures (full mesh, hub-and-spoke)
- Explain the underlying mechanisms of Meraki Auto VPN (VPN registry, UDP hold punching)
- Explain the fundamentals of Meraki SD-WAN and its processing algorithm
- Design Meraki SD-WAN architecture with performance-based routing
- Extend networks and services into the public cloud (Azure and AWS)
- Explain the default traffic flow and layer 3/layer 7 rules processing order of the MX appliance platform
- Identify the security intelligence engines and definition databases the MX appliance platform leverages for network protection services (Cisco AMP, Threat Grid, Snort)
- Identify and enable content filtering at various levels for desired traffic refinement
- Prepare access policies (802.1x) using Meraki authentication
- Properly utilize templates, cloning, and switch profiles
- Design guest access for LAN/WLAN utilizing Meraki best practices
- Configure Dashboard maps and floor plans
- Formulate RF profiles to prepare for challenging/variable RF deployments
- Configure WLAN access control options based on design requirements
- Enable the network for Bluetooth scanning and BLE beaconing
- Utilize Air Marshal for intrusion detection and mitigation
- Explain the different device enrollment and profile deployment methods
- Design a native containerization strategy to separate work from personal data on endpoints
- Identify and implement various application deployment methods
- Explain the MV platform's edge architecture and underlying video delivery mechanism (local vs. remote video access)
- Design a retention policy using various local or cloud-based storage strategies
- Configure MV cameras for wireless deployments
- Explain and demonstrate how to effectively utilize advanced analytics and MV camera APIs
- Explain how Meraki Insight is able to provide network assurance through the use of performance metrics and scores
- Qualify and properly size Meraki Insight licenses
- Configure, monitor, and track predefined and custom web application thresholds
- Explain Dashboard's integrated historical log databases (event vs. change logs) to be leveraged for effective activity analysis
- Identify the various monitoring tools within Dashboard (native analytics, Topology)
- Demonstrate effective network-wide alerting best practices
- Utilize the Dashboard API to monitor and maintain Meraki networks
- Generate and interpret on-demand or recurring Summary Reports for key performance metrics
- Track and manage firmware releases and prepare for staged upgrades
- Recommend proper actions to meet PCI DSS (2.0 and 3.0) compliance
- Interpret event and change logs to troubleshoot client and network issues
- Classify and compare security threats via the Security Center
- Assess wireless intrusions, failures, and network access issues through Dashboard's RF tools (Wireless Health, Air Marshal)
- Assess root cause of application performance issues with Meraki Insight
- Explain the detailed VPN tunnel information and the VPN Registry found on the VPN Status page
- Utilize the Local Status Page as an alternate connectivity method to perform local troubleshooting

- Assemble and implement security policies which cater to various restriction requirements
- Construct a network deployment that leverages SM Sentry

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo