ECMS2: Engineering Cisco Meraki Solutions Part 2

Course Code: ECMS2
Duration: 3 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

The course, Engineering Cisco Meraki Solutions Part 2 (ECMS2) v2.0 elevates your knowledge of Cisco Meraki technology suite. In this advanced technical training course, you'll learn how to plan for network deployments and integrations using the Cisco Meraki platform. Through practical hands-on instruction and experiences, you will learn how to operate Meraki networks and troubleshoot complex network incidents using the Meraki Dashboard and analytics. You will also learn how to design Meraki architectures for redundancy, high-density, and scalability by implementing comprehensive Meraki product features to meet design objectives.

This course is the second of two courses that prepares you for Cisco Meraki certification.

SKILLS COVERED

After taking this course, you should be able to:

- Plan new Cisco Meraki architectures and expand existing deployments
- Design the network for scalable management and high availability
- Describe how to automate and scale Meraki deployments with dashboard tools
- Use dynamic routing protocols to expand networks and improve WAN performance
- Describe proper QoS, policy and performance-based routing configurations across a Cisco Meraki network and WAN optimization through traffic shaping
- Describe Virtual Private Network (VPN) and Wide Area Network (WAN) topologies and how to integrate them
- Secure, expand, and shape the network
- Implement switched network concepts and practices, and configure guests networks
- Implement wireless configurations concepts and practices
- Describe endpoint management concepts and practices using Cisco Meraki Systems Manager
- Describe physical security concepts and practices
- Gain network insight by monitoring applications
- Describe how to prepare monitoring, logging, and alerting services
- Set up reporting and auditing capabilities in the Cisco Meraki dashboard
- Monitor and troubleshoot issues using Cisco Meraki tools

WHO SHOULD ATTEND?

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. This may include professionals with job titles or in roles such as:

- Consulting Systems Engineer
- Deployment Engineer
- Network Administrator
- Network Manager
- Network Engineer
- Site Reliability Engineer
- Systems Engineer
- Technical Solutions Architect
- Wireless Design Engineer

- Wireless Engineer

PRE-REQUISITES

Before enrolling in the ECMS2 course, it is highly recommended that you have already attended and completed the ECMS1 course before attending this training. You should also have general networking understanding, Meraki-specific proficiency, and knowledge in the following areas:

General network:

- Be actively engaged in the design, deployment, scaling, and management of enterprise networks
- Strong fundamental knowledge of IP addressing and subnetting schemas necessary to build local area networks
- Strong fundamental knowledge of dynamic routing protocols (focus/emphasis on Open Shortest Path First [OSPF] and Border Gateway Protocol [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 Virtual Private Network (VPN) technologies
- A foundational understanding of network security controls/protocols, network management best practices, and data security
- A foundational understanding of best practice Radio Frequency (RF) design principles and practical implementations
- A foundational knowledge of wireless security best practices centered around access control (802.1x) and spectrum security through Wireless Intrusion Detection Systems (WIDS) and Wireless Intrusion Prevention Systems (WIPS)
- A foundational command of standard logging/monitoring protocols (focus/emphasis on Simple Network Management Protocol [SNMP], syslog, and webhooks) and related implementation components or tools
- Be familiar with and have basic knowledge of Application Programming Interfaces (APIs) and related languages/formats (REST, JavaScript Object Notation [JSON])

Meraki knowledge:

- Be able to describe the security, reliability, and scalability of the Cisco Meraki 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 a Software-Defined Wide Area Network (SD-WAN) deployment
- 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 Meraki MV security cameras and its implications on video retention through various configurable options

The following are the recommended Cisco offerings that may help you meet these prerequisites:

- Implementing and Administering Cisco Solutions (CCNA)
- Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)
- Engineering Cisco Meraki Solutions Part 1 (ECMS1)

MODULES

Content

- Planning new Cisco Meraki architectures and expanding existing deployments
- Designing for scalable management and high availability
- Automating and scaling Meraki deployments
- Designing routing and practices on the Meraki platform
- Describing Quality of Service (QoS) and traffic shaping design
- Building VPN and WAN topologies
- Securing, expanding, and shaping the network
- Describing network concepts and practices
- Implementing wireless configuration practices and concepts
- Describing Endpoint management concepts and practices
- Describing physical security concepts and practices
- Gaining network insight through monitoring applications
- Preparing monitoring, logging, and alerting services
- Setting up reporting and auditing capabilities in the Cisco Meraki Dashboard
- Gaining visibility and resolving issues using Meraki features and built-in troubleshooting tools

Lab Outline

- Configure Tags, Link Aggregation, Port Mirroring, and High-Density SSIDs
- Establishing Auto VPN
- Configuring Virtual Interfaces and Routing on Cisco Meraki MS Switches
- Configuring Routes and Redistribution
- Configuring Quality of Service
- Configuring Traffic Shaping
- Configuring Load Balancing
- Defining Firewall Rules
- Enabling Advanced Malware Protection, Intrusion Detection, and Intrusion Prevention
- Enabling Content Filtering
- Configure and Apply Access Policies
- Configure Wireless Guest Access
- Configure Service Set Identifiers (SSIDs)
- Implementing RF Profiles
- Implement Air Marshal
- Create Cisco Meraki Systems Manager (SM) Configuration Profiles
- Define Security Policies
- Enforce End-to-End Security
- Set-up Motion Alerts
- Deploy Wireless Cameras
- Manage Video Retention
- Enable Alerts
- Add Monitoring and Reporting
- Generate and Analyze Summary Reports

- Manage Firmware
- Generate a Peripheral Component Interconnect (PCI) Compliance Report
- Troubleshoot an Offline Device
- Troubleshoot Content Filtering
- Troubleshooting Remote Site Connectivity

END OF PAGE