ProTech Professional Technical Services, Inc.

ProTech protechtraining.com

Engineering Cisco Meraki Solutions Part 2 (ECMS2)

Course Summary

Description

The course, Engineering Cisco Meraki Solutions Part 2 (ECMS2) v1.0 elevates your knowledge of Cisco Meraki technology. 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 the Cisco Meraki certification.

This course will help you:

- Acquire the advanced skills and techniques to plan, design, implement, and operate the complex Cisco Meraki platform for cloud-based network management.
- Prepare you to take the upcoming Meraki certification(s)

Objectives

At the end of this course, students will 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

Topics

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

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

- Field deployment technicians
- Network administrators
- Pre-/Post-sales engineers
- Service provider engineers
- Systems engineers
- IT professionals

Course Summary (cont'd)

Prerequisites

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 Radiofrequency (RF) design principles and practical implementations
- 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:

- 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

Duration

Three days

Engineering Cisco Meraki Solutions Part 2 (ECMS2)

Course Outline

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

Lab outline

- Creating and Applying Tags
- Configuring Link Aggregation
- Setting Up Port Mirroring
- Establishing Auto VPN
- Configuring Virtual Interfaces and Routing
- Configuring Routes and Redistribution
- Configuring Quality of Service
- Configuring Traffic Shaping
- Configuring Load Balancing
- Defining Firewall Rules
- Enabling Advanced Malware Protection
- Enabling Intrusion Detection and Protection
- Enabling Content Filtering
- Configuring and Applying Access Policies
- Configuring Wireless Guest Access
- Configuring Service Set Identifiers (SSIDs)
- Implementing RF Profiles
- Implementing Air Marshal
- Creating System Manager (SM) Configuration Profiles
- Defining Security Policies
- Enforcing End-to-End Security
- Setting Up Motion Alerts
- Managing Video Retention
- Deploying Wireless Cameras
- Enabling Alerts
- Adding Monitoring and Reporting
- Generating Summary Reports
- Managing Firmware
- Peripheral Component Interconnect (PCI) Reporting
- Troubleshooting an Offline Device
- Troubleshooting Content Filtering
- Troubleshooting Remote Site Connectivity