

Engineering Cisco Meraki Solutions – Part 2

Description

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 Meraki certification.

Classroom Registration Price (CHF)

2200

Virtual Classroom Registration Price (CHF)

2200

Course Content

Module 1: Planning new Meraki architectures and expanding existing deployments

- Lesson 1: Identify optimal Meraki networks architectures (organization/network sizing and limitations)
- Lesson 2: Plan for and complete license renewals through the Dashboard

Module 2: Designing for scalable management and high availability

- Lesson 1: Design Meraki organization administrative structure using tags (network and device tags)
- Lesson 2: Design highly available and redundant networks through the use of MX warm-spare and MS physical stacking technology
- Lesson 3: Design high density wireless networks (access point calculations and SSID configurations)

Module 3: Automation and scaling Meraki deployments

- Lesson 1: Utilize SAML for scalable role-based access control
- Lesson 2: Explain the capabilities and limitations of Templates and Network Cloning
- Lesson 3: Explain and identify ideal use cases for the Dashboard API

Module 4: Routing design and practices on the Meraki platform

- Lesson 1: Design proper static and dynamic routing topologies based on network needs
- Lesson 2: Explain dynamic routing capabilities on the MX appliance platform
- Lesson 3: Explain dynamic routing capabilities on the MS switch platform
- Lesson 4: Configure OSPF across the network as the dynamic routing protocol
- Lesson 5: Leverage BGP to expand networks and improve WAN performance

Module 5: QoS and traffic shaping design

- Lesson 1: Identify the configurable quality of service (QoS) mechanisms across the LAN and WLAN
- Lesson 2: Prepare for VoIP and video traffic using class of service (CoS), DSCP tags, and wireless traffic shaping
- Lesson 3: Configure policy and performance-based routing on the MX appliance platform

Module 6: Architecting VPN and WAN topologies

- Lesson 1: Design highly scalable VPN architectures (full mesh, hub-and-spoke)
- Lesson 2: Explain the underlying mechanisms of Meraki Auto VPN (VPN registry, UDP hold punching)

- Lesson 3: Explain the fundamentals of Meraki SD-WAN and its processing algorithm
- Lesson 4: Design Meraki SD-WAN architecture with performance-based routing
- Lesson 5: Extend networks and services into the public cloud (Azure and AWS)

Module 7: Securing the network with Advanced Security features

- Lesson 1: Explain the default traffic flow and layer 3/layer 7 rules processing order of the MX appliance platform
- Lesson 2: Identify the security intelligence engines and definition databases the MX appliance platform leverages for network protection services (Cisco AMP, Threat Grid, Snort)
- Lesson 3: Identify and enable content filtering at various levels for desired traffic refinement

Module 8: Switched network concepts and practices

- Lesson 1: Prepare access policies (802.1x) using Meraki authentication
- Lesson 2: Properly utilize templates, cloning, and switch profiles
- Lesson 3: Design guest access for LAN/WLAN utilizing Meraki best practices

Module 9: Wireless concepts and practices

- Lesson 1: Configure Dashboard maps and floor plans
- Lesson 2: Formulate RF profiles to prepare for challenging/variable RF deployments
- Lesson 3: Configure WLAN access control options based on design requirements
- Lesson 4: Enable the network for Bluetooth scanning and BLE beaconing
- Lesson 5: Utilize Air Marshal for intrusion detection and mitigation

Module 10: Endpoint management concepts and practices

- Lesson 1: Explain the different device enrollment and profile deployment methods
- Lesson 2: Design a native containerization strategy to separate work from personal data on endpoints
- Lesson 3: Identify and implement various application deployment methods
- Lesson 4: Assemble and implement security policies which cater to various restriction requirements
- Lesson 5: Construct a network deployment that leverages SM Sentry

Module 11: Physical security concepts and practices

- Lesson 1: Explain the MV platform's edge architecture and underlying video delivery mechanism (local vs. remote video access)
- Lesson 2: Design a retention policy using various local or cloud-based storage strategies
- Lesson 3: Configure MV cameras for wireless deployments
- Lesson 4: Explain and demonstrate how to effectively utilize advanced analytics and MV camera APIs

Module 12: Gaining additional network insight through application monitoring

- Lesson 1: Explain how Meraki Insight is able to provide network assurance through the use of performance metrics and scores
- Lesson 2: Qualify and properly size Meraki Insight licenses
- Lesson 3: Configure, monitor, and track predefined and custom web application thresholds

Module 13: Preparing and setting up monitoring, logging, and alerting services

- Lesson 1: Explain Dashboard's integrated historical log databases (event vs. change logs) to be leveraged for effective activity analysis

- Lesson 2: Identify the various monitoring tools within Dashboard (native analytics, Topology)
- Lesson 3: Demonstrate effective network-wide alerting best practices
- Lesson 4 Utilize the Dashboard API to monitor and maintain Meraki networks

Module 14: Setting up Dashboard reporting and auditing capabilities

- Lesson 1: Generate and interpret on-demand or recurring Summary Reports for key performance metrics
- Lesson 2: Track and manage firmware releases and prepare for staged upgrades
- Lesson 3: Recommend proper actions to meet PCI DSS (2.0 and 3.0) compliance

Module 15: Gaining visibility and resolving issues using Meraki features and built-in troubleshooting tools

- Lesson 1: Interpret event and change logs to troubleshoot client and network issues
- Lesson 2: Classify and compare security threats via the Security Center
- Lesson 3: Assess wireless intrusions, failures, and network access issues through Dashboard's RF tools (Wireless Health, Air Marshal)
- Lesson 4: Assess root cause of application performance issues with Meraki Insight
- Lesson 5: Explain the detailed VPN tunnel information and the VPN Registry found on the VPN Status page
- Lesson 6: Utilize the Local Status Page as an alternate connectivity method to perform local troubleshooting

Lab / Exercises

- Official Cisco lab and exercises

Documentation

- Digital courseware included

Participant profiles

- Anyone who regularly deploys or manages Meraki networks and want to deepen their technical expertise and understanding of the full Meraki product suite and features

Prerequisites

- Have taken ECMS1 or CMNO, or possess equivalent Meraki knowledge and experience
- Be CCNA-certified or have an equivalent level of technical expertise
- Be employed by Cisco Systems, a Meraki partner, or a Meraki customer

Objectives

- 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

Niveau

Intermédiaire

Duration (in Days)

3

Reference

CIS-ECMS2