

CS-MERAKI



MERAKI FUNDAMENTALS

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
4 Days	Intermediate	Cisco	ILT / VLT	N/A

INTRODUCTION

This new four-day Cisco Meraki Fundamentals course, delegates will gain hands-on experience with Meraki's intuitive dashboard, demystify the essentials of cloud networking, and discover scalable techniques for deploying, operating, and troubleshooting Meraki devices across wireless, switching, security, and SD-WAN environments.

AUDIENCE PROFILE

This course is designed for IT teams, system integrators, and anyone seeking to upskill in cost-effective, cloud-first operations

PREREQUISITES

Delegates attending this course must have:

- A Cisco Certified Networking Associate (CCNA) certification is highly recommended, or equivalent experience in basic networking fundamentals.
- Understanding of simple LANs, IP addressing, and subnetting.
- Familiarity with routing and switching principles.
- Basic wireless networking concepts and common terminology. Basic computer skills, such as how to use a keyboard and how to work with a removable media such as Flash Drives.

The knowledge and skills that a learner must have before attending this course are as follows:

- Ability to build and configure simple networks.
- Experience with fundamental troubleshooting strategies.
- General familiarity with network security protocols (such as IPsec VPN).
- Understanding of wired and wireless QoS mechanisms, network security controls, and firewall fundamentals.
- Knowledge of dynamic routing protocols (e.g., OSPF, BGP) is beneficial for advanced topics

COURSE OBJECTIVES

On completion of this course, participants should be familiar with:

Understand Cloud-Managed Networking Concepts:

- Grasp the fundamentals of Cisco Meraki's cloud-based architecture and the value proposition of cloud-managed networks for modern organizations.
- Explain the operational differences between cloud-managed and traditional networks

Master the Meraki Dashboard:

- Navigate and configure core features in the Meraki Dashboard for multi-site, multi-product deployments.
- Manage organizational structure, inventory, administrators, and licensing within the dashboard environment

Deploy and Configure the Full Meraki Stack:

- Install, configure, and optimize:
- Meraki MX Security Appliances (including SD-WAN, firewall, VPN, threat management)
- Meraki MS Switches (including VLANs, stacking, routing)
- Meraki MR Access Points (wireless networking, guest access, RF design, security)
- Meraki MV Cameras (surveillance configuration, analytics, retention)

- Meraki Sensors and Insight for environment monitoring and analytics

Implement and Troubleshoot Real-World Solutions:

- Diagnose and resolve common connectivity and user issues using the dashboard and built-in troubleshooting tools.
- Apply best practices for site maintenance, monitoring, and firmware management

Integrate with Enterprise and Security Solutions:

- Integrate Meraki with Cisco Umbrella, Identity Services Engine (ISE), and RADIUS for policy enforcement and security.
- Configure and manage group policies, templates, and bulk device onboarding for scalable deployments

Leverage Insights, Reporting, and Automation:

- Use Meraki Insight to monitor network health, traffic analytics, and performance baselines.
- Configure automated alerting, reporting, and auditing to support compliance and operational efficiency.

Automate and Scale Operations Using APIs:

- Understand the basics of Meraki API usage for automating deployments, monitoring, and troubleshooting at scale

Prepare for Advanced Meraki Deployments and Certifications:

COURSE CONTENT

Module 1: Fundamentals of Meraki cloud architecture

- Architecture of Dashboards
- Back-end and Cloud Architecture
- Communication from Device to Cloud
- Security and Retention of Data
- Lifecycle and Management of Firmware

Module 2: The Dashboard's construction

- Organization Creating
- Network Creating
- Adding Devices and Claiming
- Administrator and Privilege Definition
- Roles with Special Access
- SAML Roles
- Keeping the Dashboard Under Control
- Adding Tags to the Scope
- Tags Introduction
- Administrative Privilege Tagging
- Configuring Devices and Networks
- SSID Availability Configuration for MR Access Points
- Setting Up MX and Z Series Devices for Non-Meraki VPN Peer Availability
- Systems Manager for Meraki
- Alerting and Reporting on Dashboards
- Email Alerts for the Dashboard
- Webhooks
- Syslog
- SNMP Traps and SNMP Reports with Automated Summaries
- Alerts for Meraki Insight
- Hubs for Alerts
- Global Overview

Module 3: The Admin Experience with Meraki

- Org-wide Health
- Status of the Firmware
- Firmware Security and Status in Detail
- Anticipatory Replacements
- Early Access Program for Dashboards
- System of Magnetic Design
- New Landing Page
- Improvements to the Alert Hub and New Organisation Alert Page
- Switching Overview
- Global Overview
- Network-wide Perspectives on Health
- Uplink and Network-wide Health
- Health of Wireless Networks
- Views of Automated Topology
- Layer 2 Topology throughout the Network
- Layer 3 Topology throughout the Network
- Multicast Topology throughout the Network

Module 4: The Dashboard's Automation

- Templates for Configuration
- Templates: How Do They Work?
- Local Overrides
- Limitations and Caveats of the Template
- Best Practice Considerations for Templates
- Triggering Outside Automation using Webhooks, Syslog, and SNMP
- Webhooks
- Syslog
- SMP
- Dashboard pi
- How Is the API Dashboard Used and What Is It?
- Tips & Tricks for APIs

- Examples of API Dashboard
- Automated Organisation Status via API
- MR Naming Automation Using Upstream Switch
- MT Automation
- Automation Based on Dashboards

Module 5: Best Practices for MX and MG

- Scaling MX
- Modes of Deployment
- Modes of Routing
- VPN Concentrator Mode or Passthrough
- Security
- Firewall L3/L7
- Content Filtering via HTTP (TALOS)
- Cisco AMP
- IDS/IPS
- Cisco Umbrella
- Group Policy for the Dashboard
- Policy Adaptation (SGT)
- VPN
- Auto VPN Meraki
- VPN for clients
- AnyConnect from Cisco
- VPN for non-Meraki
- Routing
- Priority of Routes
- Routes That Are Static
- OSPF
- BGP
- Meraki Auto VPN deployment
- Auto VPN Configuration
- Hub vs Spoke
- Traversal of NAT
- Recommendations for Hub and Spoke
- Proper Sizing
- Prioritizing Hubs
- Comparing Full and Split Tunnel Modes
- Enhanced Configuration
- Tracking Deployment
- Insights of Meraki

- Health of Web Applications
- WAN Health
- VoIP Health
- Alerts for Insight
- Integration of ThousandEyes
- VPN Supervision
- Dashboard Alerts Reviews
- Hubs for Alerts
- Alerts for Organisations
- Meraki Dashboard Threat Evaluation
- Centre for Security
- Most Common Dangers
- Clients Most Affected
- MG cellular introduction
- 4G LTE vs 5G
- 5G NSA vs 5G SA
- MG dashboard monitoring
- Considerations for MG Deployment
- Backup or Primary Cellular
- 5G Sight Line
- You and CGNAT
- Deployment Prestaging
- Meraki Device Troubleshooting
- Page for Local Status
- Mode of Safety
- Logging for Support Data Bundles (SDB)
- Combined DM Logging

Module 6: Best Practices for MX SD-WAN

- Meraki SD-WAN introduction
- The Science of Performance in Transportation
- The Structure of SD-WAN Policies
- SD-WAN Uplink Regulations
- Personalised SD-WAN Performance Courses
- Analysis and Identification of Traffic
- Policies for Dynamic Path Selection
- Policy for Global Preferences
- Basic Policy for Load Balancing
- Simple Policy-Based Routing
- DPS Based on Performance
- Using Performance-Based DPS for Policy Routing
- SD-WAN via Cellular
- SD-Internet
- MPLS Integration
- LAN MPLS: Switchover to Meraki Auto VPN
- WAN MPLS: Meraki Auto VPN Overlay

Module 7: Design and Suggestions for Meraki Switching

- Meraki Switches Introduction
- Design of Meraki Switching
- Creating a Wired Business Network

- Organising Your Deployment
- Choosing the Appropriate Switch Product Mix
- Using Cloud Management to Plan Hybrid Campus LAN Architectures
- Access layer design
- Implementation of VLAN
- Employing Native VLAN 1
- QoS Planning
- Optimising STP in a Hybrid Setting
- Tags for Deployment Optimisation
- MTU Suggestion
- Trunk Ports Connecting
- MR Access Points linking
- Best Practices for Layer 3
- Best Practices for OSPF
- Best Practices for Multicast
- Protecting Layer 2 Functions
- Security of Infrastructure
- DHCP Surveillance
- Storm Management
- Inspection of Dynamic ARP
- Secure Port
- Profile Port
- VLAN Profile
- Security of Networks
- Sticky MAC
- Isolation of Ports
- Authentication of 802.1X
- Bypassing MAC Authentication
- Authorisation Modification using ISE Integration
- Security of End Points
- MS Micro-Segmentation (Adaptive Policy)
- Classification and Spread of Identity
- Definition of Security Policy
- Enforcing Policies
- SGT Assignment Techniques
- Warnings When Establishing an Adaptive Policy
- Managing and Improving Meraki Switches
- Stacking virtually
- Considering Firmware Upgrades on MS
- Validations of Configuration
- Config-Safe System
- Auto-Rollback in the Event of a Bad Uplink
- Budget for MS PoE
- Overview of Microsoft Power
- Utilising MS for Sustainability
- Cloud-Based Catalyst
- How to Fix Your Meraki Deployment
- Reporting on Dashboards
- Live Dashboard Tools
- Ping
- Capturing Packets

- MTR
- Table of MAC Forwarding
- Testing of Cables
- Port for Cycles
- Wake-on-LAN

Module 8: Design and Best Practices for Meraki Wireless

- Dashboard scaling and scoping
- Design of the Physical WLAN
- Wireless Network with Location Awareness
- Dual 5-GHz Mode with Wi-Fi 6E
- RF Propagation at 6-GHz
- AP Mounting Suggestions
- AP Overlap and Adjacency
- Setting Up Meraki Wireless
- Best Practices and Suggestions for RF Profiles
- Band Selection: SSID-Specific vs. All SSIDs
- Balancing Clients
- Bitrate Minimum
- Best Practices for Channel Planning
- Bands of Frequency
- Width of Channel
- Choosing a Channel: DFS Channels
- Meraki Auto RF
- Additional Meraki Wireless Design Considerations
- Distributed Networks: Why Use Them?
- Encryption and Authentication
- VLAN Factors
- Use Cases for AP Tags
- Configuring Meraki Wireless at Enterprise Level
- What Roaming Means
- Determining Domains
- Wandering Domains
- Domains at Layer 2
- Domains at Layer 3
- DHCP Scope Definition
- Security Features and Best Practices for Wireless Security
- Air Marshal
- Access Control and Traffic Segregation
- Managing the Network
- Overview of Site-Level Wi-Fi
- Overview of Wireless Health
- Identification of Anomalies (Smart Thresholds)
- RCA for servers
- Device Tracking and Reporting
- Analytics for Roaming
- Overview of the Client
- Client Information
- Timeline for the Client

- Timeline of Access Points

Module 9: MT (IoT) Design and MV Security

- The Meraki Difference: Rethinking Surveillance
- The Architecture of Meraki Cameras
- Architecture of MV Videos
- Maintaining Security
- Integrated Analytics
- Creating an Efficient Surveillance System through Purposeful Design
- Choosing Accessories and Mounting Options for Cameras
- Technology-Related Issues
- Types of Lenses
- Field of View
- Resolution
- Additional Deployment Requirements
- Cisco Meraki MV52: An Illustration of MV Camera Products
- Selecting Appropriate Storage
- Making Power Requirement Plans
- Organising Wired and Wireless Camera Connectivity
- Overarching Network Considerations
- Taking Wired Connections into Account
- Wireless Connection Considerations
- Constructing an Enhanced Camera System
- Specifying Camera Tags and Names
- Camera Administrators: A Definition
- Administrators with Dashboard-Defined Camera-only
- Camera Permissions Based on Roles for SAML/SSO
- Video Access: Meraki MV Camera Views
- Dashboard for Meraki
- The Meraki Vision Portal
- The Meraki Display App
- The Meraki Mobile App
- Setting Up and Improving MV Cameras
- Details of the Listing Camera
- Setting Up Camera Profiles
- Camera Profile Assignment

- Camera Configurations by Hand
- Capturing in Dim Light
- Motion Alerts for Cameras
- Optimising Camera Alerts
- Setting Up Windows Privacy
- Configuring Integration with RTSP
- Setting Up Video Walls
- Using Meraki MV Cameras
- Getting Around the Video Timeline
- Integrated Analytics
- Audio Recognition
- Motion Recap and Motion Search
- Distributing Videos
- Video Exporting
- Utilising Cloud Archive
- Getting to Video Event Logs
- Meraki MV Sense
- Meraki MV Cameras Troubleshooting
- Meraki Cloud Enabling Firewall Ports
- Giving Meraki Support Camera Access
- Using Meraki IoT with MV to Strengthen Security
- Using Meraki MT Sensors to Create Smarter Spaces
- Using Meraki MT Sensors to Create Smart Spaces
- Maintaining Sustainability
- Comprehending the MT Security Architecture
- MT Sensors for Business Asset Protection
- Environmental
- Physical
- Investigating MT Sensors
- Monitoring of Physical Infrastructure
- MT12 Leak/Water Sensor
- The MT20Door Sensor
- The MT40 Smart Power Controller
- Monitoring of the Environment
- Sensor for MT11Cold Storage
- Sensors for temperature, humidity, and air quality
- The MT30 Smart Automation Button
- Automation of Smart Buttons
- Meraki MT Sensor Deployment
- Basic Setup and Configuration
- Comprehending Meraki IoT Gateways
- Taking Sensor Distance into Account

- Power Factors
- Configuration-Related Issues
- Setting Up and Tracking Alerts
- Configuring Alert Types
- Examining Alerts That Were Generated
- Sight Sensor
- Best Practices for IoT Operations
- Meraki MT Sensor Troubleshooting
- Tracking the Status of the Sensor
- Examining Event Logs from Sensors
- Tracking the Strength of the BLE Signal

Lab exercise

- Set up and manage the Cisco Meraki Dashboard
- Activate advanced capabilities and enhance network performance
- Diagnose and resolve network issues through the Meraki Dashboard
- Set up tags, link aggregation, port mirroring, and manage high-density wireless networks
- Establish routing configurations within the Cisco Meraki environment
- Implement QoS policies, traffic management, and load-balancing techniques
- Set up and maintain network security measures
- Define access controls and manage wireless guest connectivity
- Configure wireless SSIDs, radio frequency profiles, and intrusion prevention using Air Marshal
- Apply endpoint administration and control
- Install and configure physical security and surveillance devices
- Turn on alerts and manage system monitoring and performance reports
- Identify and troubleshoot issues within a Cisco Meraki network

ASSOCIATED CERTIFICATIONS & EXAM

There is no exam associated with this course. Delegates will receive a Certificate of Attendance from Mecer Inter-Ed.