Current Technologies
Computer Learning Centers

6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

Meraki MX SDWAN/Security Installing, Configuring, Monitoring, and Troubleshooting v1.0 (MXSDWAN-ICMT)

This 3-day Cisco course provide students with the skills to configure, optimize, and troubleshoot a Cisco Meraki solution. Students will learn how to install and optimize Meraki MX Firewalls. Students will also learn how to configure the Meraki Dashboard Students will troubleshoot and configure the Meraki environment and learn how to diagnose and resolve user and Network issues that may arise.

Why Attend with Current Technologies CLC

- Our Instructors are the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Course Objectives

Following completion of this course, students will understand, Install, Configure, monitor, and Troubleshoot the following:

- Navigate and Configure the Dashboard
- Add MX / MR / MS / MV devices to the Dashboard
- Understand and Configure Configuration Templates
- Understand and Configure Group Policies
- Manage / Configure / Integrate Users and Radius Policies
- Configure, Monitor, and Troubleshoot MX Firewalls
- Troubleshoot devices and Connectivity

Course Duration

3 day

Course Price

$3,495.00 or 35 CLCs

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Who Should Attend

The primary audience for this course is as follows:

- IT Staff and Managers
- Network and Systems Personnel and Engineers
- Small to mid-sized organizations that require fundamental knowledge on networking terms/concepts and configuration guidance for Meraki equipment
- This also includes organizations looking to implement remote sites, provide a guest wireless solution,

and collect user analytics

Outline

Module 0: Introduction

- Module Introduction
  - Topic List
- Lesson 1: Introductions
  - Course Goal
  - WebEx Basics
  - General Administration
  - Introductions
  - The Integrated Cisco Network
- Module Summary

Module 1: Introduction to Meraki

- Module Introduction
  - Topic List
- Lesson 1: Why Cisco Meraki?
  - Cloud Management
- Lesson 2: Meraki Product Overview
  - Meraki MS Switches
  - Meraki MR Wireless Access Points
  - Meraki MX Security and SD-WAN Appliances
  - Meraki MV Vision Security Cameras (MG and MT)
  - Meraki Systems Manager (SM)
  - Meraki MT Sensors Access Points
  - Cisco Meraki Insight
- Lesson 3: Meraki API Overview
- Lesson 4: Meraki Licensing and Support
  - Enterprise Support and Hardware Warranties
  - Cisco Meraki Documentations
- Module Summary

Module 2: Cloud Management with the Meraki Dashboard

- Module Introduction
  - Topic List
- Lesson 1: Overview of the Meraki Dashboard
  - The Cisco Meraki Dashboard
  - The Meraki Phone App
  - Dashboard: Organizational Structure
  - Meraki Dashboard Best Practices - Campus
  - Dashboard Compliance and Data Protection

  - Cloud Reliability
  - Loss of Connectivity to the Cisco Meraki Cloud
  - Safe Configuration
  - Meraki Dashboard Login (1)
  - Create Dashboard Account (1)
  - Create Dashboard Account and Organization
  - Verify Created Account
  - First Login to New Organization
  - Account Login with Multiple Assigned Organizations
  - Manage Multiple Organizations
  - View Health Status for Multiple Organizations (1)
  - Meraki Dashboard Best Practices - Multiple Locations
  - Dashboard Search
  - Logged in User Profile
  - Modify User Profile (1)
  - Announcements
- Lesson 2: Help & Support
  - Meraki Help
  - Dashboard - Help - Get Help (1)
  - Dashboard - Help - Community
  - Dashboard - Help - Marketplace
  - Dashboard - Help - Cases
  - Dashboard - Help - Data Protection Requests
  - Dashboard - Help - New Features
  - Dashboard - Help - Firewall Rules Info
  - Dashboard - Help - API Docs
  - Dashboard - Help - Hardware Replacement
  - Dashboard - Give Your Feedback
- Lesson 3: Organizational Wide Configure Settings
  - Organizational Menu Settings
  - Settings - Org Name and Security Settings
  - Settings - Authentication (1)
  - Configuring SAML SSO with ADFS
  - Configuring SAML SSO with OneLogin
  - Settings - Administration Settings
  - Settings - Privacy and Support Access Settings
  - Settings - SNMP Configuration
  - Settings - Threat Grid
  - Settings - Dashboard API Access
  - Settings - Delete This Organization
  - Organization > CONFIGURE > Configuration Sync
  - Configuration Sync
  - Organization > CONFIGURE > MDM
  - Organization > CONFIGURE > Administrator
  - Create Administrator Account - Org Access
  - Create Administrator Account - Network Access
  - Create Administrator Account - Camera Access
  - Create Administrator Account
  - Verify Administrator Account
  - Deleting an Administrator Account
  - Organization > Configure > Camera Roles

- Organization > Configure > License Info
- License Information - Co-Termination
- Add Licenses to Organization - Co-Termination
- License History - Co-Termination
- Converting to PDL (Per Device Licensing) (1)
- Licensing & Inventory Page - PDL (1)
- Organization > CONFIGURE > Create Network
- Create Network - Setup Network
- Create Network - Select Devices from Inventory
- Create Network - Add Devices
- Finding Meraki Order Number
- Delete Networks
- Organization > Configure > Inventory
- Organization > Inventory - Searching for Devices
- Organization > Inventory - Claiming Devices
- Organization > Inventory - Unclaiming Devices
- Organization > Add a Device to a Network
- Recovering a Missing or Stolen Device
- Organization > Monitor > Overview > Networks
- Organization > Monitor > Overview > Networks Tags
- Organization > Monitor > Overview > Devices
- Organization > Monitor > Change Log
- Organization > Monitor > Login Attempts
- Organization > Monitor > Security Center (1)
- Organization > Monitor > Location Analytics (1)
- Organization > Monitor > VPN Status
- Organization > Monitor > Firmware Upgrades
- Firmware Upgrades - Scheduling Firmware Upgrades (1)
- Organization > Monitor > Firmware Upgrades (1)
- Organization > Firmware Upgrades > Overview
- Organization > Firmware Upgrades > Firmware Status
- Organization > Firmware Upgrades > Firmware Release Notes
- Organization > Firmware Upgrades > Firmware Roll Back (1)
- Firmware Upgrades Through APIs
- Organization > Monitor > Summary Report (1)
- Organization > Summary Report - Anomalies
- Organization > Summary Report - Clients with High Usage
- Organization > Summary Report - Usage stats
- Organization > Summary Report - Sessions
- Organization > Top SSIDs by Usage
- Organization > Summary Report - Top Devices
- Top Device Models by Usage
- Top Security Appliances by Utilization
- Summary Report - Port Utilization Graph
- Summary Report - Client Stats
- Summary Report - Top Clients by Usage
- Clients
- Organization - Top Client Device Manufacturers
- Organization - Top Operating Systems by Usage
- Organization - Top Application Categories
- Organization - Top Applications by Usage

  - Organization - Power Details
- Lesson 4: Network-Wide Settings
  - Network-Wide
  - Network-Wide > Configure > General (1)
    - Network-Wide > General > Traffic Analysis
    - Network-Wide > General > Location and Scanning
    - Network-Wide > General > SMS Auth with Twilio
    - Network-Wide > General > CloudShark
    - Network-Wide > Wireless Multicast to Unicast Conversion
    - Network-Wide > General > Device Configuration (1)
    - Network-Wide > General > Reporting > Syslog
    - Network-Wide > General > SNMP
    - Network-Wide > General > Reporting > Location
    - Network-Wide > General > NetFlow
    - Network-Wide > General > Firmware Upgrades
    - Network-Wide > General > Switch & Wireless Alternate Management Interface (1)
    - Network-Wide > General > Status & APIs
    - Network-Wide > General > Status
    - Network-Wide > General > Umbrella
  - Network-Wide > Administration > Org Admins
  - Network-Wide > Administration > Network Admin
  - Network-Wide > Administration > Guest Ambassadors
  - Network-Wide > Admin > Port Management Privileges
  - Network-Wide > General > Camera-Only Admins
  - Network-Wide > Users > Guest Access
    - Network-Wide > Users (1)
  - Network-Wide > Group Policy
    - Network-Wide > Group Policy > New Group
    - Network-Wide > Group Policy > Schedule
    - Network-Wide > Group Policy > Bandwidth
    - Network-Wide > Group Policy > Hostname Visibility
    - Network-Wide > Group Policy > Firewall
    - Firewall - Layer 7 Rules
    - Network-Wide > Group Policy > Umbrella
    - Network-Wide > Group Policy > Traffic Shaping (1)
    - Network-Wide > Group Policy > Wireless Only
    - Network-Wide > Group Policy > Security Appliance Only
  - Network-Wide > General > Add Devices
  - Network Wide > Monitor > Clients (1)
  - Searching for Clients
  - Modifying Columns
  - Network Wide > Monitor > Clients > Applications
  - Network Wide > Monitor > Clients > Ports
  - Network Wide > Monitor > Clients > HTTP Content
  - Network Wide > Monitor > Clients > Custom Pie Chart
  - Changing the Policies Applied to a Client
  - Adding a Client
  - Display Client Information - Overview (1)
  - Display Client Information - Connections (1)
  - Display Client Information - Performance (1)
  - Display Client Information - Timeline

  - Network-Wide > Monitor > Traffic Analytics (1)
  - Network-wide > Monitor > Topology
  - Topology - L2
  - Topology - L3
- Lesson 5: Packet Captures
  - Packet Capture for Multiple Devices (1)
  - Event log (1)
- Lesson 6: Location / Mapping Devices
  - Maps & Floor Plans (1)
  - Maps & Floor Plans - Drag & Drop Devices
  - Maps & Floor Plans - Assign Devices to…
  - Maps & Floor Plans - Geolocate Devices (1)
  - Maps & Floor Plans (1)
- Lesson 7: Configuring Templates
  - Organization > Monitor > Configuration Templates
  - Templates
  - Configuration Templates > Create New Template (1)
  - Configuration Templates
  - Unbinding Networks from a Template
  - Splitting Configuration Templates
  - Combining Configuration Templates
  - Deleting a Configuration Template
  - MR - Wireless Network Templates
  - MX/Z3 - Template VLAN IP Address Range Allocations
  - MX/Z3 - Template VLAN IP Address Range Allocations
  - VLAN Templates
  - Configuration Templates (1)
  - MS Templates
  - Switch Profiles
  - Configuration Templates > Local Overrides (1)
  - Configuration Templates > Local Overrides
- Module Summary

Module 3: Meraki MX Security Appliances

- Module Introduction
  - Topic List
- Lesson 1: What is MX?
  - One Unified Platform
  - Complete Connectivity and Threat Management Solution
  - Built-in Ironclad Security
  - Security Integrations/Interoperability
  - Cisco SourceFire AMP
  - AMP & Threat Grid (1)
  - Advanced Malware Protection for Meraki MX
  - Umbrella Integration for MX and Z-series
  - DNS/web-layer Security - Solution Overview
  - Backed by Cisco Talos Threat Intelligence
  - Cisco SD-WAN Solutions

  - Reliable, Cost Effective Connectivity with SD-WAN
  - Automated Site-to-Site VPN (Auto VPN)
  - VPN Options
  - High Availability and Path Redundancy
  - SD-WAN Functionality for the Branch
  - Connections that Fit your Business and Location Needs
  - VPN Health, Bandwidth, and Performance Monitoring
  - MX Appliance Licensing
  - MX Sizing Guide
- Lesson 2: Meraki Security and SD-WAN Portfolio
  - Teleworker Z3
  - Small Branch - MX64/MX64W
  - Small Branch - MX65/MX65W
  - Small Branch - MX67/MX67W
  - Small Branch - MX67C
  - Small Branch - MX68/MX68W
  - Small Branch - MX68CW
  - Small Branch - MX75
  - Medium Branch - MX84
  - Medium Branch - MX100
  - Medium Branch - MX85
  - Medium Branch - MX95
  - Medium/Large Branch - MX105
  - WAN behavior on MX75/85/95/105 (1)
  - MX250/MX450 New Design (1)
  - Large Branch, Campus / Concentrator (1)
  - Virtual Platforms - vMX
  - Virtual Platforms
  - New MX Appliance Overview
  - Meraki MX - Local Status Page
  - MX Local Status Page - Connection
  - MX Local Status Page - Configure (1)
  - MX Local Status Page - Set Interface Addresses
  - MX Local Status Page - Ethernet
  - Claim the MX Appliance
  - MX Create a Network for MX Appliance
  - Create Combined Network for MX in HQ
  - Check Newly Added Appliance Status
  - Change Name of Device
  - Set Location Data for Maps
  - Configure Warm Spare
  - View WAN Uplinks
  - Dynamic DNS
  - Device Tags & Notes
  - Remove MX From Network
  - Appliance Status - Summary Tab
  - Appliance Status - Uplink Tab (1)
  - Appliance Status - Location Tab (1)

  - Tools Tab > Ping
  - Tools Tab > Reboot Device
  - Tools Tab > Blink LEDs
  - Tools Tab > Dashboard Throughput
  - Tools Tab > Traceroute
  - Tools Tab > MTR Traceroute
  - Tools Tab > DNS Lookup
  - Tools Tab > ARP Table
  - Tools Tab > Test Umbrella Connectivity
  - Addressing & VLANs
  - Mode: Pass - Through or VPN Concentrator Mode
  - Mode: Routed
  - Addressing & VLANs - Client Tracking (1)
  - Addressing & VLANs - Enabling VLANs
  - Addressing & VLANs - Adding a VLAN
  - Edit MX Built-in Port Configuration
  - Static Routes
  - Security Appliance - Configure - DHCP
  - DHCP - Turn up and Lease Time
  - DHCP - DNS Name Servers
  - DHCP - Boot options
  - DHCP - Options
  - DHCP - Reserved IP Ranges (Excluded Addresses)
  - DHCP - Fixed IP Assignments (Reservations)
- Lesson 3: Meraki Firewall Configuration
  - Security Appliance - Configure - Firewall (1)
  - Inbound Firewall Logging
  - Layer 3 vs Layer 7 Firewall
  - Firewall - Outbound Rules
  - Firewall - Cellular Failover Rules
  - Firewall - Security Appliance Services
  - Firewall - Layer 7 Rules
  - Geo-IP Based Firewalling
  - Forwarding Rules - Port Forwarding
  - Forwarding Rules - 1:1 NAT
  - Forwarding Rules - 1:Many NAT
  - Bonjour Forwarding
  - IP source address spoofing protection
- Lesson 4: Meraki Site-to-Site VPN
  - Automated Site-to-Site VPN (Auto VPN)
  - What is a VPN?
  - Site-to-Site VPN
  - Configuring Site-to-Site VPN AutoVPN
  - Site-to-Site VPN - Hub Configuration
  - Site-to-Site VPN - Hub Configuration with Exit Hub

  - Site-to-Site VPN - Spoke Configuration Split Tunnel
  - Site-to-Site VPN - Spoke Configuration Full Tunnel
  - Site-to-Site VPN - Local Networks
  - Site-to-Site VPN - NAT Traversal
  - Site-to-Site VPN - Remote VPN Participants
  - Site-to-Site VPN - VPN Subnet Translation
  - Site-to-Site VPN - Non-Meraki VPN Peers
  - Site-to-Site VPN - Non-Meraki IPSEC Policy
  - Site-to-Site VPN - VPN Firewall Rules
  - Site-to-Site VPN - Monitor Status
- Lesson 5: Meraki Client VPN
  - Enable Meraki's L2TP Client VPN
  - Configure Meraki's L2TP Client VPN (1)
  - Meraki's Client VPN Authentication Methods (1)
  - VPN Clients
  - Enable the AnyConnect Client VPN (1)
  - AnyConnect Client VPN Authentication Methods (1)
  - AnyConnect Client VPN (1)
- Lesson 6: Meraki Active Directory
  - Active Directory Integration (1)
  - Apply Group Policy to Active Directory Groups
- Lesson 7: Meraki SD-WAN and Traffic Shaping
  - Reliable, Cost Effective Connectivity with Meraki SD-WAN
  - Intelligent path control to suit your needs
  - SD-WAN & Traffic Shaping (1)
- Lesson 8: Meraki Threat Protection
  - Threat Protection - AMP
  - Threat Protection - IDS/IPS
  - Threat Protection - Umbrella Protection
- Lesson 9: Meraki Content Filtering
  - Content Filtering (1)
- Lesson 10: Meraki Access Control
  - Access Control
  - Access Control > Network Access (1)
  - Network Access > Access Control > Radius (1)
  - Access Control > Network Access > Facebook (1)
  - Network Access > Access Control > Google (1)
- Lesson 11: Meraki Splash Page
  - Splash Page
  - Customize Splash URL
  - Customize Splash Page (1)
  - Preview Splash Page - Modern
  - Preview Splash Page - Fluid
  - Create Custom Themed Splash Page
- Lesson 12: Security and SD-WAN Wireless Concentrator
  - Teleworker VPN / L3 roaming (1)
  - Creating Teleworker Networks
- Module Summary

LAB OUTLINE

Lab 1: Configuring the Organization

- Configure Organizational Settings
- Add All Devices to Organization
- Create Networks
- Manage Network-Wide Settings
- Create group Policies
- Manage Firmware Upgrades
- Create Templates
- Manage VLAN Templates
- Bind Templates to Networks

Lab 2: Configuring MX Appliances and Z3 Teleworker Devices

- Configure MX Appliance and Configure Z3 Appliance
  - Setup VLANs and Layer 3 Interfaces
  - Setup a VPN Concentrator
  - Setup and Manage DHCP Settings
  - Configure Layer 3 Firewall Settings
  - Configure Layer 7 Firewall Settings
  - Configure Content Filtering
  - Configure Traffic Shaping
  - Configure SDWAN Feature and traffic Distribution
  - Configure Site-to-site VPN
  - Configure Client VPN
  - Integrate Active Directory with Group Policy Settings
  - Create Traffic Shaping Policies
  - Configure Access control with Radius and ISE
  - Create and Configure Splash Pages
- MX Appliances and Z3 Verification and Troubleshooting
  - Verify and Trouble Shoot Appliance Status
  - Verify and Trouble Shoot Site to Site VPN
  - Verify and Trouble Shoot Firewall Settings
  - Check the Routing Table
  - Use the Tools
  - Troubleshooting with Packet Capture