

D3 Meraki Access

Introduced: November 2017

Last Updated: October 2024

[View Introduction/Portfolio](#)[View General Requirements](#)

General Requirements

IMPORTANT NOTE: In addition to the requirements contained within this document, the Provider must meet all prerequisites and requirements listed in the [General Requirements \(GR\) document](#) for each Cisco Powered Service. If Provider is applying for multiple Cisco Powered Service specializations, Provider must meet the General Requirements for each specialization individually.

Overview

An access network connects the users and devices to other devices on the local area network and wide area networks for communication and accessing business applications. It is a critical layer of networking that delivers high performance, secure, wired, or wireless connectivity to the applications and information. The access layer of the network consists of switches, wireless access points, controllers, and a suite of management software that configures the associated equipment, manages the associated policies, and continuously monitors the performance and quality of services. Meraki Access enables Providers to offer managed wireless LAN (WLAN) and managed LAN services to interconnect end users and devices with layer 2 switching, layer 3 routing with security and quality of services with a cloud-based controller and management.

A Cisco Powered Meraki Access Service is a managed local area network (LAN) service, a managed wireless LAN (WLAN) service, or both, that is orchestrated from the cloud and managed by the Provider, using Cisco Meraki network solutions, together with support services, a Service Level Agreement, and proactive monitoring. End customers consume a set of access network services including managed LAN, managed WLAN, and other value-added services, such as presence analytics service and proximity marketing services. With Meraki Access, the Provider is able to control the infrastructure efficiently from the cloud, with the help of multi-tenancy and automation features aimed at delivering a compelling user experience, at scale. Furthermore, the Provider may make status and reporting capabilities, as well as self-service capabilities, available to End Customer administrators.

Relevant Cisco Products:

- Cisco Meraki MR series products
- Cisco Meraki MX series products with Wi-Fi capability
- Cisco Meraki MS product family
- Associated licenses for the above

Knowledge Requirements

The training below is provided at no cost as a benefit of the Provider role and is a collection of Black Belt Training Academy and other Cisco resources.

A minimum of two (2) individuals must complete each training course listed in the knowledge requirements section. There are no role-sharing limitations for the knowledge training requirements; the same individual can complete the Sales/Pre-sales and Technical focus training courses.

Sales/Pre-sales Focus

Requirements	Duration
Black Belt Meraki Pre-sales - Stage 1 Waived for an individual with Cisco Meraki Solutions Specialist (CMSS) certification *	7.5 hrs
Black Belt Meraki Pre-sales - Stage 2 Waived for an individual with Cisco Meraki Solutions Specialist (CMSS) certification *	10.0 hrs
Total Sales Hours	17.5 hrs

Technical Focus

Requirements	Duration
Black Belt Meraki Deployment - Stage 1 Waived for an individual with Engineering Cisco Meraki Solutions 1 (ECMS1) certification *	4.75 hrs
Black Belt Meraki Deployment - Stage 2 Waived for an individual with Engineering Cisco Meraki Solutions 1 (ECMS1) certification *	4.0 hrs
Black Belt Meraki Support - Stage 1 Waived for an individual with Engineering Cisco Meraki Solutions 1 (ECMS1) certification *	3.75 hrs
Black Belt Meraki Support - Stage 2 Waived for an individual with Engineering Cisco Meraki Solutions 1 (ECMS1) certification *	7.25 hrs
Total Technical Hours	19.75 hrs

* For waiving training requirements based on a certification, must provide the relevant certificate as evidence. A certification will satisfy the requirement for one (1) of the two (2) required individuals to complete the course. Two people with the specified certification would be required to completely waive the individual training course requirement.

Prerequisites

Provider must complete all Prerequisites in this section prior to scheduling the Cisco Powered Meraki Access Service audit.

#	Requirement	Evidence
D3.PR.1	Cisco Career Certifications This specialization does not require any Cisco Career Certifications.	None
D3.PR.2	Training Evidence Upload evidence of completion for all Training required for this Cisco Powered Service.	Evidence of training must be uploaded into the Provider application

Service Delivery

#	Requirement	Evidence
D3.SD.1	WLAN Management The Provider must offer WLAN management services including: <ul style="list-style-type: none"> • SSID management including network naming and authentication. • Access control policy management. • Splash page management. • Firewall rules at layer 3 and layer 7 application layer (optional service) and • Traffic shaping management (optional service). The Provider may choose to make some or all these management capabilities available for end customer self-service, via the Cisco Meraki Dashboard.	Required if Managed WLAN is included: <ul style="list-style-type: none"> • Demonstration of how WLAN Management capabilities are provided through the managed service. • Service Description document reflecting the WLAN management and reporting capabilities
D3.SD.2	WLAN Analytics and Reporting The Provider must offer WLAN analytics to end customers via the customer service portal. This should include: <ul style="list-style-type: none"> • Number of visitors, passersby. • Capture rate. • Time that visitors spent. • Number of return visitors. • Top clients of the network in terms of traffic. • Top applications of the network in terms of amount traffic. • Information of devices on the wireless network. The Provider must demonstrate these management capabilities as evidence of meeting this requirement. Additionally, these capabilities should be reflected in the Service Description document.	Required if Managed WLAN is included: <ul style="list-style-type: none"> • Demonstration of how WLAN Management capabilities are provided through the managed service. • Service Description document reflecting the WLAN management and reporting capabilities

#	Requirement	Evidence
D3.SD.3	<p>LAN Management</p> <p>The Provider must offer the following management capabilities to customers:</p> <ul style="list-style-type: none"> • Switch chassis management. • Port management. • VLAN management. • Access control policy management. • Switch stacking management. <p>The Provider can make some or all of these management capabilities available for end customer self-service.</p> <p>The Provider must demonstrate these management capabilities as evidence of meeting this requirement. Additionally, these capabilities should be reflected in the Service Description document.</p>	<p>Required for Managed LAN is included.</p> <p>Both of:</p> <ul style="list-style-type: none"> • Demonstration of how LAN management capabilities are provided through the managed service. • Service Description document reflecting the LAN management capabilities.
D3.SD.4	<p>LAN Analytics and Reporting</p> <p>The Provider must provide analytics and reporting capabilities related to network topology, network usage report at switch, port level including:</p> <ul style="list-style-type: none"> • Network level usage. • Top device by usage. • Top clients by usage. • Top application by usage. • Port level statistics such as top usage, clients and application utilization <p>The Provider must demonstrate these management capabilities as evidence of meeting this requirement. Additionally, these capabilities should be reflected in the Service Description document.</p>	<p>Required for Managed LAN is included.</p> <p>Both of:</p> <ul style="list-style-type: none"> • Demonstration of LAN analytics and reporting capabilities in use via the Meraki Dashboard. • Service description referencing the LAN analytics and reporting capabilities.
D3.SD.5	<p>Meraki CPE</p> <p>Cloud Managed Meraki Access Service requires Meraki CPE. The Provider must offer Cloud Managed Meraki Access based on the following CPE, applicable to the services offered (WLAN and/or LAN):</p> <ul style="list-style-type: none"> • Cisco Meraki MR series products, for managed WLAN. • Cisco Meraki MX series products with WiFi capability, for managed WLAN. • Cisco Meraki MS product family, for managed LAN. 	<p>Demonstration of the use of the required products in the Meraki Dashboard, and the necessary licenses.</p>
D3.SD.6	<p>Software License Management</p> <p>The Provider must ensure a valid software license is applied to CPE devices used for service delivery. Failure to properly manage the software license expiration could result in a service outage for the customer.</p>	<p>Demonstration of the license management process.</p>

#	Requirement	Evidence
D3.SD.7	Proactive Monitoring of the Managed WLAN or Managed LAN Service The Provider must offer proactive monitoring as part of cloud managed WLAN or LAN service. The access point or switching device is proactively monitored for availability and health from the Provider's operation center rather than waiting for the customer to notify the Provider of a problem. The Provider must provide an operations procedure document or demonstration of the network management systems where the status of end customer devices can be viewed as evidence of meeting this requirement.	One of: <ul style="list-style-type: none"> • Operations procedure document • Demonstration of the network management systems showing the status of end customer devices
D3.SD.8	Customer Service Portal The Provider is to offer a secure web portal to present an operational view of the managed service, for multiple audiences, designed to give a view of the network and device status. If the Provider does not provide direct access to the Cisco Meraki Dashboard and/or Meraki APIs, the Provider must provide a third-party portal integrated with the Meraki APIs	Both of: <ul style="list-style-type: none"> • Demonstration of the secure web portal • User Guide that includes information on the portal

Additional Resources

- Looking to see what has changed? Starting in August 2023, the revision log below will summarize key changes for this Cisco Powered Services Specialization. For changes prior to August 2023, please review the complete [revision log](#).
- Bookmark the [Audit and Related Documents](#) page to find previous versions of the Cisco Powered Services Portfolio.

Document Revision History

Revision history	Date	Changes
13.0	10/2024	Updated Knowledge Requirements training course names and hours for accuracy.
12.0	05/2024	Updated Knowledge Requirements training requirement language for clarity. Added certification waivers to Knowledge Requirements where appropriate. Removal of EN Meraki Sales Stage 1 training from Knowledge Requirements. Updated Knowledge Requirements training course names and hours for accuracy.
11.0	02/2024	Removed Selling Meraki Managed Services from Sales/Presales Focused knowledge requirement.
11.0	12/2023	Updated general requirements section. Added Selling Meraki Managed Services to Sales/Presales Focused knowledge requirement. The coursework is 1.5 hrs.



10.0	09/2023	Corrected Cisco Career Certification requirement PR.1. No Cisco Career Certifications are required.
10.0	08/2023	Created overview, general requirements, and specific requirements documents for each Cisco Powered Service Specialization. Effective August 2023, changes to individual Cisco Powered Service Specialization requirements will be covered in the revision history for Cisco Powered Service-specific documents. The complete revision log includes the full history through August 2023.



Americas Headquarters
San Jose, CA

Asia Pacific Headquarters
Singapore

Europe Headquarters
Amsterdam, The Netherlands

Cisco has approximately 400 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)