CLOUDSWITCHED

FREE RESOURCE — DEPLOYMENT CHECKLIST

Meraki Deployment Checklist

Step-by-step Cisco Meraki rollout for MX security appliances, MS switches, MR access points and Systems Manager. Capture serials, network names, SSIDs and VLANs in the field, work each phase from Dashboard set-up to handover, and finish with a signed-off score per phase.

5	45+	/10	Fillable
DEPLOYMENT PHASES	TASKS & CHECKPOINTS	SCORE EACH PHASE	TICK & TYPE IN ANY VIEWER

MX FIREWALL · MS SWITCHING · MR WIRELESS · SYSTEMS MANAGER

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this checklist

Work through each of the five phases in order with the engineer building the network. Do **Phase 1 (Dashboard & Licence Setup)** before any hardware is unboxed — if the organisation, network, claim and licence are wrong, every later phase compounds the mistake. Tick each checkpoint only when it is **verified in the Dashboard**, not just "configured" on a laptop.

Fill in the underscore fields as you go — organisation name, network name, MX/MS/MR serials, firmware version, WAN IP, SSIDs, VLAN IDs — so the checklist doubles as the build record. Score each phase out of 10 at the end, then transfer the scores into the summary page and sign off on the handover page. This is an **interactive PDF**: tick boxes and type into the fields in any modern viewer.

WHAT THIS CHECKLIST IS

A field-grade deployment runbook for a single-site or multi-site Cisco Meraki rollout covering MX security appliances, MS access/aggregation switches, MR wireless access points and Systems Manager enrolment. It assumes Dashboard licences are already procured and the site survey is complete. It does not replace a low-level design document for complex multi-site / SD-WAN builds.

DON'T SKIP DASHBOARD-FIRST

Meraki is cloud-managed: configuration is authored in the Dashboard *before* devices come online, then pushed down on first heartbeat. Plugging hardware in with an empty network template is the single most common cause of misconfigured VLANs, open SSIDs and broken VPNs on day one.

The five phases

- **01 Dashboard & Licence Setup** — org, network, admins, claim, licence, alerts.
- **02 MX Security Appliance** — WAN, VLANs, firewall, VPN, content filtering, IDS/IPS.
- **03 MS Switches** — port profiles, trunks, PoE, STP, QoS, rack & patching.
- **04 MR Access Points** — SSIDs, 802.1X, guest portal, radio settings, Air Marshal.
- **05 Testing & Handover** — walk-test, auth, VPN, speed, documentation, training.

01

Dashboard & Licence Setup

Configure the Meraki Dashboard organisation, network and licence stack **before any hardware is racked**. Get the naming convention, admin accounts, MFA, and alert routing right at this stage — reversing them later is painful and risky.

- ☐ Create the **Meraki Dashboard organisation** and network using the agreed naming convention *(site code, region, environment)*.
- ☐ **Claim every device** into the Dashboard using serial numbers or QR codes from packaging; assign each to the correct network.
- ☐ Verify all **licence subscriptions** are active with sufficient term and the correct edition *(Enterprise / Advanced Security / SD-WAN Plus)*.
- ☐ Configure **Dashboard admin accounts** with appropriate role-based permissions; MFA enforced on every admin.
- ☐ Set **organisation-wide settings**: timezone, regulatory domain, firmware upgrade schedule, alert preferences.
- ☐ Configure **network-level settings**: VLANs, DHCP / DNS strategy, SNMP, syslog forwarding to SIEM if required.
- ☐ Set up **Dashboard alerts**: device offline, configuration change, port-flap, rogue AP detection, security events.

Dashboard build record

ORGANISATION NAME	NETWORK NAME	LICENCE EDITION / EXPIRY
PRIMARY ADMIN EMAIL	**CLAIM / ORDER REF**	**FIRMWARE TRACK**

PHASE 01 SCORE _____ / **10** *Aim for 10. Below 8 = revisit before racking.*

02

MX Security Appliance

Configure and deploy the Meraki MX edge / firewall / SD-WAN appliance. Build the WAN and VLAN layout in the Dashboard, lock down the firewall and VPN policy, then bring the device online and verify a green status.

- ☐ Configure **WAN uplink(s)** with static IP, DHCP or PPPoE per ISP requirements; secondary uplink for failover where present.
- ☐ Configure **VLAN interfaces** for every network segment *(corporate, guest, VoIP, IoT, mgmt)* with correct subnet, DHCP scope and gateway.
- ☐ Set up **firewall rules** on least-privilege L3 & L7 policy; default-deny outbound where the design calls for it.
- ☐ Configure **site-to-site Auto VPN** hub / spoke topology for multi-site connectivity; non-Meraki peers via IPsec where required.
- ☐ Enable **client VPN or AnyConnect** for remote access; integrate with RADIUS / Entra ID with MFA enforced.
- ☐ Configure **content filtering, AMP and IDS/IPS**; set to blocking mode on appropriate categories & signature sets.
- ☐ Set up **traffic shaping** rules to prioritise VoIP, video and business-critical SaaS; cap recreational traffic.
- ☐ Physically install MX, connect WAN and LAN cables, and verify **green status** with current firmware in the Dashboard.

MX build record

MX MODEL	SERIAL NUMBER	FIRMWARE VERSION

PRIMARY WAN IP / ISP	SECONDARY WAN IP / ISP	MANAGEMENT VLAN ID

PHASE 02 SCORE _____ / **10** *Aim for 9+. Below 7 = edge security gap.*

03

MS Switches

Configure and deploy Meraki MS access and aggregation switches. Build switch port profiles, trunks, PoE and QoS in the Dashboard, then patch the physical switches into the rack and verify online status before the APs and clients arrive.

- ☐ Configure **switch port profiles** for each VLAN role *(data, voice, AP, trunk, unused / shut)*; apply by tag.
- ☐ Configure **trunk ports** between switches, to the MX, and to access points with the correct allowed-VLAN list and native VLAN.
- ☐ Enable **PoE+ / PoE++** on ports for access points, IP phones and cameras; size the PoE budget to peak draw.
- ☐ Configure **STP / RSTP** with root bridge priority set on aggregation; enable **BPDU Guard** on edge ports.
- ☐ Administratively **shut down unused ports** or push them into a quarantine / black-hole VLAN.
- ☐ Configure **QoS**: trust DSCP on uplinks, prioritise voice / video, mark egress where the application doesn't mark itself.
- ☐ Install switches in the rack / cabinet and **patch to structured cabling**; label patch leads to port numbers.
- ☐ Verify all switches show **green / online** in the Dashboard with correct firmware and port connectivity.

MS build record

SWITCH 1 — MODEL / SERIAL	SWITCH 2 — MODEL / SERIAL	SWITCH 3 — MODEL / SERIAL
STACK NAME (IF STACKED)	**FIRMWARE VERSION**	**VLANS TRUNKED**

PHASE 03 SCORE _____ / **10** *Aim for 9+. Below 7 = trunk / VLAN risk.*

04

MR Access Points

Configure and deploy Meraki MR wireless access points. Build SSIDs and radio profiles in the Dashboard, mount APs to the site-survey locations, then verify coverage, SSID broadcast and authentication before any clients are migrated.

- ☐ Configure **SSIDs**: corporate (802.1X / WPA3-Enterprise), guest (captive portal), and any IoT / contractor networks required.
- ☐ Assign each SSID to the **correct VLAN** via bridge or NAT mode; verify segmentation against the design.
- ☐ Configure **802.1X authentication** for the corporate SSID via RADIUS / NPS or cloud identity (Entra ID, Okta).
- ☐ Set up **guest WiFi**: splash page, click-through or sponsored sign-in, bandwidth limits, client isolation.
- ☐ Configure **radio settings**: channel width *(20/40 MHz on 2.4, 40/80 on 5)*, minimum bitrate, band steering, target waketime.
- ☐ Enable **Air Marshal** for rogue and neighbour AP detection; containment policy reviewed and signed off.
- ☐ Physically **mount APs at the site-survey locations**; antennas oriented, PoE budget verified, cable strain-relieved.
- ☐ Verify all APs show **green / online** in the Dashboard and are broadcasting the correct SSIDs at the expected signal.

MR build record

AP COUNT / MODEL	LEAD AP SERIAL	FIRMWARE VERSION
CORPORATE SSID	GUEST SSID	RADIUS / NPS SERVER IP

PHASE 04 SCORE _____ / **10** *Aim for 9+. Below 7 = wireless will be the support ticket.*

05

Testing & Handover

The deployment isn't done until it's been independently tested and handed over. Walk the site, verify every SSID and VPN under load, run speed tests from a representative client, then leave the customer's IT team with documentation they can actually use.

- ☐ Conduct a **WiFi walk-test**: verify signal strength ≥ -65 dBm across all working areas; document weak spots and corrective action.
- ☐ Test **corporate WiFi authentication** with multiple user accounts and device types *(Windows, macOS, iOS, Android)*.
- ☐ Test **guest WiFi**: captive portal flow, client isolation from corporate, bandwidth caps applied as configured.
- ☐ Test **VPN connectivity**: site-to-site Auto VPN tunnel up, latency normal, client VPN connects with MFA.
- ☐ Verify **firewall rules** block and permit as expected; pen-test the rule base from inside and outside.
- ☐ Run **speed tests** from multiple physical locations against an internet target and an internal target; record throughput.
- ☐ Document the deployment: **network diagram, port maps, SSID details, VLAN list, IP plan, credentials in the password vault**.
- ☐ Deliver **handover documentation** and admin training to the customer IT team; agree support escalation path.

Test results

WORST-AREA RSSI	DOWN / UP MBPS ACHIEVED	VPN TUNNEL STATE
_____	_____	_____

PHASE 05 SCORE _____ / **10** *Aim for 10. Below 8 = revisit before handover.*

Σ

Deployment summary

Transfer the score for each phase into the table. Set a priority (H/M/L) for any phase that didn't hit its target — that's the punch-list before sign-off. A clean Meraki build totals 50/50 with H/M/L all blank.

#	DEPLOYMENT PHASE	SCORE / 10	RE-WORK PRIORITY
01	Dashboard & Licence Setup	_____ / 10	☐ H ☐ M ☐ L
02	MX Security Appliance	_____ / 10	☐ H ☐ M ☐ L
03	MS Switches	_____ / 10	☐ H ☐ M ☐ L
04	MR Access Points	_____ / 10	☐ H ☐ M ☐ L
05	Testing & Handover	_____ / 10	☐ H ☐ M ☐ L
Σ	**TOTAL SCORE**	_____ / 50	—

Score interpretation

45–50	**Clean handover.** Build is ready for sign-off. Schedule the 30-day post-deployment review.
35–44	**Punch-list outstanding.** Close the H/M items before customer go-live and re-test.
Below 35	**Do not hand over.** Re-engineer the failing phase, re-test, then re-score before the customer touches it.

Punch-list, sign-off & handover

Capture any outstanding items as a numbered punch-list, log notes for the customer's IT team, and sign the build off with the engineer, the project owner, and the customer representative.

Top 3 punch-list items

01 _____

02 _____

03 _____

Handover notes

_____

_____

_____

_____

Sign-off

ENGINEER (BUILD BY)	PROJECT OWNER	CUSTOMER SIGNATORY
_____	_____	_____
BUILD COMPLETION DATE	**HANDOVER DATE**	**30-DAY REVIEW DATE**
_____	_____	_____

CLOUDSWITCHED

CISCO MERAKI NETWORK SPECIALISTS

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom