

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



Document Version: 1.2

Last Updated: July 21, 2026

Applies To: Yonomi-Enabled Wi-Fi Access Control Locks

Table of Contents

1. Introduction
2. Executive Summary
3. Wi-Fi Network Requirements
4. Network Architecture Requirements
5. Signal Coverage and Performance
6. Security Configuration
7. Firewall and Port Requirements
8. Battery Life Optimization
9. Multi-Lock Deployment Guidelines
10. Pre-Deployment Checklist
11. Wi-Fi Troubleshooting Methods *(includes visual flowcharts)*

Introduction

Purpose

This document provides comprehensive Wi-Fi network requirements for deploying Yonomi-enabled Wi-Fi access control locks in commercial environments. The requirements outlined in this document are designed to achieve:

- **Seamless network connectivity** for reliable access control operations
- **Optimal battery life** with Wi-Fi always connected
- **Stable performance** in multi-lock deployments,
- **Optimal user experience** with minimal connectivity issues

Compliance Notice

IMPORTANT: Failure to follow these minimum requirements will result in:

- Excessive battery consumption (battery life less than 1 year)
- Unreliable connectivity and communication failures
- Degraded system performance
- Potential denial of technical support

Target Audience

This document is intended for the following professionals involved in planning, deploying, and supporting Wi-Fi enabled access control systems in commercial environments:

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



- **Network / IP Administrators:** Responsible for configuring Wi-Fi infrastructure, VLANs, firewalls, and DHCP. This document provides the specific network settings required for reliable lock connectivity and optimal battery life.
- **Security Integrators:** Licensed professionals who install and commission physical access control hardware, including door locks, controllers, and wiring. This document helps integrators verify that the customer's network meets requirements before and during lock installation.
- **Facility Managers and Building Operations Staff:** — Personnel who oversee day-to-day building operations and coordinate between IT, security vendors, and building ownership. This document outlines what network resources are needed and why

Executive Summary

Battery-operated Wi-Fi locks require specific network configurations to balance connectivity, security, and power consumption. Key requirements include:

- **Wi-Fi Standard:** 2.4 GHz 802.11 b/g/n only
- **Signal Strength:** Minimum -65 dBm at each lock location
- **Network Isolation:** Dedicated VLAN for lock traffic
- **Ports Required:** 80 (HTTP), 443 (HTTPS), 8883 (MQTT), UDP Port 123 (NTP)
- **Security:** WPA2-PSK or WPA3-PSK
- **Battery Life Target:** 12 months with optimized network settings

Wi-Fi Network Requirements

1. Wireless Standards and Frequency

Required Standards

- **Frequency Band:** 2.4 GHz ONLY
- **802.11 Standards:** b/g/n

Unsupported Standards

The following standards are **NOT SUPPORTED**:

- × 802.11ac (Wi-Fi 5)
- × 802.11ax (Wi-Fi 6)
- × 802.11ax-2021 (Wi-Fi 6E)
- × 5 GHz frequency band
- × 6 GHz frequency band

Configuration Note: If your access points support dual-band operation, ensure the 2.4 GHz band is enabled and properly configured as noted below in this document. Many modern access points default to 5 GHz only, which is not supported.

2. Mandatory Connection Data Rate

Critical Setting: The Wi-Fi access point's Mandatory Connect Data Rate must be configured correctly to prevent association failures.

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



- **Maximum Rate:** 54 Mbps
- **Recommended Rate:** 24 Mbps for optimal compatibility
- **Impact:** Setting this value higher than 24 Mbps will prevent locks from connecting to the network

Why This Matters: Many access points use automatic data rate settings to optimize network performance by excluding slow devices. Battery-powered locks intentionally use lower data rates to conserve power. Setting the mandatory rate too high will exclude locks from associating with the access point.

3. SSID Configuration

Broadcasting Requirements

- **SSID Visibility:** MUST be broadcasting (visible)
- **SSID Name:** Case-sensitive, maximum 32 characters
- **Character Set:** English alphanumeric characters and standard symbols

Hidden SSID Support

Connecting to a hidden SSID **is supported**, but comes with significant drawbacks:

- Hidden SSIDs **will not appear in scan results** in the mobile YP application
- The installer must **manually enter the exact SSID string** (case-sensitive) during lock configuration
- The installer must also **manually select the correct security type** (WPA2/WPA3) and **enter the passphrase** — there is no auto-detection when the SSID is hidden
- Any typo in the SSID name, security type, or passphrase will cause the lock to fail to connect with no visible network to verify against

Recommendation: Use a **broadcasting (visible) SSID** whenever possible. Hidden SSIDs do not provide

meaningful security improvement (the SSID is still transmitted in probe requests and association frames) and

they make deployment and troubleshooting significantly harder.

SSID Best Practices

12. Use a dedicated SSID for access control devices
13. Avoid special characters that may cause encoding issues: " ' < > & ;
14. Document the exact SSID name including capitalization
15. Avoid changing the SSID after deployment (requires lock reconfiguration)

4. DTIM Beacon Interval

Delivery Traffic Indication Message (DTIM) is an access point setting that controls how often the AP sends out shared network messages (such as DHCP and ARP) to all connected devices.

- **Maximum DTIM Period:** 5
- **Recommended DTIM Period:** 1–3 (AP default is typically acceptable)
- **Impact:** Higher DTIM Period reduces battery life and increases latency

Technical Background: The lock periodically wakes up to listen to these shared messages. If the DTIM period is set higher than 5, the AP holds messages too long and the lock misses them. This leads to:

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



- The lock losing its IP address (missed DHCP renewal)
- The lock becoming unreachable on the network (missed ARP)
- Locks appearing to disconnect and reconnect on their own.

5. Channel Configuration

Channel Assignment Strategy

Required Configuration:

- **Channel Assignment:** Static (NOT automatic)
- **Channel Selection:** Staggered across multiple access points
- **Channel Width:** 20 MHz (do NOT use 40 MHz bonding)

Recommended Channels: Use only non-overlapping channels:

- Channel 1 (2.412 GHz)
- Channel 6 (2.437 GHz)
- Channel 11 (2.462 GHz)

Vendor-Specific RF Management:

Some enterprise platforms include automatic RF optimization engines that can override per-AP static channel assignments. These must be explicitly disabled in addition to setting static channels on each access point.

- **Aruba AirMatch:** AirMatch runs periodic RF optimization (typically nightly) and will reassign channels automatically. Disable AirMatch or set the channel assignment mode to “Static” in the RF Management configuration.
- **Cisco WLC (RRM/DCA):** The Radio Resource Management Dynamic Channel Assignment (DCA) feature can change channels based on detected interference or load conditions. Set DCA to “Static” or “Freeze”.
- **Cisco Meraki:** Auto Channel is enabled by default under Radio Settings. Set channel assignment to manual per AP.

Verify after configuration: Monitor AP channel assignments over 24-48 hours to confirm channels remain on their assigned values and are not being changed by an RF management engine.

Why Static Channels Are Critical

Problem with Auto-Channel Selection:

Automated RF adjustments cause access points to periodically change channels and power levels.

When an access point changes channels:

1. All connected locks lose connection
2. Locks must scan for the new channel (battery drain)
3. Locks must re-authenticate (additional battery drain)
4. This process can occur multiple times per day with auto-RF enabled

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



6. Background Scanning

Required Configuration: Background scanning MUST be disabled on all access points serving locks.

What is Background Scanning?

Some enterprise access points periodically switch to adjacent channels to scan for rogue devices or optimize RF. During scanning:

- The access point temporarily stops servicing clients on the primary channel
- Connected devices experience brief disconnections (200-500ms)
- Locks interpret this as a connectivity issue and attempt to reconnect

Battery Impact: Background scanning can trigger 10-50 reconnection attempts per day, impacting battery life of lock.

7. Client Steering / Band Steering

Required Configuration: Client Steering (also known as Band Steering or Flexible Radio Assignment) MUST be turned OFF for the SSID used by YP Enabled Wi-Fi lock devices.

What is Client Steering?

Client Steering is a function of Wi-Fi systems — particularly mesh networks — that uses protocols like 802.11k/v to encourage a device to switch to a stronger access point as it moves, or when RF conditions change. Band Steering is a related feature that guides devices to a preferred frequency band (typically steering them from 2.4 GHz to 5 GHz).

This capability is sometimes referred to as:

- *Band Steering* — pushes clients from 2.4 GHz to 5 GHz
- *AP Steering* — moves clients between access points
- *Flexible Radio Assignment* — dynamically reassigns AP radios between bands

Why It Must Be Disabled for Locks:

- Wi-Fi-enabled locks operate exclusively on the **2.4 GHz band** and cannot connect to 5 GHz or 6 GHz
- Band Steering may actively prevent locks from connecting to 2.4 GHz by attempting to push them to 5 GHz
- AP Steering may force locks to disconnect and reconnect to a different access point, causing unnecessary battery drain
- 11k/v transition requests are not supported by lock firmware and may cause connection failures

Battery Impact: When client steering is enabled, locks may experience repeated connection rejections or forced roaming events, each consuming battery power for scanning, authentication, and reassociation.

Network Architecture Requirements

1. VLAN Configuration (Critical for Battery Life)

REQUIREMENT: A separate, dedicated VLAN MUST be configured exclusively for Wi-Fi-enabled locks.

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



What is VLAN?

A **VLAN (Virtual Local Area Network)** is a logical grouping of devices on a network that separates their traffic from other devices — even if they share the same physical network infrastructure (switches, access points, cabling).

Why a Dedicated VLAN is Essential

In shared Wi-Fi networks, locks receive all broadcast and multicast traffic:

- DHCP broadcasts from other devices
- mDNS/Bonjour announcements
- ARP requests
- SSDP discovery packets
- Streaming protocols (video, audio)

Battery Impact:

Every received packet wakes the lock's radio from power-save mode to process the packet. In a busy network:

- 100-500 broadcast packets per minute
- Each packet causes 10-50ms of active radio time
- Results in battery drain over expected life

With a dedicated VLAN:

- Lock traffic is isolated from other network activity
- Only relevant packets reach the locks
- Battery life can reach up to 12+ months

VLAN Configuration Steps

16. **Create a dedicated VLAN** (e.g., VLAN 100 - Access Control)
17. **Assign a unique subnet** (e.g., 192.168.100.0/24)
18. **Configure DHCP scope** for the lock VLAN only
19. **Map the dedicated lock SSID to the VLAN**
20. **NO other devices should connect to this VLAN**
21. **Ensure NO Captive Portal resides on this VLAN**

Captive Portal Restriction

REQUIREMENT: The VLAN used for Wi-Fi-enabled lock devices **MUST NOT** have a Captive Portal configured.

What is a Captive Portal?

A captive portal is a web page that intercepts network traffic and requires user interaction — such as accepting terms of service, entering login credentials (email, social media), or making a payment — before granting full internet access. Captive portals are commonly deployed in hotels, airports, cafes, and guest networks.

Why Captive Portals Are Incompatible:

- Locks cannot interact with web-based authentication pages
- Captive portals redirect HTTP/HTTPS traffic, preventing locks from reaching cloud services
- Portal session timeouts would periodically disconnect locks, causing battery drain
- Lock firmware does not include a web browser and cannot render or respond to portal pages

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



If your network uses a Captive Portal:

- Ensure the lock VLAN is completely excluded from captive portal policies
- Verify that the lock SSID maps to a VLAN with direct internet access (no portal interception)
- Test by connecting a laptop to the lock SSID — it should reach the internet without any portal page

2. Multicast/Broadcast Traffic Filtering

REQUIREMENT: Multicast and broadcast traffic filters **MUST** be enabled to significantly reduce or eliminate unwanted network traffic.

Filter Configuration

Enable these filters on lock VLAN:

- 22. **Block mDNS/Bonjour** (UDP port 5353)
- 23. **Block SSDP** (UDP port 1900)
- 24. **Block NetBIOS** (UDP ports 137-138)
- 25. **Block WS-Discovery** (UDP port 3702)
- 26. **Allow DHCP broadcasts** (UDP ports 67-68)

Access Point Broadcast Filtering

Many enterprise access points support client isolation or broadcast filtering:

Enable:

- Client Isolation (prevents device-to-device communication)
- Broadcast/Multicast Rate Limiting
- Proxy ARP (reduces ARP broadcast storms)

3. IP Address Assignment

Supported Methods:

- ✓ DHCP (Recommended)
- ✓ Static IP assignments via DHCP reservation
 - × Manual static IP configuration (not supported on locks)

IP Protocol:

- **IPv4:** Fully supported
- **IPv6:** Not supported at this time

DHCP Best Practices

- 27. **Lease Duration:** Set to at least 24 hours
 - Shorter leases cause unnecessary DHCP renewals
 - Renewals require radio wake-ups (battery drain)
 - Recommended: 7-30 day leases
- 28. **DHCP Reservations:** Consider using reservations for locks
 - Ensures consistent IP addresses for monitoring
 - Simplifies firewall and access rules
 - Recommended: Bind reservation to lock MAC address
- 29. **DNS Configuration:** Use reliable, fast DNS servers

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



- Primary: 8.8.8.8 (Google Public DNS)
- Secondary: 8.8.4.4 (Google Public DNS)
- Avoid complex DNS redirections or internal-only DNS that may fail

4. Managed vs. Unmanaged Networks

REQUIREMENT: A managed Wi-Fi network is strongly recommended over bulk/unmanaged Wi-Fi.

Managed Wi-Fi Benefits

- Centralized configuration management
- Consistent power levels and channel assignments
- Better roaming support for mobile commissioning devices
- Monitoring and diagnostics capabilities
- VLAN and filtering capabilities

Unsuitable Network Types

- × **Consumer-grade routers** (limited device capacity, no VLAN support)
- × **Mesh Wi-Fi systems** (dynamic channel changes, unpredictable roaming)
- × **Hotspot/portal networks** (captive portal authentication not supported)
- × **Guest networks** (often reset connections periodically)

Signal Coverage and Performance

1. Signal Strength Requirements

Minimum Signal Strength: -65 dBm (RSSI) at each lock location

Signal Quality Guidelines:

RSSI (dBm)	Quality	Lock Performance	Recommendation
-30 to -50	Excellent	Optimal connectivity, fast transactions	Ideal
-50 to -60	Good	Reliable connectivity, normal performance	Acceptable
-60 to -65	Fair	Occasional delays, acceptable battery life	Minimum
-65 to -75	Poor	Frequent reconnections, reduced battery life	Unacceptable
Below -75	Very Poor	Connection failures, rapid battery drain	Deploy more APs

2. Site Survey Requirements

REQUIREMENT: A professional Wi-Fi site survey **MUST** be completed before lock deployment.

Survey Deliverables

30. Pre-Deployment Passive Survey

- RF heatmap showing 2.4 GHz coverage
- Signal strength measurements at all lock locations

Contact Technical Support for any questions concerning this Technical Bulletin.

1-877-671-7011 Option 2 – Hours of Operation 8 AM to 8 PM EST

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



- Interference source identification
- Channel utilization analysis

31. Post-Deployment Active Survey

- Verify coverage after AP installation
- Test actual throughput at lock locations
- Document dead zones or weak signal areas

Heatmap Requirements

Coverage Heatmap Must Show:

- Signal strength in dBm across the facility
- Clear indication of -65 dBm boundary
- Access point locations
- Lock deployment locations
- Physical obstructions (walls, doors, elevators)

3. Access Point Placement and Power

Placement Strategy

Goal: Maximize coverage at lock locations while minimizing overlap and interference.

Placement Principles:

- 32. **Line of Sight:** Minimize physical obstructions between AP and locks
- 33. **Avoid:** Metallic objects, elevators, electrical panels, microwaves
- 34. **Height:** Mount APs at ceiling level (8-12 feet) for optimal coverage
- 35. **Spacing:** Typically, 50-75 feet apart for 2.4 GHz in commercial buildings

Power Level Tuning

REQUIREMENT: Access point transmit power must be tuned to appropriate levels.

Why Power Tuning Matters:

- **Too High:** Excessive AP overlap causes interference and roaming issues
- **Too Low:** Insufficient coverage, weak signals, connection drops

Recommended Approach:

- 36. Start with medium power levels (10-15 dBm)
- 37. Verify signal strength at lock locations
- 38. Reduce power if signal exceeds -50 dBm (avoid over-coverage)
- 39. Increase power only if signal is below -65 dBm

Coverage Area by Power Level (Typical Commercial Building):

- Low Power (5-10 dBm): 800-1,400 sq ft
- Medium Power (10-15 dBm): 1,500-2,500 sq ft
- High Power (15-20 dBm): 2,500-4,000 sq ft

Note: Actual coverage varies significantly based on:

- Building materials (wood, drywall, concrete, metal)
- Door types (hollow core vs. solid core vs. metal)
- Wall thickness
- RF interference sources

Contact Technical Support for any questions concerning this Technical Bulletin.

1-877-671-7011 Option 2 – Hours of Operation 8 AM to 8 PM EST

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



4. Physical Environment Considerations

Building Materials Impact

Different materials attenuate Wi-Fi signals differently:

Material	Signal Loss	Impact on Coverage
Air (open space)	0 dB	None
Drywall/Wood	3-5 dB	Minimal
Solid Wood Door	6-8 dB	Moderate
Concrete Wall	10-15 dB	Significant
Metal Door	15-25 dB	Severe
Metal Stud Wall	10-20 dB	Severe
Elevator Shaft	25-35 dB	Extreme

Design Implications:

- Locks on **metal doors** may require dedicated APs in line of sight
- *Concrete walls** between AP and lock reduce effective range by 50-70%
- *Metal studs** in walls create significant attenuation
- *Fire doors** (metal core) often need nearby AP placement

Security Configuration

1. Supported Authentication Methods

The locks support the following Wi-Fi security protocols:

WPA3-PSK (Supported)

- **Description:** Wi-Fi Protected Access 3 with Pre-Shared Key
- **Encryption:** 192-bit security
- **Best For:** New deployments with WPA3-capable infrastructure
- **Password Requirements:**
 - Minimum 8 characters
 - Maximum 64 characters
 - English alphanumeric and special characters only allowed
 - Case-sensitive

WPA2-PSK (Supported)

- **Description:** Wi-Fi Protected Access 2 with Pre-Shared Key
- **Encryption:** AES (CCMP)
- **Best For:** Existing networks, broader compatibility
- **Password Requirements:** Same as WPA3
- **Note:** Ensure WPA2-PSK mode (not WPA2-Enterprise)

WPA2-Enterprise (PEAP) (Supported)

- **Description:** Enterprise authentication with RADIUS

Contact Technical Support for any questions concerning this Technical Bulletin.
1-877-671-7011 Option 2 – Hours of Operation 8 AM to 8 PM EST

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



- **Authentication:** Username and password per device
- **Best For:** High-security environments requiring device-level credentials
- **Requirements:**
 - RADIUS server configured and accessible
 - Unique username/password per lock

Not Recommended Security Methods

- **WPA (WPA1):** Supported but not recommended — outdated security with known vulnerabilities. Use WPA2 or WPA3 instead.

Unsupported Security Methods

- × **WEP:** Deprecated, insecure (legacy support only, not recommended)
- × **WPA (WPA1):** Outdated security
- × **Open Networks:** No encryption (not recommended except for testing)
- × **Captive Portals:** Web-based authentication (incompatible)
- × **802.1X with Certificates:** EAP-TLS not supported

Firewall and Port Requirements

1. Required Ports

The following ports **MUST** be open in firewall rules for outbound connections from the lock VLAN:

Port 80 (HTTP)

- **Protocol:** TCP
- **Direction:** Outbound from locks
- **Usage:** Non-confidential bulk data transfers
- **Note:** Even though HTTP is used, firmware files are cryptographically signed

Port 443 (HTTPS)

- **Protocol:** TCP
- **Direction:** Outbound from locks
- **Encryption:** TLS 1.2

Port 8883 (MQTT over TLS)

- **Protocol:** TCP
- **Direction:** Outbound from locks
- **Encryption:** TLS-encrypted MQTT
- **Note:** Persistent connection for real-time features

Port 123 (NTP)

- **Protocol:** UDP
- **Direction:** Outbound from locks
- **Purpose:** Network Time Protocol — clock synchronization with NTP servers
- **Usage:** Locks use NTP to maintain accurate time for access event logging, credential validation, and audit timestamps

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



- **Note:** Accurate time is critical for time-based access rules and audit trail integrity

Blocked/Unused Ports

- × **No inbound ports** required or accepted
- × Locks do NOT run web servers or accept incoming connections

2. Firewall URL Whitelist

The following URLs/domains MUST be allowed through firewalls and content filters:

Allegion Cloud Services

***.allegion.com**

- *Purpose:* Primary cloud platform API
- *Services:* Configuration, credentials, audits, alerts

Azure Services

***.blob.core.windows.net**

***.azurefd.net**

***.azure-devices.net**

- *Purpose:* Microsoft Azure cloud infrastructure services
- *Services:*
 - Blob storage for firmware files
 - Azure Front Door for content delivery
 - Azure IoT Hub for MQTT connectivity

Device Update Services

***.adu.microsoft.com**

- *Purpose:* Azure Device Update service
- *Services:* Over-the-air (OTA) firmware update delivery and management

3. DNS Requirements

DNS Resolution:

- Locks require functional DNS resolution for all cloud services
- Primary DNS server must reliably resolve external domains
- DNS failures will prevent lock connectivity

Recommended DNS Configuration:

- *Primary DNS:* 8.8.8.8 (Google Public DNS)
- *Secondary DNS:* 8.8.4.4 (Google Public DNS)

Avoid:

- × Internal-only DNS that cannot resolve external domains
- × DNS services that redirect unknown domains to internal pages
- × DNS firewalls that block categories (may interfere with Azure services)

When Google Public DNS Is Blocked

Some organizations block external DNS providers (8.8.8.8, 1.1.1.1, etc.) and require all DNS traffic to route through internal corporate DNS servers. This is acceptable as long as the internal DNS server can resolve all external domains required by the locks.

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



If your organization uses its own DNS servers:

40. Ensure your internal DNS can resolve the following domains:

- *.allegion.com
- *.blob.core.windows.net
- *.azurefd.net
- *.azure-devices.net
- *.adu.microsoft.com

41. **Configure the lock VLAN DHCP scope** to point to your internal DNS servers instead of Google DNS

42. **Verify resolution works** by running these tests from a device on the lock VLAN (Virtual LAN to which Lock is connected):

```
nslookup api.allegion.com <your-dns-server-ip>
nslookup adu.microsoft.com <your-dns-server-ip>
nslookup blob.core.windows.net <your-dns-server-ip>
```

43. **Do NOT use DNS-based content filtering** that blocks or redirects Azure-related domains — this will break lock connectivity

Firewall Application Service Requirements

When using next-generation firewalls (e.g., Palo Alto, Fortinet, Check Point) that classify traffic by application rather than just port/IP, the following **application services** must be explicitly allowed in your firewall security policy for the lock VLAN. These are in addition to the URL/domain whitelist defined in [Section 2: Firewall URL Whitelist](#).

Required Application Services (allow outbound from lock VLAN):

Application Service	Purpose	Why It's Needed
Microsoft-Azure	Core Azure cloud platform traffic	Locks communicate with Azure-hosted backend services for configuration, credentials, audit logs, and alerts
Microsoft-Azure.Front.Door	Azure Front Door CDN/load balancer	Used for content delivery and global load balancing of lock cloud services — firmware downloads and API routing pass through Azure Front Door
Microsoft-Azure.Storage	Azure Blob Storage	Firmware update files and certificate bundles are stored in Azure Blob Storage — blocking this prevents OTA updates

Why This Matters:

Next-generation firewalls inspect traffic at the application layer (Layer 7) and may block connections even when the correct ports (80, 443, 8883) are open. If your firewall uses application-based rules, simply opening ports is not enough — you must also allow the application services listed above.

Verification Steps:

44. After configuring the rules, connect a test laptop to the lock VLAN

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



45. Browse to <https://api.allegion.com> — should load without errors
46. Check firewall traffic logs — verify connections from the lock VLAN are classified under the allowed application services and are not being blocked
47. Look for any "deny" or "drop" entries for traffic from the lock subnet — these indicate missing application or URL allowances

4. Proxy and SSL Inspection

HTTP/HTTPS Proxy

- **Support:** Proxies are NOT supported
- **Locks connect directly to cloud services**
- **Workaround:** Create firewall bypass rule for lock VLAN

SSL Inspection (TLS Decryption)

- **Support:** NOT supported
- **Issue:** SSL inspection breaks TLS certificate validation
- **Workaround:** Exclude lock VLAN from SSL inspection policies

Battery Life Optimization

Target Battery Life

Design Goal: 12 months of operation on a single set of batteries with Wi-Fi always connected.

Factors Affecting Battery Life

Network Configuration Impact (Properly Configured vs. Suboptimal)

Configuration Factor	Optimized	Suboptimal	Battery Life Impact
Dedicated VLAN	Yes	No (shared network)	+40-50% life
Multicast Filtering	Enabled	Disabled	+30-40% life
Static Channels	Yes	Auto-channel	+20-30% life
Background Scanning	Disabled	Enabled	+15-25% life
Signal Strength	-50 to -60 dBm	-65 to -75 dBm	+10-20% life
DTIM Interval	3-5 seconds	1-2 seconds	+5-10% life

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



Cumulative Effect: With all optimizations in place, battery life can improve from **4-6 months** (suboptimal) to **12-14 months** (optimized).

Vendor-Specific Note: Cisco Meraki Access Points

- Cisco Meraki access points send ARP (Address Resolution Protocol) requests to connected clients approximately every 8 seconds.
- This is built-in behavior that Meraki uses to track client connectivity and cannot be disabled — there is no user-facing setting to turn off or reduce these periodic ARP probes.

Impact on locks:

- Each ARP request forces the lock's Wi-Fi radio to wake up and respond
- With probes arriving every 8 seconds, the radio never enters deep sleep
- This constant wake cycle significantly shortens battery life compared to other AP vendors

What to expect:

- Locks connected to Meraki access points will have noticeably shorter battery life than the 12-month target
- This is not a lock defect — it is caused by the Meraki AP's network behavior

Multi-Lock Deployment Guidelines

Scalability Considerations

Commercial deployments often include dozens to hundreds of locks per building. Network design must account for:

48. Access Point Capacity

49. Network Congestion Management

1. Access Point Capacity Planning

Devices per Access Point:

- *Recommended Maximum:* 25-30 locks per access point
- *Absolute Maximum:* 50 locks per access point

Why Capacity Matters:

- Each lock maintains a persistent Wi-Fi connection 24/7 (always connected)
- All locks are concurrently connected at all times, continuously consuming AP resources
- Access points have finite resources for concurrent connections

Capacity Planning Formula:

Number of APs Required = (Total Locks / 25) rounded up

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



Example:
100 locks in building
 $100 / 25 = 4$ access points minimum

Coverage vs. Capacity:

- You may need more APs for capacity rather than coverage
- Even if signal strength is adequate, add APs if device count exceeds 30 per AP

2. Same Router Multi-Lock Best Practices

For commercial deployments with many locks on a single router or access point:

50. Enable QoS (Quality of Service):

- Prioritize lock traffic to ensure reliable always-on connectivity
- Prevents interference from other devices on the network

51. Disable Power-Saving for Access Points:

- Ensure APs remain at full power 24/7 since locks are always connected
- Some APs reduce power at night (energy saving) which can disrupt lock connectivity

52. Plan Network Maintenance Carefully:

- Since locks are always connected, any network downtime affects lock communication
- Schedule router reboots and maintenance during lowest-traffic periods
- Notify stakeholders before planned outages

53. Stagger Firmware Rollouts:

- For very large deployments (>200 locks), stagger firmware updates across groups
- Example: Roll out to 25-50 locks at a time to manage bandwidth

54. Monitor AP Load:

- Use access point dashboards to monitor client count
- Watch for high retry rates or low throughput (indicates overload)

Pre-Deployment Checklist

Use this checklist to verify network readiness before deploying Wi-Fi-enabled locks.

Network Infrastructure

- ☐ **2.4 GHz Wi-Fi enabled** on all access points
- ☐ **802.11 b/g/n standards configured** (NOT ac/ax)
- ☐ **Dedicated VLAN created** for lock traffic (no other devices)
- ☐ **Unique SSID configured** and broadcasting (not hidden)
- ☐ **Mandatory Connect Data Rate set to ≤24 Mbps**
- ☐ **DTIM period set to AP default** (1-3 recommended)
- ☐ **Static channel assignments** configured (NOT auto-channel)
- ☐ **Non-overlapping channels selected** (1, 6, 11)
- ☐ **Background scanning disabled** on all APs

Contact Technical Support for any questions concerning this Technical Bulletin.
1-877-671-7011 Option 2 – Hours of Operation 8 AM to 8 PM EST

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



- ☐ **Client Steering / Band Steering disabled** for lock SSID
- ☐ **Client isolation or multicast filtering enabled**
- ☐ **Captive Portal excluded** from lock VLAN (no portal on lock network)

Security Configuration

- ☐ **WPA2-PSK or WPA3-PSK configured**
- ☐ **SSL inspection disabled** for lock VLAN
- ☐ **HTTP proxy bypassed** for lock VLAN

DHCP and IP Configuration

- ☐ **DHCP enabled** on lock VLAN
- ☐ **IP address pool sized appropriately** (locks × 1.5 + 10)
- ☐ **DHCP lease duration ≥24 hours** (7-30 days recommended)
- ☐ **DNS servers configured** (8.8.8.8, 8.8.4.4 recommended)
- ☐ **If external DNS is blocked:** Internal DNS servers can resolve all required domains ([*.allegion.com](https://allegion.com), [*.blob.core.windows.net](https://blob.core.windows.net), [*.azurefd.net](https://azurefd.net), [*.azure-devices.net](https://azure-devices.net), [*.adu.microsoft.com](https://adu.microsoft.com))
- ☐ **DNS-based content filtering** does NOT block or redirect Azure-related domains
- ☐ **Gateway configured** for internet access

Firewall Configuration

- ☐ **Port 80 (HTTP) outbound allowed** from lock VLAN
- ☐ **Port 443 (HTTPS) outbound allowed** from lock VLAN
- ☐ **Port 8883 (MQTT) outbound allowed** from lock VLAN
- ☐ **URL whitelist configured:**
 - ☐ [*.blob.core.windows.net](https://blob.core.windows.net)
 - ☐ [*.adu.microsoft.com](https://adu.microsoft.com)
 - ☐ [*.allegion.com](https://allegion.com)
 - ☐ [*.azurefd.net](https://azurefd.net)
 - ☐ [*.azure-devices.net](https://azure-devices.net)
- ☐ **No inbound ports opened** to lock VLAN (security)
- ☐ **Application services allowed** (for next-gen firewalls: Palo Alto, Fortinet, Check Point, etc.):
 - ☐ Microsoft-Azure
 - ☐ Microsoft-Azure.Front.Door
 - ☐ Microsoft-Azure.Storage

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



Coverage and Signal

- ☐ **Wi-Fi site survey completed** with heatmap
- ☐ **Signal strength $\geq$ -65 dBm** at all lock locations
- ☐ **Access point placement optimized** for lock locations
- ☐ **Transmit power levels tuned** to avoid over-coverage
- ☐ **Physical obstructions documented** (metal doors, concrete walls)

Testing and Validation

- ☐ **Test device connected** to lock Wi-Fi network successfully
- ☐ **Internet connectivity verified** from lock VLAN
- ☐ **DNS resolution tested** for *.allegion.com
- ☐ **Firewall logs reviewed** to confirm no blocked connections

Wi-Fi Troubleshooting Methods

General Troubleshooting Approach

When locks experience connectivity issues, follow this systematic approach:

- 55. Identify the Symptom**
- 56. Check Network Configuration**
- 57. Test Connectivity**
- 58. Review Logs and Diagnostics**
- 59. Implement Solution**
- 60. Verify Resolution**

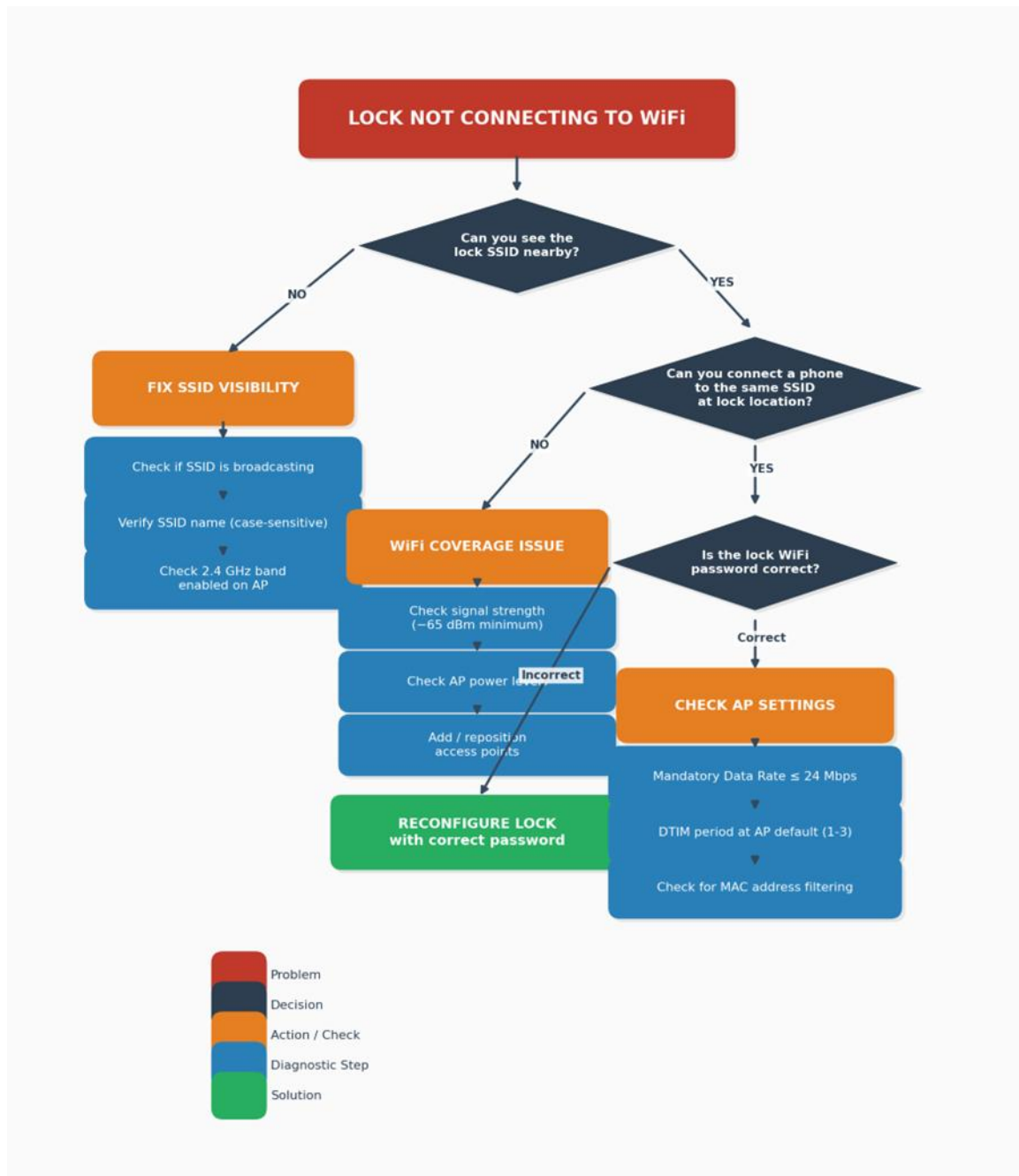
Troubleshooting Flowcharts

The following visual flowcharts guide you through diagnosing the most common lock connectivity issues. Each flowchart addresses a specific symptom category.

Flowchart 1: Lock Not Connecting to Wi-Fi

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements

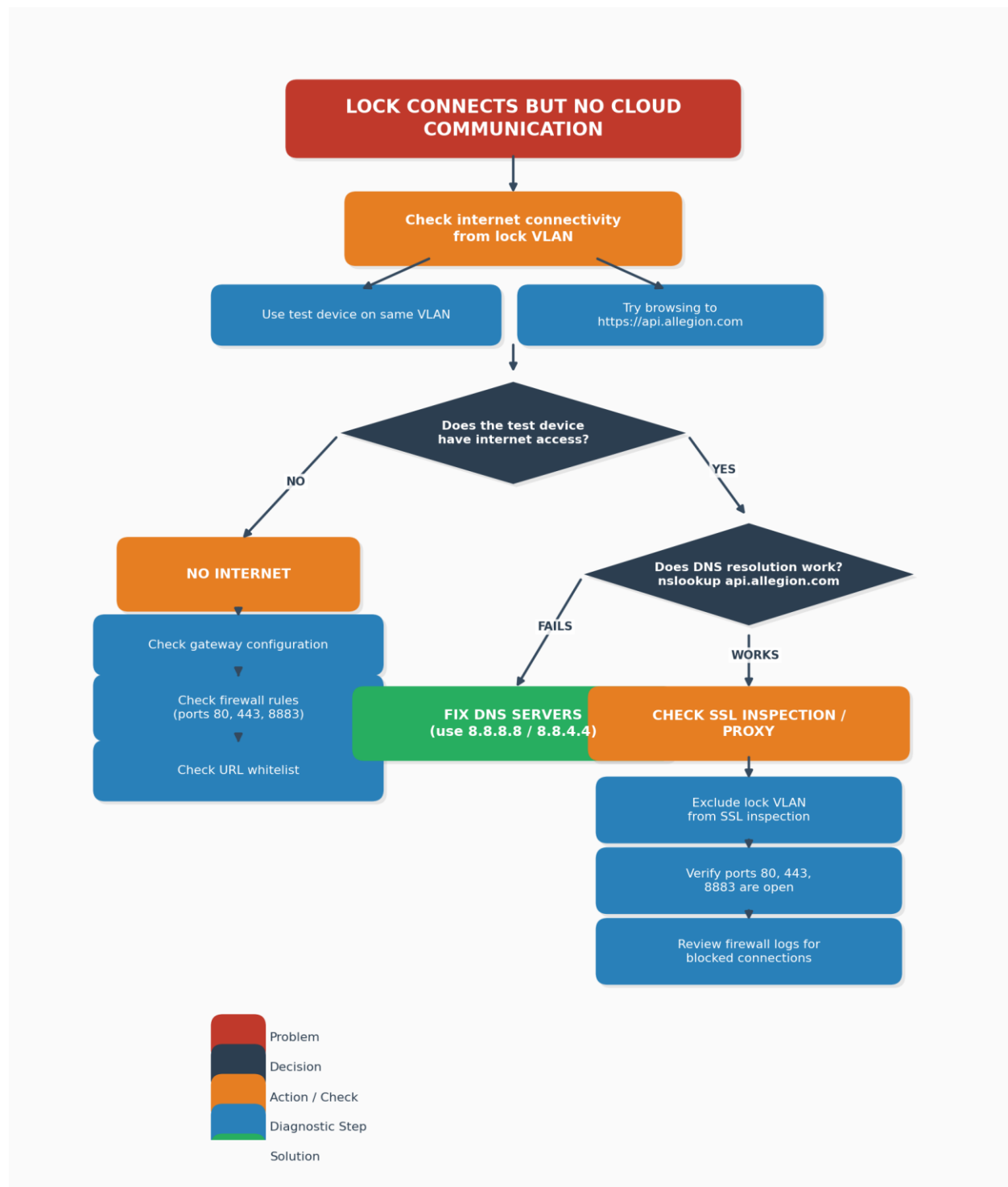


Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



Flowchart 2: Lock Connects but Doesn't Communicate with Cloud

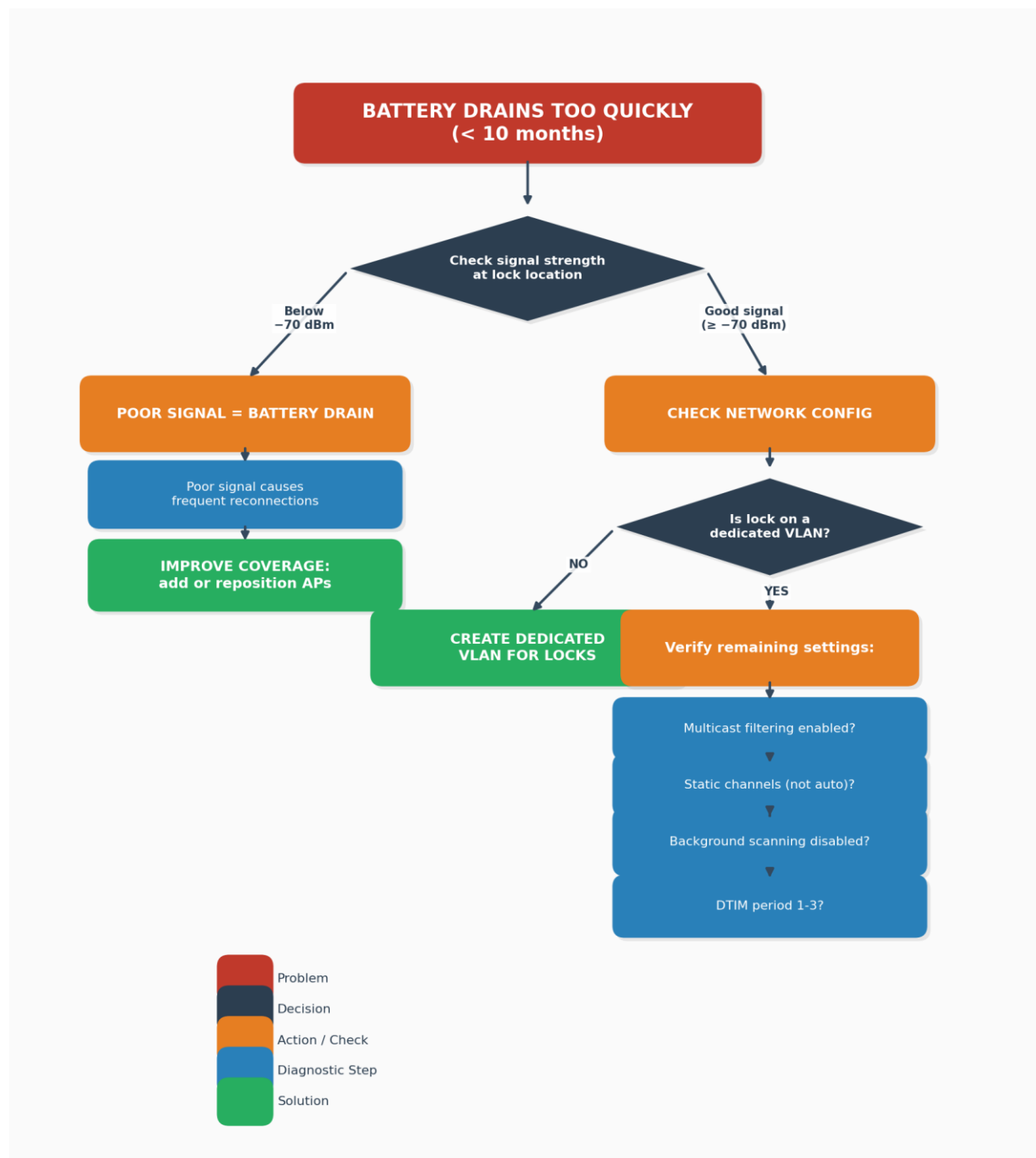


Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



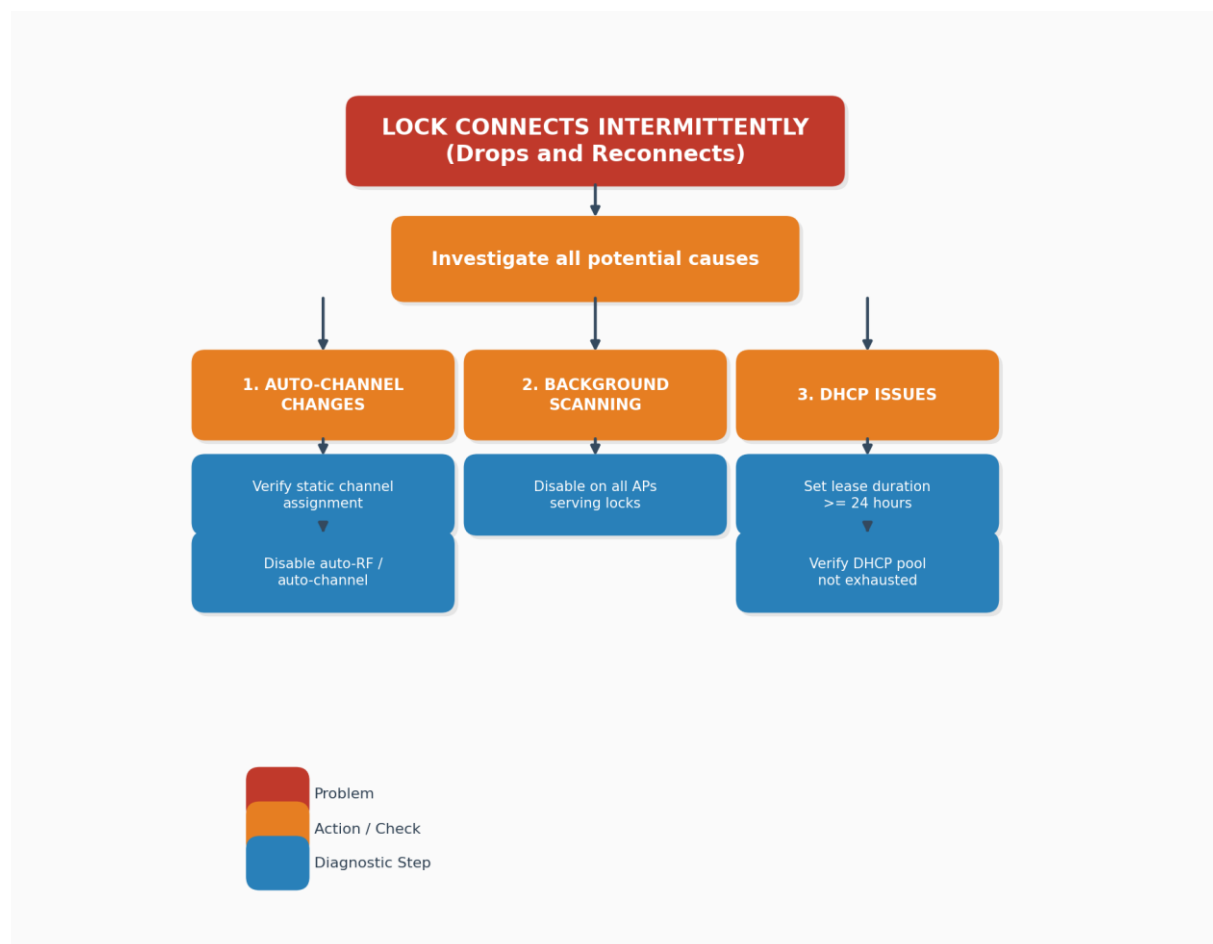
Flowchart 3: Lock Battery Drains Too Quickly (< 10 months)



Flowchart 4: Lock Connects Intermittently (Drops and Reconnects)

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



Error Code Reference (as per YP Telemetry Error codes)

Locks report specific error codes in audit logs when connection issues occur:

Error Code (Number or String)	Description	Troubleshooting
09	Failed to connect to AP (wrong credentials)	Verify SSID and password (case-sensitive)
04	DNS failure	Configure DNS servers or Allow Azure Services.
"IoT Hub Disconnection"	HTTP error from server	Check internet connectivity and firewall rules
"IoT Hub Disconnection"	Failed to connect to host server	Check firewall, ports 80/443, URL whitelist
18	Access point not found	Check SSID broadcasting, verify name is correct

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



Appendix: Quick Reference

Ideal Wi-Fi Settings Summary

Setting	Recommended Value
Frequency	2.4 GHz
Standard	802.11 b/g/n
Channel Assignment	Static (1, 6, or 11)
Channel Width	20 MHz
Mandatory Data Rate	≤24 Mbps
DTIM Interval	1-3 (AP default)
Security	WPA2-PSK or WPA3-PSK
SSID Broadcast	Enabled (visible)
Background Scanning	Disabled
Client Isolation	Enabled
Multicast Filtering	Enabled
Signal Strength (RSSI)	≥-65 dBm at lock
DHCP Lease	7-30 days
DNS Servers	8.8.8.8, 8.8.4.4

Required Firewall Rules

Outbound from Lock VLAN:

- Port 80 (HTTP) - Allow
- Port 443 (HTTPS) - Allow
- Port 8883 (MQTT) - Allow
- DNS (UDP 53) - Allow

URL Whitelist:

- *.allegion.com
- *.blob.core.windows.net
- *.adu.microsoft.com
- *.azurefd.net
- *.azure-devices.net

Inbound to Lock VLAN:

- No inbound ports required

Technical Information:

Yonomi™-Enabled Wi-Fi Network Requirements



Document Revision History

Version	Date	Changes	Author
1.0	February 16, 2026	Initial release - Comprehensive Wi-Fi requirements for YP-Enabled Wi-Fi locks	AN
1.1	March 18, 2026	Review comments update	AN
1.2	May 08, 2026	Minimum RSSI updated to -65 dBm	AN
1.3	July 21, 2026	Updated Branding and Messaging	JW

End of Document