

UNIFI NETWORK HEALTH CHECK

The Example Café Ltd

The Example Café, Worcester · 23 October 2026



Healthy

Internet		97
Security		100
WiFi		60
Switching		100
Devices		100
Networks		90
Controller		100

0

Act now

2

Plan next

11

Monitor

29

Working well

CONTROLLER

UniFi Network 10.6.106 on UniFi OS
5.1.33

REVIEWED

2 × access point, 2 × switch, 1 ×
console and gateway

CHECKS

36 of 36 run, up to 30 days of history

OVERVIEW

Summary

The network is in good shape overall. The internet line is fast with plenty of spare capacity, every device is online and up to date, and the security settings are sound. The terrace access point is the weak spot: its 2.4 GHz channel is 68% busy, devices connecting to it on 5 GHz have a weak signal, and it resends about a quarter of its traffic. Its 5 GHz radio has also moved off the channel it was set to. Any of these can make card payments on the terrace time out. Six IP address conflicts in the last 30 days may also have knocked devices offline, and the main café access point is close to its limit at the busiest times.

WHAT YOU TOLD US

WiFi on the terrace is slow and card payments out there sometimes time out.

5

UniFi devices managed

135 (105 on WiFi)

Devices connected now

157 devices

Busiest day, last 30 days

100.00%

Internet availability, 24 h

10 ms

Average latency, 30 days

684.6 GB

Internet data used this month

1325 / 118 Mbps

Last speed test

273

Neighbouring WiFi networks

Top priorities

- 1 Terrace AP is resending 27% of its WiFi traffic**
Check where its clients are, and whether a closer access point or a cleaner channel would serve them better.
- 2 6 IP address conflicts logged**
Find the device with a fixed address set by hand, and give it a reservation instead.
- 3 Café AP served 102 devices at its busiest hour**
Add an access point to share the load, or move one closer to where people gather.

RECOMMENDED NEXT STEP

A short remote session to fix the channel plan, find the device behind the IP conflicts and review the Café Devices network's security and roaming settings. If the terrace is still slow after that, a site visit to check where its access point is mounted and whether the café needs another one. Comparing the card reader's failure times with the controller's records would also help pin down the cause.

We ran 36 checks across the controller, devices, internet, WiFi, switching, networks, firewall and event log, using up to 30 days of history the controller keeps. Appendix A lists every check and its result.

FINDINGS

What we found

Plan next 2 findings

Plan next

WiFi

Quote

Café AP served 102 devices at its busiest hour

WHY IT MATTERS

Beyond about 60 devices on one access point, they all share its airtime, so WiFi slows down just when the site is busiest.

WHAT WE RECOMMEND

Add an access point to share the load, or move one closer to where people gather.

Plan next

Networks

Remote fix

6 IP address conflicts logged

WHY IT MATTERS

Two devices claimed the same address, so one of them loses its connection until it renews.

WHAT WE RECOMMEND

Find the device with a fixed address set by hand, and give it a reservation instead.

Monitor 11 things to keep an eye on

WHAT WE FOUND

WHAT WE RECOMMEND

Internet

The internet connection went down 4 times in the last 30 days, between 1 and 2 October

Each outage stops payments, calls and anything in the cloud.

Report the times to the ISP. A second connection for failover is worth considering if outages are costly.

WiFi

"Café Devices" uses WPA2 only

WPA2 is still acceptable, but WPA3 protects the password far better against guessing attacks.

Switch to WPA2/WPA3 transition mode, then check your older devices still connect. Keep WPA2 for any that do not.
Where in UniFi: Settings → WiFi → the network

WiFi

Café AP (2.4 GHz) channel is 52% busy

A busy channel means devices wait their turn, so WiFi feels slow even with a good signal. Neighbouring networks often cause it.

Try a quieter channel. If it stays busy, an on-site survey can find the source.
Where in UniFi: UniFi Devices → the access point → Radios

WiFi

Terrace AP (2.4 GHz) channel is 68% busy

A busy channel means devices wait their turn, so WiFi feels slow even with a good signal. Neighbouring networks often cause it.

Try a quieter channel. If it stays busy, an on-site survey can find the source.
Where in UniFi: UniFi Devices → the access point → Radios

WHAT WE FOUND

WHAT WE RECOMMEND

WiFi

Terrace AP is resending 27% of its WiFi traffic

Retries mean data had to be sent twice. Its clients average -69 dBm, and the weakest -76 dBm, so weak signal or interference is the likely cause.

Check where its clients are, and whether a closer access point or a cleaner channel would serve them better.

Where in UniFi: UniFi Devices → the access point → Radios

WiFi

Terrace AP is on 5 GHz channel 132, not its set channel 40

Its set channel is outside the radar range, so something else moved it, usually UniFi's automatic channel optimisation.

Check whether automatic channel optimisation is on, and pin the channel if the move made things worse.

Where in UniFi: UniFi Devices → the access point → Radios

WiFi

6 strong neighbouring networks overlap our 2.4 GHz channel 1

Networks at -70 dBm or stronger on or next to our channel share its airtime with us, which slows everyone down at busy times.

On 2.4 GHz use only channels 1, 6 or 11, and pick the one with the fewest strong neighbours. The chart in the WiFi section counts them per channel.

Where in UniFi: UniFi Devices → the access point → Radios

WiFi

10 strong neighbouring networks overlap our 2.4 GHz channel 6

Networks at -70 dBm or stronger on or next to our channel share its airtime with us, which slows everyone down at busy times.

On 2.4 GHz use only channels 1, 6 or 11, and pick the one with the fewest strong neighbours. The chart in the WiFi section counts them per channel.

Where in UniFi: UniFi Devices → the access point → Radios

WiFi

63 of 105 wireless devices are on 2.4 GHz

2.4 GHz is slower and more crowded. Smart-home devices often only support it, but phones and laptops should be on 5 GHz.

Check which devices are on 2.4 GHz. If phones and laptops are among them, review band steering and 5 GHz coverage.

Where in UniFi: UniFi Devices → the access point → Radios

WiFi

Café AP carries 90 of 105 wireless devices

One access point doing most of the work while the others sit idle usually means coverage or power settings are uneven.

Review access point placement and transmit power.

Where in UniFi: UniFi Devices → the access point → Radios

WiFi

Roaming assistance (802.11v) is off on "Café Devices"

With it on, access points can tell a device a better one is nearby, so phones and laptops move as you walk around instead of clinging to a weak signal.

Turn on BSS transition for these networks, then check older devices still connect. Leave it off on any network where they do not.

Where in UniFi: Settings → WiFi → the network

FINDINGS

What is working well

- ✓ UniFi measured the internet connection as available 100.00% of the time.
- ✓ The last speed test reached 1325 Mbps, 83% of the 1600 Mbps plan.
- ✓ UPnP is off, so devices cannot open ports to the internet on their own.
- ✓ No ports are forwarded from the internet.
- ✓ Device SSH login is off.
- ✓ The firewall zones block guests and devices from your other networks by default, with 18 narrower exceptions listed for review in the firewall section.
- ✓ Most wireless devices have a good signal (median -59 dBm across 105 devices).
- ✓ UniFi's built-in WiFi optimisations are all applied.
- ✓ Wireless devices average a 100% experience score.
- ✓ All 5 UniFi devices are online and managed by the controller.
- ✓ UniFi devices install firmware updates automatically.
- ✓ No meshed access points, PoE faults or blocked switch ports.
- ✓ The site uses 4 separate networks.
- ✓ The UniFi Network application is on version 10.6.106 with no update waiting.
- ✓ Country and time zone are set correctly for the UK.
- ✓ Even the busiest hour of the last 7 days averaged 75 Mbps, 5% of the line's speed.
- ✓ Average latency over the last 30 days was 10 ms, with no repeated spikes.
- ✓ Intrusion prevention is on at the gateway.
- ✓ Content filtering is on, so known malicious sites are blocked by name.
- ✓ The firewall has 33 custom rules across 8 zones, on top of UniFi's defaults.
- ✓ Intrusion prevention blocked 6 threats in the last 30 days, and has inspected 41 GB.
- ✓ 98% of 97 WiFi connection attempts succeeded in the last 24 hours.
- ✓ We mapped 273 neighbouring WiFi networks. 22 are strong enough to matter.
- ✓ No port errors, slow links or PoE limits found.
- ✓ Firmware is up to date on every device.
- ✓ No device is overloaded or overheating.
- ✓ Every device is supported by this controller version.
- ✓ Every network has plenty of free addresses.
- ✓ Configuration is backed up automatically on the console.

SECURITY

Firewall and network separation

The firewall decides which of your networks can talk to each other. UniFi groups networks into zones and sets a rule for each pair. This is how yours is set up now, and what we suggest.

Your networks

Network	Purpose	Firewall Zone	VLAN	Address Pool	Devices Now
Staff	Standard	Internal	untagged	176 addresses	31
Café Devices	Standard	IoT	20	176 addresses	98
Remote access	Remote access VPN	VPN	untagged	253 addresses	0
Office	Standard	Office	30	176 addresses	3
Guest	Guest	Guest (Hotspot)	50	249 addresses	3

Who can start a connection to whom

From ↓ To →	Internal	Internet	VPN	Guest (Hotspot)	IoT	Office
Internal Staff	Allowed	Allowed 2 exceptions	Allowed	Allowed	Allowed	Blocked
Internet	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked
VPN Remote access	Blocked 1 exception	Allowed	Allowed	Allowed	Blocked 1 exception	Blocked
Guest (Hotspot) Guest	Blocked	Allowed 1 exception	Blocked	Blocked	Blocked	Blocked
IoT Café Devices	Blocked 13 exceptions	Allowed 2 exceptions	Blocked	Blocked	Blocked	Blocked
Office Office	Blocked 4 exceptions	Allowed 1 exception	Blocked	Blocked	Blocked 1 exception	Blocked

Read each row across: it shows where a connection starts. Replies to an allowed connection always get back. Exceptions are narrower rules for particular devices or services, and we review each one during a fix.

Suggested firewall setup

Rule	Suggested	Now
Internet → Internal, VPN, Guest (Hotspot), IoT, Office Nothing on the internet should be able to start a connection into the site.	Block	Blocked In place
Guest (Hotspot) → Internal, VPN, IoT, Office Guests should reach the internet and nothing else.	Block	Blocked In place
IoT → Internal, VPN, Guest (Hotspot), Office Devices in their own zone should not be able to start connections to your other networks.	Block	Blocked (exceptions: 13 to Internal) Review exceptions
Office → Internal, VPN, Guest (Hotspot), IoT Devices in their own zone should not be able to start connections to your other networks.	Block	Blocked (exceptions: 4 to Internal, 1 to IoT) Review exceptions

HOW WE CAN HELP

Let's get this sorted

11 findings

Fix it remotely

We make the changes for you over a remote session, and confirm the time and cost before any work starts.

- 6 IP address conflicts logged
- The internet connection went down 4 times in the last 30 days, between 1 and 2 October
- "Café Devices" uses WPA2 only
- Café AP (2.4 GHz) channel is 52% busy
- Terrace AP (2.4 GHz) channel is 68% busy
- and 6 more

1 finding

Site visit

For work that needs hands on the equipment. £75 for the first hour including travel, then £25 for each extra 30 minutes.

- Terrace AP is resending 27% of its WiFi traffic

1 finding

Bigger changes

New equipment or a change to how the network is laid out. We will quote for it, with options.

- Café AP served 102 devices at its busiest hour

KEEP IT HEALTHY

Remote Network Monitoring & Support

A health check shows the network on one day. Monitoring keeps an eye on it every day after that. It starts once any agreed fixes are done and we have recorded the network as a supported baseline.

- ✓ We watch your UniFi network continuously through UniFi Site Manager and Alarm Manager, and look into every alert.
- ✓ Firmware is kept up to date in a quiet-hours window agreed with you.
- ✓ You get a monthly health summary.
- ✓ Cancel any time. You stay the owner of your UniFi console.

For your network, monitoring would keep watch on internet outages and WiFi quality.

£25

per month

£25/month, cancel any time

Guest WiFi sign-in page

You already run a guest WiFi network. We can add a sign-in page in your branding that asks guests for marketing consent properly before they join, and lets you export the guests who opted in. On a UniFi network installed by someone else, setup is £250, then £19/month for hosting. £29/month includes network monitoring as well.

Ready to get this sorted?

Reply to this report or get in touch, and we will take it from there.

Call or WhatsApp **07432 214653**

Email **info@netintellect.co.uk**

THE DETAIL

Internet and gateway

Example Broadband

Provider

1600 / 115 Mbps

Plan speed

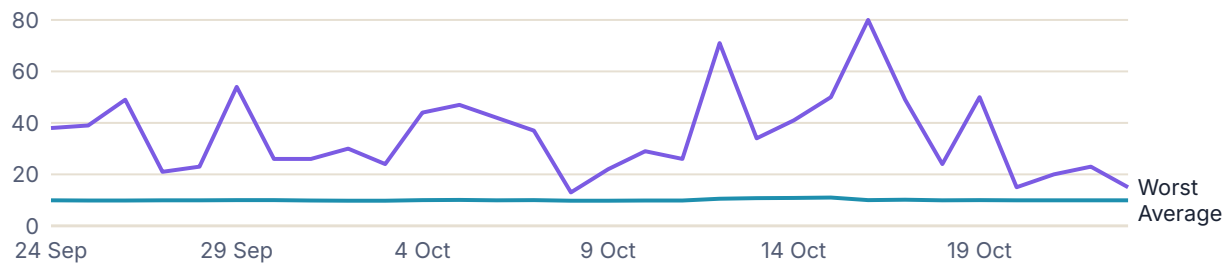
100.00%

Availability, 24 h

Healthy

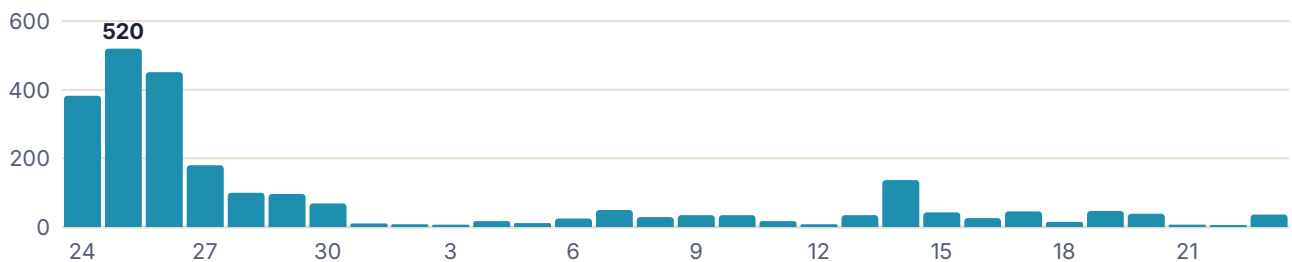
Status now

Latency, last 30 days (ms)



Lower is better. Under 30 ms feels instant; spikes above 100 ms are felt on calls.

Internet data used per day, last 30 days (GB)



2.5 TB in total. The busiest day was Friday 25 September.

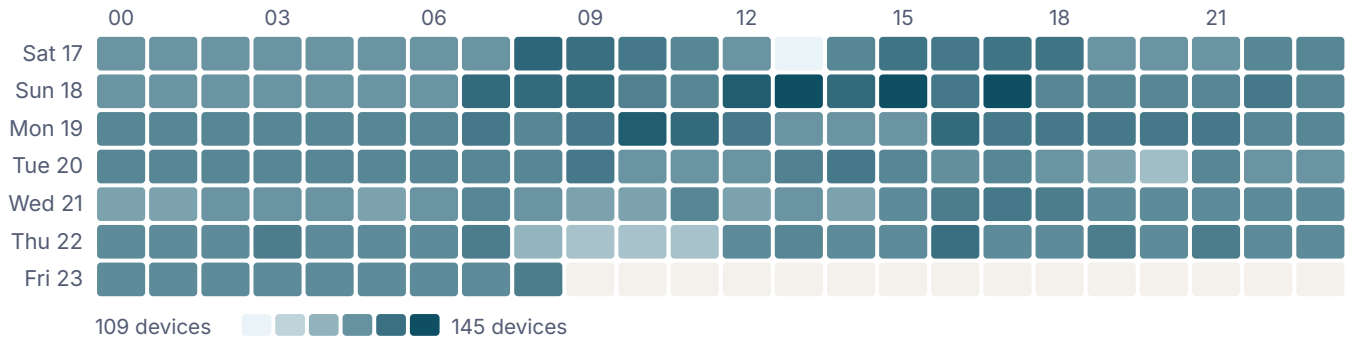
Recent speed tests

WHEN	DOWNLOAD	UPLOAD	LATENCY	AGAINST THE PLAN
28 Sep 06:25	896 Mbps	119 Mbps	10 ms	56% of download
5 Oct 06:25	761 Mbps	116 Mbps	9 ms	48% of download
12 Oct 06:25	1265 Mbps	119 Mbps	10 ms	79% of download
19 Oct 06:25	1325 Mbps	118 Mbps	10 ms	83% of download

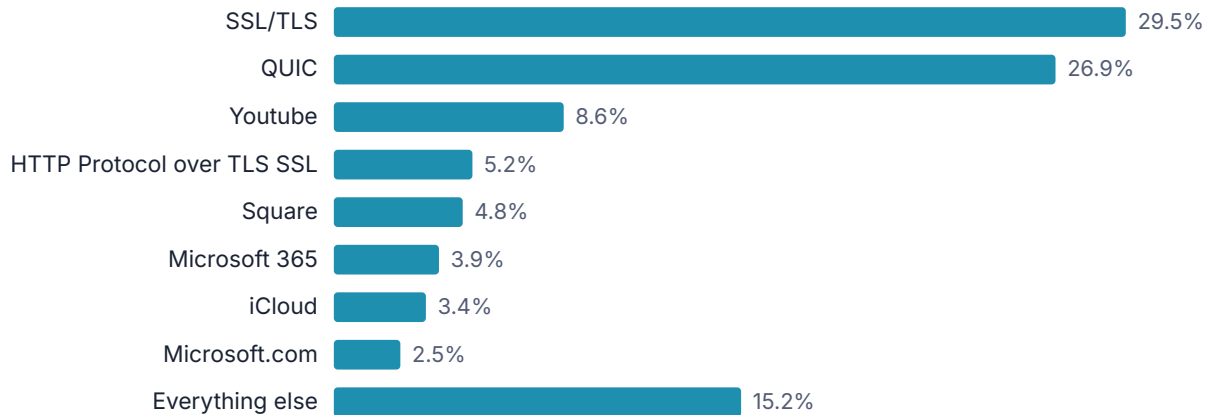
The gateway's busiest day used 27% of its processor and 73% of its memory, so it has room to spare.

How the network is used

When the network is busiest: devices connected by hour, last 7 days



Top traffic types, last 7 days (share of identified traffic)



96% of traffic was not recognised by the gateway and is left out. Encrypted traffic is shown by protocol where the gateway cannot see the application.

THE DETAIL

WiFi

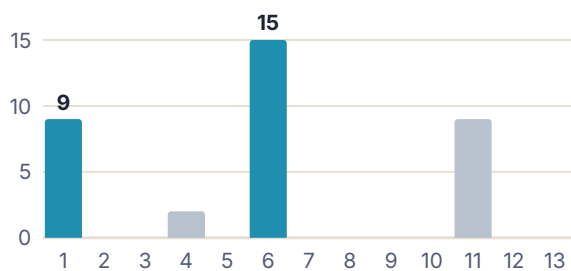
WiFi networks

NETWORK	SECURITY	BANDS	GUEST	CLIENT ISOLATION	ROAMING HELP (11V)	FAST ROAMING (11R)
Staff	WPA3	6 GHz, 5 GHz, 2.4 GHz	No	No	Yes	No
Café Devices	WPA2	2.4 GHz, 5 GHz	No	No	No	No
Tills	WPA2/WPA3	2.4 GHz, 5 GHz	No	Yes	Yes	No
Café Guest WiFi	Open (Enhanced Open)	2.4 GHz, 5 GHz	Yes	Yes	Yes	No

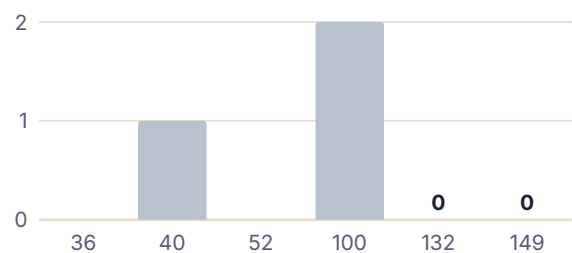
Access points

ACCESS POINT	BAND	CHANNEL	WIDTH	CHANNEL BUSY	CLIENTS	AVG SIGNAL	RETRIES
Café AP	2.4 GHz	6	20 MHz	52%	54	-50 dBm	6%
Café AP	5 GHz	149	80 MHz	2%	24	-63 dBm	7%
Café AP	6 GHz	37	160 MHz	1%	12	-62 dBm	8%
Terrace AP	2.4 GHz	1	20 MHz	68%	9	-65 dBm	17%
Terrace AP	5 GHz	132	80 MHz	3%	6	-76 dBm	28%

Neighbouring networks per 2.4 GHz channel

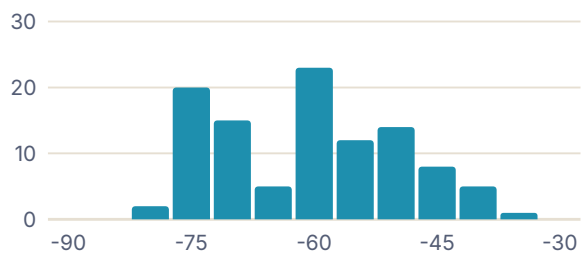


Neighbouring networks per 5 GHz channel



Blue bars are the channels your access points use. Fewer neighbours on a channel means more airtime for you. Only networks stronger than -80 dBm are counted.

Signal strength of WiFi devices (dBm)



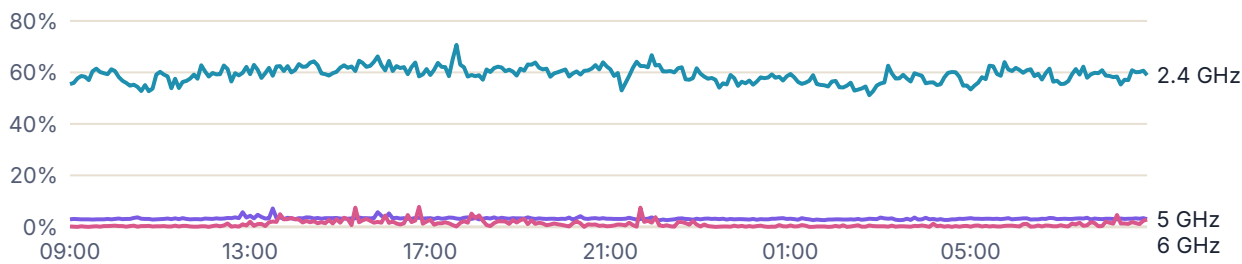
105 devices. Right is stronger; below -75 dBm is weak.

Which band WiFi devices use



36 of 105 devices support WiFi 6 or newer.

How busy each band's channels were, last 24 hours (%)

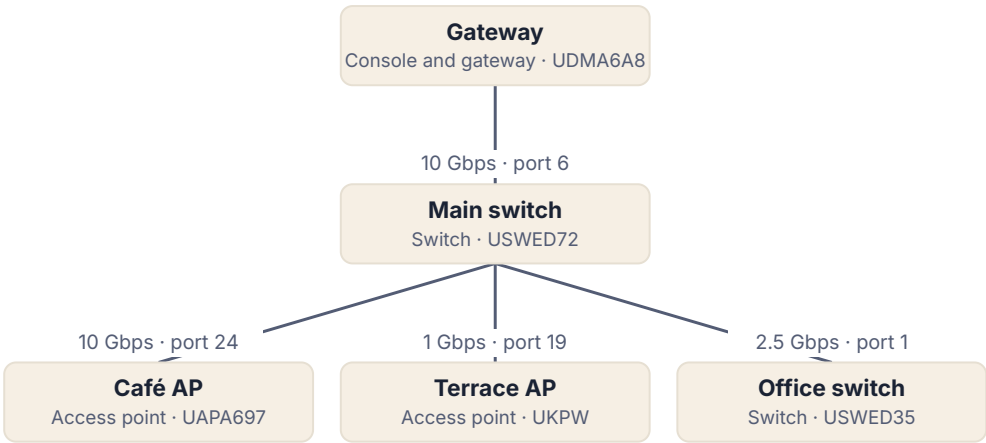


WiFi connection attempts, last 24 hours

BAND	ATTEMPTS	JOINED	AUTHENTICATED	GOT AN ADDRESS	DNS WORKING	FAILED
2.4 GHz	59	100%	100%	100%	100%	0
5 GHz	17	100%	100%	100%	86%	1
6 GHz	21	100%	100%	100%	100%	0

Devices and switching

How your UniFi devices connect



Device inventory

DEVICE	MODEL	FIRMWARE	SUPPORT	STATUS	UPTIME	CPU	MEMORY	TEMP
Gateway Console and gateway	UDMA6A8	5.1.33.34087	Current	Online	15 days	27%	72%	
Café AP Access point	UAPA697	8.7.11.19419	Current	Online	20 days	5%	33%	
Terrace AP Access point	UKPW	8.7.11.19419	Current	Online	46 days	2%	83%	
Main switch Switch	USWED72	7.5.15.17146	Current	Online	43 days	6%	16%	52 °C
Office switch Switch	USWED35	2.1.8.971	Current	Online	377 days	6%	77%	

Main switch: 15 of 28 ports in use, PoE 36 W of 600 W

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2.5G	1G	100M	1G	100M	—	—	—	—	—	—	—	1G	2.5G	2.5G	2.5G
17	18	19	20	21	22	23	24	25	26	27	28				
—	100M	1G	—	1G	—	10G	10G	—	—	—	10G				

Office switch: 4 of 5 ports in use

1	2	3	4	5
2.5G	2.5G	2.5G	—	2.5G

Port colours: green 1 Gbps or faster, amber below 1 Gbps, red errors or half duplex, grey nothing connected.

THE DETAIL

Security settings

Intrusion prevention	Blocks threats	Threats blocked, 30 days	6
Traffic inspected	41 GB	UPnP	Off
Ports open to the internet	0	Device SSH	Off
SNMP	Off	Ad blocking	Off
Content filtering (DNS)	On	Encrypted DNS (DoH)	Off
Country blocking	On	Remote access VPN	On
UniFi Teleport	Off	Firewall	8 zones, 33 custom rules
Connections blocked, 24 h	995 of 159,921	Automatic device updates	On
Honeypot	Off		

Green: as it should be. Coral: worth reviewing. Grey: a choice that depends on how the site is used.

THE DETAIL

Event log, last 30 days

8,022 Events, 30 days	19 High severity	1056 Security	428 Admin activity
---	--	---	--

Notable events

Everyday device joins and VPN logins are left out.

SEVERITY	EVENT	TIMES
Very high	Threat blocked by intrusion prevention	5
Very high	Internet connection failed	3
Very high	Internet connection failed repeatedly	2
High	Two devices claimed the same IP address	6
High	Switch port kept toggling loop protection	1
High	Threat blocked by intrusion prevention	1

SEVERITY	EVENT	TIMES
High	Device unreachable	1
Medium	Traffic blocked by the firewall	1049
Medium	Administrator signed in	285
Medium	A setting was changed	55

APPENDIX A

Every check we ran

Every device online and managed	Pass	Device hardware: mesh links, PoE faults and loop protection	Pass
Firmware current, no end-of-life models	Pass	Double NAT, line quality and speed against the plan	Pass
Controller software up to date	Pass	Latency over the last 30 days	Pass
Automatic backups	Pass	WiFi connection success rate	Pass
Internet status, availability, latency and drops	Pass	WiFi retransmissions per access point	Issues found
UPnP off	Pass	UniFi's own optimisation suggestions	Pass
Intrusion detection and prevention	Pass	Access points moved off their set channel (radar)	Issues found
Ports open to the internet	Pass	Neighbouring WiFi networks on our channels	Issues found
Automatic device updates	Pass	Client mix: bands, WiFi generations and experience	Issues found
Content filtering	Pass	Roaming assistance where there are several access points	Issues found
Busiest-hour load per access point	Issues found	Address pools large enough for the devices	Pass
Busiest-hour internet use against the line speed	Pass	Regional, time and monitoring settings	Pass
Device SSH access	Pass	Firewall rules in use	Pass
Port errors, duplex, slow uplinks and PoE budget	Pass	Firewall zones keep guests and devices apart	Pass
Device load and temperature	Pass	Threats seen by intrusion prevention	Pass
WiFi security, guest separation and SSID count	Issues found	Event log: outages, conflicts and loops (30 days)	Issues found
Channel plan, width and utilisation	Issues found	Unsupported devices	Pass
Client signal strength	Pass		
Network separation	Pass		

APPENDIX B

How we score

Each area starts at 100. An Act now finding takes off 30 points, Plan next 10 and Monitor 3. The overall score is the average of the areas we could check, and any Act now finding holds it below 70. Grades: A 90 and above, B 75 to 89, C 60 to 74, D 40 to 59, E below 40. Checks that could not run are listed as limitations and never counted as passes.

APPENDIX C

Glossary

Access point (AP)

The device on the wall or ceiling that broadcasts WiFi.

Channel

A slice of a band. Access points on the same channel take turns, so a good plan spreads them out.

dBm

Signal strength. Closer to zero is stronger: -50 is excellent, -67 is good for calls, below -75 is weak.

Retries

Data the access point had to send again because it was not received. High retries mean weak signal or interference.

PoE

Power over Ethernet: the network cable also powers the access point or camera.

IDS / IPS

Intrusion detection / prevention: the gateway checks traffic against known attacks and blocks matches.

DFS

5 GHz channels shared with radar. An access point must leave them when it detects radar.

Band

WiFi runs in three radio bands: 2.4 GHz (longest range, slowest, most crowded), 5 GHz (faster) and 6 GHz (fastest, newest devices only).

Channel utilisation

How much of the time a channel is busy. Above about 50% devices start waiting to transmit.

Latency

The time a message takes to reach the internet and come back. Under 30 ms feels instant.

VLAN

A separate network running over the same cables, used to keep guests, staff and devices apart.

UPnP

A feature that lets devices open ports to the internet on their own.

Double NAT

Two routers in a row, usually the ISP's router plus yours. It can break calls, VPNs and remote access.

Firmware

The software inside each UniFi device. Updates fix security issues and faults.

Scope and limitations

No configuration changes were made during this review. The findings are based on information visible remotely in the UniFi controller at the time shown above, including the history the controller keeps. This review did not include an on-site survey, RF heatmap, physical cabling inspection, ISP fault ownership, emergency response, a penetration test, a major redesign, a documentation pack, non-UniFi estate review, remediation or ongoing monitoring. A physical fault or intermittent condition may need further investigation on site. UniFi renames menus between versions, so the "Where in UniFi" hints name the area to look in, and the exact screen may differ.

One email clarification about this report is included. Remediation and site work are separate and will not begin without approval.

Access closeout

Temporary access was removed by the customer on 23 October 2026. No customer password, recovery code or API key is recorded in this report.