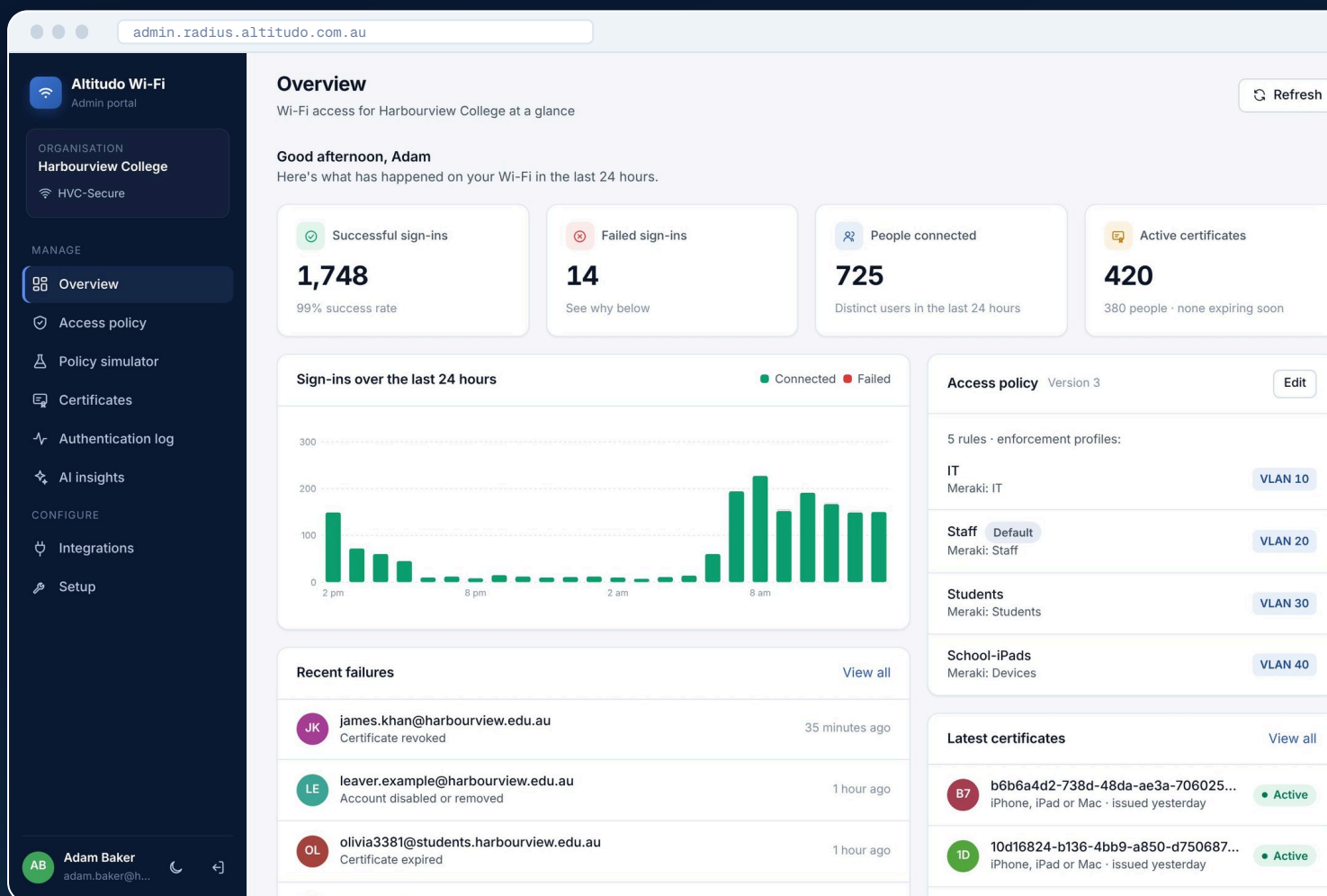


SECURE SCHOOL WI-FI, WITHOUT THE PASSWORDS

Wi-Fi that just works. Secure by design.

Staff and students sign in once with their school account. Every device gets its own certificate, lands on the right network and stays connected. No Wi-Fi passwords to share, reset or leak, and no servers in your comms room.



Hosted in Australia

AWS Sydney and Melbourne, so school data stays onshore.

Fully managed

Run, patched and monitored around the clock by Altitude.

Works with what you have

Microsoft 365, Intune, Jamf, Cisco Meraki, Aruba and Palo Alto Networks.

WHY SCHOOLS ARE MOVING

Shared passwords and on-premises servers are holding your Wi-Fi back

Most school Wi-Fi still relies on a shared password or an ageing Windows NPS server. Both create work for IT and risk for the school. Altitude Cloud RADIUS replaces them with certificate-based sign-in, run for you in the cloud.

THE WAY IT IS TODAY

- ✗ Passwords shared on whiteboards, in emails and with former students
- ✗ A password change breaks every device at once, and the help desk queue fills
- ✗ NPS servers to patch, back up and keep alive, tied to on-premises Active Directory
- ✗ No clear view of who is on the network, or why someone can't connect
- ✗ Leavers keep Wi-Fi access until someone remembers to change the password

WITH ALTITUDE CLOUD RADIUS

- ✓ **No Wi-Fi passwords.** Each device proves who it is with its own certificate (EAP-TLS).
- ✓ **Set up in about two minutes** by the user, or automatically through Intune or Jamf.
- ✓ **Nothing to host.** Two Australian regions, patched and monitored around the clock.
- ✓ **Microsoft Entra ID groups** decide who gets which network, with no AD dependency.
- ✓ **Leavers are cut off automatically** the moment their account is disabled.

0

Wi-Fi passwords to share, reset or leak

2 min

for a person to set up a new device

99.9%

availability target, across Sydney and Melbourne

<0.5 s

typical sign-in, every time

BUILT AROUND CONFIDENTIALITY, INTEGRITY AND AVAILABILITY



Confidentiality

Only the right people and school devices get on, each with their own certificate. Signing keys are protected in hardware security modules.



Integrity

Every sign-in, policy change and revocation is recorded. Changes are tested and versioned, and you can see exactly who changed what.



Availability

Multiple servers in Sydney and Melbourne. If one fails, access points move to the next with no one noticing. Updates without downtime.

HOW IT WORKS

Sign in once. Connected for the year.

People set up their own devices from a simple sign-up page, using the school account and multi-factor sign-in they already have. School-owned devices are set up automatically through Intune or Jamf.

1

Open the school's Wi-Fi link

Staff and students open the link on the device they want to connect: iPhone, iPad, Mac, Windows, Android or Chromebook.

2

Sign in with the school account

The usual Microsoft 365 sign-in, with the school's MFA and Conditional Access. Nobody types a Wi-Fi password, and Altitude never sees one.

3

Install, and you're on

One tap installs a personal certificate and the Wi-Fi settings. The device joins the secure network on its own, today and every day after.

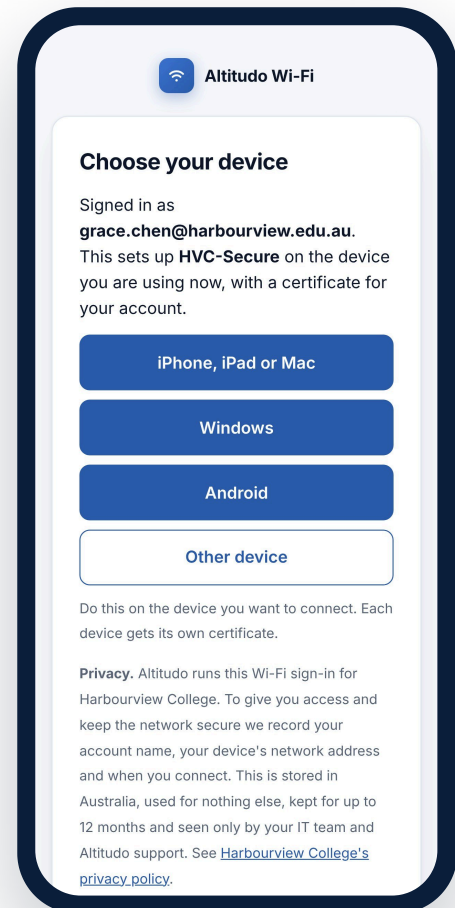
4

On the right network, automatically

Your access policy puts staff, students, IT and school iPads on their own VLANs and firewall rules, based on Entra ID groups, device type, time of day and more.

SCHOOL-OWNED DEVICES

Intune and Jamf install certificates silently on managed laptops and iPads. No sign-up page, no user action, and the certificate renews itself.



The sign-up page, after the school sign-in

YOUR ADMIN PORTAL

Everything your IT team needs, on one screen

Your IT team signs in with their own school accounts. The overview shows how Wi-Fi is doing right now, and every page is written in plain English, not error codes.



At a glance

Successful and failed sign-ins, people connected and certificates in use, for the last 24 hours.



Failures explained

"Certificate revoked", "account disabled", "certificate expired": you see the reason, not a code.



One-click revoke

Lost phone or stolen laptop? Revoke its certificate and it is refused within minutes, everywhere.

Altitude Wi-Fi

Admin portal

ORGANISATION

Harbourview College

HVC-Secure

MANAGE

Overview

Access policy

Policy simulator

Certificates

Authentication log

AI insights

CONFIGURE

Integrations

Setup

Adam Baker

adam.baker@h...

admin.radius.altitudo.com.au/certificates

Certificates

Certificates issued to people's devices through the Wi-Fi sign-up page

Export CSV

Sign-up link

Search people or serial numbers

Active 420

Revoked 1

Expired 0

All 421

420 people with active certificates

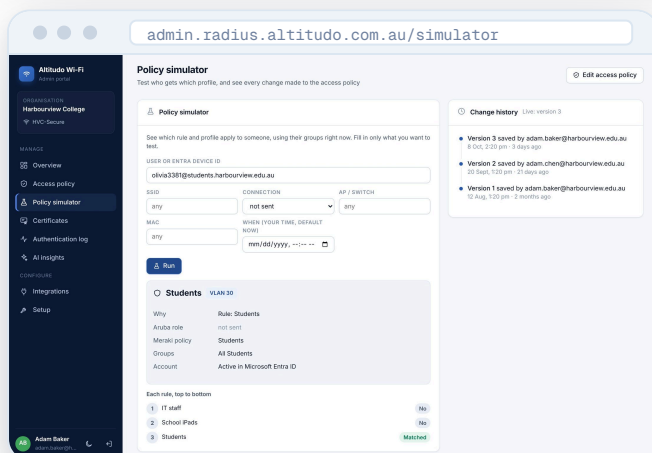
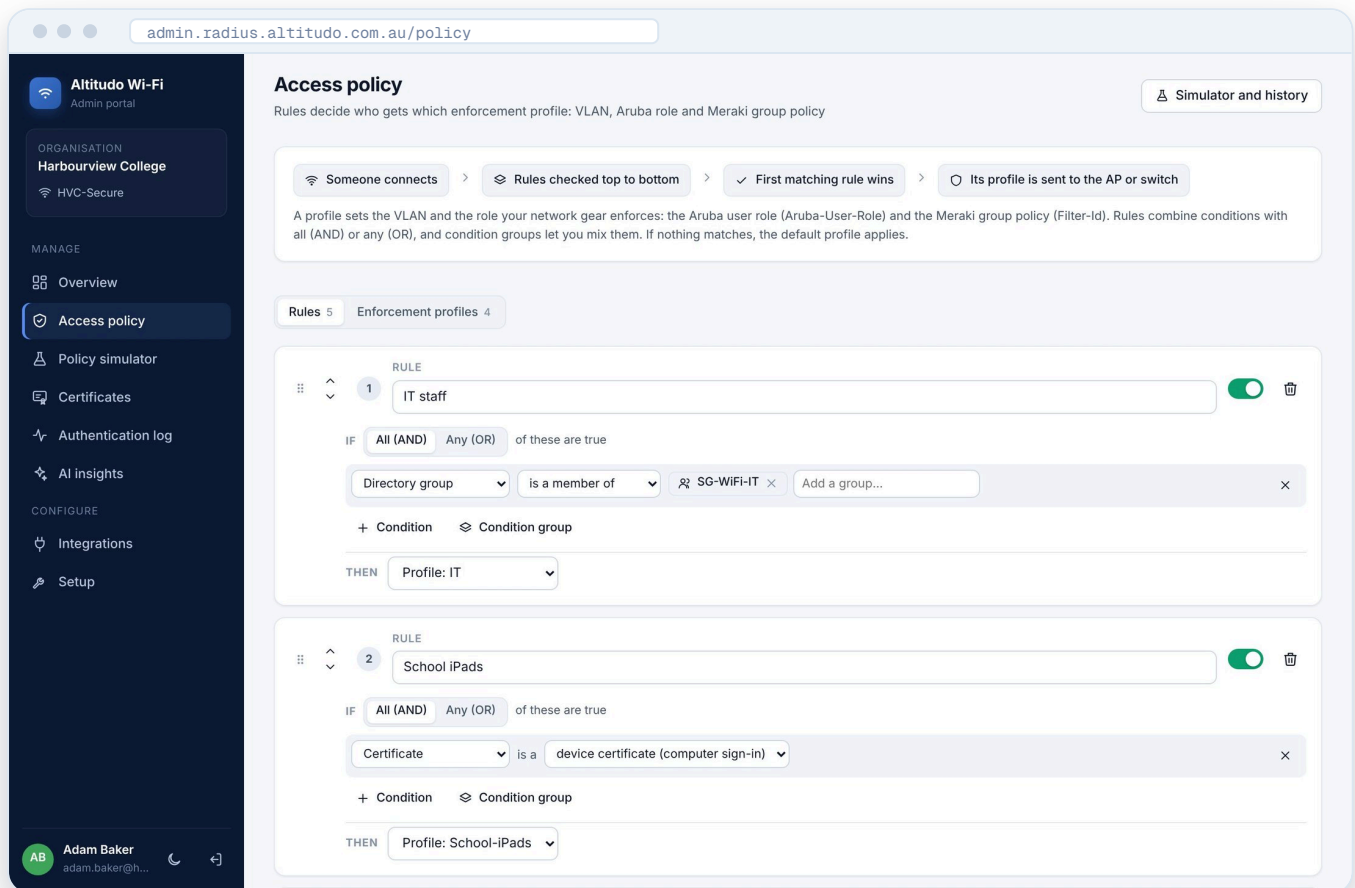
PERSON	DEVICE	ISSUED	EXPIRES	STATUS
B7 b6b6a4d2-738d-48da-ae3a-7060250bc6e7 Serial 14108444d42cc...	iPhone, iPad or Mac	10 Oct 2026	10 Oct 2027 in 12 months	Active Revoke
ID 10d16824-b136-4bb9-a850-d750687abf5b Serial d411b9a6ebf3...	iPhone, iPad or Mac	10 Oct 2026	10 Oct 2027 in 12 months	Active Revoke
HC henry.chen@harbourview.edu.au Serial 126c7bc33ba7...	Windows	9 Oct 2026	9 Oct 2027 in 12 months	Active Revoke
IS isla.scott@harbourview.edu.au Serial bf4de2b1f838...	iPhone, iPad or Mac	9 Oct 2026	9 Oct 2027 in 12 months	Active Revoke
SW sophie.walker@harbourview.edu.au Serial 1f4ba4018c02...	Windows	9 Oct 2026	9 Oct 2027 in 12 months	Active Revoke
DA daniel8571@students.harbourview.edu.au Serial e82b60c8cd1b...	iPhone, iPad or Mac	8 Oct 2026	8 Oct 2027 in 12 months	Active Revoke
EM emily7629@students.harbourview.edu.au Serial 72c9b21ce0d8...	iPhone, iPad or Mac	7 Oct 2026	7 Oct 2027 in 12 months	Active Revoke
OB 0fab53e5-4aa2-4df7-a1b9-bb1ff43cc03a Serial fb48436d415c...	iPhone, iPad or Mac	7 Oct 2026	7 Oct 2027 in 12 months	Active Revoke
HB henry.brown@harbourview.edu.au Serial 5ff4c5c04ecd...	iPhone, iPad or Mac	7 Oct 2026	7 Oct 2027 in 12 months	Active Revoke
JW jack.wilson@harbourview.edu.au Serial 8b2612347b19...	Windows	6 Oct 2026	6 Oct 2027 in 12 months	Active Revoke
DA daniel6467@students.harbourview.edu.au Serial 6bd5d98c001f...	iPhone, iPad or Mac	6 Oct 2026	6 Oct 2027 in 12 months	Active Revoke

Certificates: every certificate issued through the sign-up page, with search, export and revoke

ACCESS POLICY

The right people on the right network

Build rules the way you think about your school: IT staff on the IT VLAN, students on the student network during school hours, school iPads on their own. Drag to reorder, test before you save, and every change is versioned.



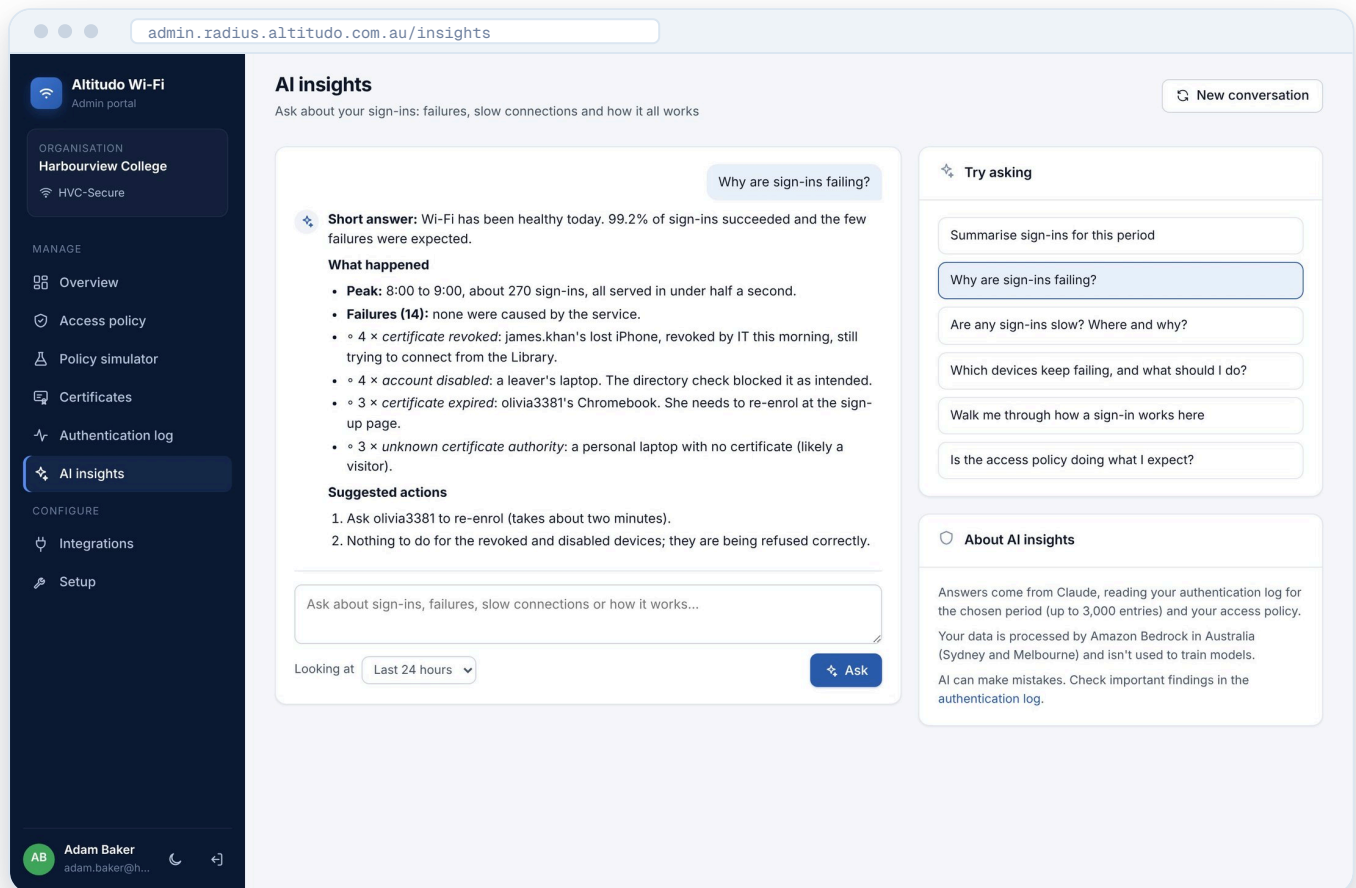
Rules you can read

- ✓ Entra ID groups, user domain, device or user certificate
- ✓ SSID, wired or wireless, access point or switch, MAC address
- ✓ Time of day and day of week, in your time zone
- ✓ VLAN, Meraki group policy and Aruba role sent to the network
- ✓ **Policy simulator:** see which rule a person would match before anything changes

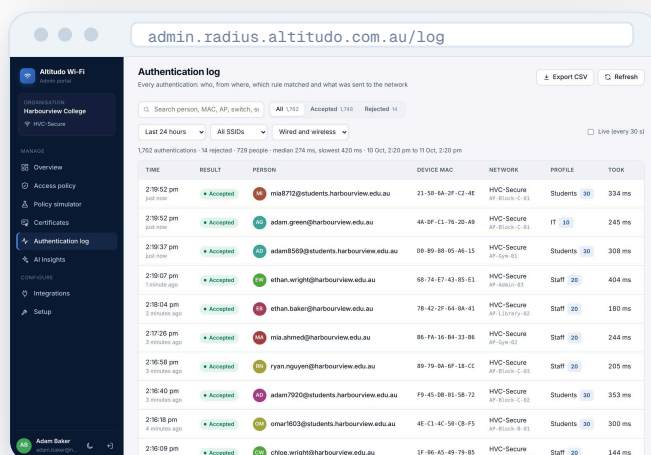
VISIBILITY AND AI INSIGHTS

Answers, not log files

Every sign-in is recorded: who, which device, which access point, which rule matched and how long it took. Ask questions in plain English and get a clear answer with suggested next steps.



The screenshot shows the Altitude Wi-Fi Admin portal interface. On the left is a sidebar with navigation options: Overview, Access policy, Policy simulator, Certificates, Authentication log, AI insights (selected), Integrations, and Setup. The main content area is titled "AI insights" and includes a "New conversation" button. Below this, there's a section "Why are sign-ins failing?" with a "Short answer" stating that Wi-Fi has been healthy today with a 99.2% success rate. It then lists "What happened" with details on peak times, failures (14), and suggested actions like asking a user to re-enrol. A text input field at the bottom allows users to ask questions about sign-ins, failures, or slow connections, with a dropdown for "Looking at" set to "Last 24 hours" and an "Ask" button. To the right, a "Try asking" section provides example prompts like "Summarise sign-ins for this period" and "Why are sign-ins failing?". Below that, an "About AI insights" section explains that answers come from Claude, reading authentication logs and access policies, and that data is processed by Amazon Bedrock in Australia.



The screenshot shows the "Authentication log" interface in the Altitude Wi-Fi Admin portal. It includes a search bar and filters for "All 1702" entries, with "Accepted" and "Rejected" counts. A table lists authentication events with columns for Time, Result, Person, Device MAC, Network, Profile, and Took. The table shows a list of successful sign-ins for various users, including students and staff, with their respective device MACs, networks, and connection times.

TIME	RESULT	PERSON	DEVICE MAC	NETWORK	PROFILE	TOOK
2:18:52 pm	Accepted	mia712@students.harbourview.edu.au	21-16-6A-2F-C2-4E	HVC-Secure AP-Bunch-C-01	Students 30	334 ms
2:18:52 pm	Accepted	adam.green@harbourview.edu.au	4A-8F-C2-76-20-48	HVC-Secure AP-Bunch-C-01	IT 36	245 ms
2:18:37 pm	Accepted	adrian555@students.harbourview.edu.au	08-89-88-85-46-13	HVC-Secure AP-Sign-02	Students 30	308 ms
2:18:07 pm	Accepted	ethan.wright@harbourview.edu.au	68-74-E7-43-85-E1	HVC-Secure AP-Bunch-B1	Staff 20	404 ms
2:18:04 pm	Accepted	ethan.baker@harbourview.edu.au	78-42-2F-64-8A-41	HVC-Secure AP-Bunch-B1	Staff 20	180 ms
2:17:26 pm	Accepted	ms.ahmed@harbourview.edu.au	86-FA-16-84-37-86	HVC-Secure AP-Sign-02	Staff 20	244 ms
2:16:58 pm	Accepted	ryan.nguyen@harbourview.edu.au	49-79-98-6F-18-C2	HVC-Secure AP-Bunch-C-01	Students 30	205 ms
2:16:40 pm	Accepted	adrian7920@students.harbourview.edu.au	F9-43-98-81-58-72	HVC-Secure AP-Bunch-C-02	Students 30	353 ms
2:16:18 pm	Accepted	omar603@students.harbourview.edu.au	4E-C1-4C-58-C8-F3	HVC-Secure AP-Bunch-B-01	Students 30	300 ms
2:16:09 pm	Accepted	choe.wright@harbourview.edu.au	1F-86-A0-49-79-83	HVC-Secure AP-Sign-01	Staff 20	144 ms

Authentication log

“Why can’t Year 9 connect in the gym?”

AI insights reads your sign-in log and access policy and explains what happened, in plain English.

Search every sign-in

Filter by person, device, access point, network or result, and export to CSV for reporting.

Private by default

Processed in Australia on Amazon Bedrock. Your data is never used to train AI models.

WORKS WITH WHAT YOU HAVE

Fits your network, your directory and your firewall

Microsoft Entra ID

Microsoft Intune

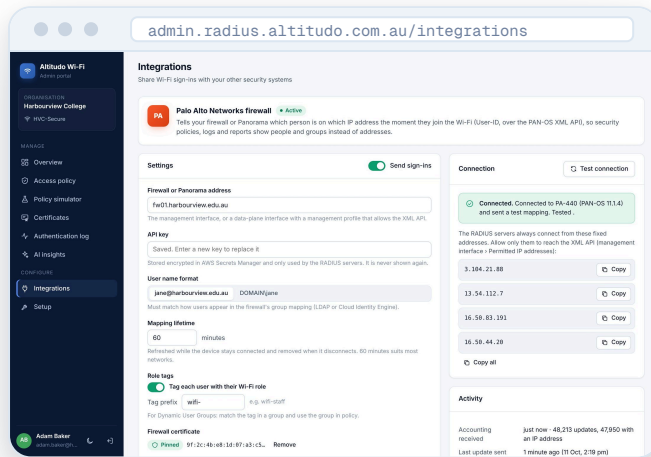
Jamf Pro

Cisco Meraki

HPE Aruba

Palo Alto Networks

Windows, macOS, iOS, Android, ChromeOS



Palo Alto Networks User-ID

The moment someone joins the Wi-Fi, your firewall knows who they are. Security policies, web filtering logs and reports show people and groups instead of IP addresses, with no agents to install.

Meraki and Aruba, encrypted

Access points talk to the service over RadSec (RADIUS over TLS), so sign-in traffic is encrypted all the way to the cloud. No VPN, no on-site server.

SECURITY AND COMPLIANCE

Built for the way schools are audited

- ✓ **Australian data.** Everything stays in AWS Sydney and Melbourne.
- ✓ **Privacy Act and APPs.** A clear collection notice for staff and students, and minimal data.
- ✓ **Essential Eight.** Supports the MFA, patching and restricted admin privilege strategies.
- ✓ **Safer Technologies 4 Schools (ST4S).** Designed with the ST4S criteria in mind.
- ✓ **Hardware-protected keys.** Certificate authority keys live in AWS KMS (FIPS 140 validated HSMs).
- ✓ **Continuous monitoring.** Threat detection, vulnerability scanning and alerts, 24x7.
- ✓ **Full audit trail.** Sign-ins and admin actions kept for 12 months.
- ✓ **Zero-downtime updates.** Servers are patched monthly without dropping a connection.

WHAT YOU GET

A fully managed service, set up for you

CLOUD RADIUS SERVICE

Run for you, every day

One subscription, no per-user licences

- ✓ Sydney and Melbourne, 99.9% availability target
- ✓ Admin portal, access policy and AI insights
- ✓ Unlimited certificates and sign-ins
- ✓ 24x7 monitoring, patching and support

IMPLEMENTATION

Done with your team

Typically live within 4 to 6 weeks

- ✓ Design workshop and access policy
- ✓ Entra ID, Intune and Jamf set-up
- ✓ Meraki or Aruba configuration
- ✓ Palo Alto Networks User-ID included
- ✓ Pilot, staff rollout and NPS retirement

How it compares

	ALTITUDO CLOUD RADIUS	WINDOWS NPS ON SITE	SHARED WI-FI PASSWORD
Passwords	None, a certificate per device	Usually user passwords	One password for everyone
Servers to run	None, fully managed	Two or more to patch and back up	None
Leavers	Blocked automatically	Depends on AD clean-up	Until the password changes
Visibility	Portal, log and AI insights	Windows event logs	None
Resilience	Two Australian regions	Your server room	Not applicable

NEXT STEP

See it working at your school

Book a 30-minute demonstration. We will show the sign-up on your own devices, walk through the admin portal and map out how you would move off NPS or shared passwords.



sales@altitudo.com.au

02 8660 1544

altitudo.com.au/service/cloud-radius