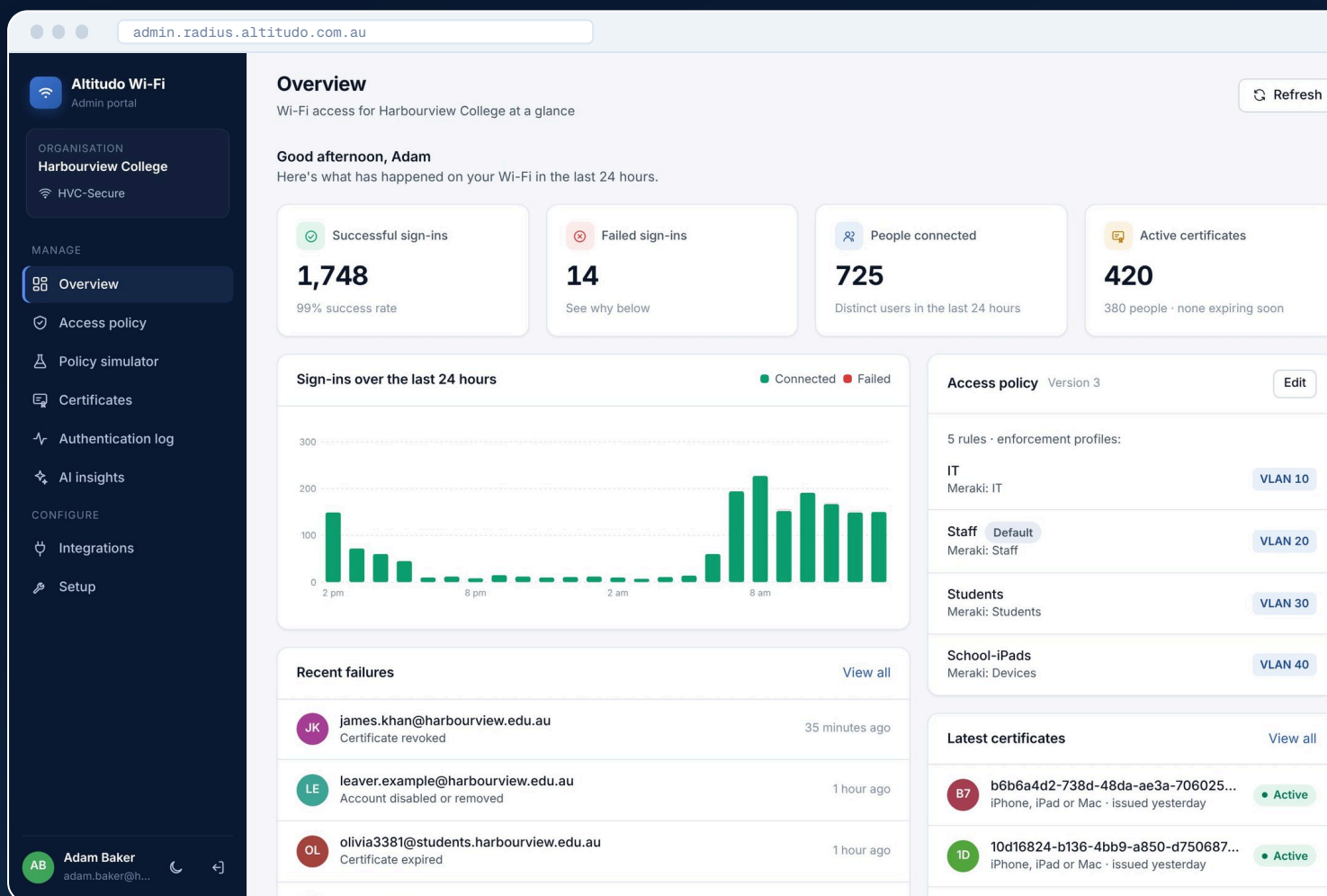


SECURE BUSINESS WI-FI, WITHOUT THE PASSWORDS

# Wi-Fi that just works. Secure by design.

Your people sign in once with their work 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 your 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 ORGANISATIONS ARE MOVING

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

Most office Wi-Fi still relies on a shared password or an ageing Windows NPS server. Both create work for IT and risk for the business. 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 contractors and former staff
- ✗ 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 company 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

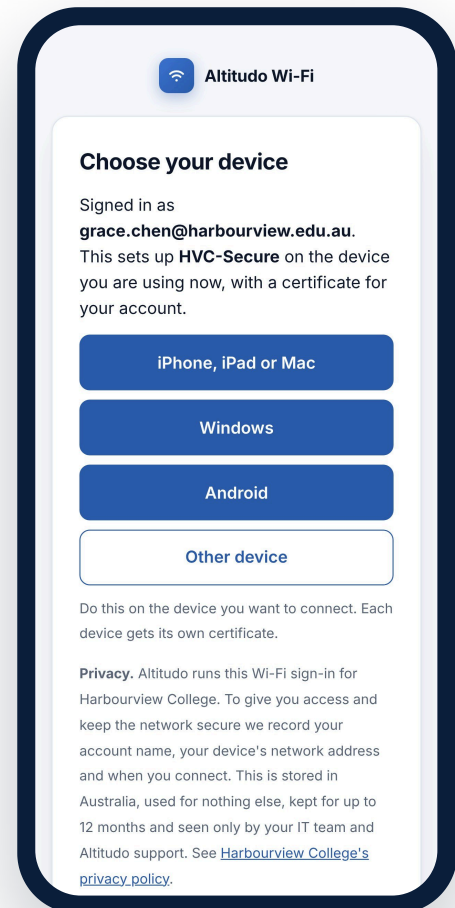
# Sign in once. Connected for the year.

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

- 1 Open your Wi-Fi sign-up link**  
 Staff open the link on the device they want to connect: iPhone, iPad, Mac, Windows, Android or Chromebook.
- 2 Sign in with the work account**  
 The usual Microsoft 365 sign-in, with your 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, IT, finance and shared devices on their own VLANs and firewall rules, based on Entra ID groups, device type, time of day and more.

## COMPANY-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 Microsoft 365 sign-in

## YOUR ADMIN PORTAL

# Everything your IT team needs, on one screen

Your IT team signs in with their own work 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...

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

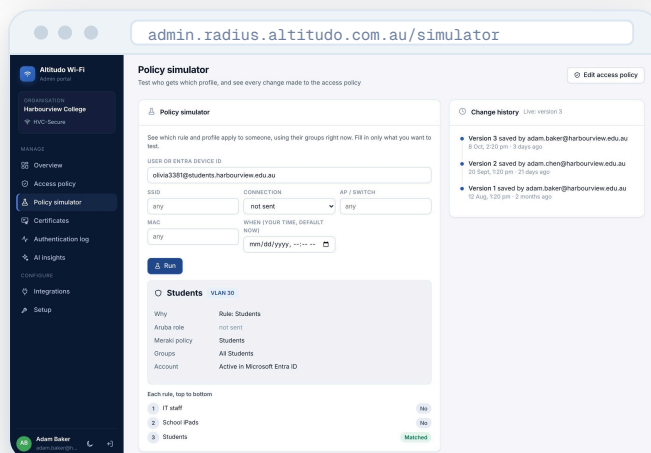
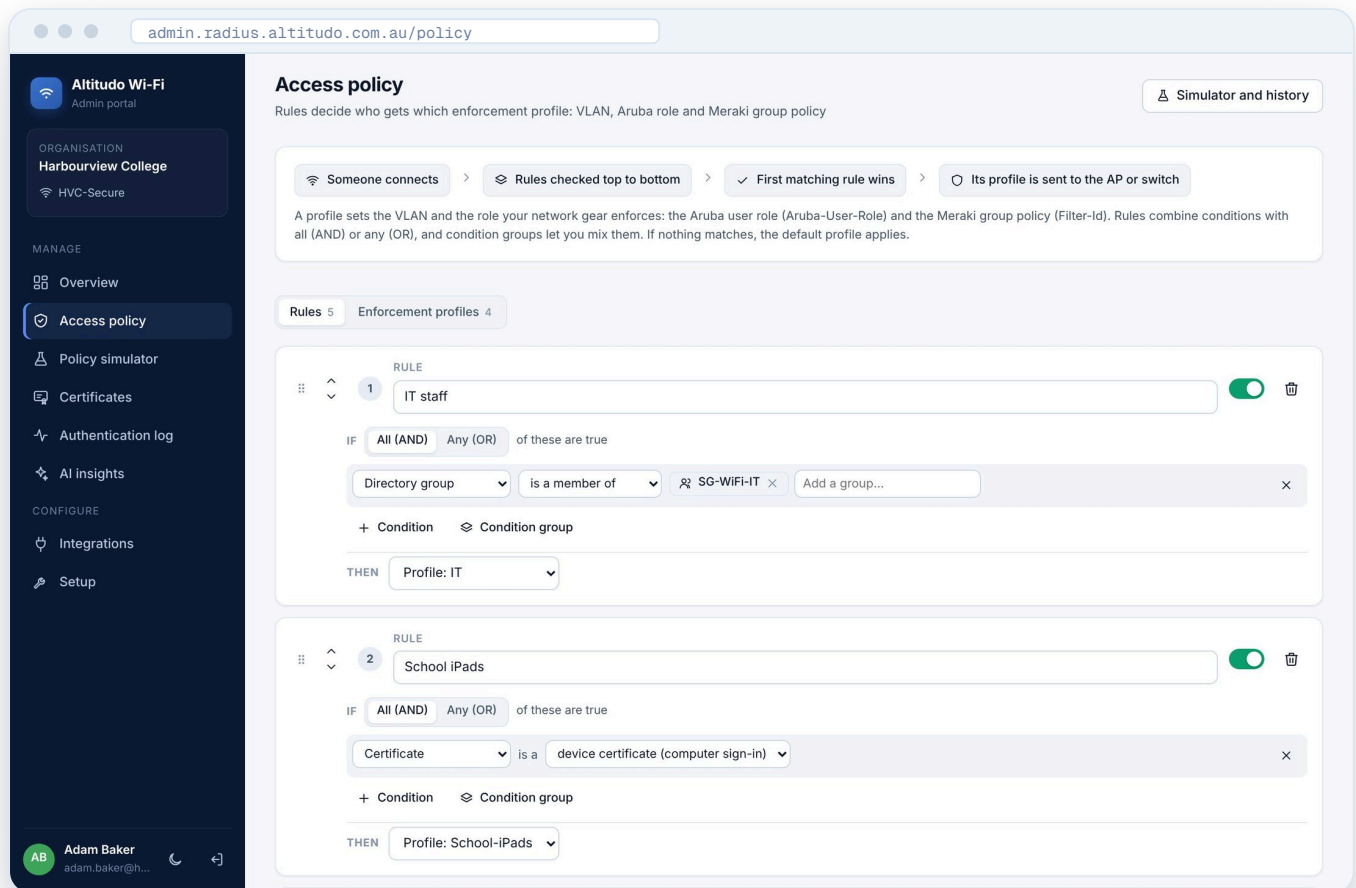
| PERSON                                                           | DEVICE              | ISSUED      | EXPIRES                     | STATUS |
|------------------------------------------------------------------|---------------------|-------------|-----------------------------|--------|
| b6b6a4d2-738d-48da-ae3a-7060250bc6e7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

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 business: IT on the IT VLAN, contractors on a limited network during business hours, meeting-room devices on their own. Drag to reorder, test before you save, and every change is versioned.



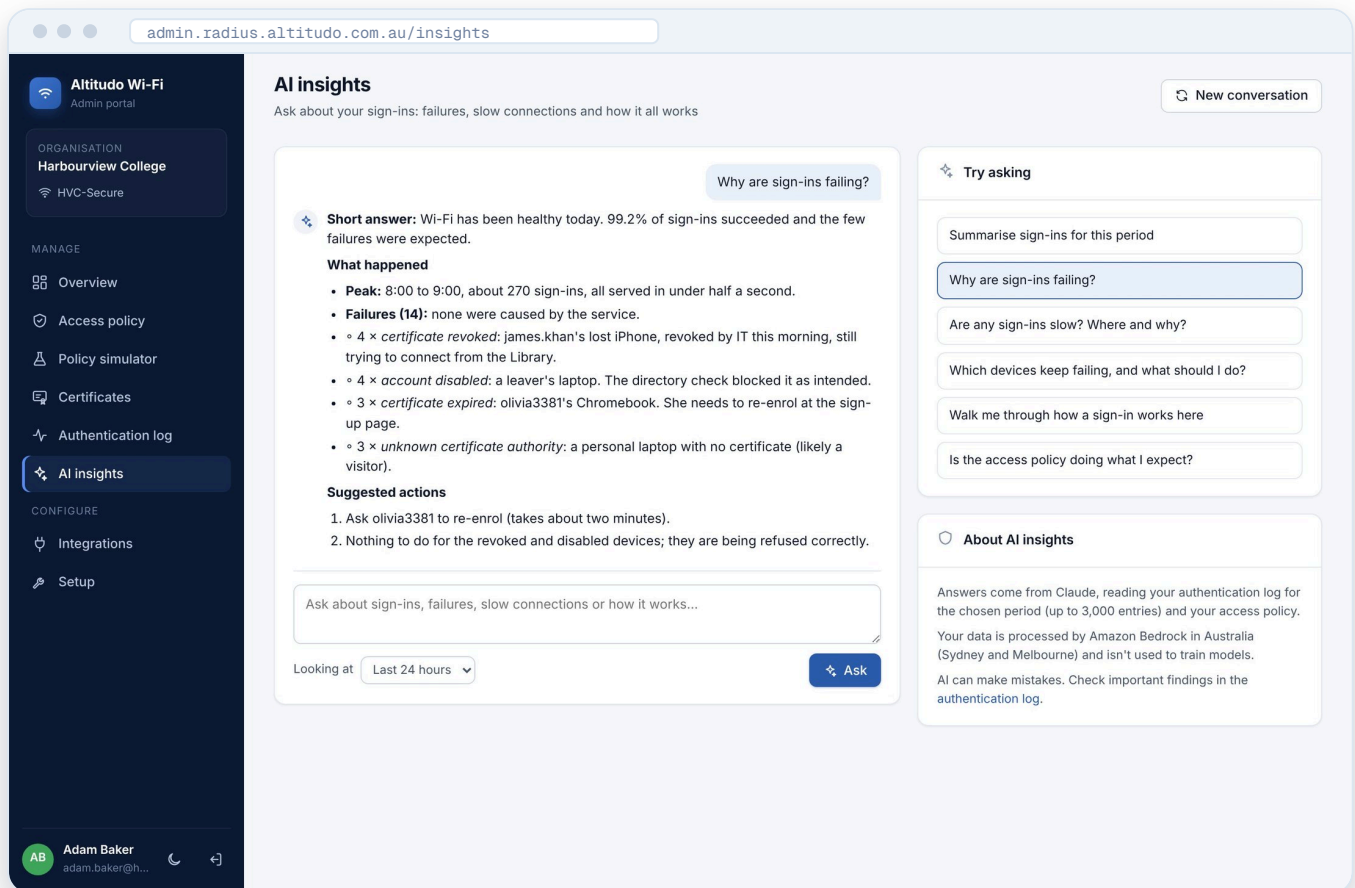
## Rules you can read

- ✓ 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.



**AI insights**

Ask about your sign-ins: failures, slow connections and how it all works

**Why are sign-ins failing?**

**Short answer:** Wi-Fi has been healthy today. 99.2% of sign-ins succeeded and the few failures were expected.

**What happened**

- **Peak:** 8:00 to 9:00, about 270 sign-ins, all served in under half a second.
- **Failures (14):** none were caused by the service.
- 4 × **certificate revoked:** james.khan's lost iPhone, revoked by IT this morning, still trying to connect from the Library.
- 4 × **account disabled:** a leaver's laptop. The directory check blocked it as intended.
- 3 × **certificate expired:** olivia3381's Chromebook. She needs to re-enrol at the sign-up page.
- 3 × **unknown certificate authority:** a personal laptop with no certificate (likely a visitor).

**Suggested actions**

1. Ask olivia3381 to re-enrol (takes about two minutes).
2. Nothing to do for the revoked and disabled devices; they are being refused correctly.

Ask about sign-ins, failures, slow connections or how it works...

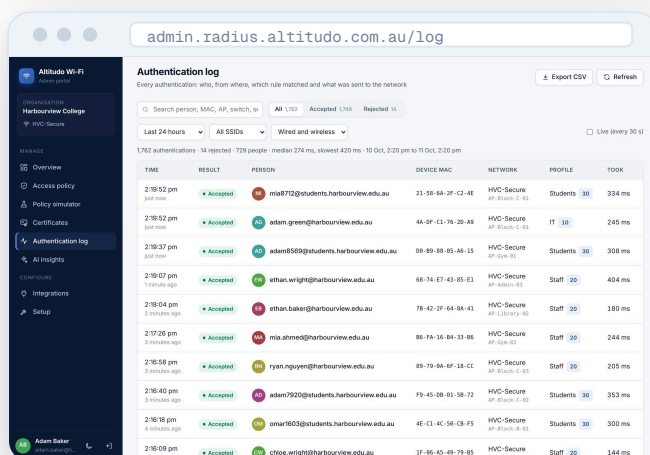
Looking at: Last 24 hours

**Try asking**

- Summarise sign-ins for this period
- Why are sign-ins failing?
- Are any sign-ins slow? Where and why?
- Which devices keep failing, and what should I do?
- Walk me through how a sign-in works here
- Is the access policy doing what I expect?

**About AI insights**

Answers come from Claude, reading your authentication log for the chosen period (up to 3,000 entries) and your access policy. Your data is processed by Amazon Bedrock in Australia (Sydney and Melbourne) and isn't used to train models. AI can make mistakes. Check important findings in the authentication log.



**Authentication log**

Every authentication: who, from where, which rule matched and what was sent to the network

Search person, MAC, AP, switch, n

Last 24 hours | All SSIDs | Wired and wireless | Live (every 30 s)

| TIME       | RESULT   | PERSON                                | DEVICE MAC        | NETWORK                  | PROFILE     | TOOK   |
|------------|----------|---------------------------------------|-------------------|--------------------------|-------------|--------|
| 2:18:52 pm | Accepted | mia872@students.harbourview.edu.au    | 21-16-6A-2F-C2-4E | HVC-Secure AP-Busck-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-Busck-C-01 | IT 36       | 245 ms |
| 2:18:37 pm | Accepted | adrian559@students.harbourview.edu.au | 08-89-85-85-46-13 | 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-Busck-C-01 | Staff 20    | 404 ms |
| 2:18:04 pm | Accepted | ethan.baker@harbourview.edu.au        | 78-42-2F-6A-8A-41 | HVC-Secure AP-Busck-C-01 | 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-Busck-C-01 | Staff 20    | 205 ms |
| 2:16:40 pm | Accepted | adrian559@students.harbourview.edu.au | F9-43-98-81-58-72 | HVC-Secure AP-Busck-C-01 | Students 30 | 353 ms |
| 2:16:18 pm | Accepted | omar603@students.harbourview.edu.au   | 4E-C1-4C-58-C8-F3 | HVC-Secure AP-Busck-C-01 | Students 30 | 300 ms |
| 2:16:09 pm | Accepted | choce.wright@harbourview.edu.au       | 1F-86-A0-49-79-83 | HVC-Secure AP-Sign-02    | Staff 20    | 144 ms |

Authentication log

## “Why can’t the Level 3 meeting rooms connect?”

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

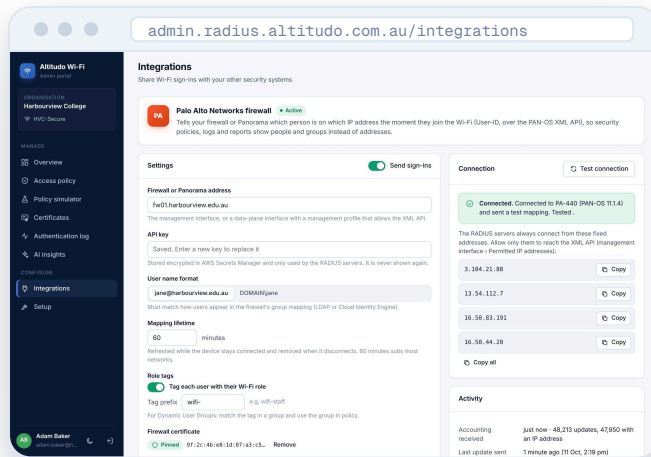
Jamf Pro

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 you are audited

- ✓ **Australian data.** Everything stays in AWS Sydney and Melbourne.
- ✓ **Privacy Act and APPs.** A clear collection notice for staff, and minimal data.
- ✓ **Essential Eight.** Supports the MFA, patching and restricted admin privilege strategies.
- ✓ **Tenant isolation.** Every certificate is bound to your organisation, and one from another tenant is refused.
- ✓ **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

|                | ALTITUDE 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 in your office

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@altitude.com.au](mailto:sales@altitude.com.au)

02 8660 1544

[altitude.com.au/service/cloud-radius](https://altitude.com.au/service/cloud-radius)