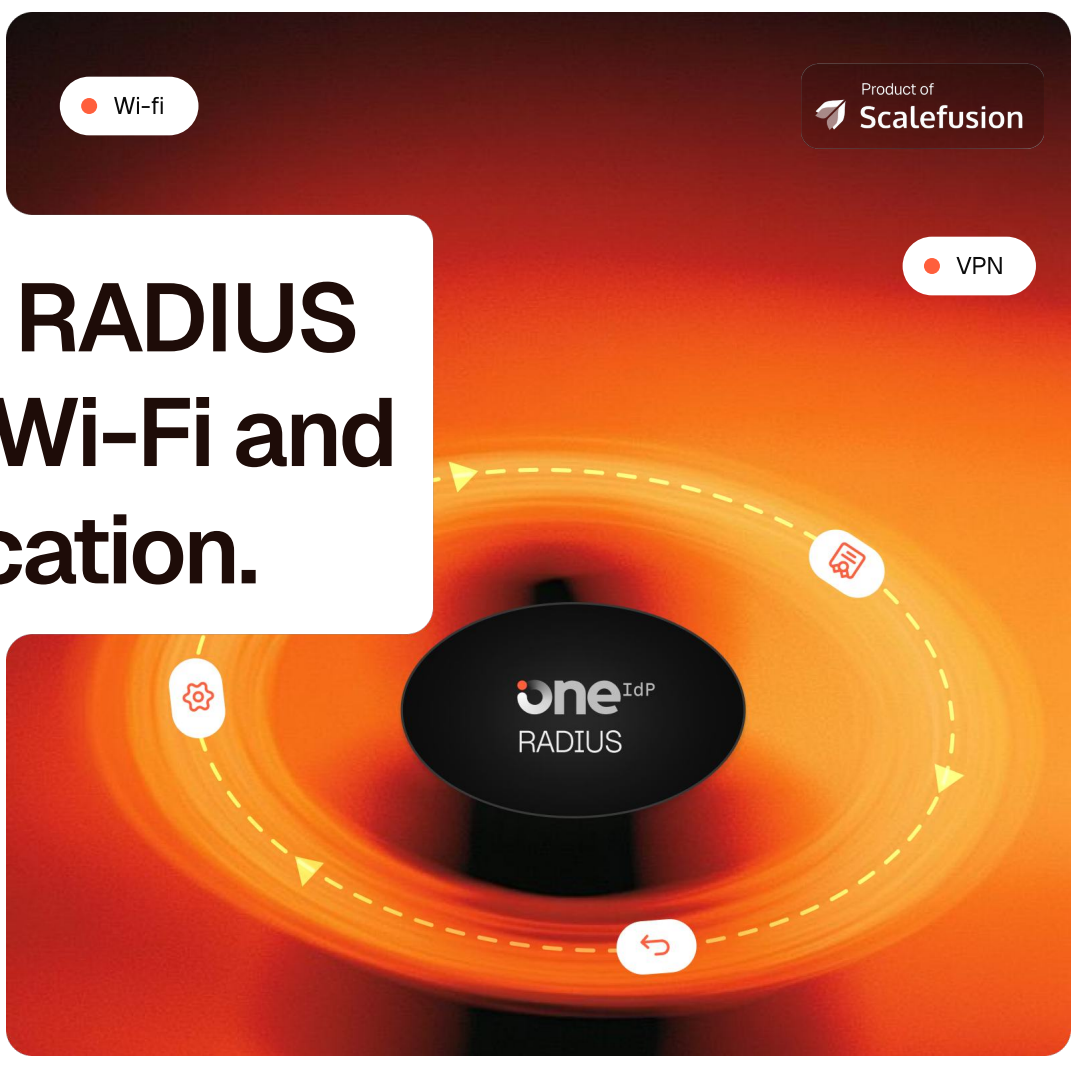
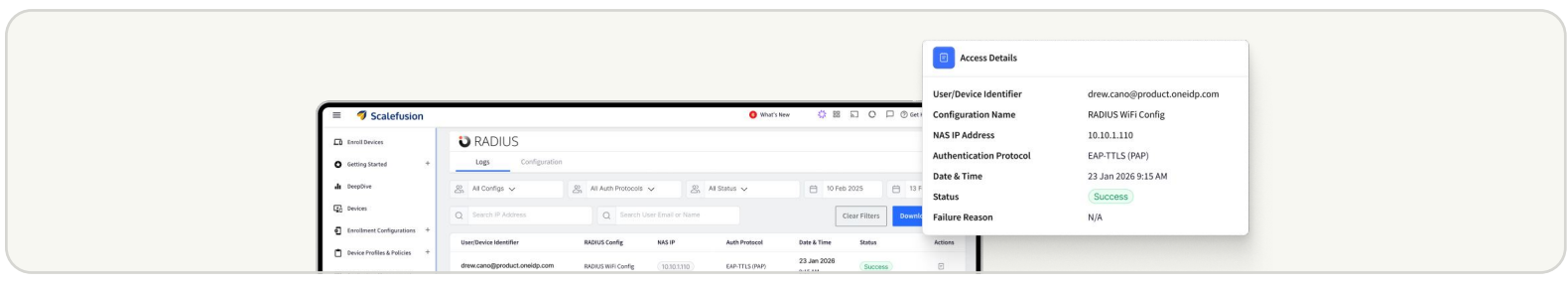
oneIdP Zero Trust Access



Cloud-hosted RADIUS for corporate Wi-Fi and VPN authentication.

Identity-based network authentication,
built around the users and devices you manage.



Reduce RADIUS management overhead by moving corporate Wi-Fi and supported VPN authentication to a cloud-hosted service. Manage configurations centrally through OneIdP.

Eliminate shared Wi-Fi credentials with individual user authentication through existing identity sources. Map access to User Groups and enforce MFA on supported methods.

Strengthen device authentication with digital certificates tied to recognized identities and Device Groups. Give employees a seamless way to connect to the enterprise Wi-Fi network.

Accelerate device onboarding by deploying client certificates, RADIUS server trust, and matching 802.1X Wi-Fi configurations together through UEM.

Tailor network access to every group with configurable VLAN assignments, session timeouts and Reply Attributes. Apply common settings globally or customize them by group.

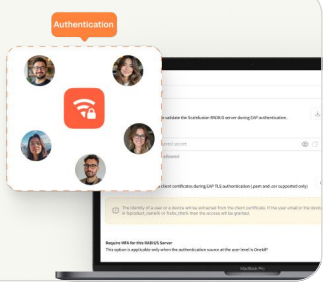
Resolve authentication issues faster with detailed connection records, failure reasons and identity and MFA results. Filter and export logs for investigations and audits.

Core authentication capabilities

Authentication for users and devices.

Flexible Network Authentication

Support certificate-based EAP-TLS and password-based methods including EAP-TTLS, PEAP, MS-CHAPv2 and PAP. Authenticate users through supported identity sources and managed devices with certificates.

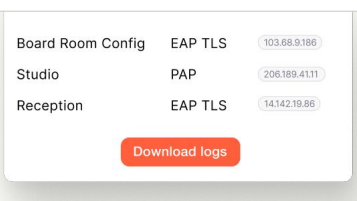


Enterprise Wi-Fi Provisioning

Get managed devices ready for enterprise Wi-Fi in one deployment. Push client certificates, RADIUS server trust certificates and matching 802.1X Wi-Fi configurations through Scalefusion UEM.

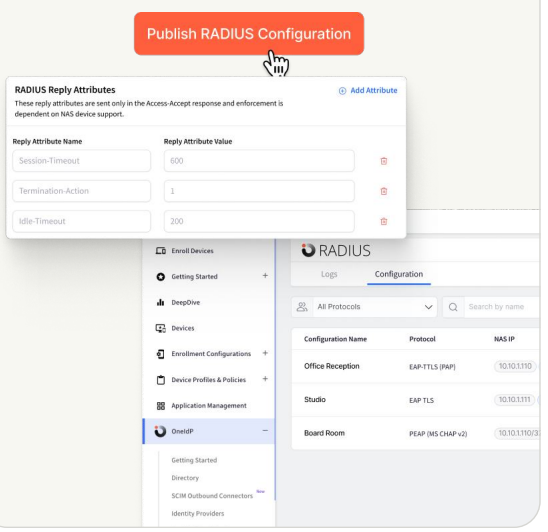
RADIUS Logs & Activity Reports

Review authentication outcomes, failure reasons, IdP and MFA results. Filter and export RADIUS logs, and track administrator changes through Activity Reports.



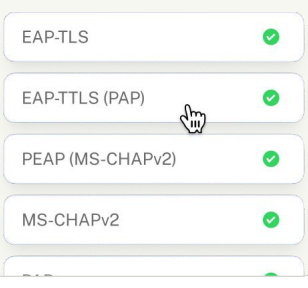
RADIUS Reply Attributes

Define how approved connections are handled with VLAN assignments, session timeouts, firewall filters and vendor-specific attributes. Set common configurations or customize responses for User Groups and Device Groups.



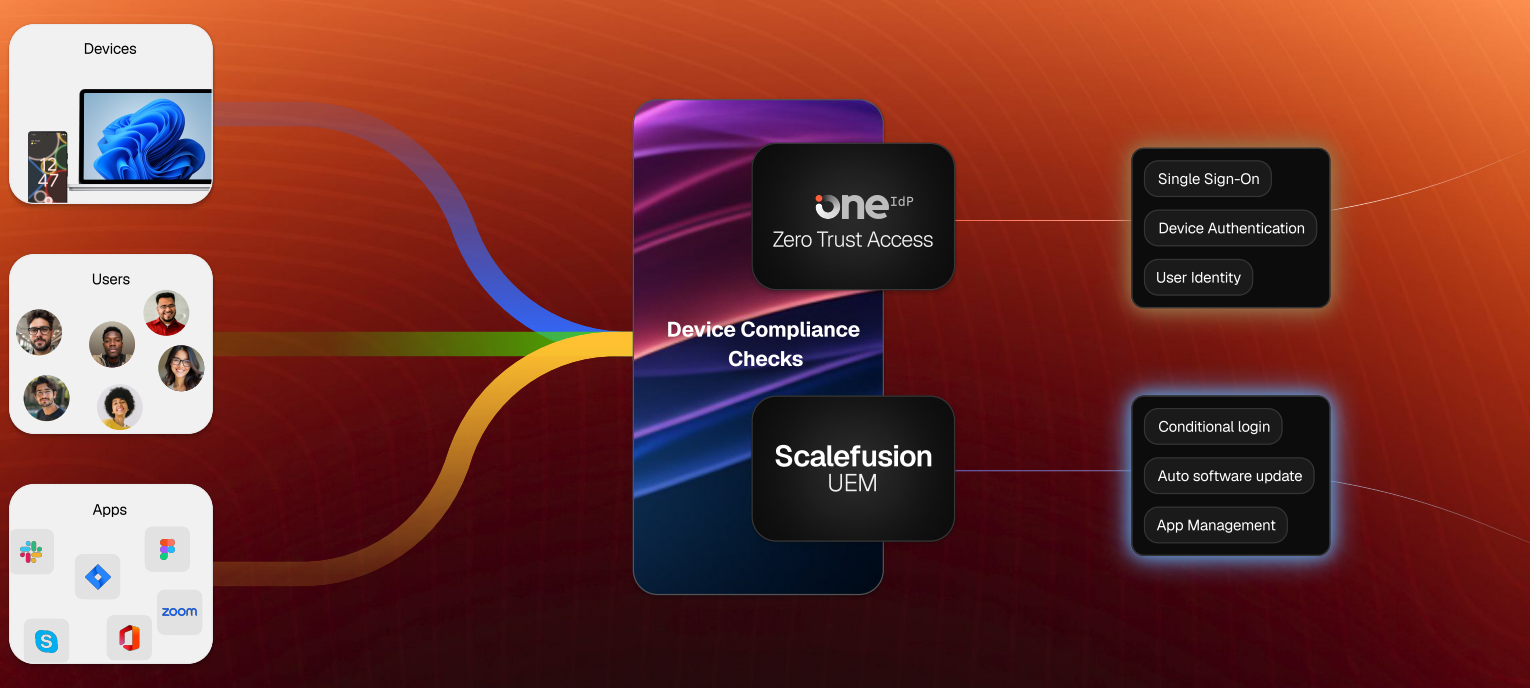
Certificate Management

Connect Generic SCEP, SCEPMan or Smallstep CA servers. Configure certificate templates to map user and device identities for EAP-TLS authentication.



Multi-Factor Authentication

Add an additional verification step to password-based network authentication. Enforce OneIdP or supported third-party authenticator apps to verify users beyond their primary credentials.



Protect corporate network access with identity and device verification.

Move beyond shared network passwords with individual user authentication, device certificates and group-based access policies.

Contact Sales | Book a Demo

LinkedIn YouTube

www.scalefusion.com