3 WAYS
CERTIFICATES SAVE WI-FI

Ruckus
Simply Better Wireless.

white paper

Three Ways Certificates Save Wi-Fi

The expectation that Wi-Fi connectivity is easy, predictable and consistent has evolved from a luxury to burning demand. Meanwhile, the number and types of devices are exploding, making it more difficult than ever to establish (then maintain) a favorable first impression with students, faculty and guests.

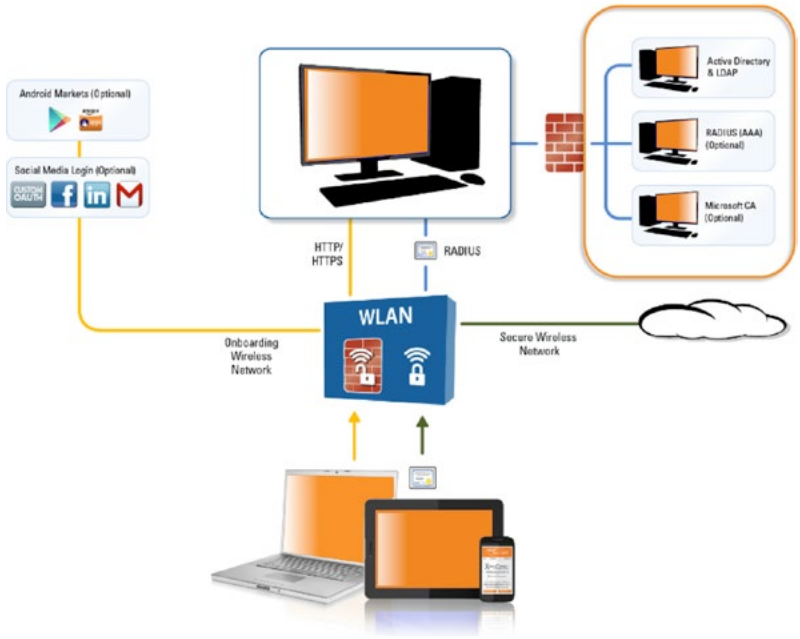
The solution to alleviating Wi-Fi pain in higher education has been available for a long time. It's certificate-based Wi-Fi, in the form of WPA2-Enterprise with EAP-TLS. Certificates eliminate passwords from Wi-Fi, meaning that passwords are neither cached on devices, nor transmitted on every connection attempt, and connectivity continues to function in spite of password changes. In essence, a device registered one time should continue to function throughout the year without disruption. This means happier users and fewer support tickets.

Certificate-based EAP-TLS onboarding is the new standard for secure Wi-Fi in higher education. Extend 802.1X and WPA2-Enterprise to all users; including students, visitors, alumni and contractors, for a uniform wired or wireless approach to save Wi-Fi.

1: Get On

With certificates, user's devices (including laptops, phones, tablets, and more) connect quickly the first time and continue to connect, free from interruption (as long as the user remains valid) without IT involvement.

- **Self-Service Onboarding:** Simplifying device enrollment with a self-service, web-based set-up wizard offers valid users consistent, unobstructed access to join the secure campus network on all devices with a one-time setup. No middle man, no trips to the help desk, no pesky password problems inhibiting the process.
- **Consistent Configuration:** Just because it works, doesn't mean it is set-up correctly from a security perspective. With the set-up wizard doing the heavy lifting, rest assured all devices are configured in the appropriate manner connecting all parties to the correct, secure SSID.
- **Anytime, Anywhere Access:** Students today expect Wi-Fi to work 24/7/365 and often require assistance outside of a Help Desk's office hours. Users avoid these challenges with access to a web-based platform where they're able to quickly access services and information to onboard and manage any device, anywhere, at anytime—often with just one click.



2: Stay On

Once connected, users expect their devices to work throughout the year without disruption. Splash pages and captive portals are despised; Having multiple devices disconnected on each password change is infuriating to your end user.

Certificates ensure end users have a great Wi-Fi experience across all of their devices by delivering users the ability to connect quickly the first time and stay connected as long as they remain a valid user.

- **Uninterrupted Connection:** No more "device dominoes" wherein a user, after a password change, to reconnect multiple devices to a password-based (PEAP/ MSCHAPv2) network, without locking their account.
- **Eduroam:** Participation in Eduroam increases the value of Wi-Fi, allowing educational institutions to support roaming. However, it also creates a perfect storm for password-based issues, which are more difficult to resolve for remote users. The universal nature of the Eduroam wireless network means an inappropriately configured device has greater risk of exposure. Certificates provide the assurance that only valid Eduroam users, with valid devices, remain connected to the campuses secure wireless network and doesn't leave visiting professors or traveling students to fend for themselves.
- **Gold Standard in Security:** WPA2-Enterprise with EAP-TLS ensures that every device connecting to the Wi-Fi network is identified, has the appropriate policy, and when necessary, is removable. This ensures that valid users have access and invalid users do not while verifying each device is authenticated, authorized, and assigned the appropriate VLAN, ACLs, bandwidth, and more—all without the user being interrupted by a captive portal page on every connection.

3: Scale

Supporting an ever-increasing number of devices (and subsequent password churn) is a challenge impacting organizations worldwide;

to reduce risk, lower the burden on IT resources and maintain harmony amongst users, a secure and scalable solution "that just works" is imperative.

Your organization can seamlessly accommodate this influx of users and BYOD devices while achieving a more secure network by migrating from passwords to automated certificate distribution.

- **Reduce Load on Radius:** During device enrollment Certificate-optimized RADIUS servers associate user, device, and policy information into a unified and optimized store, allowing policies such as VLAN, role, and ACL, to be applied easily and efficiently, reducing EAP timeout issues commonly plaguing RADIUS deployments. Certificate-optimized RADIUS servers, as well as support for external RADIUS servers, simplify the definition and enforcement of RADIUS policies.

- **Reduce Load on LDAP/AD:** When PEAP and cached password are replaced with EAP-TLS and certificates, password-related disconnects are eliminated and enrolled devices are no longer impacted, allowing them to continue to function normally. For a user with multiple devices, this greatly improves their experience on the network, while reducing load on LDAP/AD. Guest users, not defined in Active Directory or LDAP, may be granted access without the need to establish another set of credentials. Certificates also provide a simple mechanism to connect IT-owned devices, like cameras, printers, and VoIP phones, to the WPA2-Enterprise network.
- **Beyond BYOD:** Along with the growth of student usage, more users (and devices) than ever need access to secure Wi-Fi. These include short- and long-term guests, alumni, contractors, and partners who have traditionally been left to fend for themselves on unencrypted Wi-Fi, annoyed by recurring web logins and password-related disconnects. Certificates present the opportunity to linearly scale to hundreds of thousands of users while adding certificate-based Wi-Fi security software onto a broad range of IoT devices to enable a secure network, making it possible for IT to successfully manage extensive and ever-evolving Wi-Fi environments.

Conclusion

It's time to dump passwords for certificate-based Wi-Fi onboarding. Give the people what they want and give yourself a break. Certificates can seamlessly accommodate all users, all devices, create a more secure network, reduce IT expense and essentially save Wi-Fi.

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA
(650) 265-4200 Ph \ (408) 738-2065 Fx