Ruckus
Simply Better Wireless.

solution brief

Simple & Secure Connectivity in Higher Ed

Wi-fi Opportunities

- Drive higher utilization of secure Wi-Fi.
- Provide secure visitor, alumni, partner, and contractor access.
- Provide a more secure and reliable eduroam experience.
- Support gaming and other non-WPA2-Enterprise devices.

Password Pickle:

The game played by a user, after a password change, to reconnect multiple devices to a password-based (PEAP/MSCHAPv2) network, without locking their account.

Wi-Fi Challenges in Education

The expectation that Wi-Fi connectivity is easy and predictable is higher than ever. Users expect to connect quickly, easily, and conveniently. Once connected, they expect their devices to work throughout the year without disruption. As the Wi-Fi network has grown from a luxury to an expectation, the value of Wi-Fi connectivity has multiplied, leading to always-connected options like eduroam. Meanwhile, the number of devices and the types of devices are expanding, making it more difficult to establish a favorable first impression.

Wi-Fi networks in education continue to be plagued by persistent issues. Password-based (PEAP, TTLS) networks experience high rates of user disruption based on password changes. Inconsistent implementation of security bypasses in modern operating systems, designed to ease WPA2-Enterprise, leads to environments where security is inconsistently applied. Increased use of single sign-on (SSO) credentials means passwords are more valuable than ever.

Participation in eduroam increases the value of Wi-Fi, allowing educational institutions to support roaming. However, it also creates a perfect storm for these persistent issues. Password-based issues are more difficult to resolve for remote users and represent a larger inconvenience. The universal nature of the eduroam wireless network means an inappropriately configured device has greater risk of exposure. Finally, a compromised password provides an attacker greater access via SSO, jeopardizing educational and financial systems.

Along with the growth of student usage, more users 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.

The Solution: Certificate-Based Wi-Fi

The solution to the persistent Wi-Fi challenges 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.

Certificates also present the opportunity to support more users and more devices in a secure, consistent manner. 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.

Certificate-based Wi-Fi with personal devices has traditionally had its own challenges. Setting up the certificate infrastructure has required extensive knowledge of PKI, the need to distribute certificates to personal devices has created support overhead, and the need to manage the lifecycle of certificates has duplicated directory management.

Certificates Simplified: Cloudpath ES

Cloudpath ES allows devices to be assimilated easily, securely, and without IT involvement. Through smart, policy-associated certificates and WPA2-Enterprise, Cloudpath ES provides visibility and control over personal and IT-owned devices with broad device support. Built upon industry-leading onboarding capabilities, the Cloudpath ES:

- Provides automated, self-service onboarding for all users, including students, faculty, staff, visitors, and contractors.
- Automatically assigns and enforces policy based on the user, device, ownership, and more.
- Automates the distribution of certificates from built-in and third-party certificate infrastructure.
- Automates the configuration of WPA2-Enterprise and wired 802.1X with EAP-TLS.
- Enforces and remediates NAC best practice requirements, including antivirus, firewalls, pinlocks, and system updates.
- Supports a broad array of devices, including laptops, tablets, phones, and headless devices such as printers, cameras, VoIP phones, and barcode scanners.
- Provides onboarding options for various use cases, including BYOD, guest sponsorship, secure hotspot, and time-limited access.
- Provides visibility into users, devices, and policy assignment and per-device control over access rights.

Using your existing WLAN infrastructure, Cloudpath ES enables more users and more devices to connect while reducing support costs, leading to a better user experience.

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

Ruckus
Simply Better Wireless.

www.ruckuswireless.com