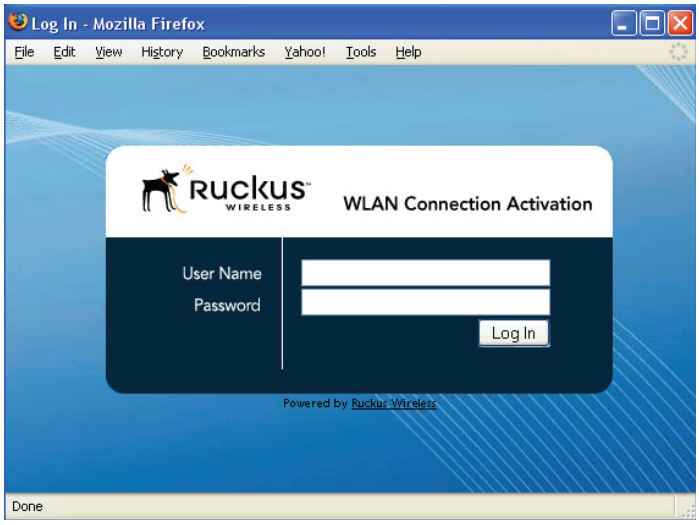
Dynamic PSK™

Encryption Key Technology

Dynamic Pre-Shared Key (PSK) is a patented technology developed to provide robust and secure wireless access while eliminating the arduous task of manual configuration of end devices and the tedious management of encryption keys.



Dynamic PSK creates a unique 63-byte encryption key for each user upon accessing the wireless LAN for the first time and then automatically configures end devices with the requisite wireless settings (i.e., SSID and unique passphrase) without any manual intervention.

Wireless Security Choice for Enterprises

Wireless security remains a primary concern for enterprises when deploying a WLAN. But securing a WLAN is complex and time consuming. This is a major problem for enterprises with limited IT staff that don't have the time or expertise to implement robust wireless security. Authentication (i.e., who is the user and what is the device) and encryption (the scrambling of data) are the two primary security issues to be addressed.

Three popular security options available tradeoff security and ease of deployment *(see Table 1)*. But none of these options provides an optimal solution.

While simple to implement, an open wireless network is clearly not a secure solution as it leaves user transmissions in the clear inviting would-be snoopers to easily grab data out of the air or penetrate the internal network.

A more commonly used wireless security option is the common pre-shared encryption key. A key or passphrase is configured on the APs and on every laptop.

While this option is perceived to be more secure, it's not. Using the same PSK for all employees means that key can be easily compromised. The common PSK also tends to be a relatively short string that can be easily compromised. And for every new employee, IT staff must configure the laptop with the SSID and the key. If there's a need to replace the key (e.g., employee leaves), every laptop must be reconfigured.

FEATURES

- Automatic provisioning of unique encryption key to each user/device
- No manual client configuration
- Unique 63-byte key per user per device
- Easily deactivated when employee leaves
- New key can be generated periodically
- Configurable per WLAN

BENEFITS

- Robust security simplified
- Highly secure
- "IT Lite" — simple to deploy and maintain
- No expensive AAA or RADIUS servers needed
- Secures handheld devices

Ruckus™ WIRELESS

The third option uses an enterprise-class solution such as 802.1X. Through a highly secure solution, 802.1X is very complex to set up. It requires having the right infrastructure starting with the RADIUS server all the way to 802.1X supplicants on each and every client. Configuring and maintaining 802.1X is time consuming for enterprises that do not have the resources to manage such an endeavor.

A new approach, Dynamic PSK solves these problems.

How does Dynamic PSK work?

Instead of manually configuring each individual laptop with an encryption key and the requisite wireless SSID, Dynamic PSK automates and centralizes this process *(See Figure 1)*.

Once enabled for the entire system, a new user simply connects to the Ethernet LAN and authenticates via a captive portal hosted on the Ruckus ZoneDirector. Mobile devices like the Apple® iPhone® can also be authenticated through a captive portal over wireless. This information is checked against any standard back-end authentication (AAA) server such as Active Directory, RADIUS, LDAP or an internal user database on the ZoneDirector.

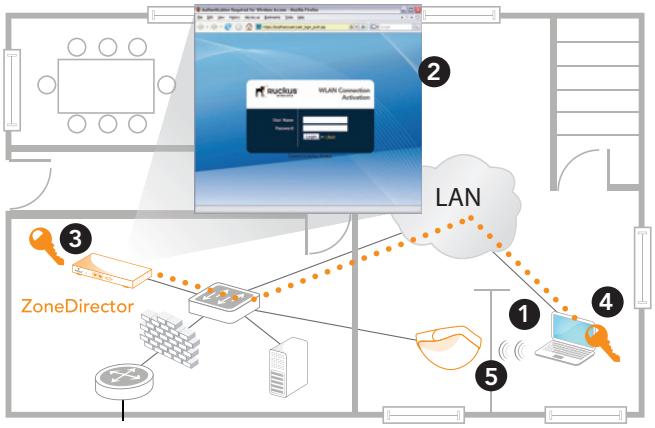
Upon successful authentication, the ZoneDirector generates a unique encryption key for each user. The lifetime of the key can be configured to align with company policies. A temporary applet with the unique user key and other wireless configuration information is then pushed to the client. This applet automatically configures the user's device without any human intervention.

The user then detaches from the LAN and connects to the wireless network. Once associated, the Dynamic PSK is bound to the specific user and the end device being used.

TABLE 1. Wireless Security Options

Security Option	Benefits	Drawbacks
Open network	• Simple to use and deploy	• Completely insecure • Some client configure still required
Pre-Shared Key	• Straightforward implementation • Link layer encryption	• Easily compromised • Same key for all employees • Client configuration required
802.1X	• Robust and comprehensive framework • Strong encryption and authentication	• Expensive authentication server • Requires 802.1X supplicant on every end device • Highly complex • Time-consuming to implement
Dynamic PSK	• Easy to use • Strong encryption without 802.1X • No admin intervention • Works with existing authentication without EAP	• Manual configuration required for handheld devices (e.g., phones, PDA)

FIGURE 1. Dynamic Pre-Shared Key automates secure wireless LAN access



1. User attaches to wired LAN (or open a dedicated provisioning WLAN)
2. User challenged to authenticate at captive portal page
3. Upon authentication, a unique encryption key is dynamically generated for user by the ZoneDirector
4. Key is passed to user device where it is automatically configured within the wireless configuration
5. User detaches from the LAN and can now safely connect to the WLAN

Ruckus Wireless, Inc.
880 West Maude Avenue, Suite 101, Sunnyvale, CA 94085 USA (650) 265-4200 **Ph** \ (408) 738-2065 **Fx**