

# Dynamic PSK™

## Encryption Key Technology

Dynamic Pre-Shared Key (PSK) is a patent pending 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

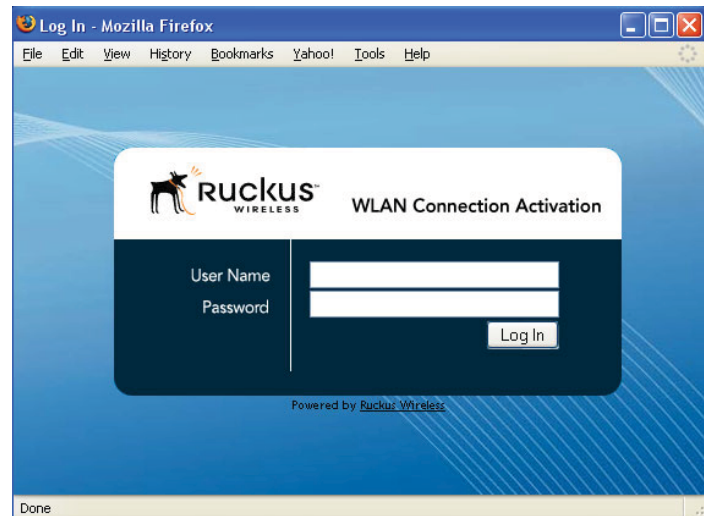
Wireless security remains a primary concern for enterprises when deploying a WLAN. But securing a WLAN is complex and time consuming. This is a major problem for enterprises with limited IT staff that don't have the time or expertise to implement robust wireless security. Authentication (i.e., who is 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



