

# Dynamic PSK™

## Encryption key technology for secure network access

### BENEFITS

- Increases security for BYOD and guest users connecting to a RUCKUS® network
- Automates provisioning of unique per-user or per-device encryption keys
- Gives administrators control over which users and devices can access the network
- Requires no manual client configuration
- Supports virtually every Wi-Fi-enabled device

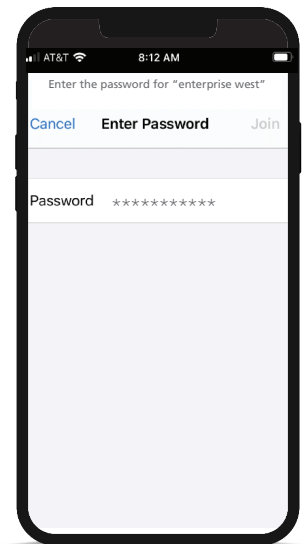
### Challenges with default methods for getting BYOD and guest users connected

Lacking a better mechanism for getting BYOD and guest users connected to the wireless network, administrators typically use MAC authentication or conventional pre-shared keys (PSKs). These methods come with serious drawbacks in terms of security and user experience. For example, with MAC authentication, wireless traffic over the air between the access point and the device is not encrypted, and there is no way to associate a user with a device. The increasing use of private MAC addresses (also known as MAC randomization) also creates the potential to disrupt the user experience. MAC addresses are easy to spoof, creating the possibility for unauthorized access. With conventional PSKs, multiple (or all) users share the same Wi-Fi password. Because changing the PSK disrupts access for all, the temptation is not to change it. Users can share the key with anyone and take it with them when they leave the organization. There is no way to revoke access for a specific user without disrupting access for all.

### Dynamic PSK—increased security for users, devices and the network

Dynamic Pre-Shared Key (DPSK) is a CommScope-patented technology that addresses these shortcomings to increase security for users and devices connecting to the network.

It provides encryption key technology for secure network access for RUCKUS networks. Depending upon the specific implementation of DPSK technology, users may self-serve to obtain a DPSK, or they may receive the key from an IT administrator. Users simply enter the DPSK into their devices the same way they would enter a conventional PSK. Because this process is very similar to the way they would connect to a consumer-grade router on their home network, getting connected is very intuitive for users. As with home Wi-Fi, they don't have to re-enter the key repeatedly when they re-enter the network environment—it's a set-it-and-forget-it user experience. Unlike with conventional PSKs, each user gets a unique key. That means the IT admin can revoke access for a user/device without disrupting access for other users. Wireless traffic over the air is encrypted using WPA2-Personal, which nearly every Wi-Fi-enabled device supports. (While WPA2/3-Enterprise offers even stronger security, some devices do not support these protocols.)



Dynamic PSKs provide an easy and secure way for BYOD and guest users to connect to the network.

There are various ways to deploy Dynamic PSK. The key may be associated with a specific device or with multiple devices per user. Since the key need not be linked to the device's MAC address, it addresses the user experience issues associated with MAC randomization. The deployment mode depends on the requirements of the specific customer use case.

## Platform support for Dynamic PSK

Dynamic Pre-Shared Keys are a core technology feature of RUCKUS control and management platforms. These include SmartZone™, RUCKUS Cloud™, ZoneDirector™ and Unleashed™. Each of these platforms has its own capabilities with respect to DPSK.

Cloudpath Enrollment System is a cloud service (or on-premises software) that offers the most complete and robust implementation of DPSK. The Cloudpath service is a purpose-built system for delivering secure network access in support of BYOD, guest users and IT-owned devices. It supports a wide variety of methods of authentication besides DPSK, including digital certificates. Admins can also use Cloudpath to define and manage granular policies that govern the level of network access based upon the individual's role in the organization. A fully customizable onboarding portal lets IT teams define intuitive self-service workflows so internal and guest users can onboard their devices without IT intervention.



---

commscope.com

Visit our website or contact your local CommScope representative for more information.

© 2021 CommScope, Inc. All rights reserved.

Unless otherwise noted, all trademarks identified by ® or ™ are registered trademarks, respectively, of CommScope, Inc. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to CommScope products or services. CommScope is committed to the highest standards of business integrity and environmental sustainability with a number of CommScope's facilities across the globe certified in accordance with international standards, including ISO 9001, TL 9000, and ISO 14001. Further information regarding CommScope's commitment can be found at [www.commscope.com/About-Us/Corporate-Responsibility-and-Sustainability](http://www.commscope.com/About-Us/Corporate-Responsibility-and-Sustainability).

PA-115991-EN (07/21)