FICHE TECHNIQUE

Dynamic PSK™

Technologie de clé de chiffrement pour un accès réseau sécurisé

COMMSCOPE® RUCKUS®

AVANTAGES

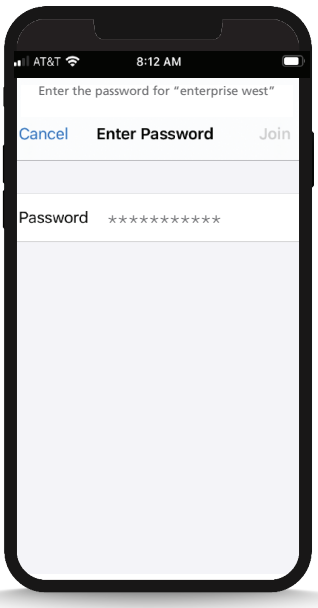
- Renforce la sécurité des utilisateurs BYOD et invités qui se connectent à un réseau RUCKUS®
- Automatise le provisionnement des clés de chiffrement par utilisateur ou par appareil
- Permet aux administrateurs de choisir les utilisateurs et appareils qui peuvent accéder au réseau
- Ne nécessite aucune configuration client manuelle
- Prend en charge pratiquement tous les appareils Wi-Fi

Problèmes des méthodes habituelles utilisées pour la connexion des utilisateurs BYOD et invités

Ne disposant pas d'un meilleur mécanisme pour connecter les utilisateurs BYOD et invités au réseau sans fil, les administrateurs utilisent généralement une authentification MAC ou des clés pré-partagées (PSK) traditionnelles. Ces méthodes risquent de compromettre sérieusement la sécurité et l'expérience des utilisateurs. Par exemple, avec une authentification MAC, le trafic sans fil entre le point d'accès et l'appareil n'est pas chiffré et il n'est pas possible d'associer un utilisateur à un appareil. L'utilisation d'adresses MAC privées (également appelée randomisation MAC) risque de perturber l'expérience des utilisateurs. Les adresses MAC sont faciles à usurper, ce qui risque de permettre des accès non autorisés. Avec les clés PSK conventionnelles, plusieurs (ou tous les) utilisateurs partagent le même mot de passe Wi-Fi. Étant donné que le changement de clé PSK perturbe l'accès des utilisateurs, la tentation est de ne pas utiliser cette méthode. Les utilisateurs peuvent partager la clé avec d'autres personnes et la prendre avec eux lorsqu'ils quittent l'organisation. Il n'y a aucun moyen de retirer l'accès à un utilisateur donné sans perturber l'accès de tous les autres utilisateurs.

PSK dynamique : sécurité renforcée pour les utilisateurs, les appareils et le réseau

DPSK (Dynamic PSK ou clé pré-partagée dynamique) est une technologie brevetée CommScope qui résout ces problèmes et améliore la sécurité des utilisateurs et appareils connectés au réseau. Cette technologie de chiffrement sécurise l'accès aux réseaux RUCKUS. Selon la mise en œuvre de la technologie DPSK, les utilisateurs peuvent obtenir une clé DPSK en libre service ou la demander à un administrateur IT. La clé DPSK est saisie dans un appareil de la même manière qu'une clé PSK conventionnelle. Cette procédure est pratiquement identique à la manière dont un utilisateur se connecte à un routeur sur son réseau domestique et est donc très intuitive. Comme avec le Wi-Fi domestique, l'utilisateur n'a pas à saisir cette clé plus d'une fois. Contrairement aux clés PSK traditionnelles, chaque utilisateur bénéficie d'une clé unique. Cela signifie que l'administrateur IT peut retirer les privilèges d'accès à un utilisateur (ou à un appareil) sans perturber l'accès des autres utilisateurs. Le trafic sans fil est chiffré à l'aide du protocole WPA2-Personal qui est pris en charge par pratiquement tous les appareils compatibles Wi-Fi. (Le chiffrement WPA2/3 Enterprise fournit une sécurité encore plus robuste mais certains appareils ne prennent pas en charge ces protocoles.)



Les clés DPSK permettent aux utilisateurs BYOD et aux invités de se connecter au réseau aisément et en toute sécurité.

Il existe plusieurs manières de déployer la clé DPSK. Cette clé peut être associée à un appareil spécifique ou à plusieurs appareils d'un utilisateur. Étant donné que la clé n'a pas besoin d'être liée à l'adresse MAC de l'appareil, elle résout les problèmes d'expérience utilisateur associés à la randomisation MAC. Le mode de déploiement dépend des cas d'utilisation du client.

Plateforme supportant la clé DPSK

Les clés DPSK jouent un rôle vital au sein des plateformes de contrôle et gestion de RUCKUS. Ces plateformes incluent SmartZone™, RUCKUS Cloud™, ZoneDirector™ et Unleashed™. Chacune de ces plateformes est dotée de ses propres capacités en matière de DPSK.

Le système d'enregistrement Cloudpath est un service Cloud (ou en VM sur site) qui offre la mise en œuvre la plus complète et la plus robuste de DPSK. Le service Cloudpath est un système spécialement conçu pour la fourniture d'un accès réseau sécurisé au BYOD, aux utilisateurs invités et aux appareils appartenant au service IT. Outre DPSK, il prend en charge diverses méthodes d'authentification dont les certificats numériques. Les administrateurs peuvent également utiliser Cloudpath pour définir et gérer des politiques d'accès granulaires servant à régir le niveau d'accès au réseau en fonction du rôle d'une personne au sein de l'organisation. Un portail d'enregistrement entièrement personnalisable permet aux équipes informatiques de définir comment les utilisateurs et leur terminaux seront authentifiés et contrôlés. Ce portail peut être en libre-service permettant aux utilisateurs internes et aux invités d'enregistrer leurs appareils sans l'aide du service technique.

COMMSCOPE®

commscope.com

Consultez notre site Web ou contactez votre représentant local CommScope pour plus d'informations.

PA-115991-FR (07/21)