RUCKUS One Online Help (index.html)

Search

Supported Network Types and Security Protocols

RUCKUS One supports many network types that you can deploy to your venue.

Network Types

Network types supported by RUCKUS One range from networks that are typically deployed in enterprise or office environments in addition to networks that are typically deployed in public places (such as coffee shops, libraries, airports, hotels, and so on) where there is a high, but temporary, number of network users. RUCKUS One supports the following authentication methods:

- Pre-Shared Key (PSK): Require users to enter the passphrase (that you have defined for the network) to connect.
- Dynamic Pre-Shared Key (DPSK): A unique passphrase is dynamically created for each user to connect to the network.
- Enterprise AAA: Use 802.1X standard and WPA2 security protocols to authenticate users using an authentication server on the network.
- Hotspot 2.0 Access: Enable users to automatically and securely connect to Wi-Fi networks while roaming by supporting multiple roaming partners over a single SSID.
- Captive Portal: Use a third party captive portal and authentication service to authenticate users. There are six methods that allow users to gain access through the captive portal:
  - Click-Through: Allows users to accept Terms and Conditions to access the network.
  - Self Sign In: Allows users to access the network temporarily using their social media account, or register their details and get a personal password.
  - Cloudpath Captive Portal: Allows users to connect through an enhanced captive portal with Cloudpath.
  - Host Approval: Allows users to register their details in the portal including their host email. A host must approve the guest request in order to provide the temporary network credentials to the guest user.
  - Guest Pass: Allows users to access the network temporarily using a personal password which they receive in advance from the network administration staff.

- 3rd Party Captive Portal (WISPr): Allows users to access the network through a 3rd party captive portal, authenticated by a RADIUS server.
- Active Directory/LDAP Server: Allows users to join by entering an organization-based username and password, which is authenticated by an associated Active Directory (AD) server or a Light Directory Access Protocol (LDAP) server.

- Open Network (not recommended): Allow users to access the network without any authentication .

Note:
Demonstration of Choosing a Wi-Fi Network Type. This video explains the Wi-Fi network types available in the RUCKUS One.

Click to play video in full screen mode. (https://play.vidyard.com/HTFJ1S86WzkSwcaAAAZJWP)

Security Protocols

Security protocols are necessary rules that are implemented in networks. These protocols enforce encryption and authentication to prevent unauthorized access and data manipulation. The following security protocols are available:

- Wired Equivalent Privacy (WEP): This is a first wireless security protocol. It was the first used to encrypt data on Wi-Fi networks but has known vulnerabilities and weak encryption, making it highly susceptible to unauthorized access and considered obsolete. This uses 64-bit and 128-bit fixed key encryption. WEP is retired in year 2004 by Wi-Fi Alliance. It is still exists in RUCKUS One as it helps administrator to manage Wi-Fi network that contains very old devices which are expensive and difficult to replace.

  Note: Do not use this method to transmit sensitive information.

  Note: Due to security concerns, WEP will no longer be supported for users. However, this change will not impact existing networks that currently utilize WEP.

- Wi-Fi Protected Access (WPA): This is the updated version of WEP that fixes the problems. It introduced the

Temporal Key Integrity Protocol (TKIP) for encryption and improved authentication processes. This generates a new key for each data packet, providing better Wi-Fi networks protection against unauthorized access. WPA supports legacy devices built after 2006.

- Wi-Fi Protected Access 2 (WPA2): This is the upgraded version of WPA. It uses Advanced Encryption Standard (AES) for data encryption and authentication. It supports the 802.1x and Pre-Shared Key (PSK) modes.
- Wi-Fi Protected Access 3 (WPA3): This is an updated version of WPA2 and the most recent wireless security standard. It supports 6-GHz radios. It introduces the Simultaneous Authentication of Equals (SAE) protocol, that makes it resistant to password-related attacks such as brute force attempt and Opportunistic Wireless Encryption (OWE) for public Wi-Fi, which encrypts data without requiring a password. It includes Management Frame Protection (802.11w), which encrypts management frames between the end-user device and the AP. After 2020, the WAP3 can only be used with Wi-Fi certified devices. The backward compatibility is not guaranteed.

  Note: If you are configuring PSK network setting with WPA3 network protocol. The SAE replaces the PSK passphrase with SAE passphrase.

- WPA2/WPA3 Mixed Mode: This is a Wi-Fi network configuration that allows APs to support both WPA2 and WPA3 at the same time. This is also known as WPA3 transition mode. This mode allows devices with different capabilities to connect to the network, allowing for a progressive transition to the more secure WPA3 while continuing to support older devices that depend on WPA2. If you choose this option, you must configure WPA2 and WPA3 SAE passphrase separately.

For optimal security, RUCKUS recommends WPA2. Organizations and enterprises are advised to use WPA3, but home users can use WPA2 or a WPA2/WPA3 mixed mode if necessary.

Note:
Demonstration of Choosing a Security Protocol for a Wi-Fi Network. This video explains the security protocols available in the RUCKUS One.

Click to play video in full screen mode. (https://play.vidyard.com/G66xxCjyvPyfRq4B1SUAiF)

800-73730-001 Rev D 29 April 2025