RUCKUS One Online Help (index.html)

Search

Wireless Networks Overview

This feature enables access management and network security by implementing any of the authentication methods mentioned in this topic. Create an authentication-based wireless network to deploy services at your venue. The setup process varies based on network type and chosen authentication method for user access.

RUCKUS One supports the following authentication methods:

- **Pre-Shared Key**: Requires users to enter the passphrase (that you have defined for the network) to connect to RUCKUS One. Refer to *Creating a Network That Uses a Passphrase (PSK/SAE) (GUID-EBBB942A-3E3B-4C02-9E2A-8E6E5F9AF5F1.html)*.
- **Enterprise AAA**: Uses the 802.1X standard and WPA2 security protocols to authenticate users using an authentication server on the network. This authentication method requires an AAA server on the network. Refer to *Creating a Network That Uses an Enterprise AAA Server (GUID-E311B82D-804B-4A64-B93B-7D7014873A31.html)*.
- **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. Refer to *Creating a Network That Uses Hotspot 2.0 Access (GUID-F5EE7E34-EFB1-4B37-B4EA-51123FEFED56.html)*.
- **Captive Portal**: Uses a third-party captive portal and authentication service to authenticate users. There are six methods that can be used to gain access through the captive portal:
  - **Click-Through**: Allows users to accept terms and conditions to access the network. Refer to *Creating a Network That Uses a Captive Portal with Click-Through (GUID-1895C048-E674-451B-8416-251A86955444.html)*.
  - **Self Sign In**: Allows users to access the network temporarily using a social media account, or register their details and get a personal password. Refer to *Creating a Network That Uses a Captive Portal with Self Sign In (GUID-BA9D6CA9-C716-4AAC-B2B8-B0FDF4790CD6.html)*.
  - **Cloudpath Captive Portal**: Users connect through an enhanced captive portal experience with Cloudpath. Refer to *Creating a Network That Uses a Cloudpath Captive Portal (GUID-37BA406F-ABE9-40B6-BBAD-3F73768B67B6.html)*.
  - **Host Approval**: Allows users to register their details in the portal including their host email. A host must approve the guest request to provide the temporary network credentials to the guest user. Refer to *Creating a Network That Uses a Captive Portal with Host Approval (GUID-8DD5DFFD-AAE7-4C71-9507-77D42EA56955.html)*.

- **Guest Pass**: Allows users to access the network temporarily using a personal password which they receive in advance from the network administration staff. Refer to *Creating a Network That Uses a Captive Portal with a Guest Pass (GUID-3FD9223D-4BD8-482E-B2C7-EA89C4E18298.html)*.
- **Third-Party Captive Portal (WISPr)**: Allows users to access the network through a third-party captive portal, authenticated by a RADIUS server. Refer to *Creating a Network That Uses a Third-Party Captive Portal (WISPr Feature) (GUID-CA7D13C6-C142-4D15-B854-C15BAB9FD24D.html)*.
- **Active Directory/LDAP Server**: Allows users to access the network 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. Refer to *Creating a Network That Uses a Captive Portal with Active Directory or LDAP Server (GUID-AFAE3299-8E9A-48B6-B1F7-C44550B761C9.html)*.

- **Open** (not recommended): Allows users to access the network without any authentication. Refer to *Creating an Open Network (GUID-A53B97ED-67C3-4498-9B60-B587D52890AF.html)*.

Note:

Demonstration of Wireless Network Authentication Methods. This video walks you through the Wireless Network feature page and demonstrates how to access the wireless network authentication method.

Click to play video in full screen mode. (https://play.vidyard.com/aFcwaPCgGoJuM8n6SiqfJg)