WAP121和WAP321接入点上的WiFi保护访问预共享密钥(WPA-PSK)复杂性配置

目标

Wi-Fi保护访问(WPA)是用于无线网络的安全协议之一。与有线等效保密(WEP)安全协议相比，WPA改进了身份验证和加密功能。如果在AP上配置了WPA，则会选择WPA预共享密钥(PSK)来安全地对客户端进行身份验证。启用WPA-PSK复杂性后，可以配置身份验证过程中使用的密钥的复杂性要求。更复杂的密钥可提高安全性。

本文介绍如何在WAP121和WAP321接入点上配置WPA-PSK复杂性。

适用设备

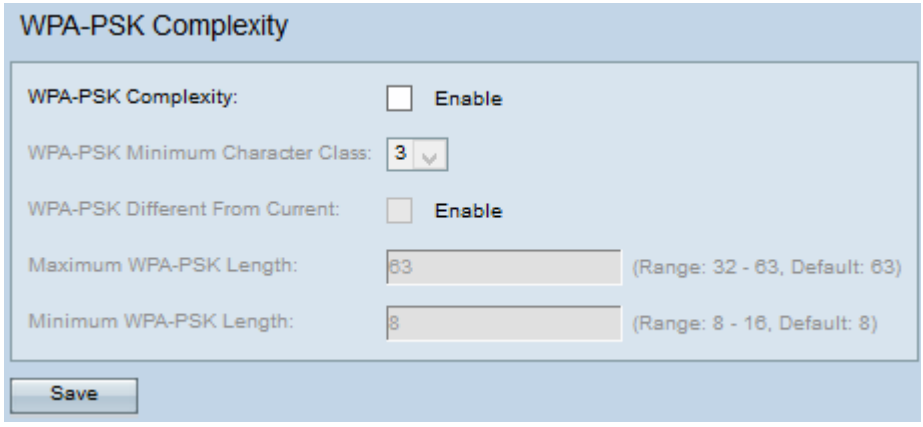
·WAP121
· WAP321

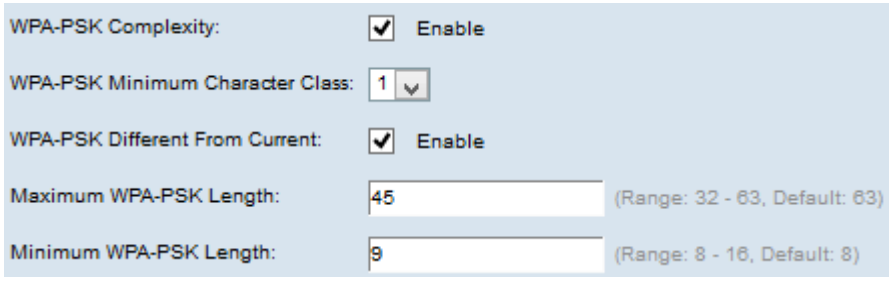
软件版本

•1.0.3.4

WPA-PSK复杂性配置

步骤1.登录Web配置实用程序，然后选择**System Security > WPA-PSK Complexity**。WPA-*PSK复杂性*页面打开：





步骤2.选中WPA-PSK复杂性字段中的**启用**复选框，使AP能够检查新的WPA-PSK密钥的复杂性。

步骤3.从WPA-PSK Minimum Character Class下拉列表中，选择键字符串中必须表示的最小

字符类数。四种可能的字符类是大写字母、小写字母、数字和标准键盘上可用的特殊字符。

步骤4.（可选）要在当前密钥过期时配置不同的密钥，请选中WPA-PSK Different From Current字段中的**Enable**复选框。取消选中**Enable**复选框，允许用户在当前密钥过期时重新输入之前的密钥。

步骤5.在Maximum WPA-PSK Length字段中输入预共享密钥的最大长度。值范围为32到63。

步骤6.在Minimum WPA-PSK Length字段中输入预共享密钥的最小长度。值范围为8到16。

第 7 步： 点击 **Save（保存），以保存设置。**