在WAP571或WAP571E上配置第三方身份验证

目标

本文将指导您在WAP571或WAP71E接入点上配置第三方身份验证。

简介

网络用户通常连接到无线接入点(WAP)，以获得比移动设备运营商服务更快的互联网速度。流畅的登录过程和轻松的导航可确保这些用户获得良好的体验。 您可以配置WAP571或WAP571E，以便在保持网络安全的同时提供一些用户登录的简单选项。

通过Google或Facebook进行第三方身份验证是此最新更新的可用功能。使用时，用户的第三方帐户充当一种“护照”，允许用户访问您的无线网络。无论您是经营咖啡店还是房地产办公室，它都可确保访客轻松访问您的网络，并获得卓越的访客体验。

适用设备

WAP571

WAP571E

软件版本

1.1.03

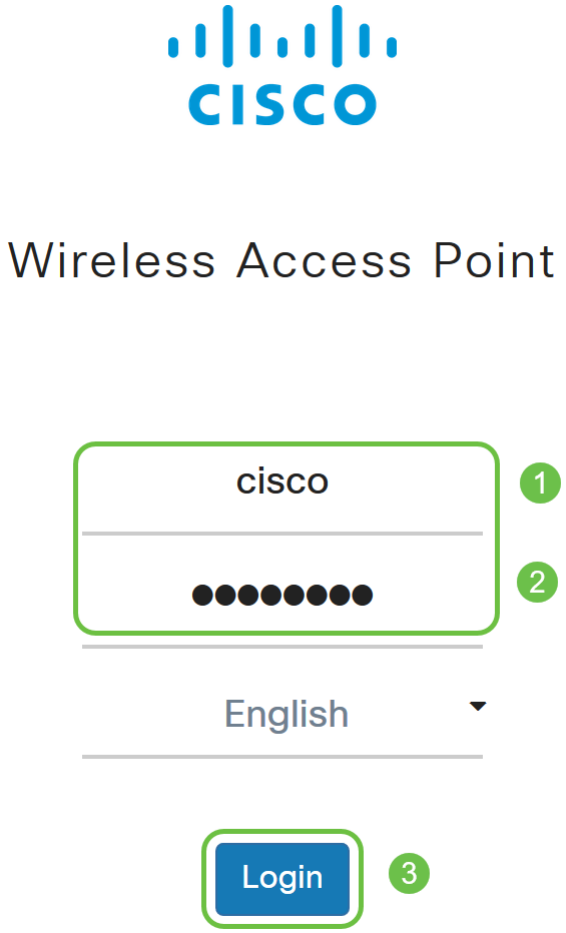
要求

互联网接入，因此您可以连接Google和/或Facebook身份验证服务器。

用户必须拥有Google和/或Facebook的现有帐户。

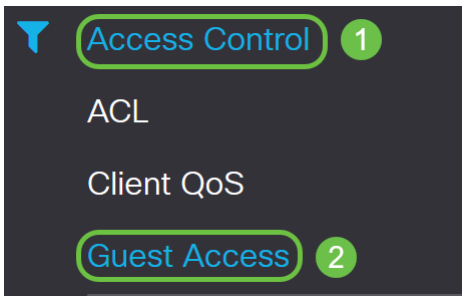
配置第三方身份验证

步骤1.通过输入用户名和密码登录WAP的Web配置实用程序。默认用户名和密码为*cisco/cisco*。如果已配置新的用户名或密码，请输入这些凭证。单击 **Login**。



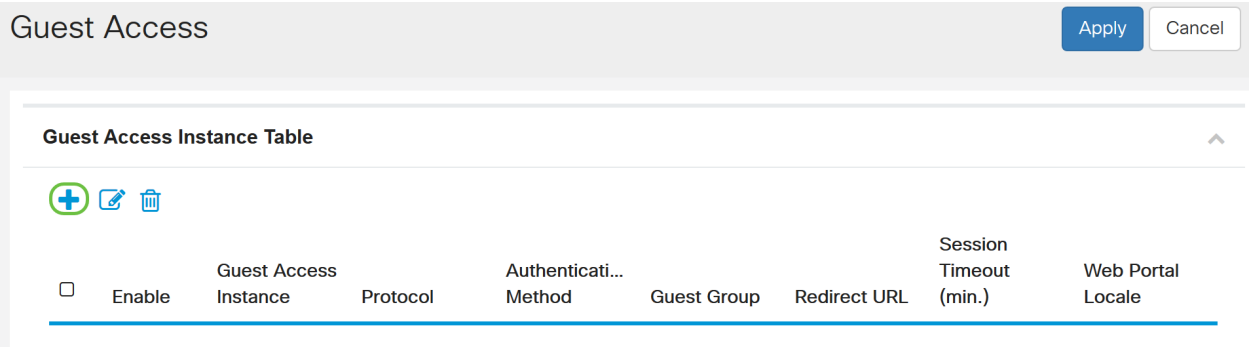
注意：本文使用WAP571E来演示第三方访客身份验证的配置。菜单选项可能会根据设备型号稍有不同。

步骤2.选择**Access Control > Guest Access**。

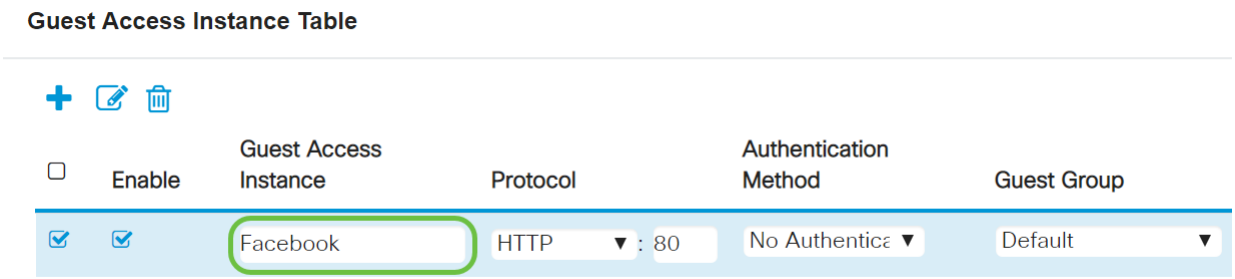


步骤3.在“访客访*问实例表*”中，可以添加新的访客*访问实例*或编辑现有实例。

在本示例中，通过单*击加号图*标来添加新的访客访**问实例**。



步骤4.命名访*客访问实例*。在本例中，它被命名为**Facebook**。

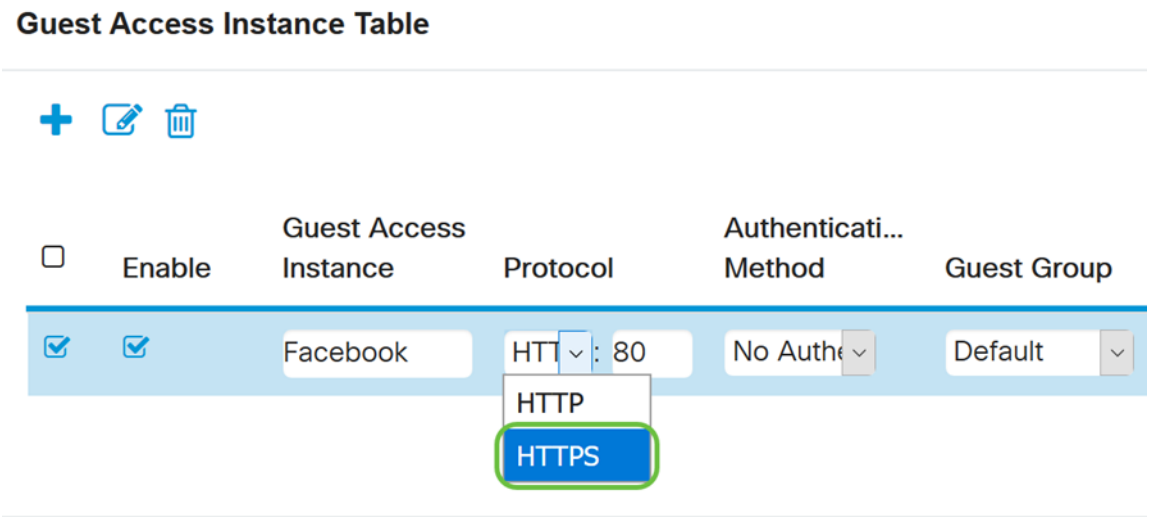


步骤5.从下拉菜单中选择*在验*证过程中使用的协议。

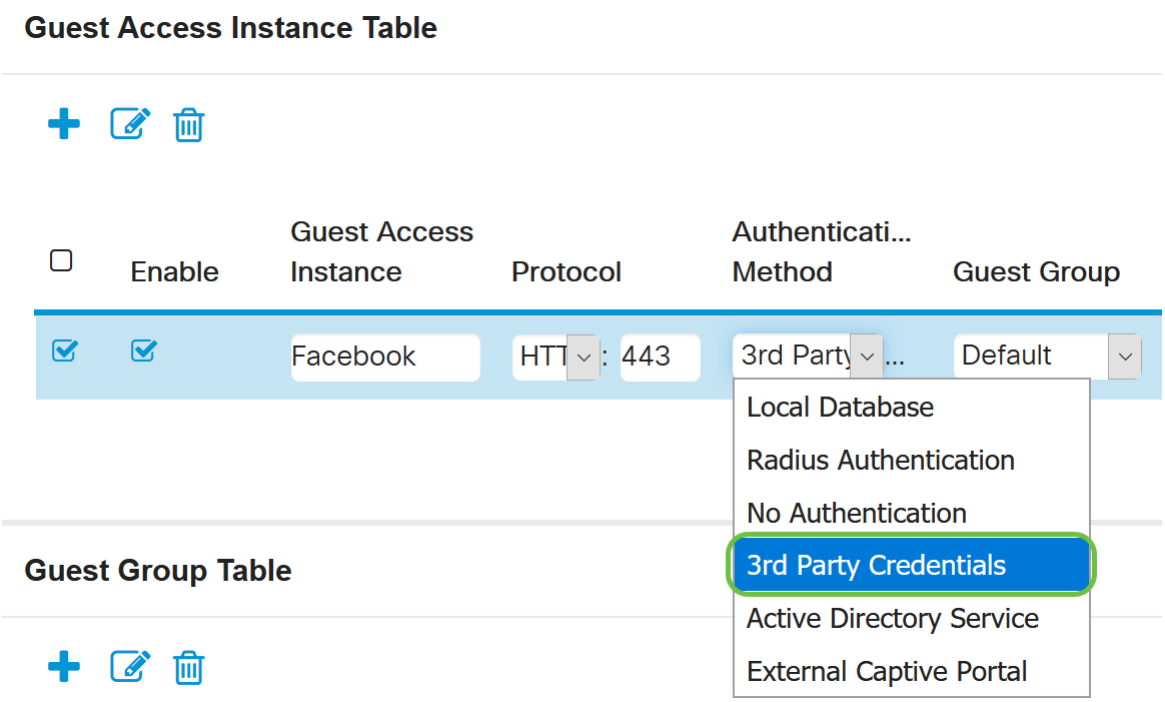
HTTP — 在验证期间不使用加密。

HTTPS — 使用安全套接字层(SSL)，该层要求证书提供加密。证书在连接时提供给用户。

注意：客户端应将强制网络门户页面配置为使用HTTPS而不是HTTP，这一点非常重要，因为前者更加安全。如果客户端选择HTTP，则它们可能会以未加密的明文形式传输用户名和密码，从而不经意地暴露用户名和密码。最好使用HTTPS强制网络门户页面。

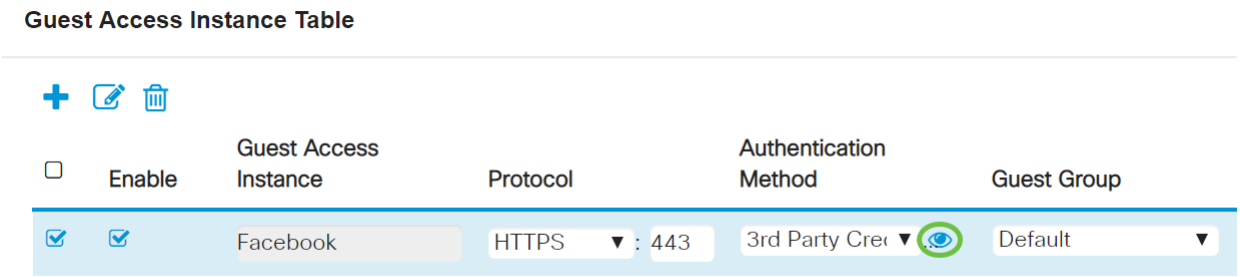


步骤6.选择Authentication Method*作为*第**三方凭据**。



注意：WAP设备使用社交媒体帐户上的凭证对用户进行身份验证。

步骤7.在Authentication Method列**中**，**单**击第3*方*凭据旁边*的蓝眼图*标。

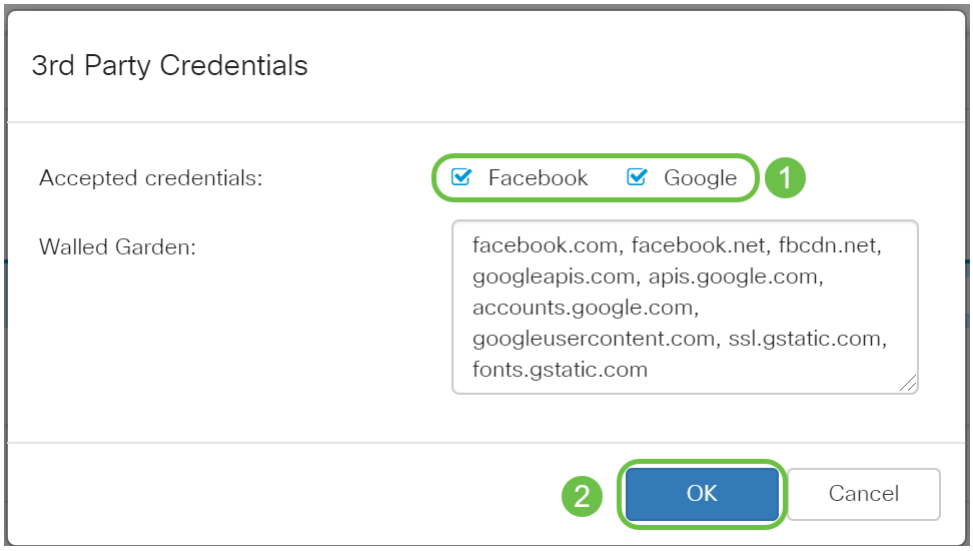


步骤8.配置以下第*三方凭据身*份验证设置。

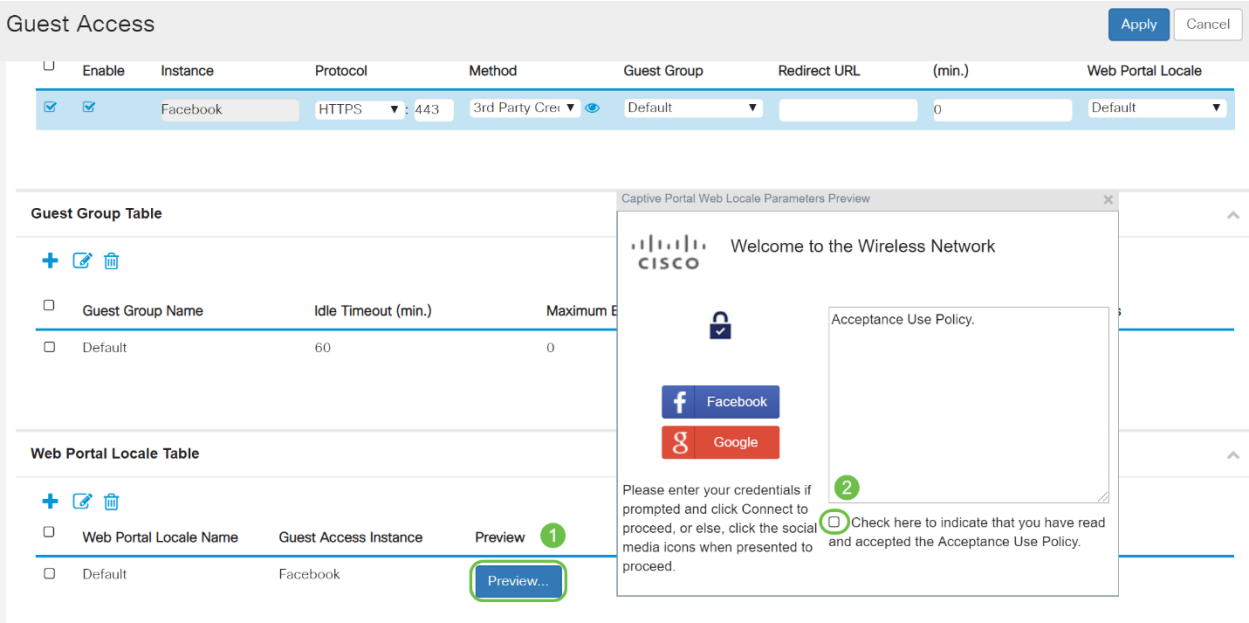
*接受的凭*据 — 选择Facebook、Google或两者。

Walled Garden — 在选择Accepted凭证时，将自动设置相关默认配置。

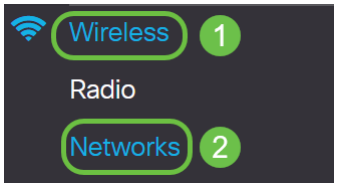
在本例中，选**择**Facebook**和**Google。Click **OK**.



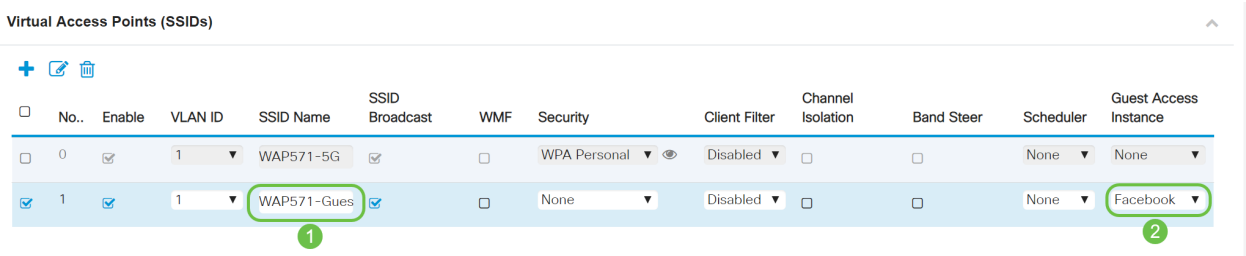
步骤9.（可选）要预览强制网络门户页面，请单击Web门户区域设置表**下的**“预览”*按钮*。新窗口将显示预览页面，提示用户输入其Facebook或Google凭证。用户还必须选中接受使用策略复选框。



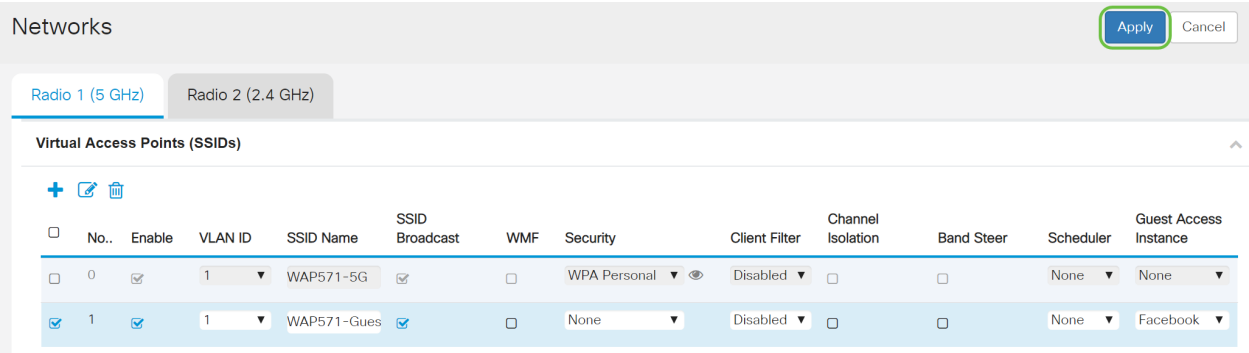
步骤10.转到菜单并选择“无线”**>“网络”**。



步骤11.选择网络并指定它将选择Facebook作为**访客**访问实*例进行身*份验证。在本例中，网络为**WAP571-Guest。**



步骤12.单击“**应用**”。



结论

您已成功在WAP571或WAP571E上通过Google、Facebook或两者配置第三方身份验证。