1.0.1版中用于WAP125和WAP581的功能

目标

本文旨在重点介绍并概述无线接入点(WAP)的固件更新中的最新功能。

适用设备

- WAP125
- WAP581

软件版本

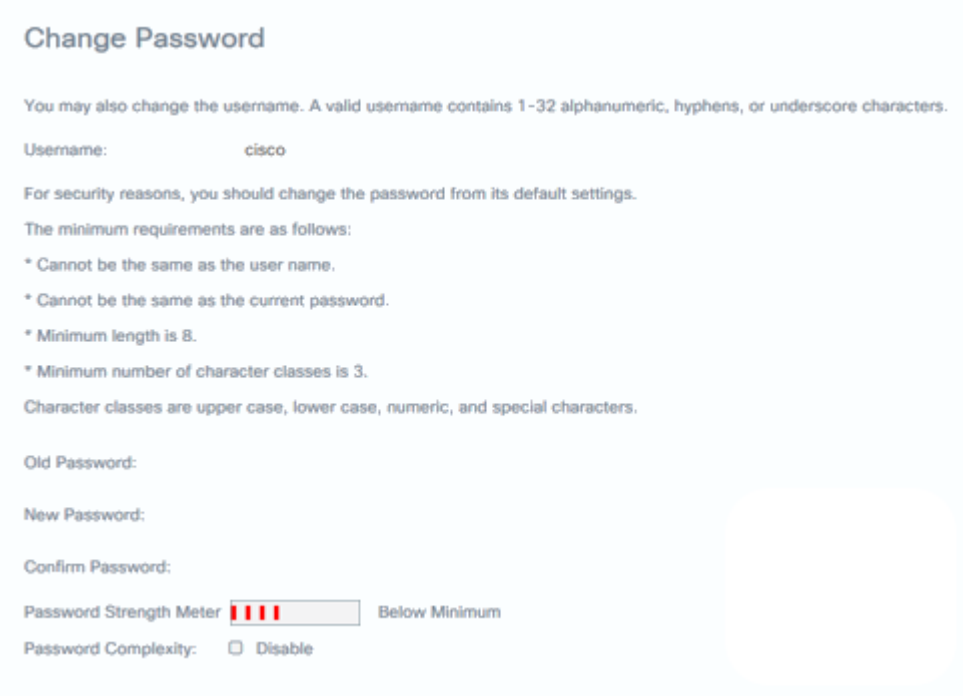
- 1.0.1

设置向导

在WAP125和WAP581的早期版本中，如果取消设置向导，您将从WAP中注销。

1.0.1固件允许您取消安装向导。系统会向您发送警报。

确认警报后，您可以设置WAP的本地密码。



您可以在另一时间手动配置所有设置。

移动优化设置向导

WAP125和WAP581设备现在包括针对移动设备优化的管理页面、强制网络门户页面和设置向导。

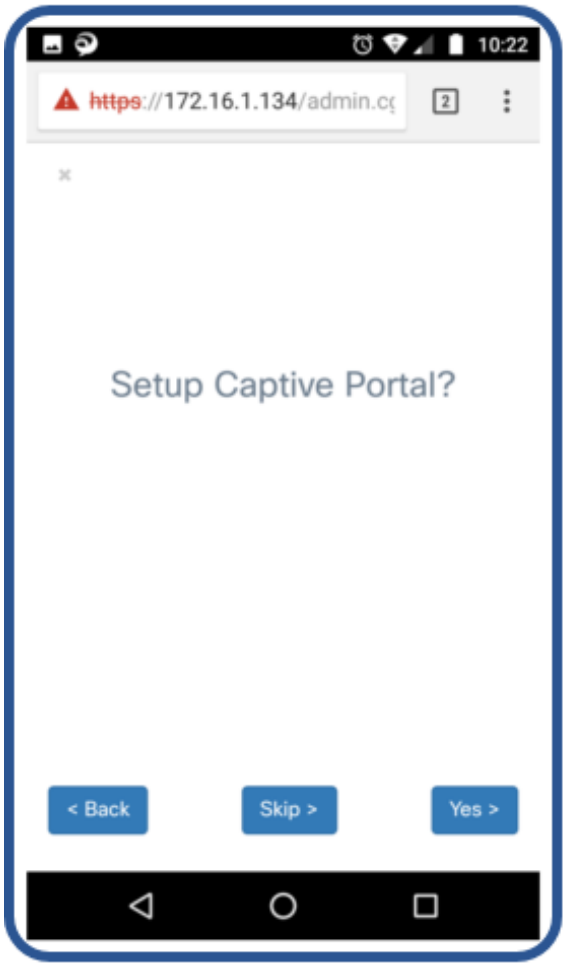
您可以通过使用新的移动优化设置页面通过移动设备运行设置向导来配置WAP。

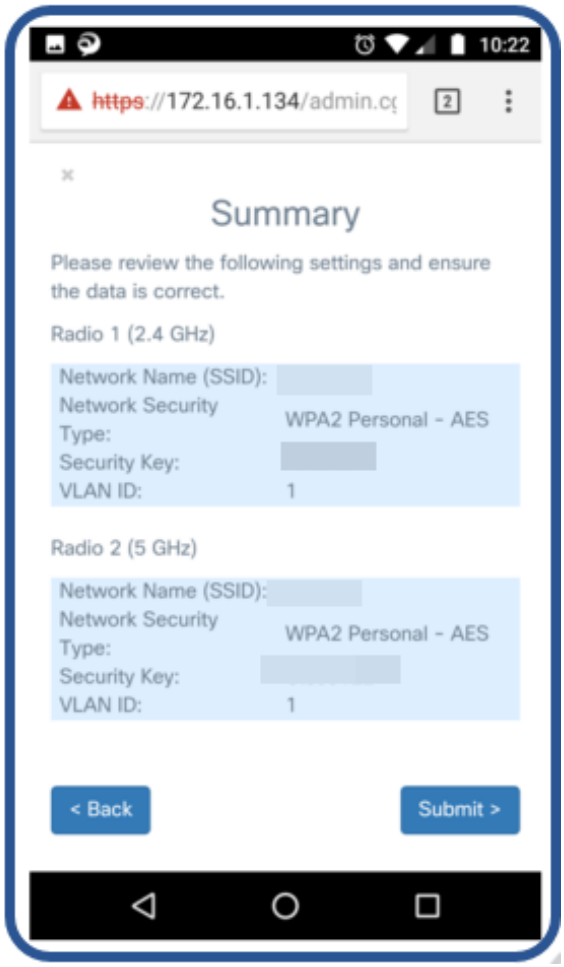
连接到ciscoSB-Setup SSID，然后转到WAP的IP地址或默认IP 192.168.1.245以配置设备。

“设置向导”(Setup Wizard)在移动优化页面上与标准页面上相同。

10:21
https://172.16.1.134/admin.cg
Configure Your Wireless Network
Radio 1 (2.4 GHz)
Radio 2 (5 GHz)
Enter a name for your wireless network:
Network Security Type: WPA2 Personal - AES
Enter a security key with 8-63 characters.
Enter a VLAN ID for your wireless network:
1
Apply same configuration to Radio 2 (5 GHz)
< Back
Next >

10:22
https://172.16.1.134/admin.cg
Configure Your Wireless Network
Radio 1 (2.4 GHz)
Radio 2 (5 GHz)
Enter a name for your wireless network:
Network Security Type: WPA2 Personal - AES
Enter a security key with 8-63 characters.
Enter a VLAN ID for your wireless network:
1
Apply same configuration to Radio 1 (2.4 GHz)
< Back
Next >





第三方访客身份验证

第三方访客身份验证允许您使用Facebook或Google身份验证配置访客网络，这是由第三方验证的安全身份验证。WAP125允许一个访客接入实例，而WAP581允许多个实例。

要求:

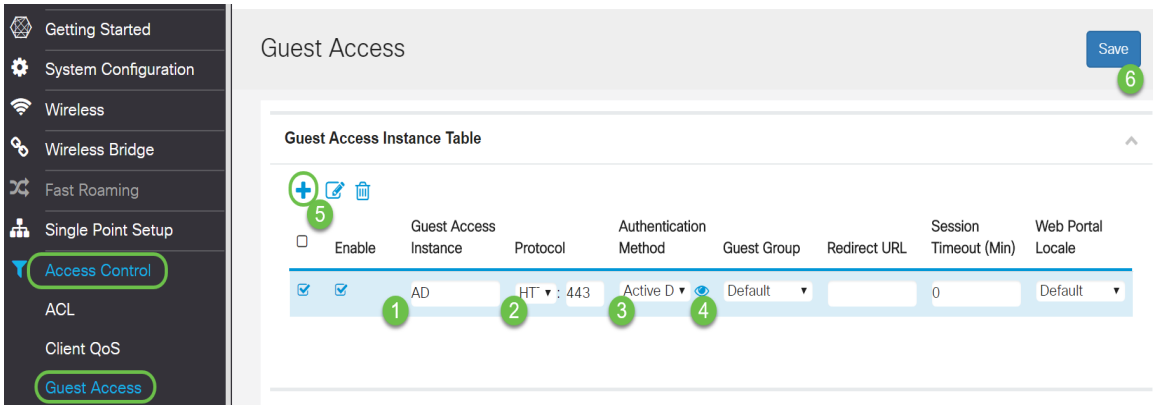
- 与Facebook或Google的Internet连接
- 用户必须拥有或创建Facebook或Google帐户，并无线访问其公共资料
- 身份验证完成前，必须可以访问Facebook或Google，以便最终用户可以登录以验证其凭证。

企业也可以选择在身份验证之前提供其他站点，如其企业网站。

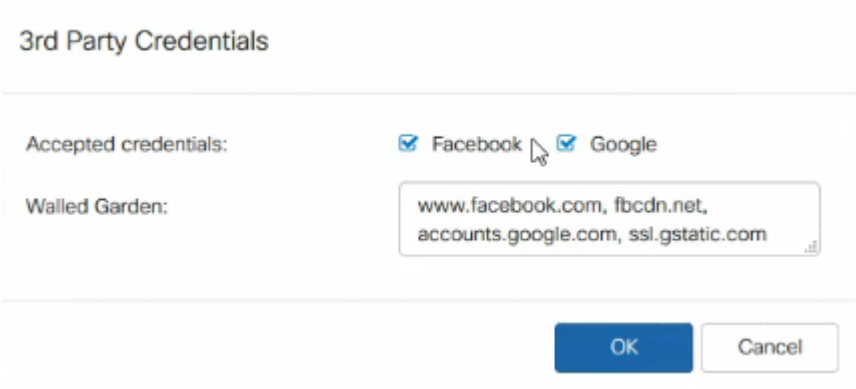
单击**Access Control > Guest Access**，然后单击加号。

以下每个数字的简要说明：

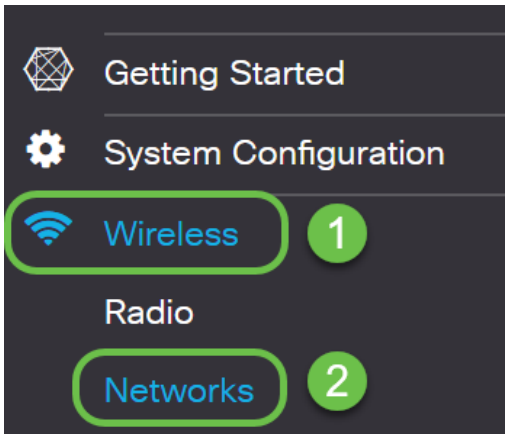
1. 添加Active Directory的名称
2. 您应将强制网络门户页面配置为使**用HTTPS**，而不是HTTP。如果选择HTTP，则可能会无意中暴露用户名和密码，通过空中以未加密的明文形式传输它们。建议使用安全HTTPS强制网络门户页面。
3. 选择**第3方凭据**。
4. 单击眼睛的图形**以选**择接受的凭据和正确的网站。
5. 如果您选择添加另一个访客访问实例，请点击此处。
6. 请务必保**存**。



此示例显示Facebook和Google已选择。Walled Garden的网站列出。



然后，您需要导航到导**航窗格上的**“无线”>“网络”，以将访客访问实例添加或更改为Active Directory的名称。

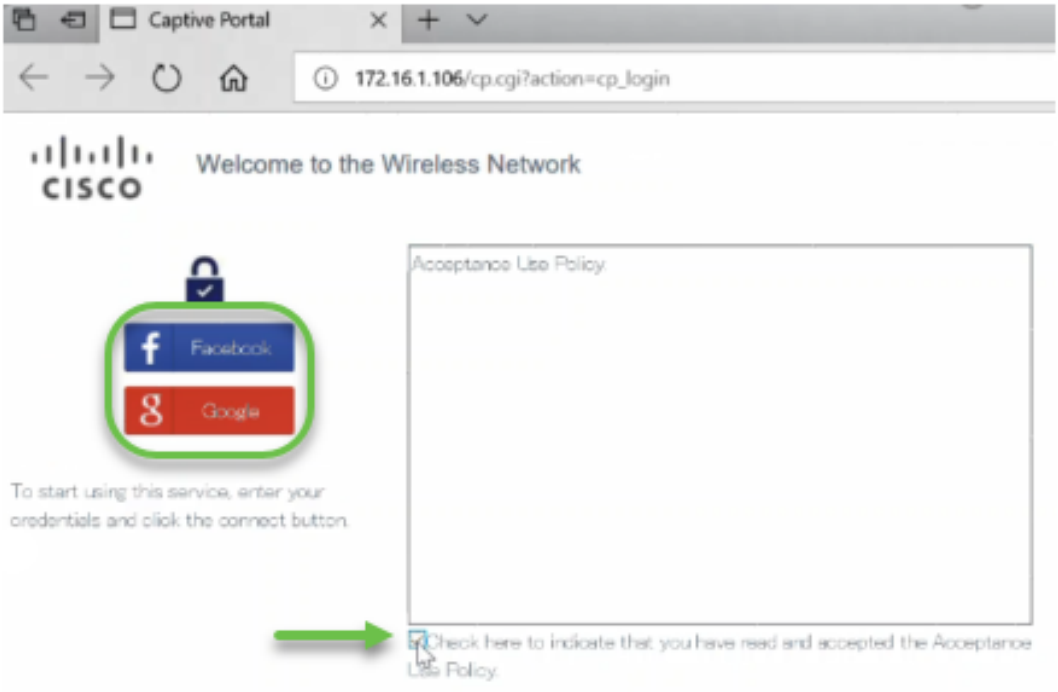


注意：WAP125允许您使用一个访客接入实例，因此您必须决定是否要为第三方身份验证或Active Directory身份验证进行配置。WAP581允许使用多种身份验证方式。

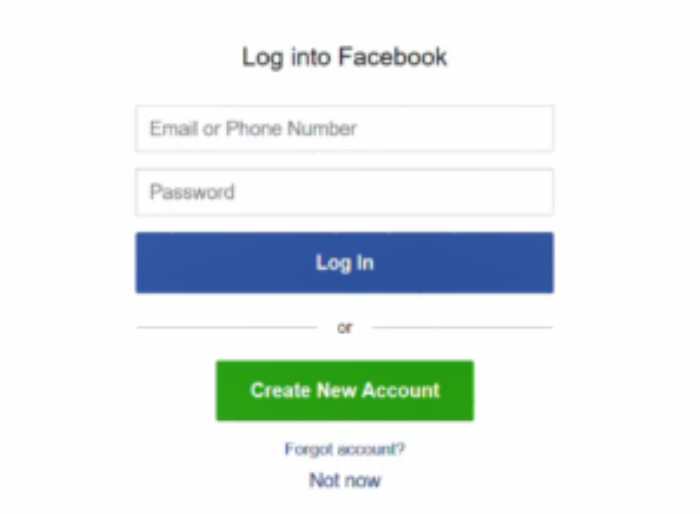
第三方客户端身份验证

当客户端单击以加入无线连接时，强制网络门户将打开。在本例中，Facebook和Google是选项。客户需要选中此框以指示他们已阅读并接受*接受使用策*略，然后选择**Facebook**或**Google**选项登录。

注意：首次登录客户端时，系统会收到询问他们是否要使用强制网络门户的问题。他们需要选择*是*。



然后，客户端可以输入凭证。在本例中，使用了Facebook。



客户端现在可以使用Internet。

Active Directory访客身份验证

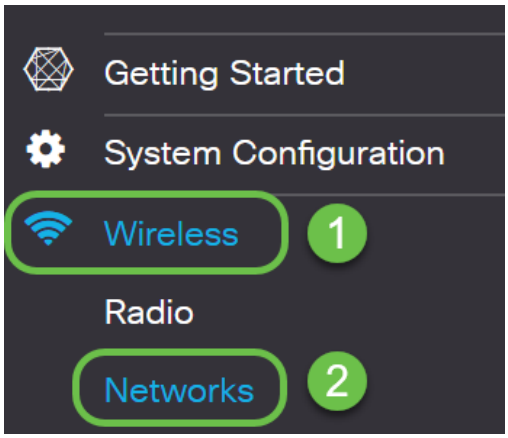
要支持Active Directory身份验证，WAP需要与Windows域控制器通信以提供身份验证。作为管理员，您最多可以设置三个Windows域控制器以在WAP581上通信。

单击**Access Control > Guest Access**，然后单击加号。

以下每个数字的简要说明：

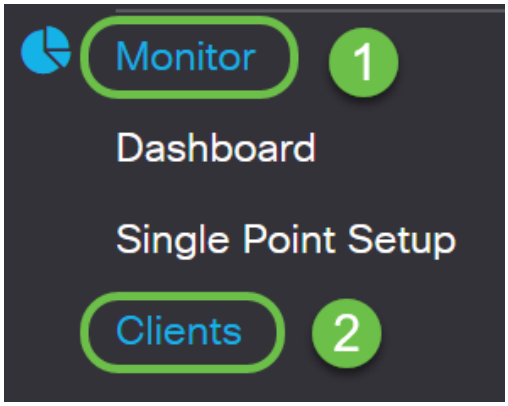
1. 添加Active Directory的名称
2. 您应将强制网络门户页面配置为使**用HTTPS**，而不是HTTP。如果选择HTTP，则可能会无意中暴露用户名和密码，通过空中以未加密的明文形式传输它们。建议使用安全HTTPS强制网络门户页面。
3. 选择**Active Directory服务**
4. 单击眼睛的图**形**添加IP地址。您可以从那里进行测试以检查连接。
5. 如果您选择添加另一个访客访问实例，请点击此处。
6. 确保保存。

然后，您需要导航到导**航窗格上的**“无线”>“网络”，以将访客访问实例添加或更改为Active Directory的名称。



要查看网络上的客户端，请在导航窗格**上单击“监控”>**“客户端”。

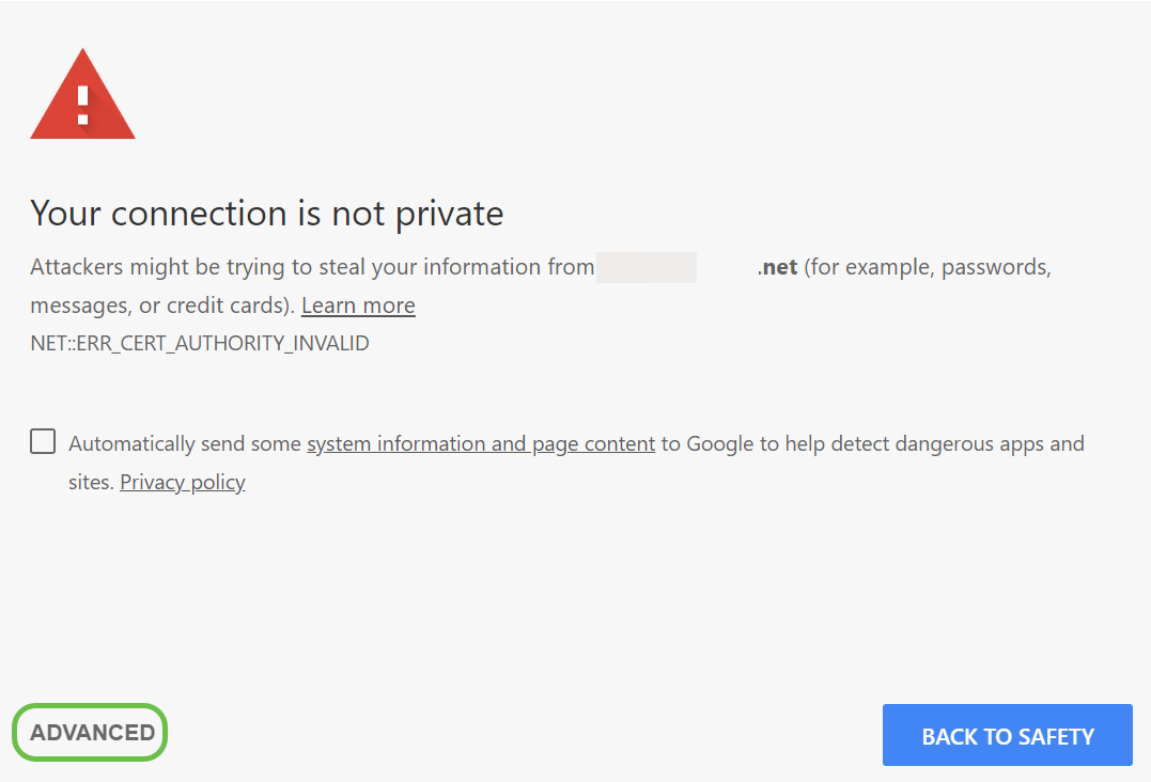
1. *监控*器显示连接的客户端数
2. *客户*端显示客户端的详细信息。如果您想记录连接的人员，可以导出这些。



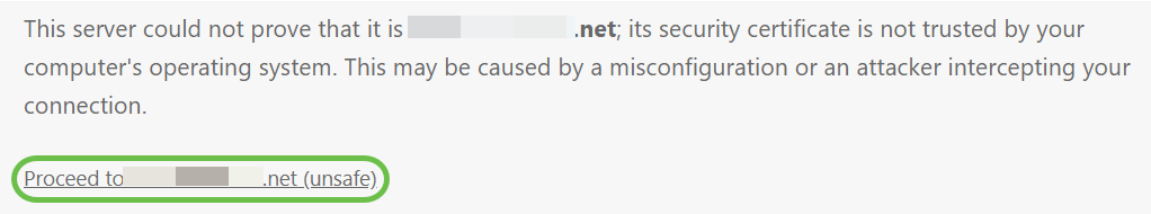
有关如何监控访客的详细信息，请单击此处。

Active Directory客户端身份验证

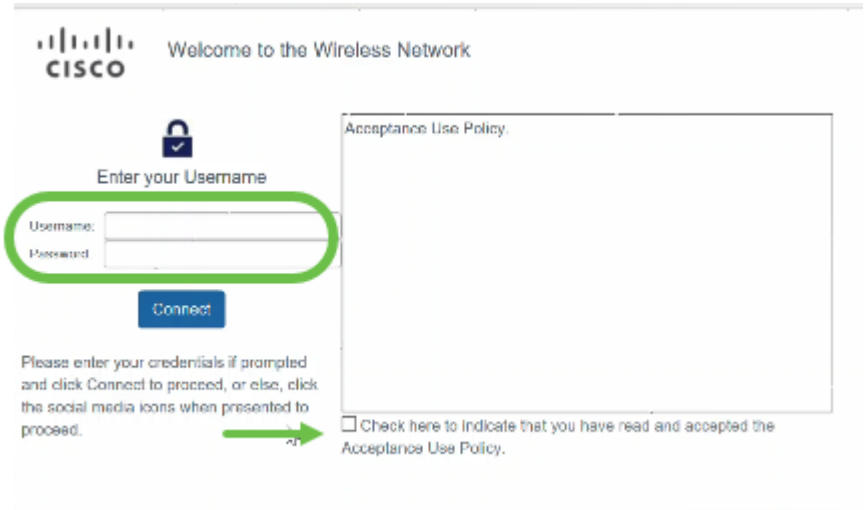
当客户端在Active Directory中时，它们能够登录WAP访问互联网。当他们选择无线接入点时，可能会收到类似于此的警告消息，具体取决于他们使用的Web浏览器。如果受信任证书颁发机构未向页面分配证书，则会出现警告。客户端需要单击“高**级**”。



然后，客户端可能会收到类似于以下内容的警告消息：



已启动门户页面。在此页上，他们应输入其凭据并选中此框，以指示他们已阅读并接受“接受使*用策略*”。



他们将收到欢迎信息，并能够安全地使用互联网。

您现在已熟悉最新WAP125和WAP581更新中的一些最新功能。

有关这些功能和其他新功能的更多详细信息，请点击下面的配套文章链接。

在WAP125或WAP581上使用设置向导

在移动设备上为WAP125或WAP581使用设置向导

如何：思科Umbrella集成

如何：Cisco CloudShark集成

如何：在WAP125或WAP581上配置第3方身份验证设置

如何：Microsoft Active Directory访客身份验证

如何：Umbrella — 如果丢失API密钥密钥，则注册新设备

自定义强制网络门户的外观

查看与本文相关的视频……

单击此处查看思科提供的其他技术讲座