在WAP125或WAP581上使用设置向导

目标

设置向导是一个内置功能，您可以用它来帮助您初始配置无线接入点(WAP)设备。设置向导使配置提供分步说明的设置变得非常简单。

本文档说明如何在Web配置实用程序上使用设置向导配置WAP125和WAP581。

要在移动设备上使用安装向导配置WAP，请单击此处。

适用设备

- WAP125
- WAP581

软件版本

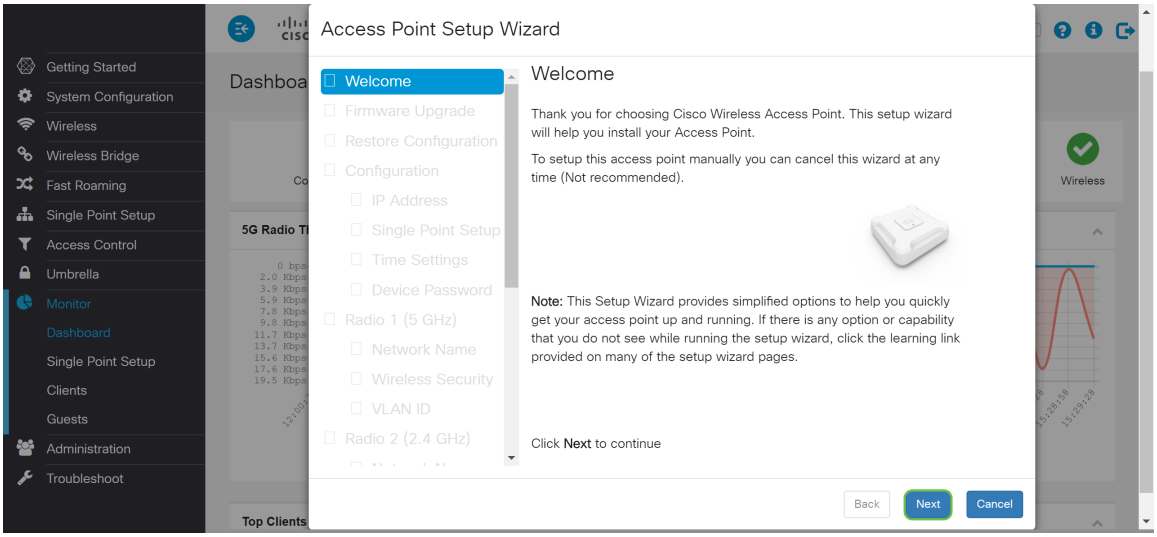
- 1.0.1.3

如何使用安装向导

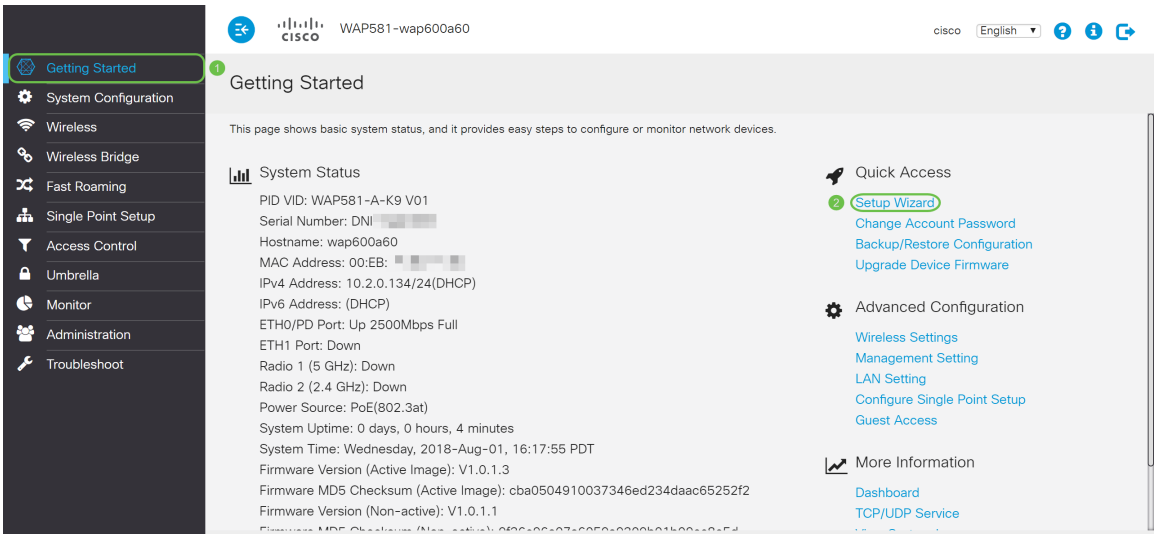
步骤1.通过在Web浏览器中输入WAP的IP地址登录WAP的Web配置实用程序。如果这是您第一次配置WAP，则默认IP地址为192.168.1.254。

注意：本指南中使用WAP581来演示安装向导。外观可能因型号而异。

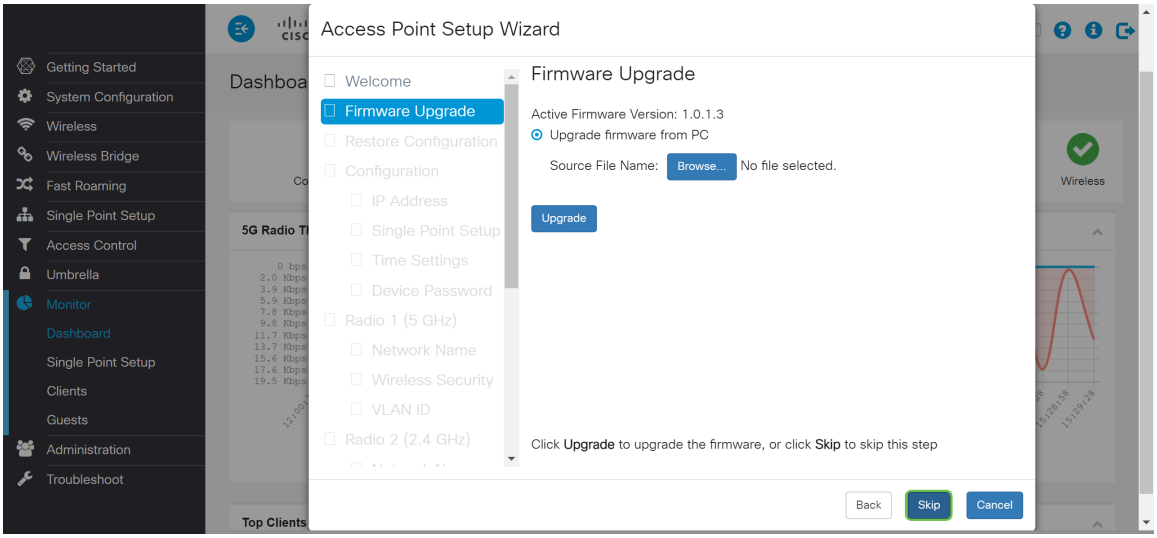
步骤2.首次登录接入点或将其重置为出厂默认设置后，将显示“接入点设*置向导*”。单击“下一步”继续。



注意：如果已配置WAP，但仍要访问设置向导，请导*航至*"入门"**>"设置向导"**。将出*现"Access Point Setup Wizard*（接入点设置向导）"窗口。

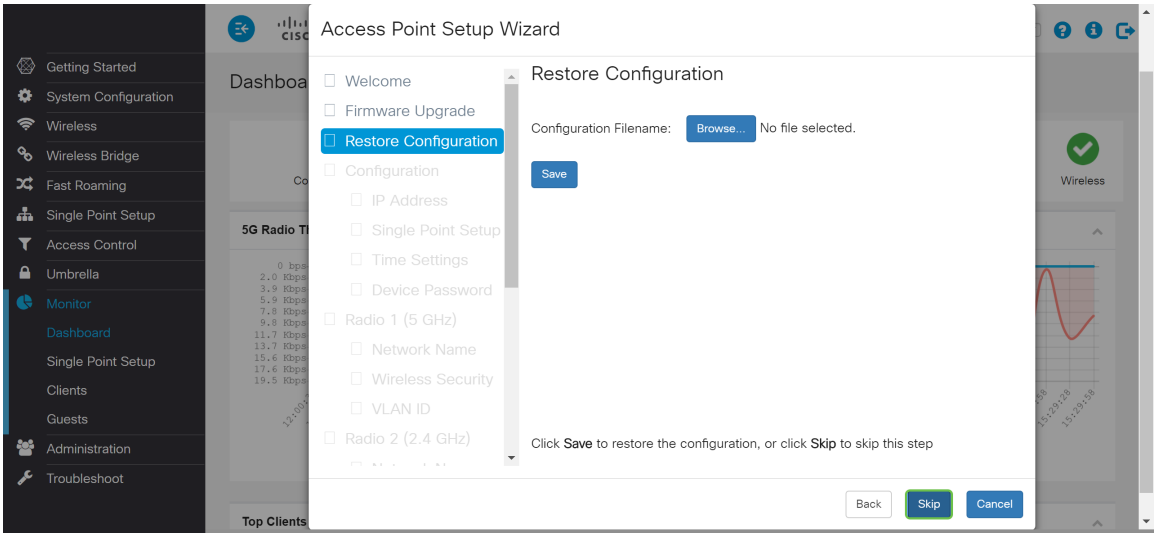


步骤3.在Firmware Upgrade(固*件升级*)窗口中，单击**Browse...** 按钮，然后选择要升级到的固件文件。然后按**Upgrade**升级到该固件。升级固件后，设备将自动重新启动并直接进入登录页面。在本示例中，我们将单击**Skip**，因为我们有所需的固件版本。



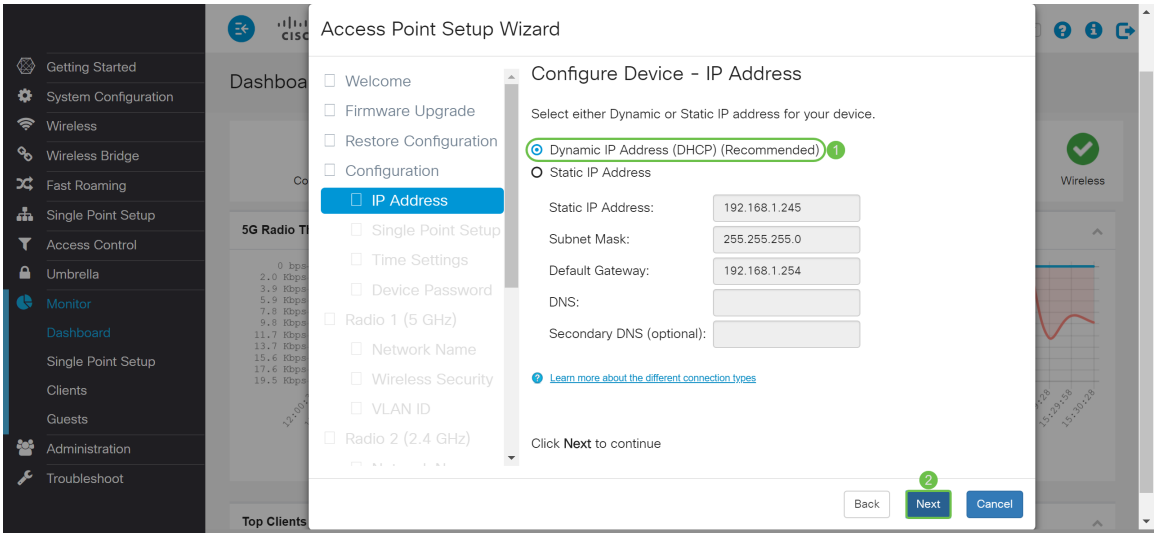
步骤4.如果您有要应用到设备的先前配置，请单击"**浏览.....**" 按钮，*然后选*择要应用的配置文件。然后单击**Save**将配置文件应用到设备。在本例中，我们将单击"**跳过**"。

注意：当设备应用相关配置时，它将重新启动并引导您进入登录页。



步骤5.在*配置设备 — IP地址*窗口中，选择**动态IP地址(DHCP)（建议）**从动态主机配置协议(DHCP)服务器获取IP地址，或单击**静态IP地址**手动配置IP地址。然后单击**“下一步”**继续下一部分。DHCP为Internet主机提供配置参数。在这种情况下，DHCP将IP地址分配给客户端一段有限的时间，或直到客户端明确放弃该地址。

在本例中，我们将选择**动态IP地址(DHCP)（推荐）**。



步骤6.单点设置提供了一种集中管理和控制多个设备间无线服务的方法。这将允许您创建无线设备的单个组或集群，您可以将无线网络作为单个实体进行查看、部署、配置和保护。单点设置有助于简化无线服务中的信道规划，从而减少无线干扰并最大限度地提高无线网络的带宽。

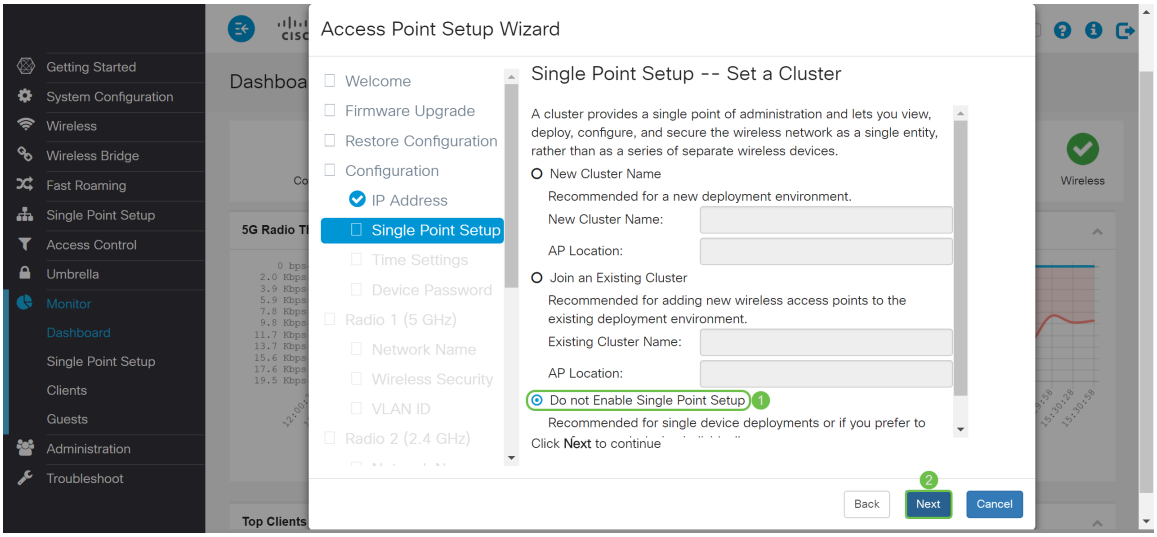
要创建WAP设备的新单点设置，请单击“新建集**群名称”**并指定新名称。当您使用相同的集群名称配置设备并在其他WAP设备上启用单点设置模式时，这些设备会自动加入组。

如果网络中已有集群，可以通过单击**加入现有集群**将此设备添加到其中，然后输入**现有集群名称**。WAP根据集群配置其余设置。单击**Next**并确认确认加入群集。单击**Submit**以加入群集。完成配置后，单击“完**成”**退出“设*置向导*”。

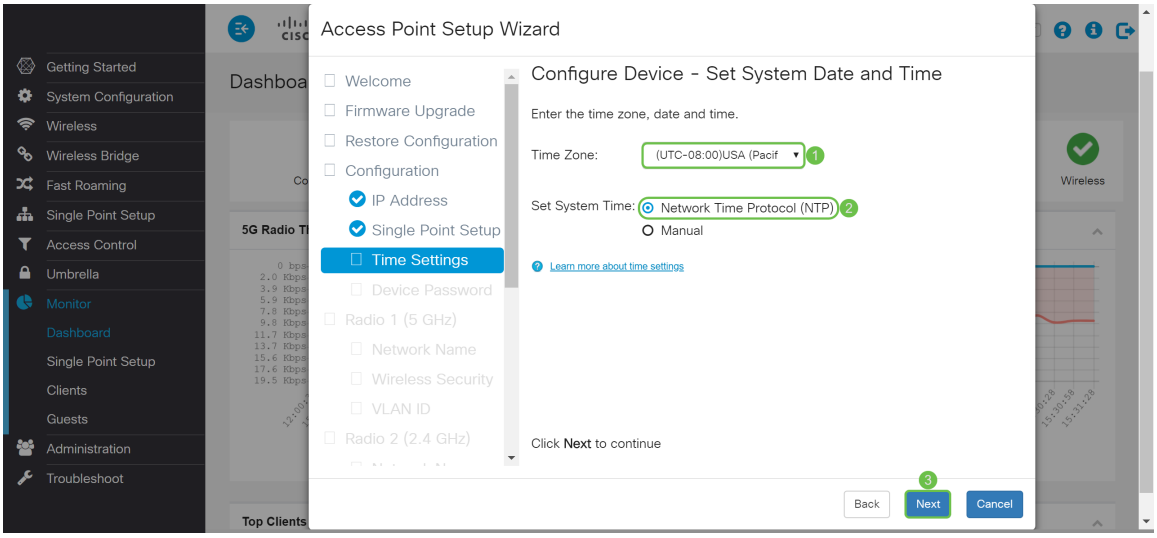
注意：您可以在AP Location字段中输入接**入点**位置，以记录WAP设备的物理位置。

如果此时不希望此设备参与单点设置，请单击“不启**用单点设置”**。

在本例中，我们将选择**“不启用单点设置”**。然后单击**Next(下一步)**继续下一节。



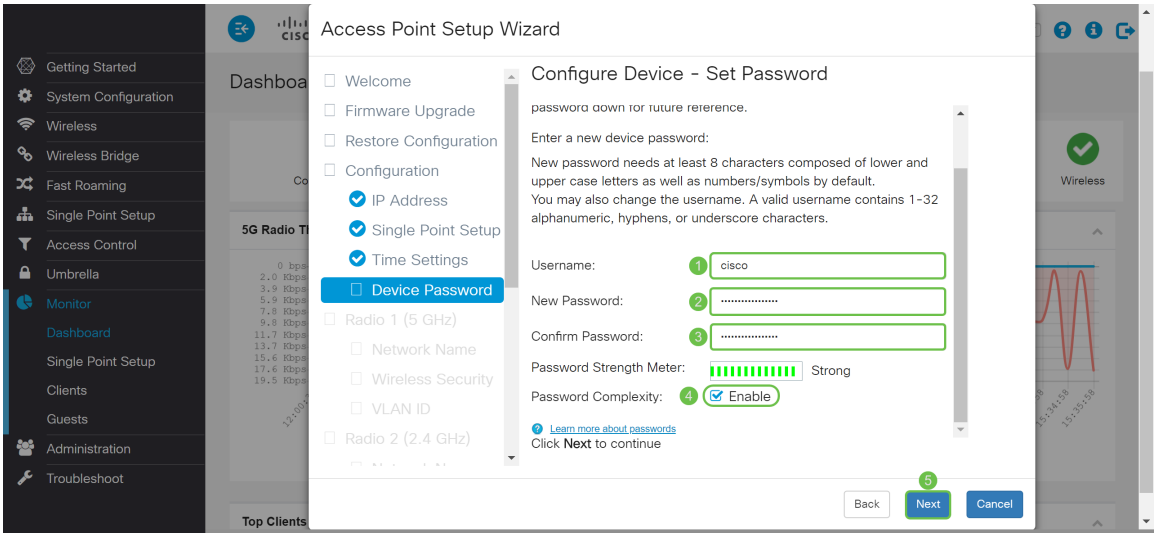
步骤7.在*配置设备 — 设置系统日期和时间*窗口中，选择**时区**，然后选择是希望系统时间自动从网络时间协议(NTP)服务器获取时间设置，还是选择**手动**以手动配置时间设置。系统时钟为消息日志提供网络同步时间戳服务。系统时钟可以手动配置，也可以配置为从服务器获取点击数据的NTP客户端。单击"**下一步**"以继*续安装向导*。



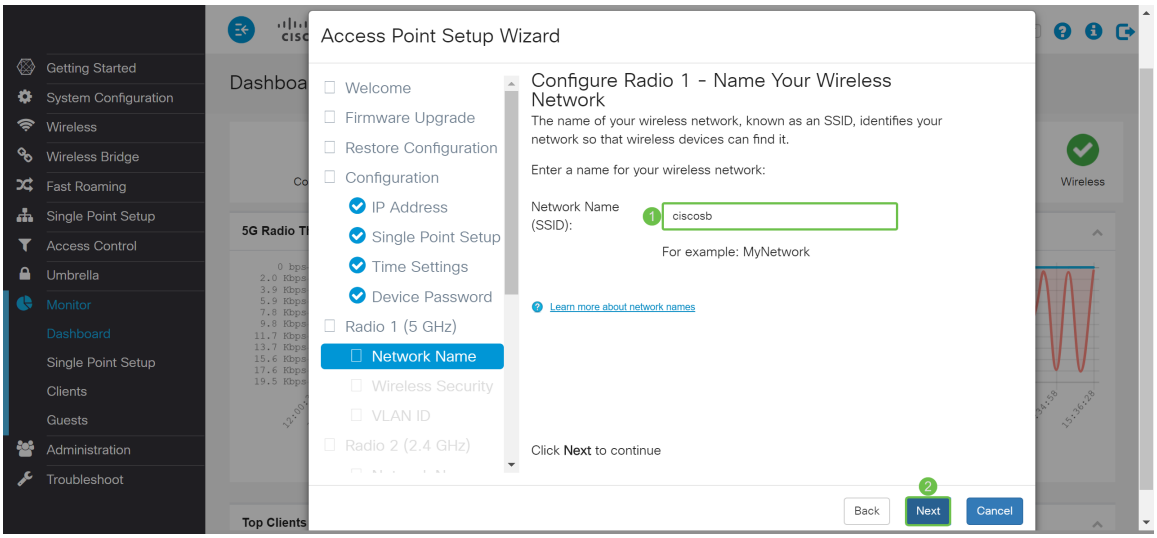
步骤8.在Username字段**中输**入新*Username*，默认情况下用户名为cisco。输入用**户名**的新*密码*。然后在"确认密**码"字**段中再次*输入新*密码。您可以取消选中密码复*杂性以*禁用密码安全规则。但是，我们强烈建议保持密码安全规则的启用状态。新密码必须符合以下复杂性设置：

- 与用户名不同。
- 与当前密码不同。
- 最小长度为8个字符。
- 包含至少三个字符类（大写字母、小写字母、数字和标准键盘上可用的特殊字符）的字符。

然后单击**Next**以配*置Radio 1*。



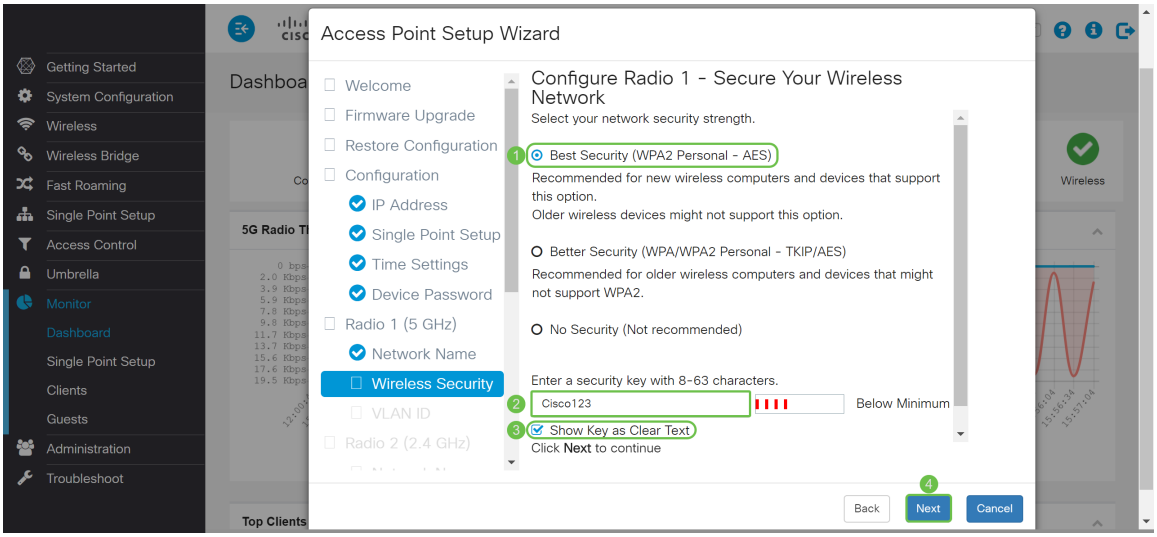
步骤9.在Network Name(SSID)中输入无线网络*的名称*。 这有助于识别您的网络，以便无线设备能够找到它。默认情况下，**ciscosb**用作网络名称。然后单击**Next(下**一步)继续下一节。



步骤10.点击与要应用到无线网络的网络安全对应的单选按钮。然后在安全密钥字段中输入网络*的密*码。要在键入时查看密码，请选中**Show Key as Clear Text复**选框。单击“下一步”继续。

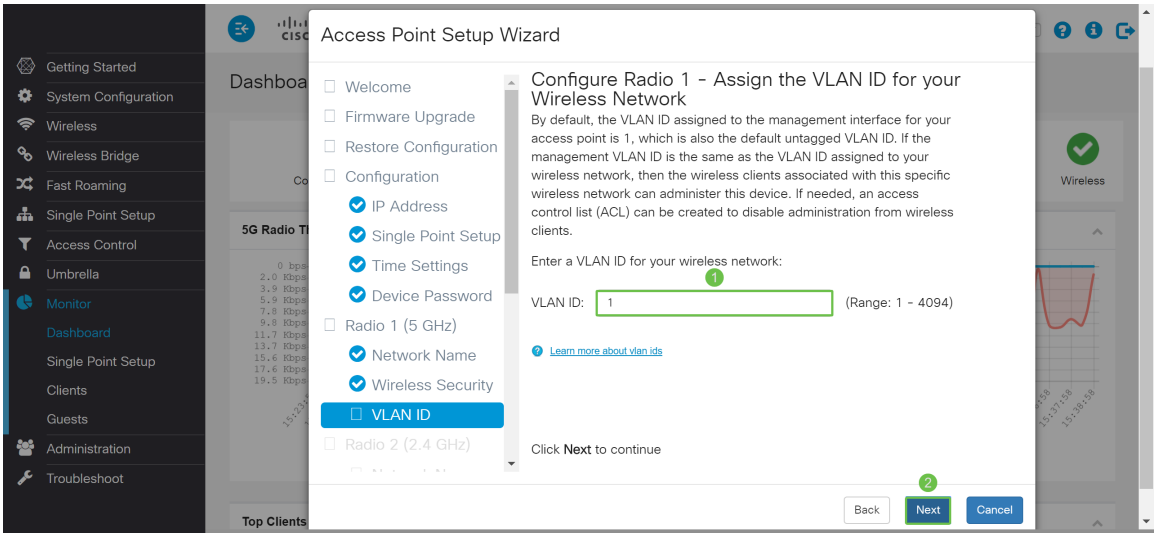
注意：如果网络有客户端组合，其中一些客户端支持WPA2，而其他客户端仅支持原始WPA，请同时选择两者(WPA/WPA2)。 这样，WPA和WPA2客户端站点便可进行关联和身份验证，但对支持WPA2的客户端使用更强健的WPA2。此WPA配置允许更多的互操作性，而不是某些安全性。

- 最佳安全(Wi-Fi保护访问2(WPA2)个人 — 高级加密标准(AES)) 网络上的所有客户端工作站都支持使用计数器模式和密码块链消息验证码协议(AES-CCMP)密码/安全协议的WPA2和高级加密标准加密算法。这为IEEE 802.11i标准提供最佳安全性。根据最新的Wi-Fi联盟要求，AP必须始终支持此模式。
- 更好的安全性（WPA/WPA2个人 — TKIP/AES） WPA个人是Wi-Fi联盟IEEE802.11i标准，包括AES-CCMP和TKIP加密。当存在支持原始WPA但不支持较新WPA2的较旧无线设备时，它提供安全性。
- 无安全防护（不推荐） 无线网络不需要密码，任何人都可以访问。

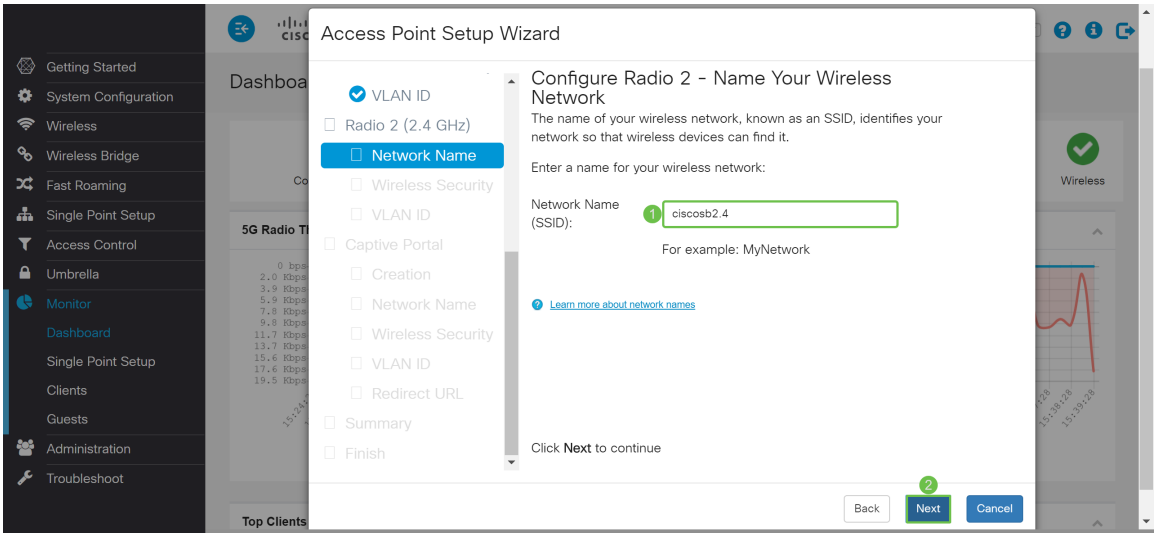


步骤11.在*VLAN ID*字段中，输入您希望Radio 1(5 GHz)*属于的VLAN*的ID号。在本例中，我们将VLAN ID保*留为*1。单击**下一步**以*配置Radio 2(2.4 GHz)*。

注意：我们建议您为无线流量分配不同的VLAN ID（默认值为1），以便将其与VLAN 1上的管理流量分离。单击此处了解有关虚拟接入点(VAP)的详细信息。



步骤12.在Network Name(SSID)字段中*输入新网络*名称。默认情况下**使用**ciscosb。网络名称称为SSID，它标识您的网络，以便无线设备能够找到它。在本示例中，**ciscosb2.4**用于区分5 GHz网络名称。单击**Next**为Radio 2(2.4 GHz)*配置无线安全性*。

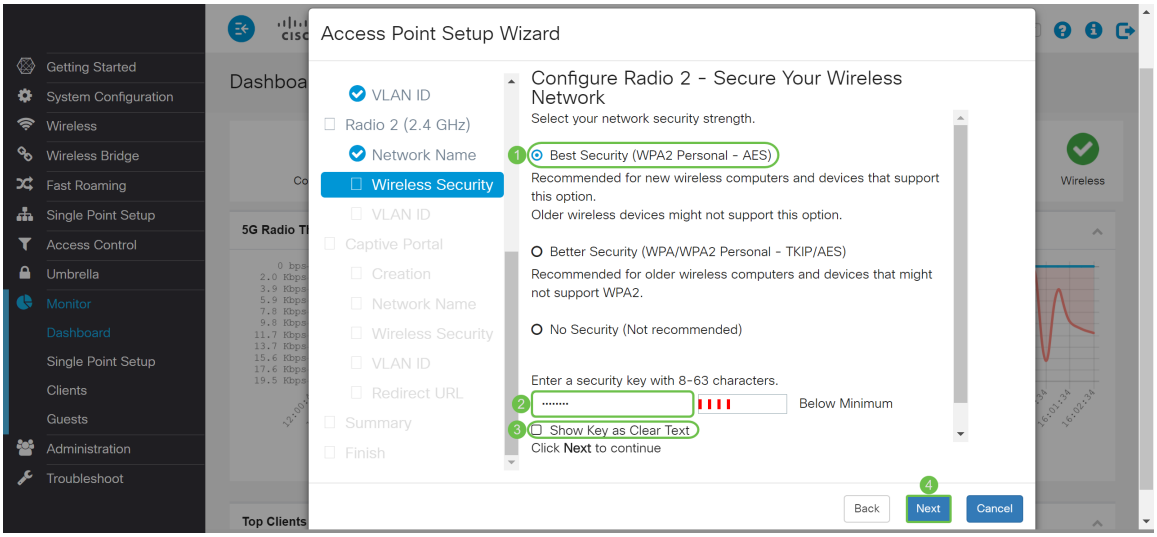


步骤13.点击与要应用到无线网络的网络安全对应的单选按钮。然后在安全密钥字段中输入网络*的密*码。要在键入时查看密码，请选中**Show Key as Clear Text复**选框。默认**情况下会选中**Show Key as

Clear Text。单击“下一步”继续。

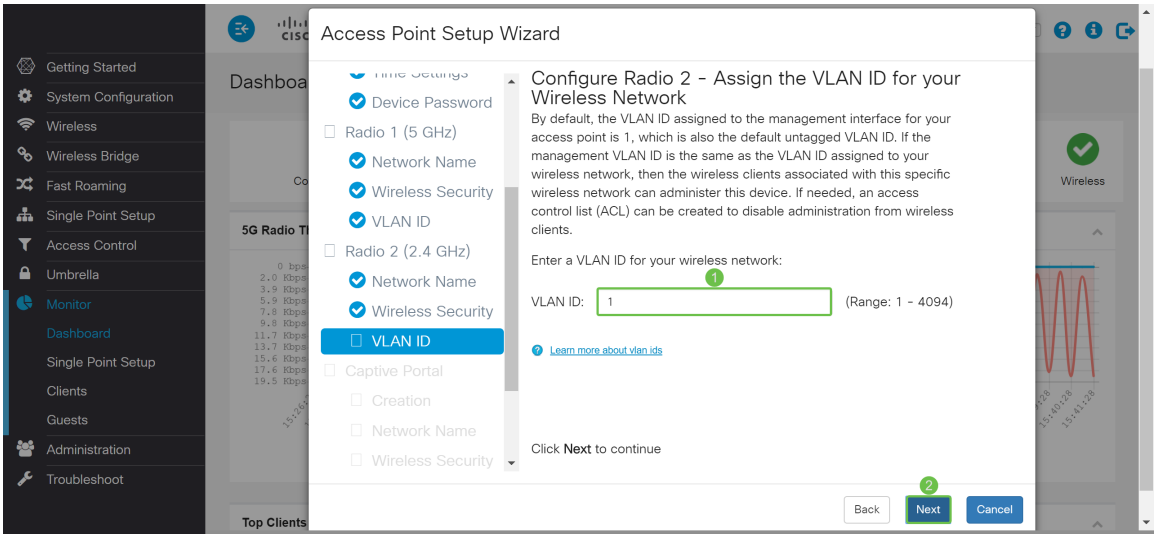
注意：如果网络有客户端组合，其中一些客户端支持WPA2，而其他客户端仅支持原始WPA，请同时选择两者(WPA/WPA2)。 这样，WPA和WPA2客户端站点便可进行关联和身份验证，但对支持WPA2的客户端使用更强健的WPA2。此WPA配置允许更多的互操作性，而不是某些安全性。

- 最佳安全(Wi-Fi保护访问2(WPA2)个人 — 高级加密标准(AES)) 网络上的所有客户端工作站都支持使用计数器模式和密码块链消息验证码协议(AES-CCMP)密码/安全协议的WPA2和高级加密标准加密算法。这为IEEE 802.11i标准提供最佳安全性。根据最新的Wi-Fi联盟要求，AP必须始终支持此模式。
- 更好的安全性（WPA/WPA2个人 — TKIP/AES） WPA个人是Wi-Fi联盟IEEE802.11i标准，包括AES-CCMP和TKIP加密。当存在支持原始WPA但不支持较新WPA2的较旧无线设备时，它提供安全性。
- 无安全防护（不推荐） 无线网络不需要密码，任何人都可以访问。

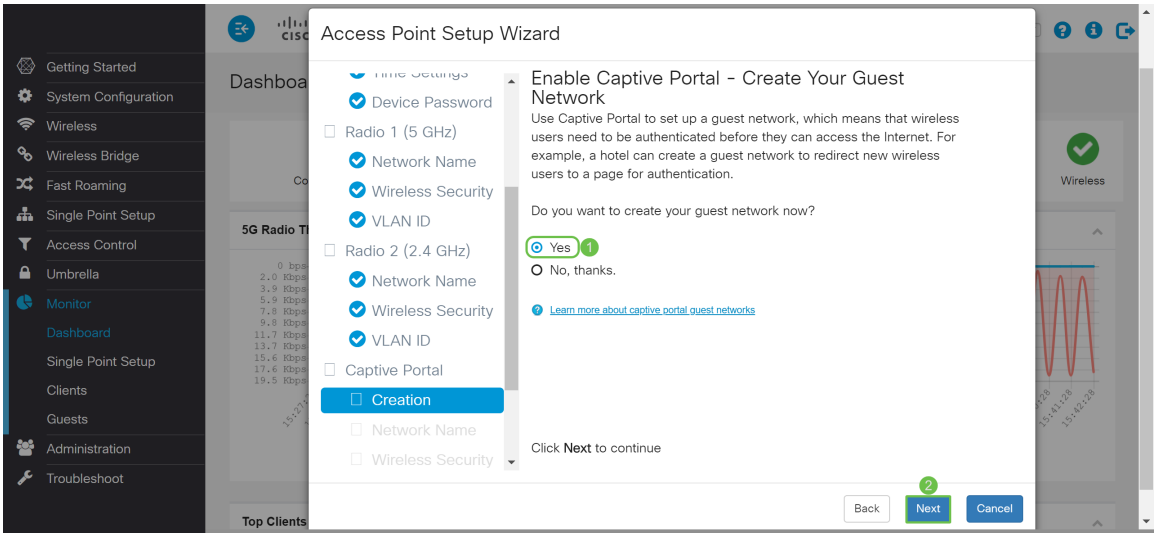


步骤14.在*VLAN ID*字段中，输入您希望Radio 1(2.4 GHz)*属于的VLAN*的ID号。在本例中，我们将使用默认值1作为*VLAN ID*。单击**Next**以配置强*制网络门户*。

注意：我们建议您为无线流量分配不同的VLAN ID（默认值为1），以便将其与VLAN 1上的管理流量分离。单击此处了解有关虚拟接入点(VAP)的详细信息。

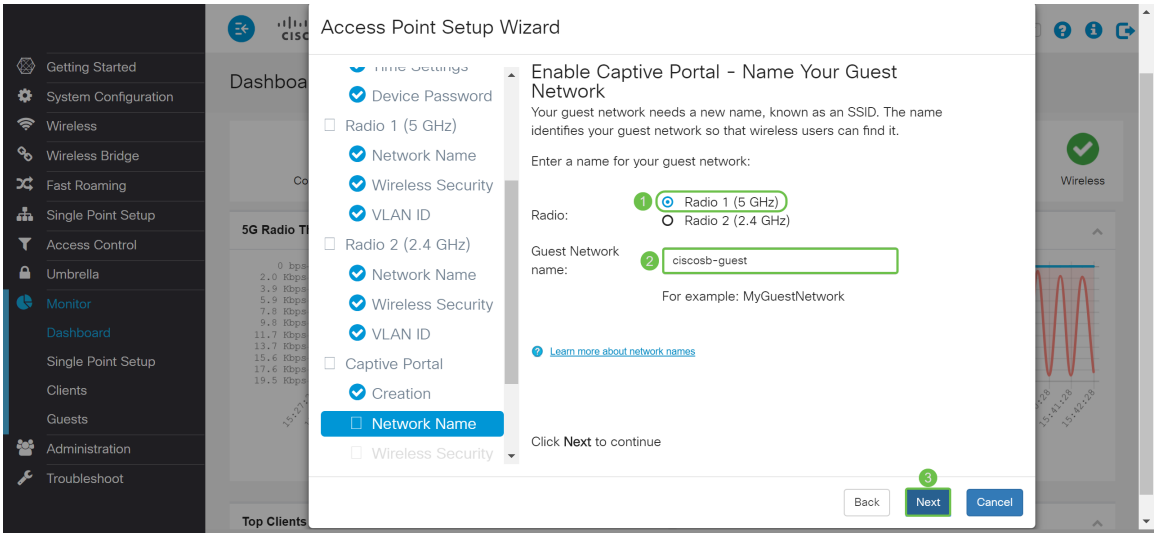


步骤15.（可选）不需要访客网络。如果要创建访客网络，请单击**是**单选按钮。如果不想创**建访**客网络，请单击“否”单选按钮，然后跳至步骤20。单击**下一步**按钮继续。



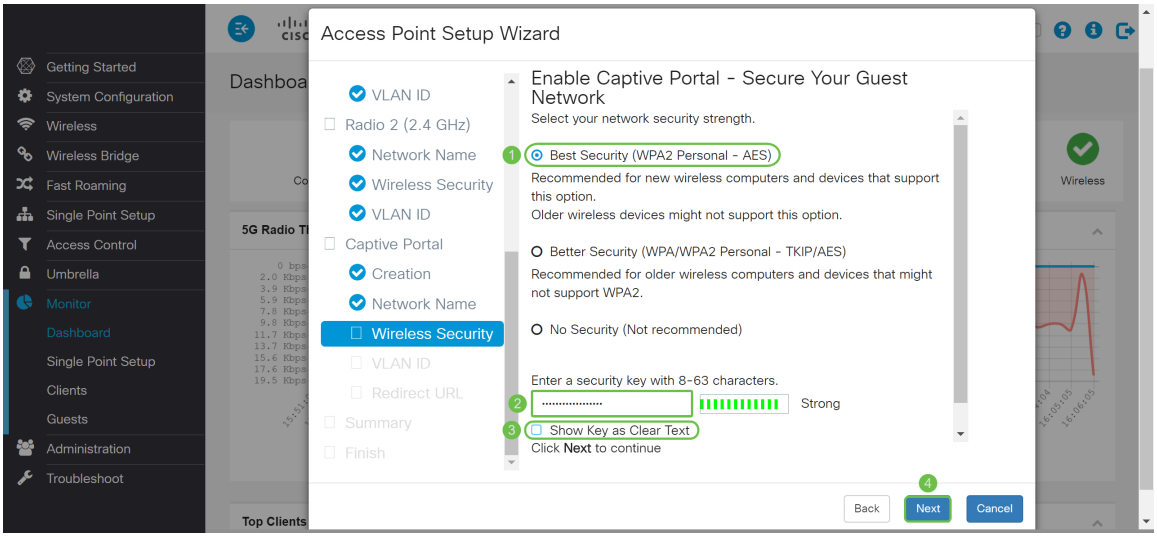
第16步。（可选）选择与您要放置访客网络的*Radio*对应的单选按钮。然后在Guest Network name字段中*创建网络*名称。单击**Next**为访客网*络配*置无线安*全设置*。

在本示例中，我们将选择**Radio 1(5 GHz)**作为*Radio*，并将默认网络名称保留为**ciscosb-guest**，以便您的无线访客用户可以找到网络名称。

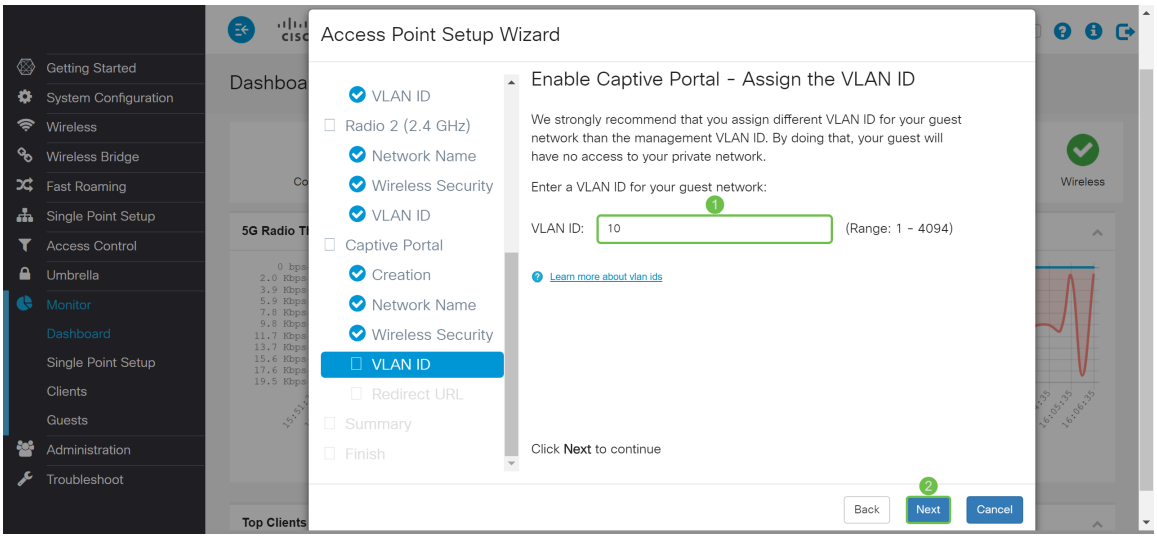


第17步。（可选）选择与要应用于访客网络的网络安全性对应的单选按钮。然后，在Security Key（安全密钥）字段（如果适用）*中输入访*客网络的密码。要将**密钥显示为明文**，请选中此复选框以将安全密钥显示为明文。默认情况下启用该接口。单击“下一步”继续。网络安全选项包括：

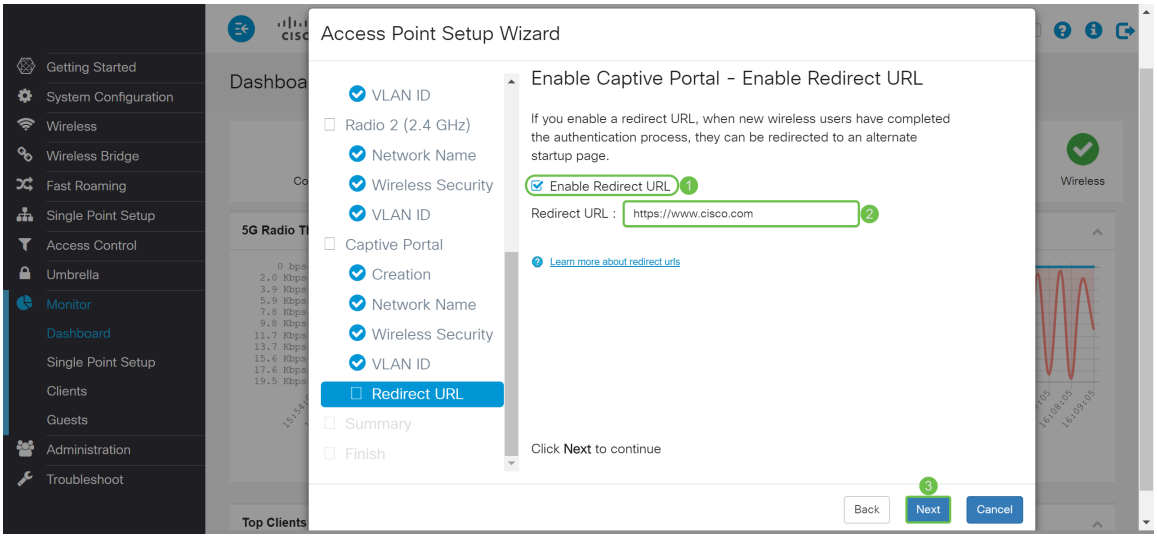
- 最佳安全性（WPA2个人 — AES）— 建议用于支持此选项的新无线计算机和设备。
- 更好的安全性（WPA/WPA2个人 — TKIP/AES）— 建议用于可能不支持WPA2的旧式无线计算机和设备。
- 无安全（不推荐）— 这是默认选择。



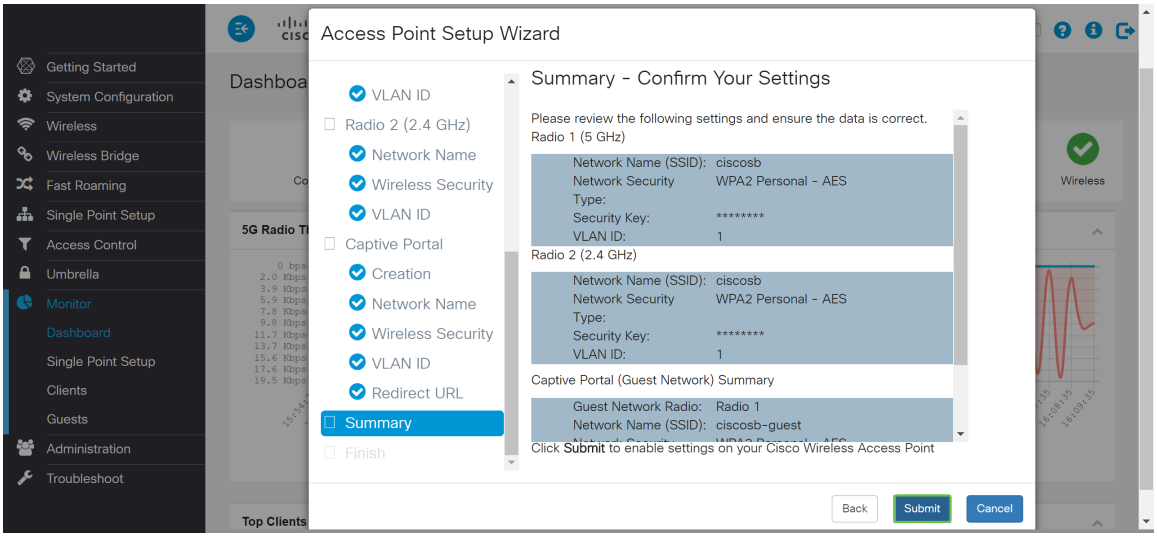
步骤18.（可选）为访*客网*络指定VLAN ID。访客网络VLAN ID应与管理VLAN ID不同。在本示例中，我们*使用VLAN ID* 10作为访客网络的VLAN ID。单击**Next**为访**客网***络配*置重定向URL。



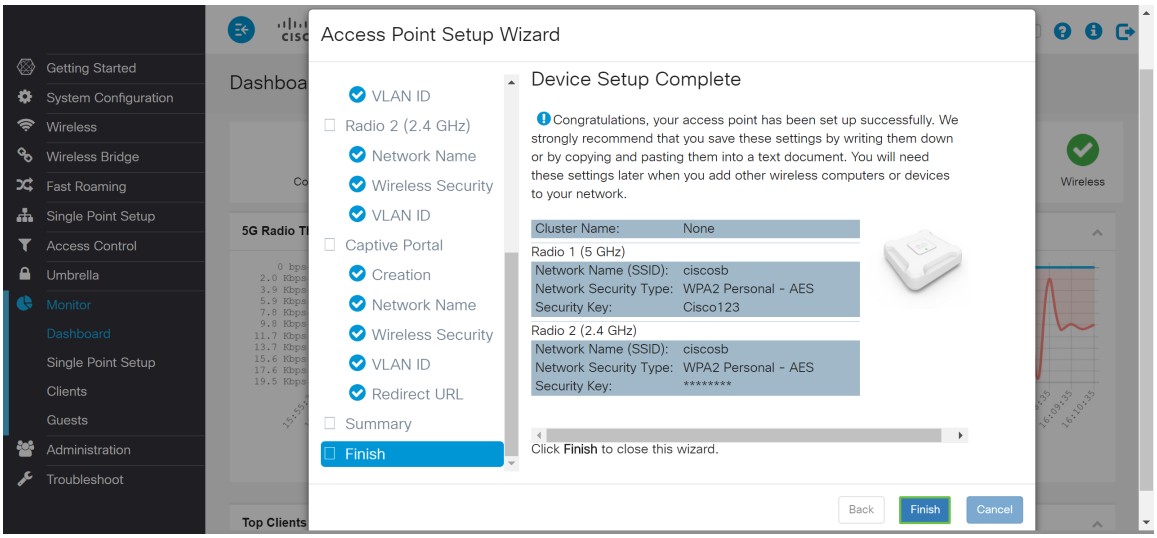
第19步。（可选）选中**启用重定向URL**复选框，将新无线用户重定向到备用启动页。在重定向URL字段(包括http://或https://)中输入完全限*定域*名(FQDN)或IP地址。 然后单**击下**一步以继续*进入*Summary页。



步骤20.在“摘*要 — 确认设置”页*面中，查看您配置的设置。单击“**Back**”**按钮以重新配置一个或多个设置。**如果单击“**取消**”，则所有设置都将返回到以前或默认值。如果配置正确，请单击“**Submit**”。设置设置已保存，并显示确认窗口。



步骤21.配置完设置后，将显示“设备设置完成”页，以告知您接入点已成功设置。单击**Finish**，您将需要使用新密码重新登录。



结论

您现在已使用设置向导成功配置WAP。您应该看到您刚在Wi-Fi网络列表中配置的SSID。要在WAP上配置其他功能，您需要重新登录。