使用WAP125或WAP581上的安裝嚮導

目標

安裝嚮導是一個內建功能，可用於幫助您初始配置無線接入點(WAP)裝置。設定嚮導使配置設定非常簡單，提供逐步說明。

本文檔介紹如何在Web配置實用程式上使用安裝嚮導配置WAP125和WAP581。

要在流動裝置上使用安裝嚮導配置WAP，請按一下此處。

適用裝置

- WAP125
- WAP581

軟體版本

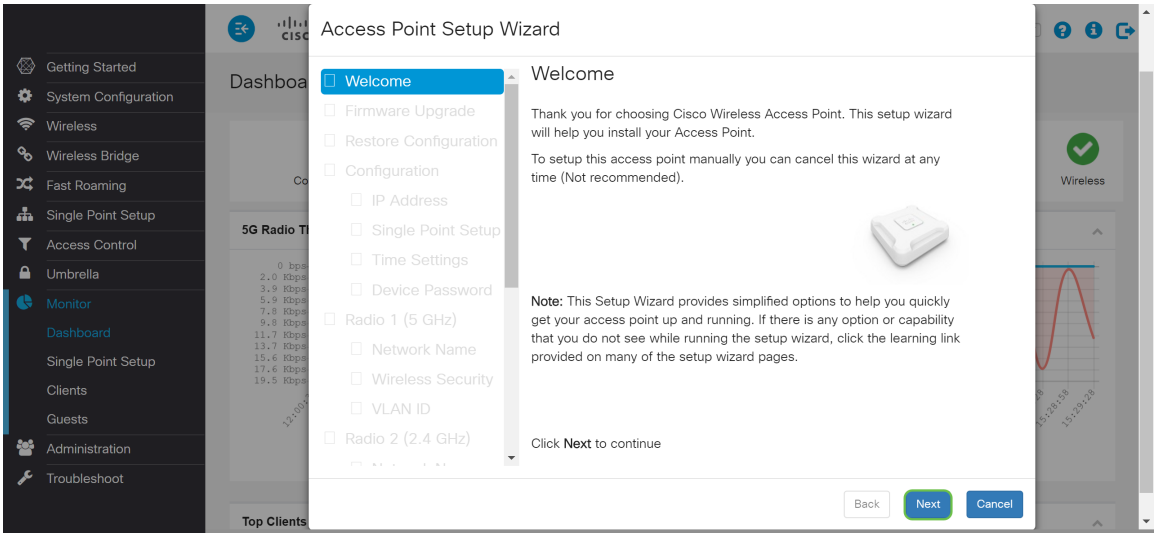
- 1.0.1.3

如何使用安裝嚮導

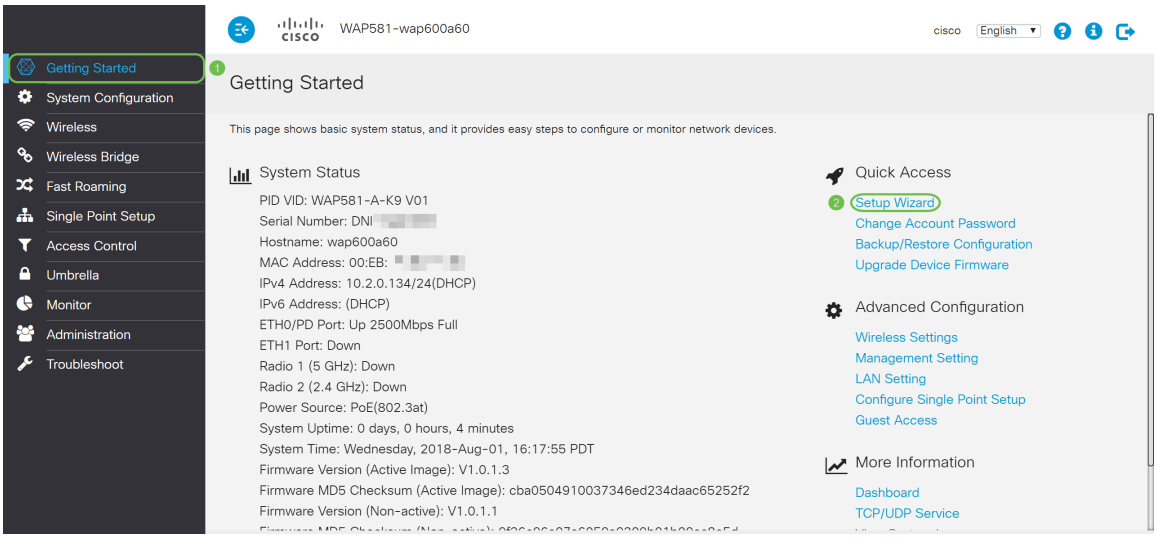
步驟1.將WAP的IP地址輸入到Web瀏覽器中，以登入到WAP的Web配置實用程式。如果這是您首次配置WAP，則預設IP地址為192.168.1.254。

附註：本指南使用WAP581來演示安裝嚮導。外觀可能因型號而異。

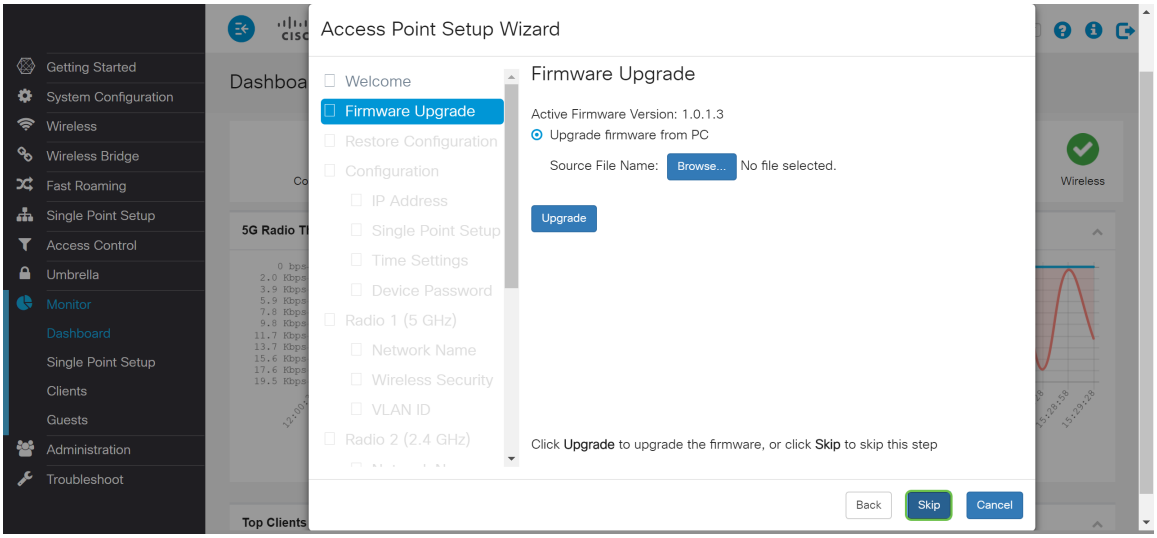
步驟2.首次登入接入點或將其重置為出廠預設設定後，將出現*接入點設定嚮導*。按一下**下一步**繼續。



附註：如果已配置WAP，但您仍想訪問*安裝嚮導*，請導航到**入門>安裝嚮導**。將會顯示*Access Point Setup Wizard*視窗。

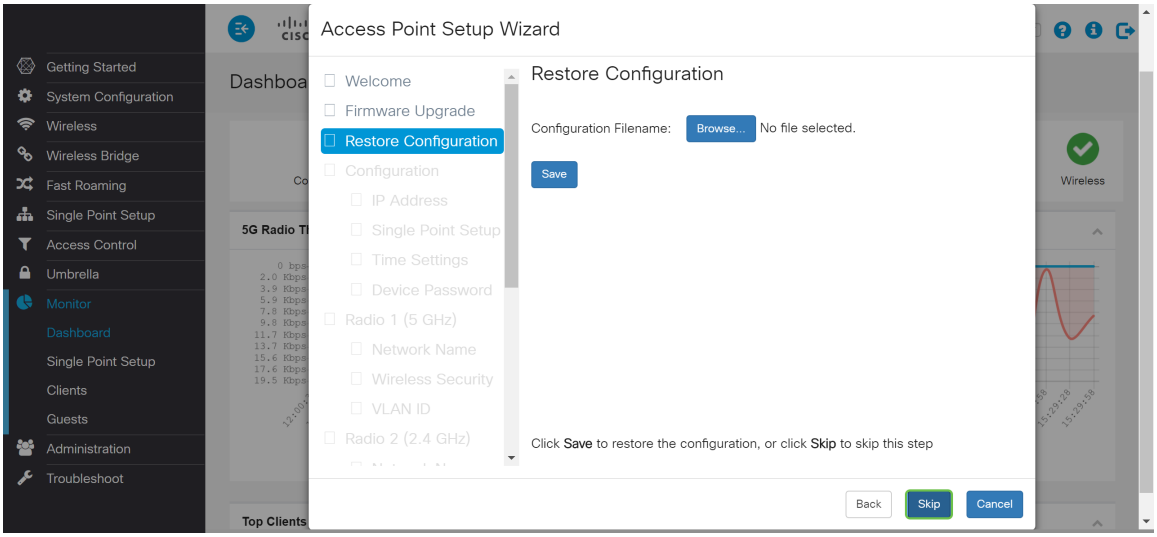


步驟3.在*Firmware Upgrade*視窗中，按一下**Browse...** 按鈕，並選擇要升級到的韌體檔案。然後按升級以升級至該韌體。升級韌體後，裝置將自動重新啟動並直接轉到登入頁面。在本例中，我們將點選**Skip**，因為我們需要韌體版本。



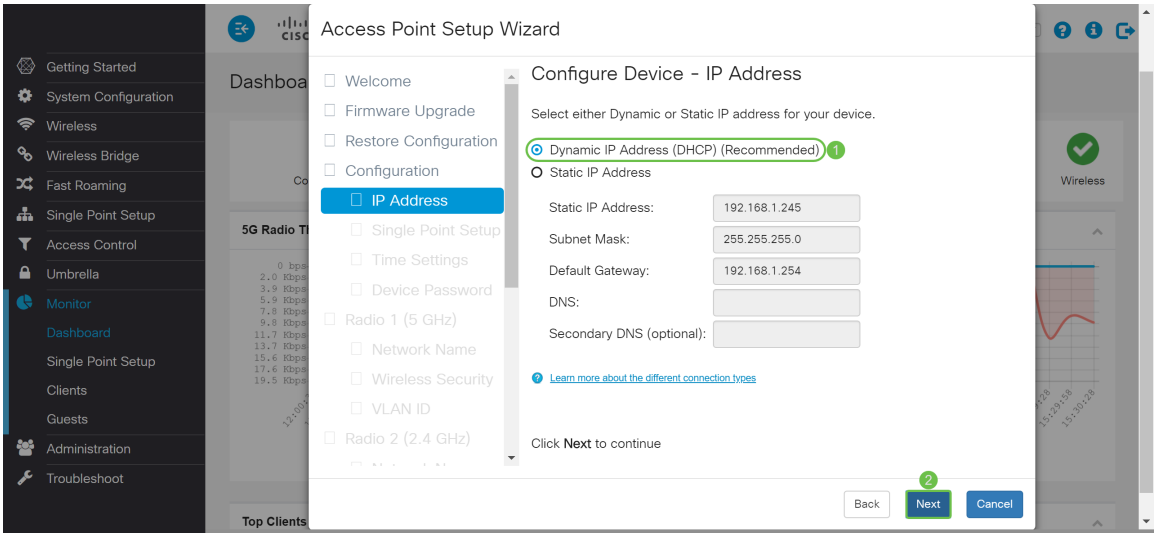
步驟4.如果您有要應用到裝置的先前配置，請按一下**Browse...** 按鈕，並選擇要應用的配置檔案。然後按一下**Save**將配置檔案應用到裝置。在本例中，我們將按一下**Skip**。

附註：當裝置應用相關配置時，它會重新啟動並引導您進入登入頁面。



步驟5.在*Configure Device - IP Address* 視窗中，選擇**Dynamic IP Address(DHCP)（建議）**以從動態主機配置協定(DHCP)伺服器獲取IP地址，或按一下**Static IP Address**手動配置IP地址。然後按一下**下一步**繼續下一部分。DHCP為網際網路主機提供配置引數。在這種情況下，DHCP會在一段有限的時間內或客戶端明確放棄該地址之前，將IP地址分配給客戶端。

在本例中，我們將選擇**動態IP地址(DHCP)（推薦）**。



步驟6.單點設定提供了一種集中方法，用於跨多個裝置管理和控制無線服務。這將允許您建立單個無線裝置組或集群，您可以將其作為單個實體檢視、部署、配置和保護無線網路。單點設定可幫助簡化整個無線服務的通道規劃，以減少無線電干擾並最大化無線網路的頻寬。

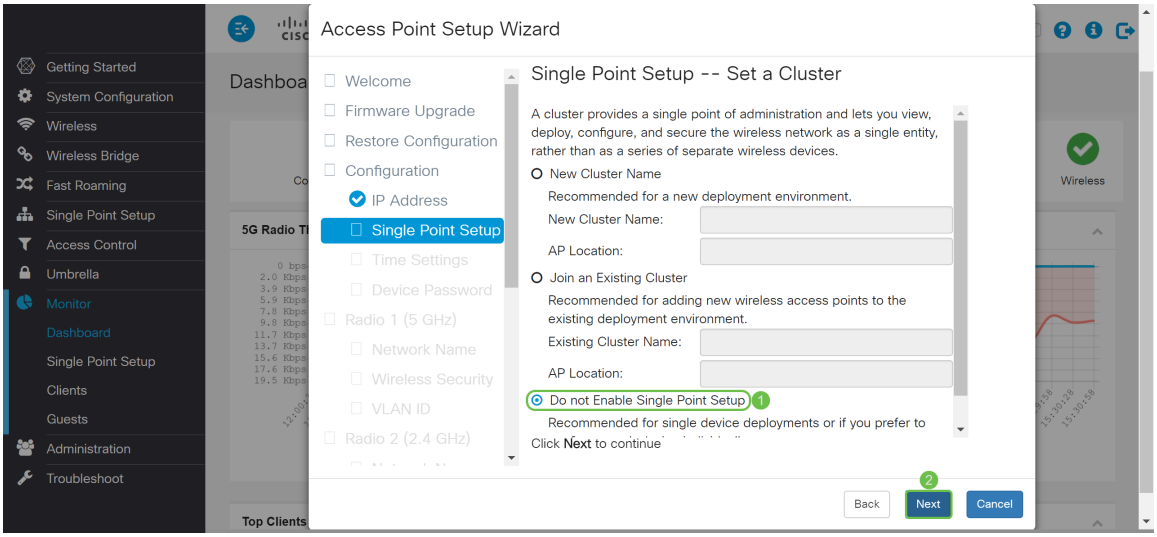
要建立WAP裝置的新的單點設定，請按一下**New Cluster Name**並指定一個新名稱。當使用相同的集群名稱配置裝置並在其他WAP裝置上啟用單點設定模式時，這些裝置會自動加入該組。

如果網路上已經有一個集群，可以通過按一下**Join an Existing Cluster**（加入現有集群），然後輸入**Existing Cluster Name**來將此裝置新增到該集群中。WAP根據群集配置其餘設定。按一下**下一步**並確認要加入群集的確認。按一下**Submit**以加入群集。配置完成後，按一下**Finish**退出安裝*嚮導*。

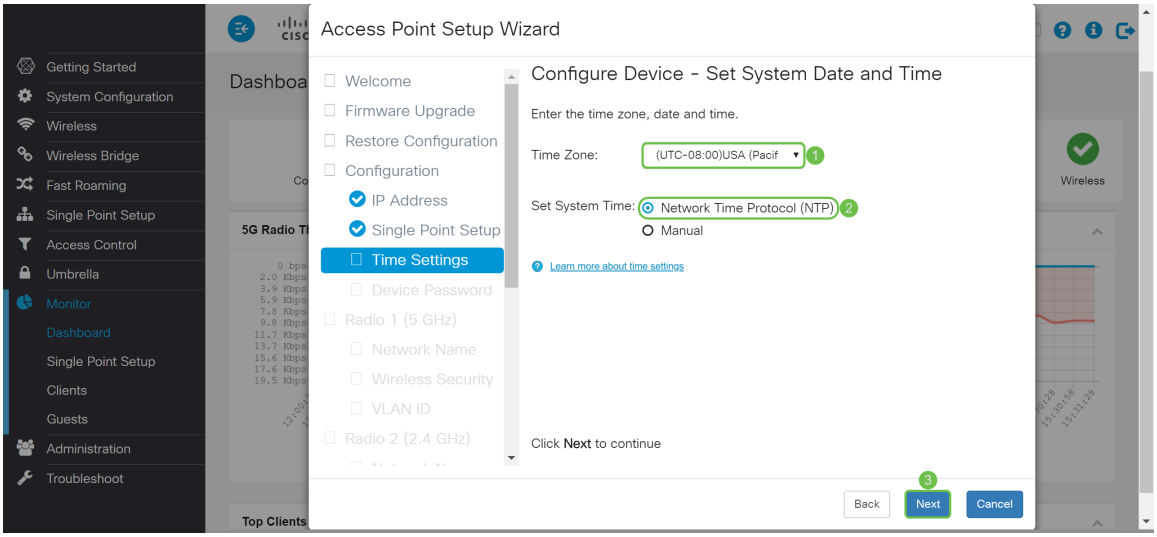
附註：您可以在**AP Location**欄位中輸入接入點位置，以記錄WAP裝置的物理位置。

如果此時不希望此裝置參與單點設定，請按一下**不啟用單點設定**。

在本例中，我們將選擇**Do not Enable Single Point Setup**。然後按一下**下一步**繼續下一部分。



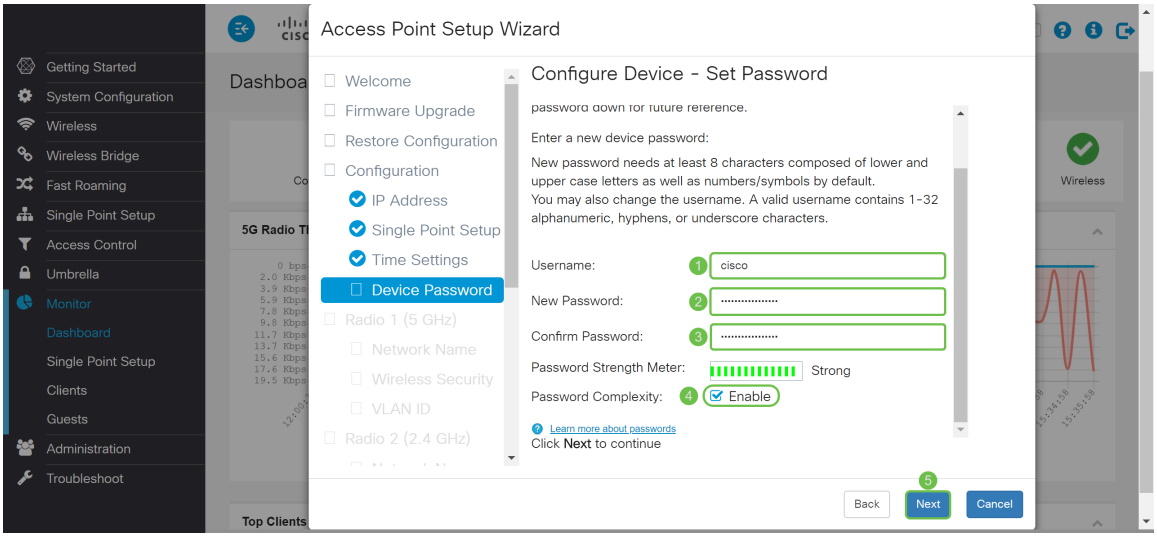
步驟7.在*Configure Device - Set System Date and Time*視窗中，選擇**時區**，然後選擇是希望系統時間從**Network Time Protocol(NTP)**伺服器自動獲取時間設定，還是選擇**Manual**手動配置時間設定。系統時鐘為消息日誌提供網路同步時間戳服務。系統時鐘可以手動配置，也可以配置為NTP客戶端，從伺服器獲取點選資料。按一下**下一步**繼續安裝*嚮導*。



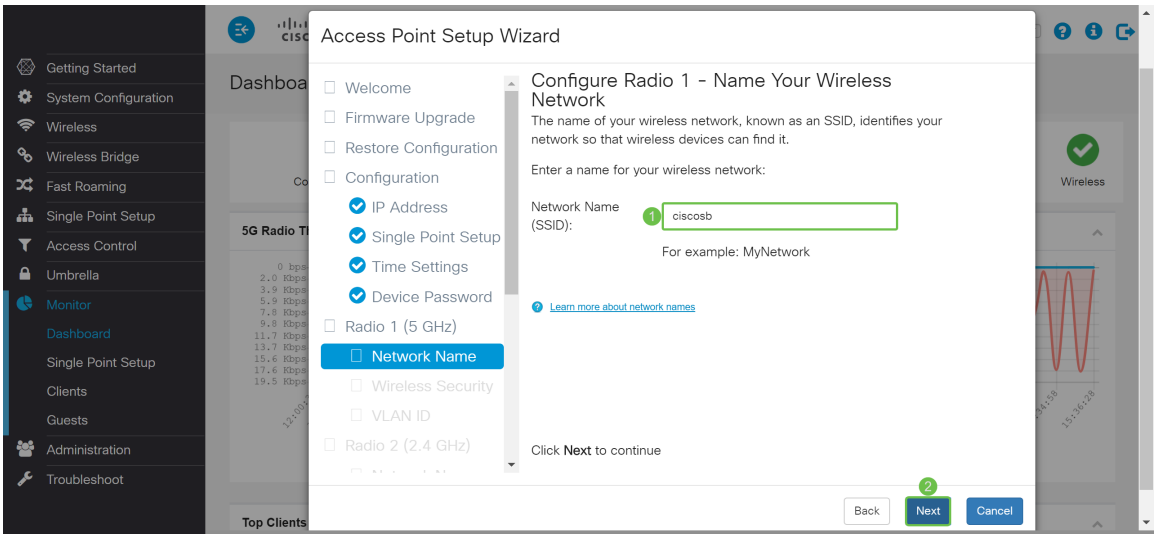
步驟8.在*Username*欄位中輸入新的**Username**，預設使用者名稱為cisco。輸入**New Password**作為*使用者名稱*。然後在*確認密碼*欄位中再次輸入**新密碼**。您可以取消選中*Password Complexity*以禁用密碼安全規則。但是，強烈建議啟用密碼安全規則。新密碼必須符合以下複雜性設定：

- 與使用者名稱不同。
- 與當前密碼不同。
- 至少包含8個字元。
- 包含至少三個字元類（大寫字母、小寫字母、數字和標準鍵盤上可用的特殊字元）中的字元。

然後按一下**Next**配置*Radio 1*。



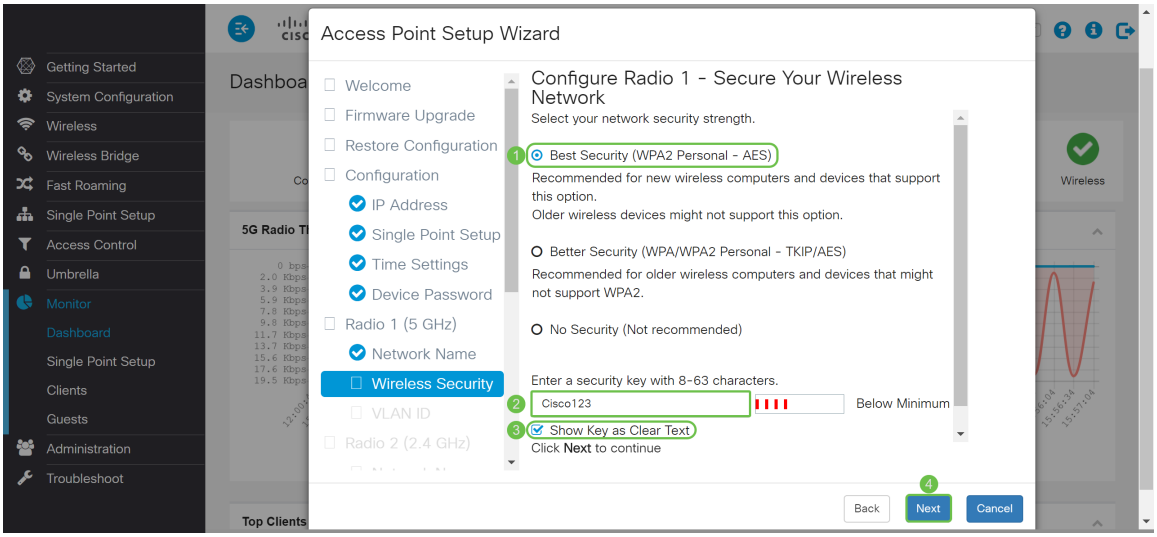
步驟9.在*網路名稱(SSID)*中輸入您的無線網路的名稱。 這有助於識別您的網路，以便無線裝置可以找到它。預設情況下,**ciscosb**用作網路名稱。然後按一下**下一步**繼續下一部分。



步驟10.點選與要應用於無線網路的網路安全對應的單選按鈕。然後在*Security Key*欄位中輸入網路的密碼。要在鍵入時檢視密碼，請選中**Show Key as Clear Text**覈取方塊。按一下**下一步**繼續。

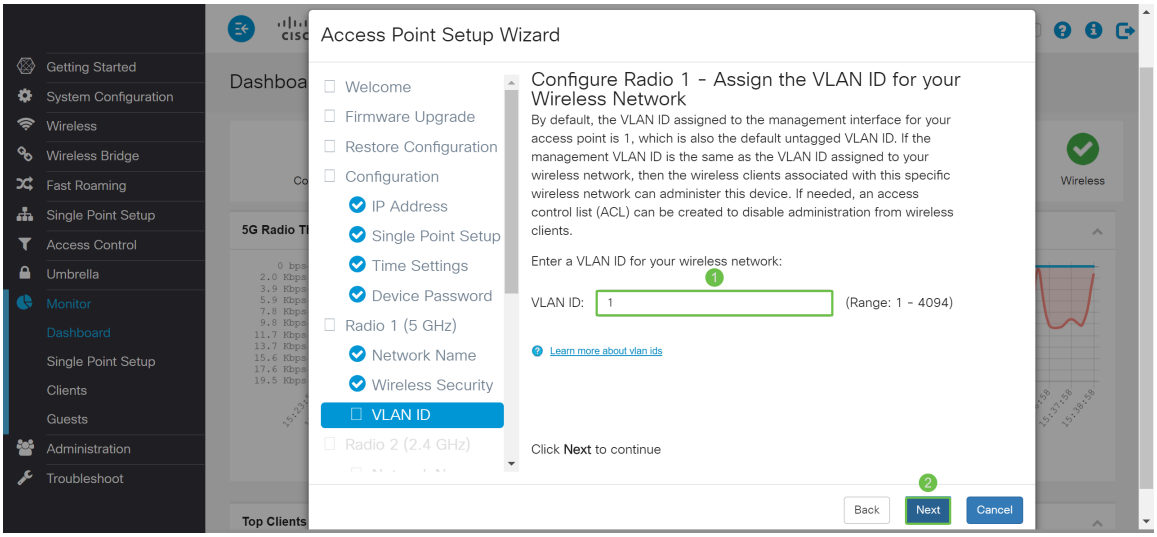
附註：如果網路包含多個客戶端，其中有些支援WPA2，有些僅支援原始WPA，請選擇兩者(WPA/WPA2)。 這允許WPA和WPA2客戶端工作站進行關聯和身份驗證，但是對於支援它的客戶端，使用更強大的WPA2。此WPA配置允許更多的互操作性來代替某些安全性。

- 最佳安全(Wi-Fi保護訪問2(WPA2)個人 — 高級加密標準(AES)) 網路上的所有使用者端站都支援使用「計數器模式」和「密碼塊鏈結訊息驗證碼通訊協定」(AES-CCMP)密碼/安全通訊協定的無線存取清單和進階加密標準加密演演算法。這按照IEEE 802.11i標準提供最佳安全性。根據最新的Wi-Fi聯盟要求，AP必須始終支援此模式。
- 更好的安全性（WPA/WPA2個人 — TKIP/AES） WPA Personal是Wi-Fi Alliance IEEE802.11i標準，包括AES-CCMP和TKIP加密。當存在支援原始WPA但不支援較新WPA2的較舊無線裝置時，它可提供安全性。
- 無安全性（不推薦） 無線網路不需要密碼，任何人都可以訪問。

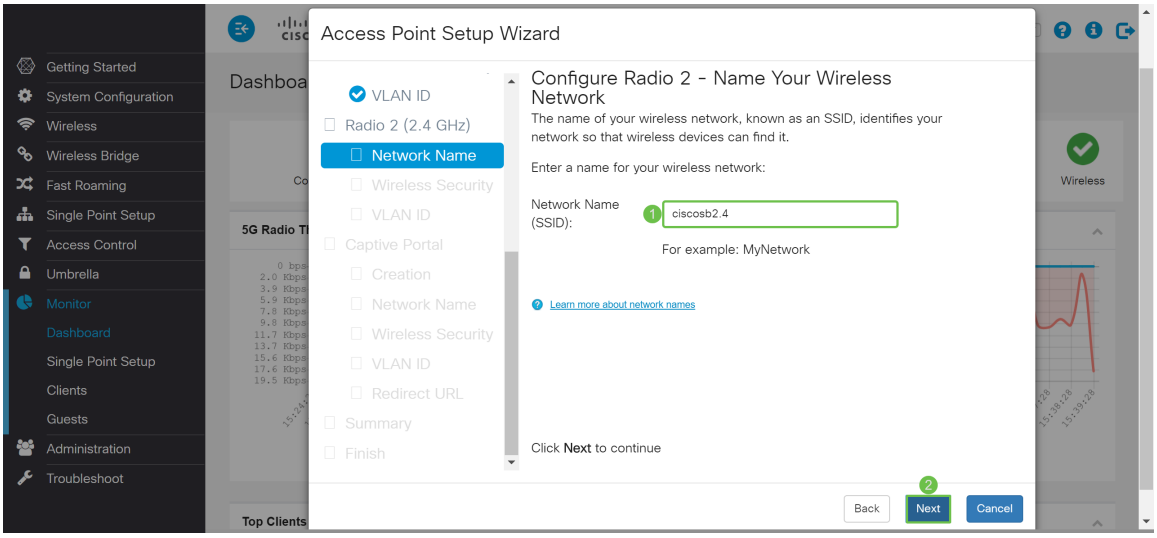


步驟11.在「*VLAN ID*」欄位中，輸入您希望*Radio 1(5 GHz)所屬的VLAN的ID*編號。在本例中，我們將將*VLAN ID*保留為1。按一下**下一步**以配置*Radio 2(2.4 GHz)*。

附註：我們建議您將預設(1)的VLAN ID分配給無線流量，以便將其與VLAN 1上的管理流量隔離。按一下此處瞭解有關虛擬接入點(VAP)的詳細資訊。



步驟12.在*Network Name(SSID)字段中輸入新的網路*名稱。預設情況下使用**ciscosb**。網路名稱稱為SSID，它標識您的網路，以便無線裝置可以找到它。在本示例中，**ciscosb2.4**用於區分5 GHz網路名稱。按一下**下一步**為*Radio 2(2.4 GHz)配置無線安全*。

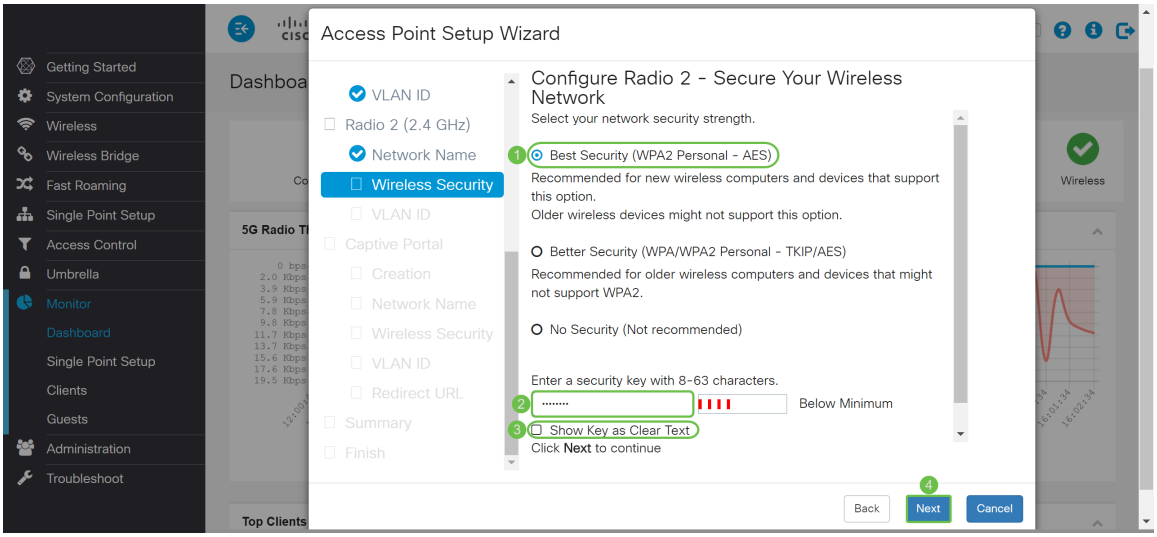


步驟13.點選與要應用於無線網路的網路安全對應的單選按鈕。然後在*Security Key*欄位中輸入網路的密碼。要在鍵入時檢視密碼，請選中**Show Key as Clear Text**覈取方塊。預設情況下，會選中

Show Key as Clear Text。按一下**下一步**繼續。

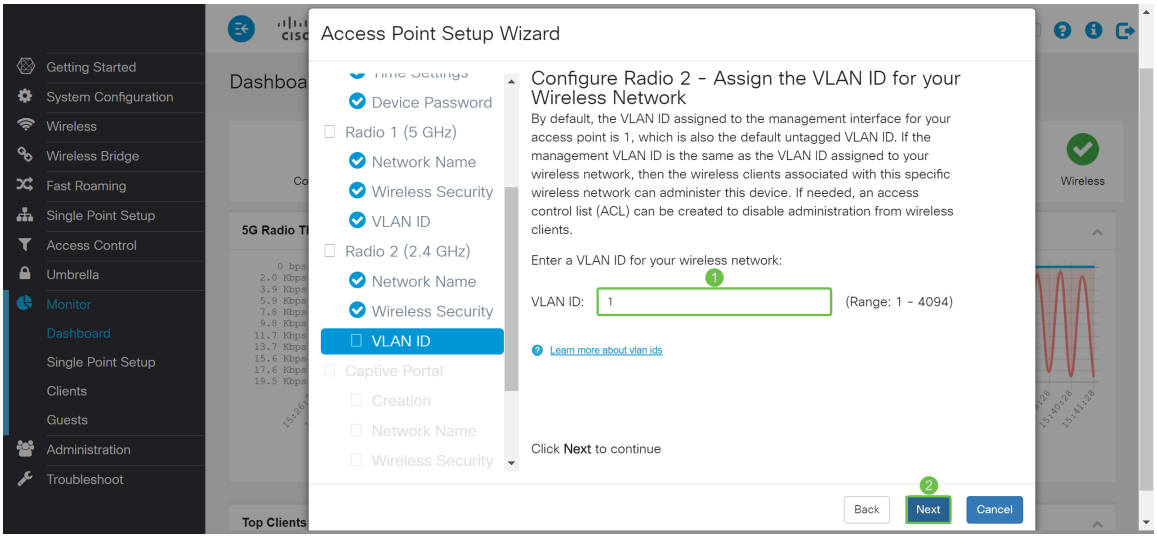
附註：如果網路包含多個客戶端，其中有些支援WPA2，有些僅支援原始WPA，請選擇兩者(WPA/WPA2)。 這允許WPA和WPA2客戶端工作站進行關聯和身份驗證，但是對於支援它的客戶端使用更強大的WPA2。此WPA配置允許更多的互操作性來代替某些安全性。

- 最佳安全(Wi-Fi保護訪問2(WPA2)個人 — 高級加密標準(AES)) 網路上的所有使用者端站都支援使用「計數器模式」和「密碼塊鏈結訊息驗證碼通訊協定」(AES-CCMP)密碼/安全通訊協定的無線存取清單和進階加密標準加密演演算法。這按照IEEE 802.11i標準提供最佳安全性。根據最新的Wi-Fi聯盟要求，AP必須始終支援此模式。
- 更好的安全性（WPA/WPA2個人 — TKIP/AES） WPA Personal是Wi-Fi Alliance IEEE802.11i標準，包括AES-CCMP和TKIP加密。當存在支援原始WPA但不支援較新WPA2的較舊無線裝置時，它可提供安全性。
- 無安全性（不推薦） 無線網路不需要密碼，任何人都可以訪問。

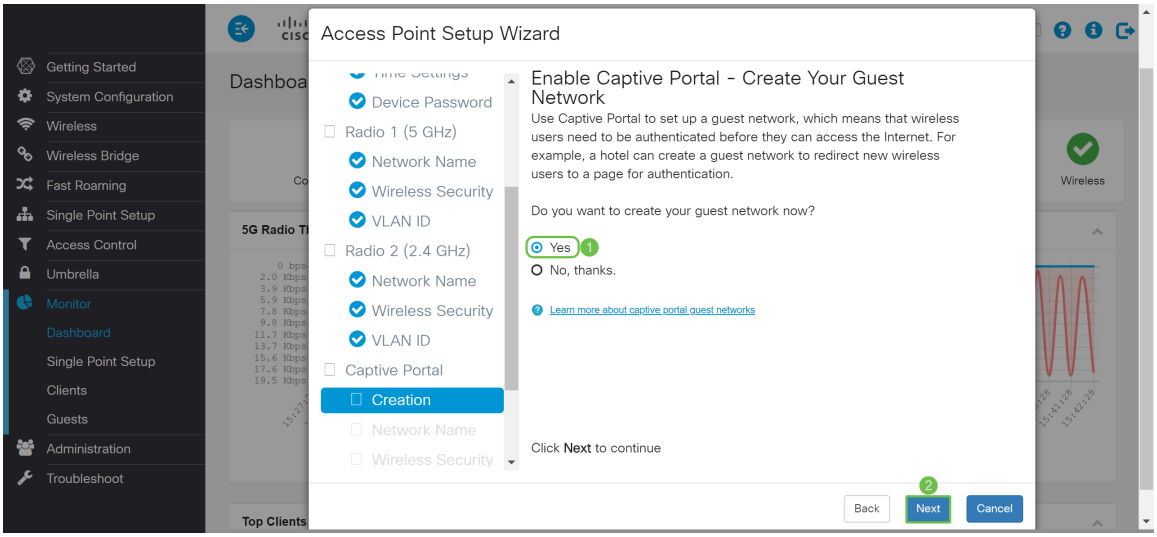


步驟14.在「*VLAN ID*」欄位中，輸入您希望*Radio 1(2.4 GHz)所屬的VLAN的ID*編號。在本例中，我們將使用預設值1作為我們的*VLAN ID*。按一下**下一步**配置*強制網路門戶*。

附註：我們建議您將預設(1)的VLAN ID分配給無線流量，以便將其與VLAN 1上的管理流量隔離。按一下此處瞭解有關虛擬接入點(VAP)的詳細資訊。

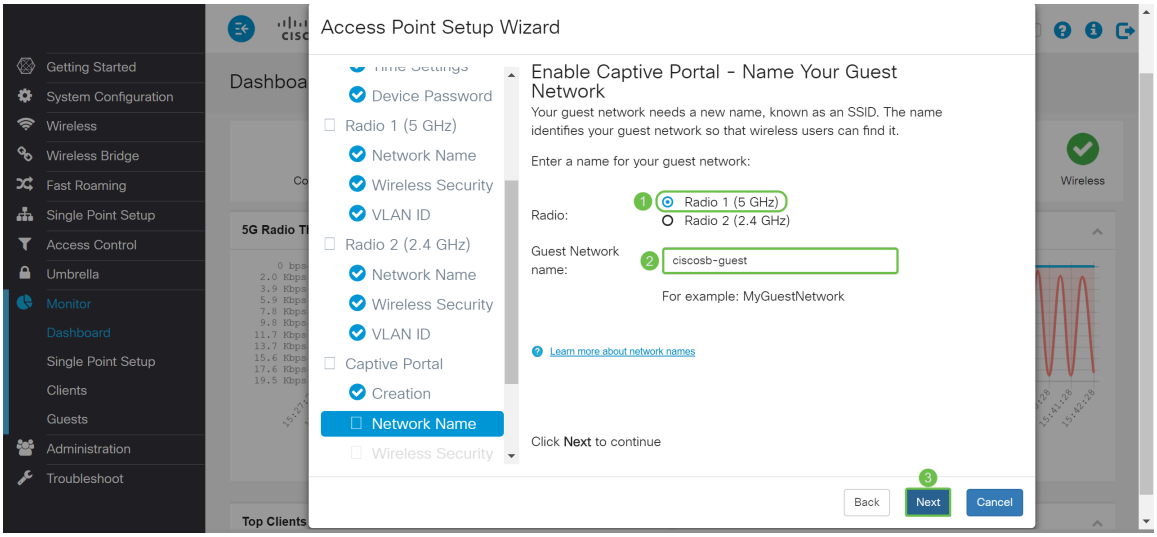


步驟15.（可選）不需要訪客網路。如果要建立訪客網路，請按一下**Yes**單選按鈕。如果您不想建立訪客網路並跳至步驟20，請按一下**No**單選按鈕。按一下Next按鈕繼續。



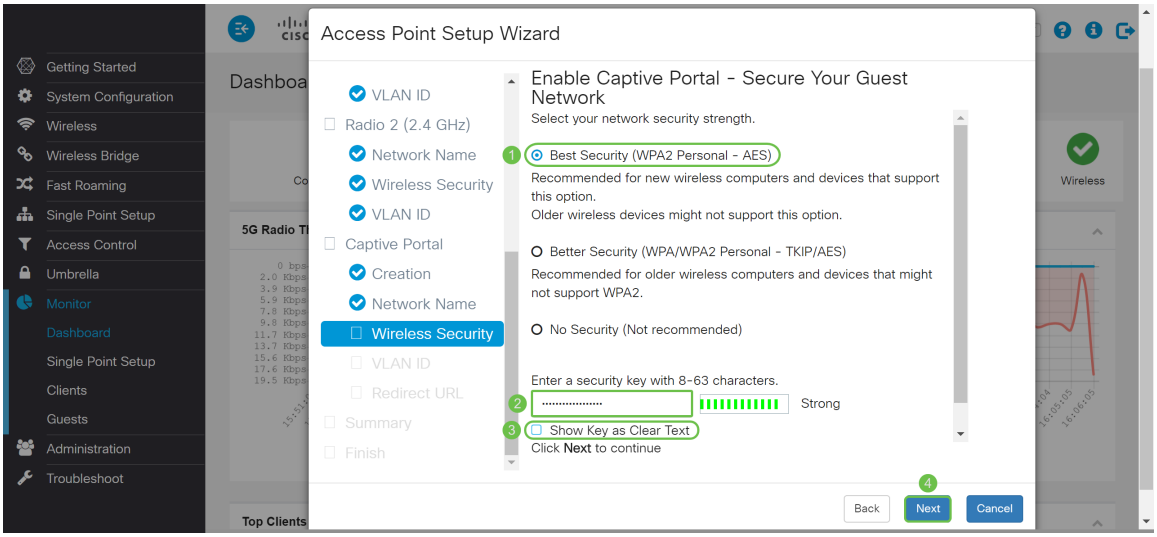
步驟16。（可選）選擇與要放置訪客網路的*Radio*對應的單選按鈕。然後在*Guest Network name*欄位中創*建網路名*稱。按一下**Next**為*Guest Network*配置*Wireless Security*設定。

在本例中，我們將選擇**Radio 1(5 GHz)**作為*Radio*，並將預設網路名稱保留為*ciscosb-guest*，以便您的無線訪客使用者可以找到網路名稱。

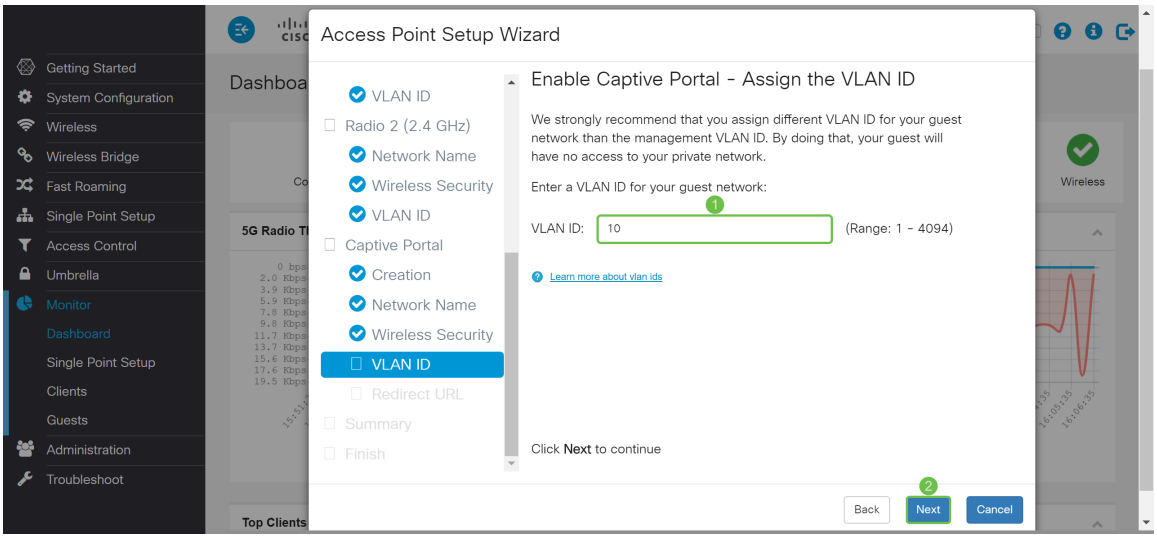


步驟17。（可選）選擇與要應用於訪客網路的網路安全對應的單選按鈕。然後在*Security Key*欄位中輸入訪客網路的密碼（如果適用）。要將金鑰顯示為明文，請選中此覈取方塊以將安全金鑰顯示為明文。預設情況下啟用。按一下**下一步**繼續。網路安全選項包括：

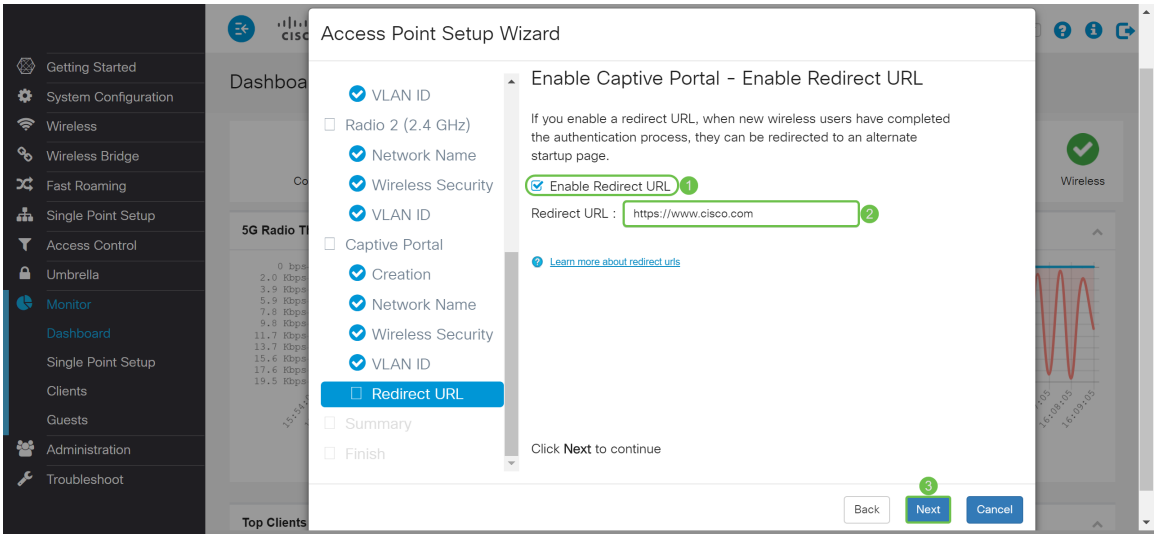
- 最佳安全性（WPA2個人 — AES）— 建議用於支援此選項的新無線電腦和裝置。
- 更好的安全性（WPA/WPA2個人 — TKIP/AES）— 建議用於可能不支援WPA2的較舊無線電腦和裝置。
- 無安全性（不推薦）— 這是預設選擇。



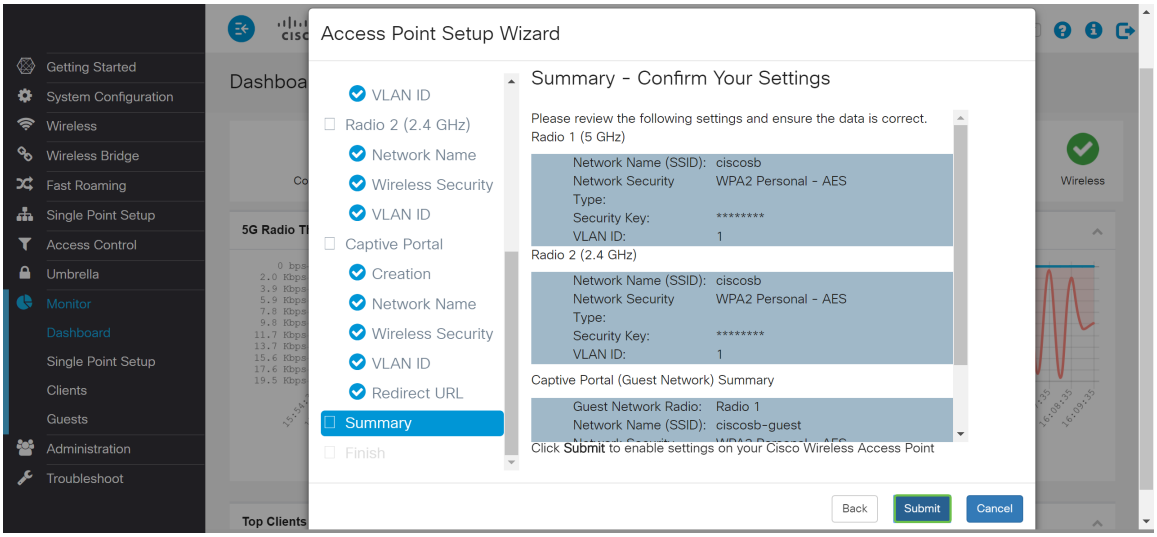
步驟18。（可選）為訪客網路指定*VLAN ID*。訪客網路VLAN ID應與管理VLAN ID不同。在本例中，我們將*VLAN ID* 10用作訪客網路的VLAN ID。按一下「**Next**」以設定訪客網路的*重新導向URL*。



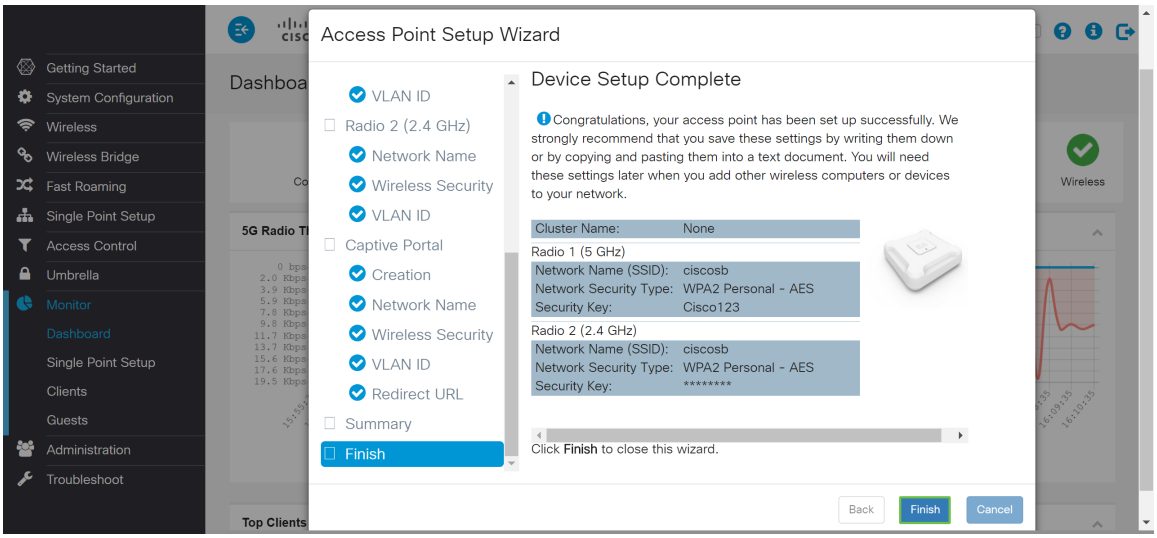
步驟19。（可選）勾選**Enable Redirect URL**覈取方塊以將新的無線使用者重定向到備用啟動頁。在*Redirect URL*欄位中輸入完全限定的域名(FQDN)或IP地址(包括http://或https://)。 然後按一下**Next**繼續到*Summary*頁面。



步驟20.在*Summary - Confirm Your Settings*頁面中，檢查您配置的設定。按一下**Back**按鈕以重新配置一個或多個設定。如果按一下**Cancel**，則所有設定都將返回上一個或預設值。如果配置正確，請按一下**Submit**。您的設定設定已儲存，並且出現確認視窗。



步驟21.配置設定後，將顯示*Device Setup Complete*頁，該頁會通知您已成功設定接入點。按一下**Finish**，系統將要求您使用新密碼重新登入。



結論

現在，您已使用安裝嚮導成功配置WAP。您應該看到您剛剛在Wi-Fi網路清單中配置的SSID。要在WAP上配置其他功能，您需要重新登入。