Utilizzo dell'Impostazione guidata su WAP125 o WAP581

Obiettivo

L'Installazione guidata è una funzionalità incorporata che può essere utilizzata per la configurazione iniziale di una periferica WAP (Wireless Access Point). L'Installazione guidata semplifica notevolmente la configurazione delle impostazioni fornendo istruzioni dettagliate.

In questo documento viene spiegato come configurare WAP125 e WAP581 con l'Installazione guidata nell'utility di configurazione Web.

Per configurare WAP utilizzando l'Installazione guidata in un dispositivo mobile, fare clic qui.

Dispositivi interessati

- WAP125
- WAP581

Versione del software

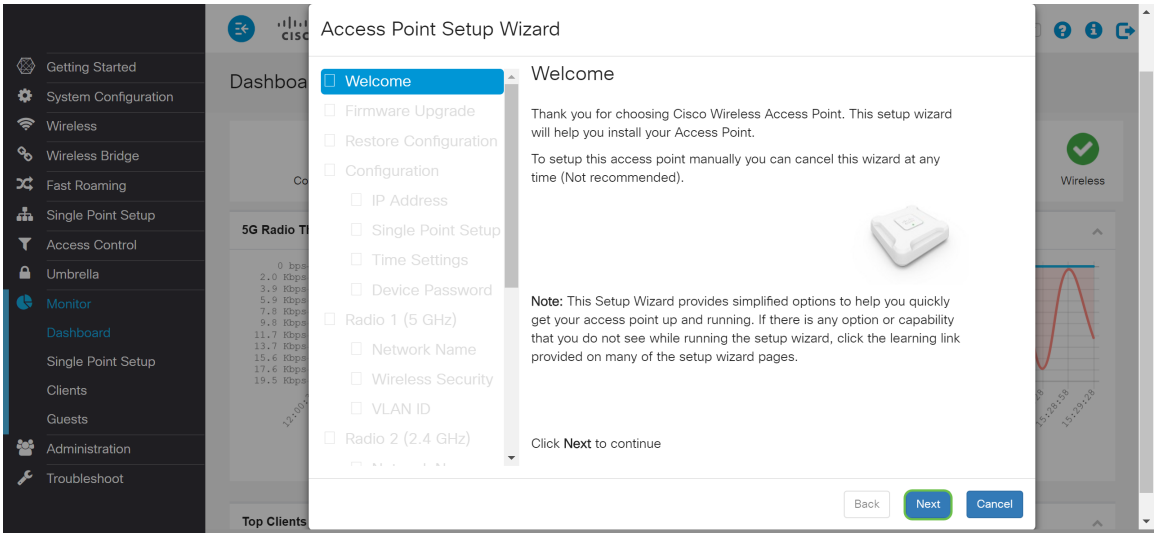
- 1.0.1.3

Come utilizzare l'Installazione guidata

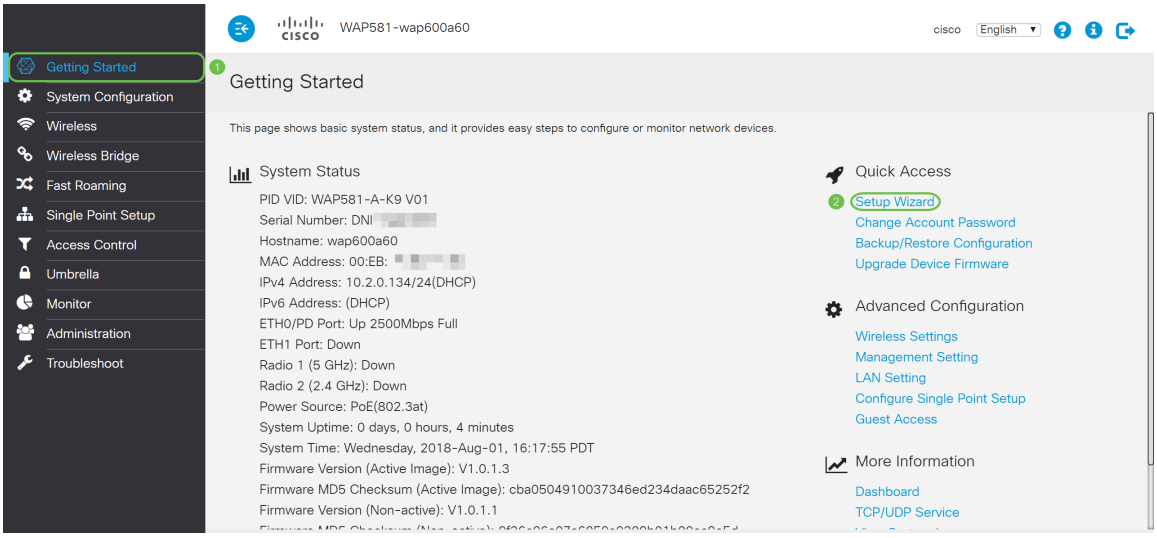
Passaggio 1. Accedere all'utility di configurazione Web del WAP immettendo l'indirizzo IP del WAP nel browser Web. Se è la prima volta che si configura il WAP, l'indirizzo IP predefinito è 192.168.1.254.

Nota: In questa guida viene utilizzato WAP581 per illustrare l'Installazione guidata. L'aspetto può variare a seconda del modello.

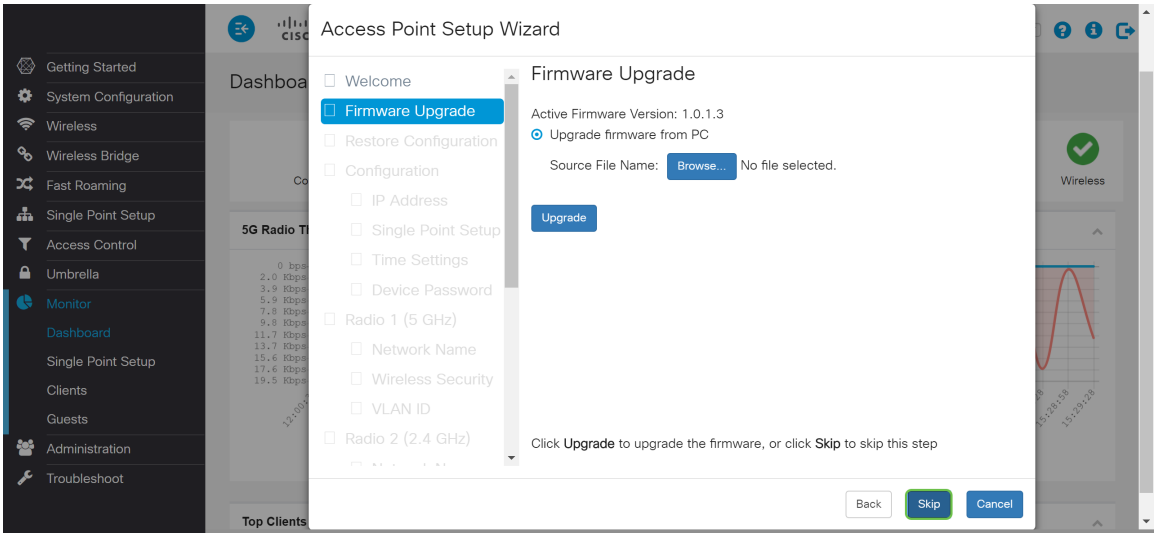
Passaggio 2. La prima volta che si accede al punto di accesso o dopo aver ripristinato le impostazioni predefinite di fabbrica, viene visualizzata la *Configurazione guidata punto di accesso*. Fare clic su **Avanti** per continuare.



Nota: Se WAP è già configurato ma si desidera comunque accedere all'*Installazione guidata*, passare a **Guida introduttiva > Installazione guidata**. Verrà visualizzata la finestra *Configurazione guidata Access Point*.



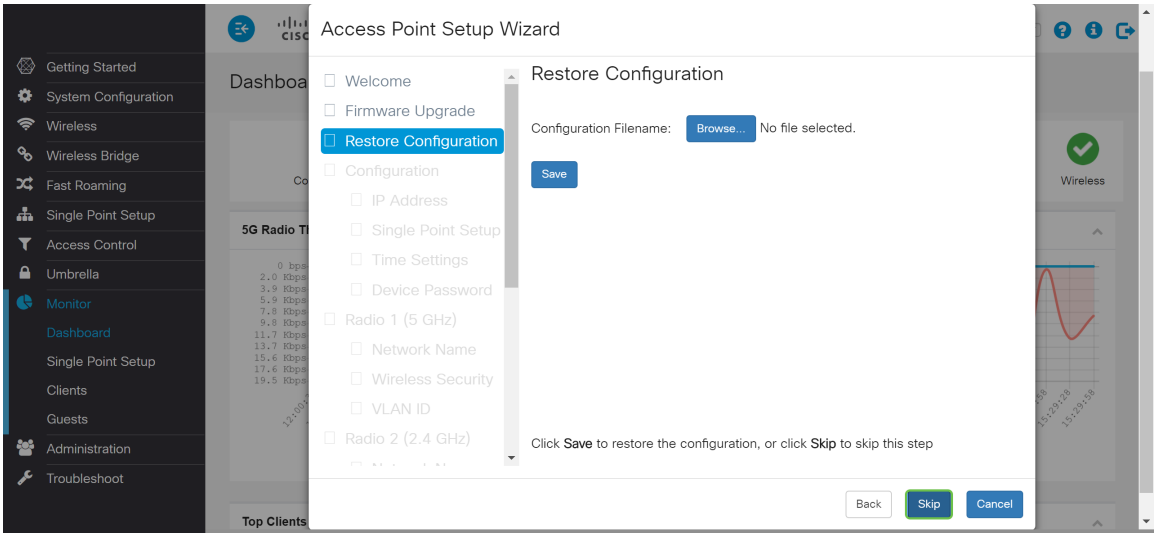
Passaggio 3. Nella finestra *Aggiornamento firmware*, fare clic sul pulsante **Sfoglia...** e selezionare il file del firmware a cui si desidera effettuare l'aggiornamento. Quindi premere **Aggiorna** per aggiornare il firmware. Una volta aggiornato il firmware, il dispositivo si riavvierà automaticamente e verrà visualizzata la pagina di accesso. In questo esempio, si farà clic su **Skip** (Ignora) perché è disponibile la versione del firmware desiderata.



Passaggio 4. Se si desidera applicare al dispositivo una configurazione precedente, fare clic su **Sfoglia...** nella finestra *Ripristina configurazione* e selezionare il file di configurazione da applicare.

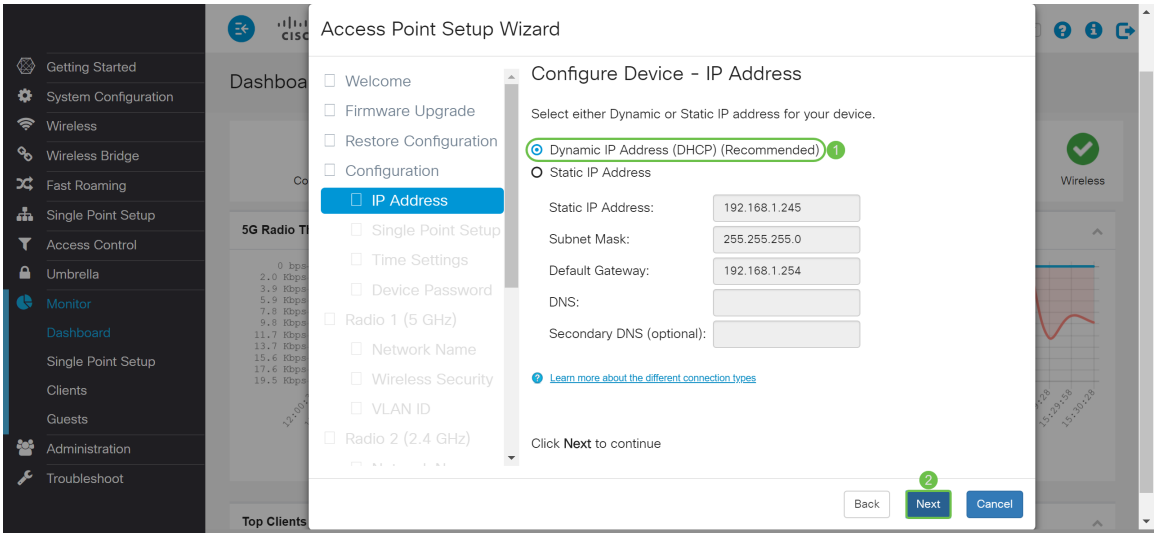
Quindi fare clic su **Save** per applicare il file di configurazione al dispositivo. In questo esempio verrà fatto clic su **Ignora**.

Nota: Quando il dispositivo applica la configurazione pertinente, si riavvia e viene visualizzata la pagina di accesso.



Passaggio 5. Nella finestra *Configure Device - IP Address*, selezionare **DHCP (Dynamic IP Address) (consigliato)** per ottenere un indirizzo IP da un server DHCP (Dynamic Host Configuration Protocol), oppure fare clic su **Static IP Address** per configurare manualmente l'indirizzo IP. Quindi fare clic su **Next** (Avanti) per passare alla sezione successiva. DHCP fornisce i parametri di configurazione agli host Internet. In questo caso, il DHCP assegna un indirizzo IP a un client per un periodo di tempo limitato o fino a quando il client non lo rifiuta esplicitamente.

Nell'esempio, verrà selezionato **DHCP (Dynamic IP Address) (consigliato)**.



Passaggio 6. La configurazione a punto singolo fornisce un metodo centralizzato per amministrare e controllare i servizi wireless su più dispositivi. In questo modo sarà possibile creare un singolo gruppo o cluster di dispositivi wireless da visualizzare, distribuire, configurare e proteggere la rete wireless come se fosse un'unica entità. Single Point Setup semplifica la pianificazione dei canali nel servizio wireless, riducendo le interferenze radio e massimizzando la larghezza di banda della rete wireless.

Per creare una nuova installazione punto singolo della periferica WAP, fare clic su **Nuovo nome cluster** e specificare un nuovo nome. Quando si configurano i dispositivi con lo stesso nome di cluster e si attiva la modalità Single Point Setup su altri dispositivi WAP, questi si uniscono

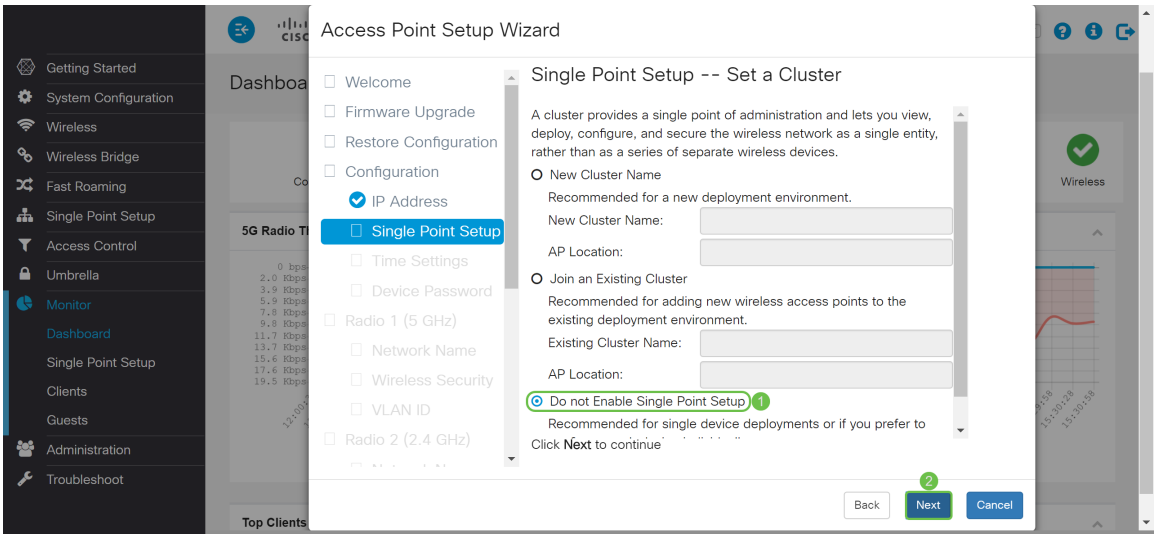
automaticamente al gruppo.

Se nella rete è già presente un cluster, è possibile aggiungervi il dispositivo facendo clic su **Aggiungi a cluster esistente**, quindi immettere il **nome del cluster esistente**. WAP configura le altre impostazioni in base al cluster. Fare clic su **Avanti** e confermare la partecipazione al cluster. Fare clic su **Invia** per unirsi al cluster. Al termine della configurazione, fare clic su **Fine** per uscire dall'*Installazione guidata*.

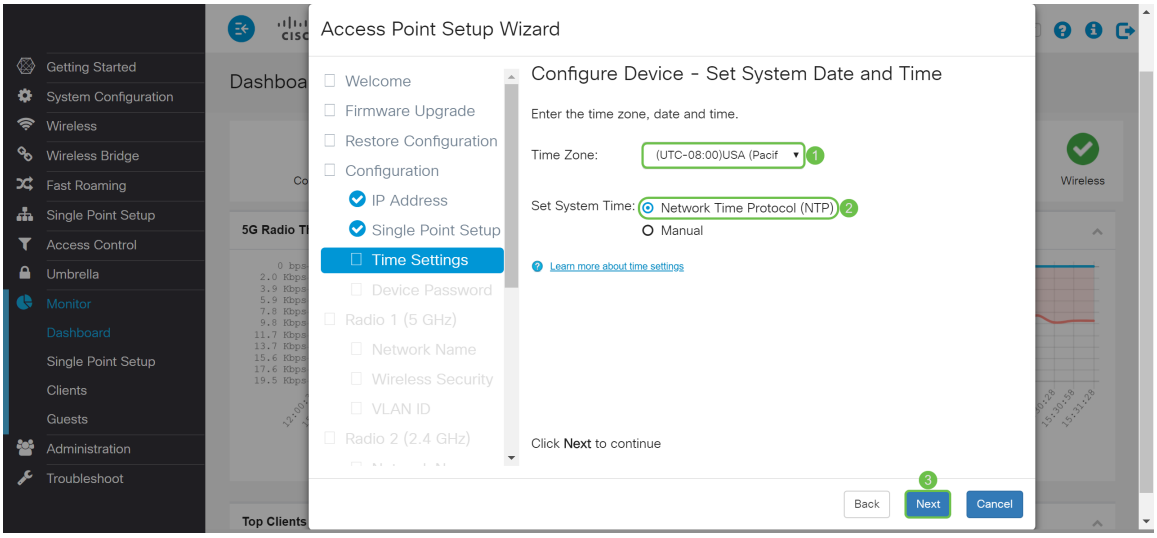
Nota: È possibile immettere la posizione del punto di accesso nel campo **Posizione AP** per annotare la posizione fisica del dispositivo WAP.

Se non si desidera che il dispositivo partecipi a un'installazione punto singolo in questo momento, fare clic su **Non attivare l'installazione punto singolo**.

In questo esempio verrà selezionata l'opzione **Non abilitare Single Point Setup** (**Non abilitare Single Point Setup**). Quindi fare clic su **Next** (Avanti) per passare alla sezione successiva.



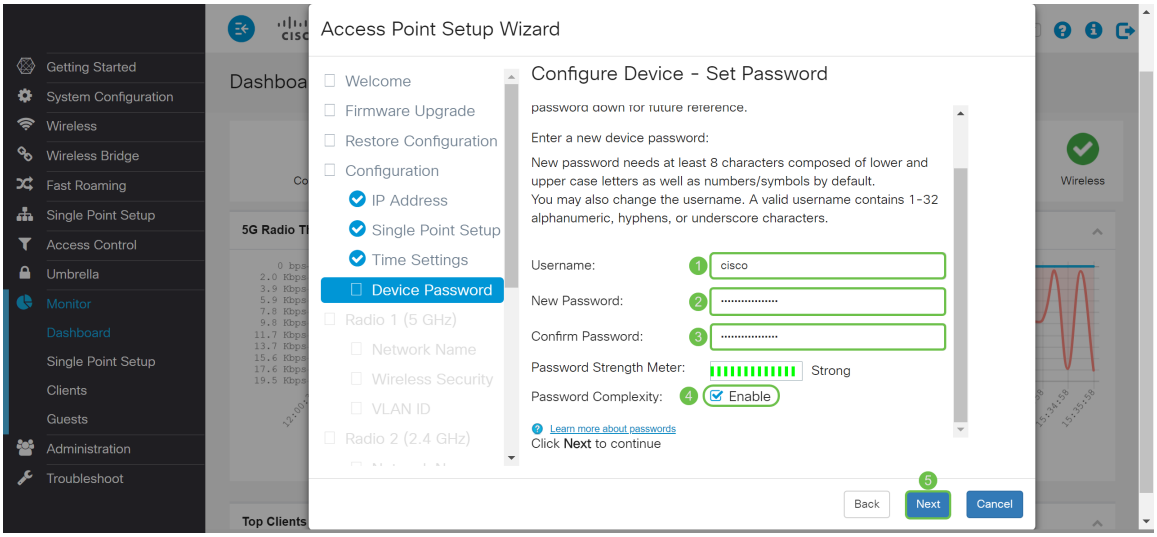
Passaggio 7. Nella finestra *Configura dispositivo - Imposta data e ora di sistema*, scegliere il **fuso orario**, quindi selezionare se si desidera che l'ora di sistema acquisisca automaticamente l'impostazione dell'ora da un server **NTP (Network Time Protocol)** o selezionare **Manuale** per configurare manualmente le impostazioni dell'ora. L'orologio di sistema fornisce un servizio di timestamp sincronizzato in rete per i log dei messaggi. L'orologio di sistema può essere configurato manualmente o come client NTP che ottiene i dati click da un server. Fare clic su **Avanti** per continuare l'*installazione guidata*.



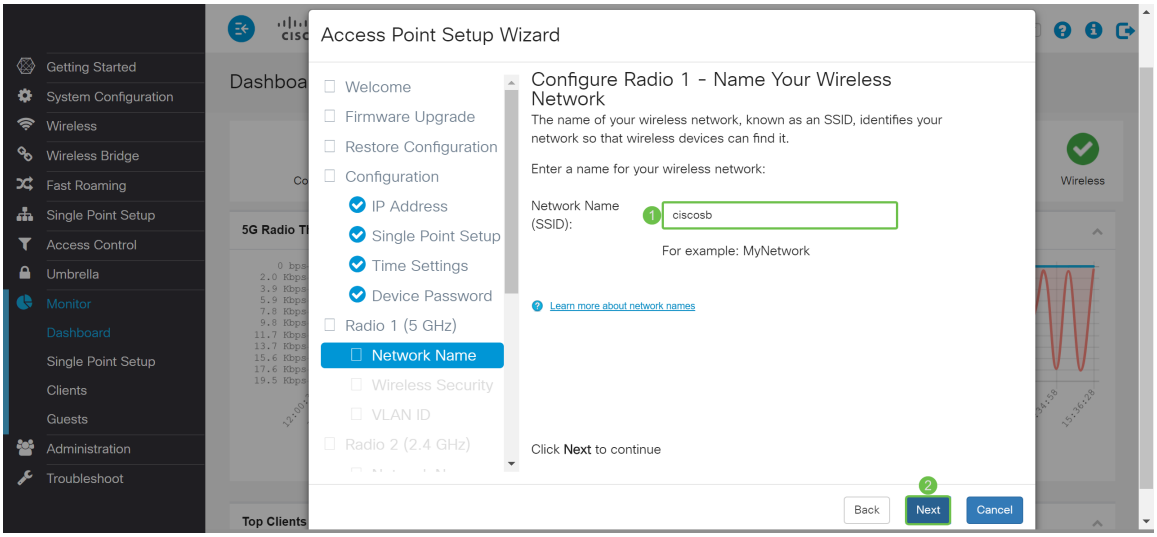
Passaggio 8. Inserire un nuovo **nome utente** nel campo *Nome utente*. Per impostazione predefinita, il nome utente è cisco. Immettere una **nuova password** per il *nome utente*. Immettere quindi di nuovo nel campo *Conferma password* della casella **Nuova password**. È possibile deselezionare *Complessità password* per disabilitare le regole di sicurezza delle password. È tuttavia consigliabile mantenere abilitate le regole di sicurezza delle password. La nuova password deve essere conforme alle seguenti impostazioni di complessità:

- Èdiverso dal nome utente.
- Èdiversa dalla password corrente.
- Ha una lunghezza minima di otto caratteri.
- Contiene caratteri appartenenti ad almeno tre classi di caratteri (lettere maiuscole, lettere minuscole, numeri e caratteri speciali disponibili su una tastiera standard).

Quindi fare clic su **Next** (Avanti) per configurare la *radio 1*.



Passaggio 9. Immettere un nome per la rete wireless in *Nome rete (SSID)*. Ciò consente di identificare la rete in modo che i dispositivi wireless possano individuarla. Per impostazione predefinita, il nome della rete è **ciscosb**. Quindi fare clic su **Next** (Avanti) per passare alla sezione successiva.

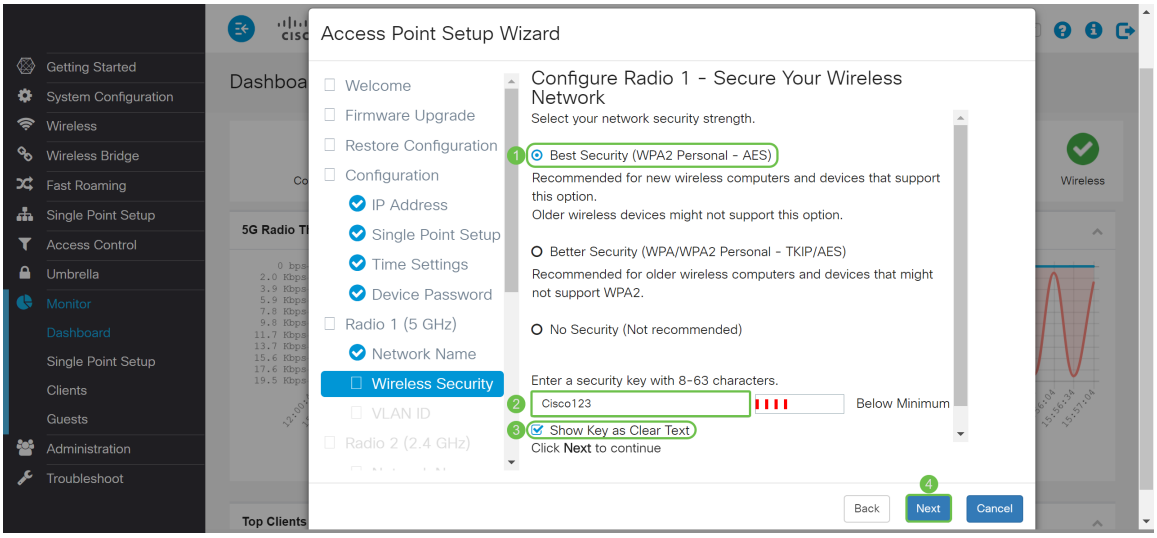


Passaggio 10. Fare clic sul pulsante di opzione corrispondente alla protezione di rete che si desidera applicare alla rete wireless. Immettere quindi la password per la rete nel campo *Chiave di accesso*. Per visualizzare la password durante la digitazione, selezionare la casella di controllo **Mostra chiave come testo non crittografato**. Fare clic su **Avanti** per continuare.

Nota: Se la rete dispone di una combinazione di client, alcuni dei quali supportano WPA2 e altri

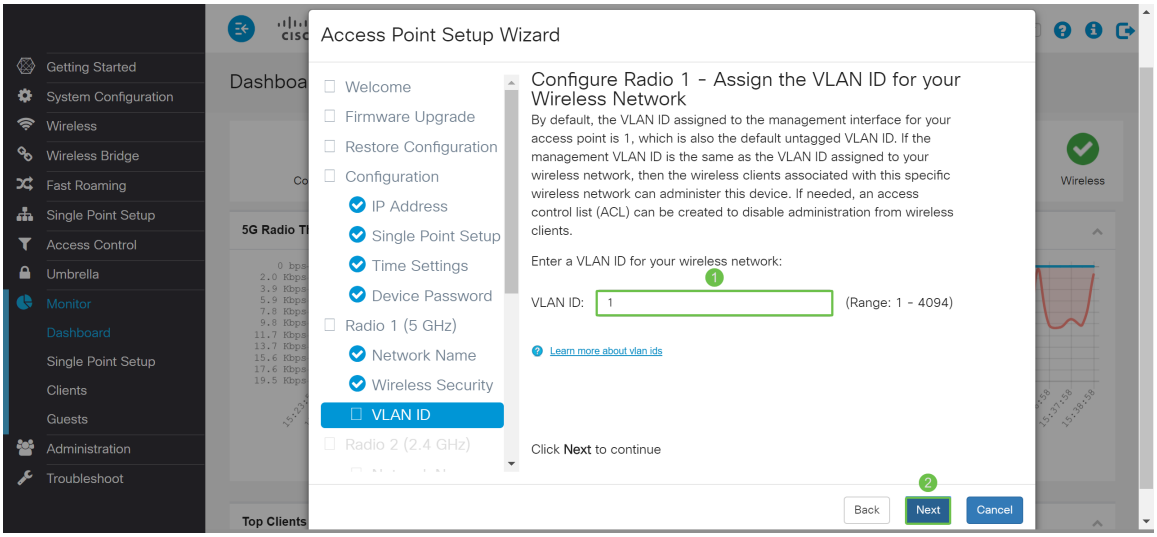
che supportano solo WPA originale, selezionare entrambi (WPA/WPA2). Ciò consente l'associazione e l'autenticazione delle stazioni client WPA e WPA2, ma utilizza il più affidabile WPA2 per i client che lo supportano. Questa configurazione WPA consente una maggiore interoperabilità al posto di una certa sicurezza.

- Massima sicurezza (WPA2 (Wi-Fi Protected Access 2) Personale - AES (Advanced Encryption Standard)) Tutte le stazioni client della rete supportano l'algoritmo di crittografia WPA2 e Advanced Encryption Standard utilizzando la modalità contatore con il protocollo AES-CCMP (Cipher Block Chaining Message Authentication Code Protocol). Ciò garantisce la migliore sicurezza in base allo standard IEEE 802.11i. In base al più recente requisito di Wi-Fi Alliance, l'access point deve supportare questa modalità in ogni momento.
- Maggiore sicurezza (WPA/WPA2 Personal - TKIP/AES) WPA Personal è uno standard Wi-Fi Alliance IEEE802.11i, che include la crittografia AES-CCMP e TKIP. Garantisce la sicurezza quando esistono dispositivi wireless meno recenti che supportano WPA originale ma non la nuova WPA2.
- Nessuna protezione (scelta non consigliata) La rete wireless non richiede una password e può essere utilizzata da chiunque.

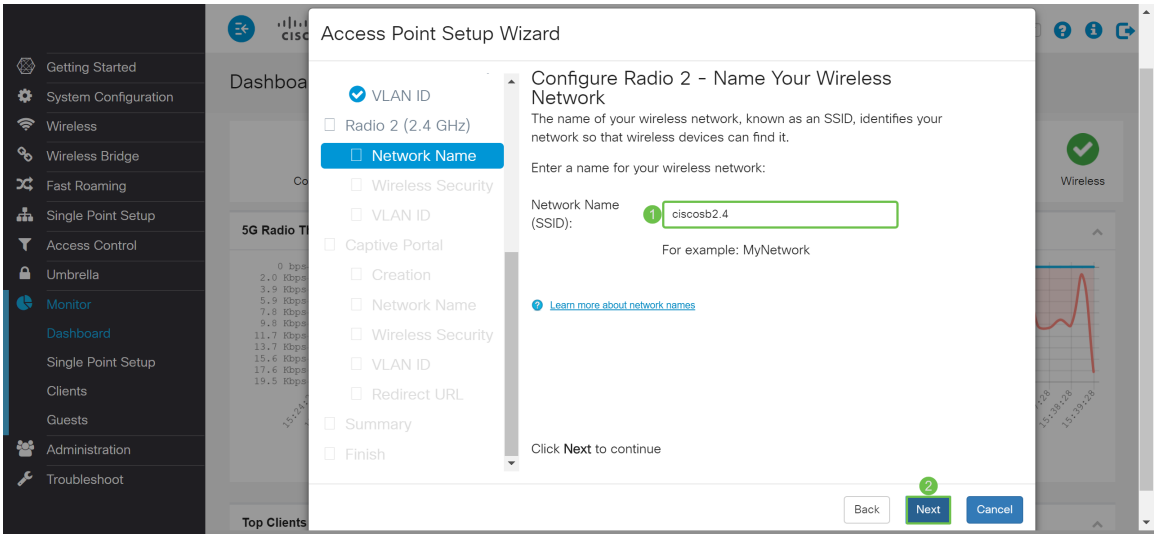


Passaggio 11. Nel campo *VLAN ID*, immettere il numero ID della VLAN a cui si desidera che la *radio 1 (5 GHz)* appartenga. Nell'esempio, l'*ID VLAN* rimarrà 1. Fare clic su **Avanti** per configurare *Radio 2 (2,4 GHz)*.

Nota: È consigliabile assegnare un ID VLAN diverso da quello predefinito (1) al traffico wireless, in modo da separarlo dal traffico di gestione sulla VLAN 1. Fare clic qui per ulteriori informazioni sui punti di accesso virtuali (VAP).



Passaggio 12. Immettere un nuovo nome di rete nel campo *Nome rete (SSID)*. Per impostazione predefinita viene utilizzato **ciscosb**. Il nome di rete è noto come SSID e identifica la rete in modo che i dispositivi wireless possano individuarla. Nell'esempio, il nome della rete a 5 GHz è stato differenziato con **ciscosb2.4**. Fare clic su **Avanti** per configurare la protezione wireless per *Radio 2 (2,4 GHz)*.



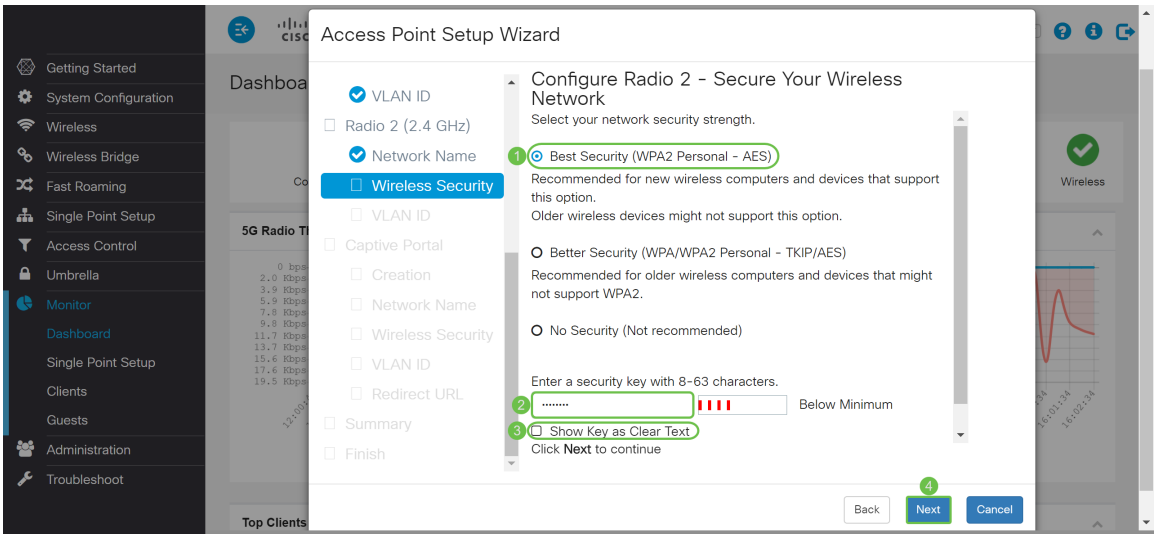
Passaggio 13. Fare clic sul pulsante di opzione corrispondente alla protezione di rete che si desidera applicare alla rete wireless. Immettere quindi la password per la rete nel campo *Chiave di accesso*. Per visualizzare la password durante la digitazione, selezionare la casella di controllo **Mostra chiave come testo non crittografato**. L'opzione **Mostra chiave come testo non crittografato** è selezionata per default. Fare clic su **Avanti** per continuare.

Nota: Se la rete dispone di una combinazione di client, alcuni dei quali supportano WPA2 e altri che supportano solo WPA originale, selezionare entrambi (WPA/WPA2). Ciò consente l'associazione e l'autenticazione delle stazioni client WPA e WPA2, ma utilizza il più affidabile WPA2 per i client che lo supportano. Questa configurazione WPA consente una maggiore interoperabilità al posto di una certa sicurezza.

- Massima sicurezza (WPA2 (Wi-Fi Protected Access 2) Personale - AES (Advanced Encryption Standard)) Tutte le stazioni client della rete supportano l'algoritmo di crittografia WPA2 e Advanced Encryption Standard utilizzando la modalità contatore con il protocollo AES-CCMP (Cipher Block Chaining Message Authentication Code Protocol). Ciò garantisce la migliore sicurezza in base allo standard IEEE 802.11i. In base al più recente requisito di Wi-Fi Alliance, l'access point deve supportare questa modalità in ogni momento.
- Maggiore sicurezza (WPA/WPA2 Personal - TKIP/AES) WPA Personal è uno standard Wi-Fi

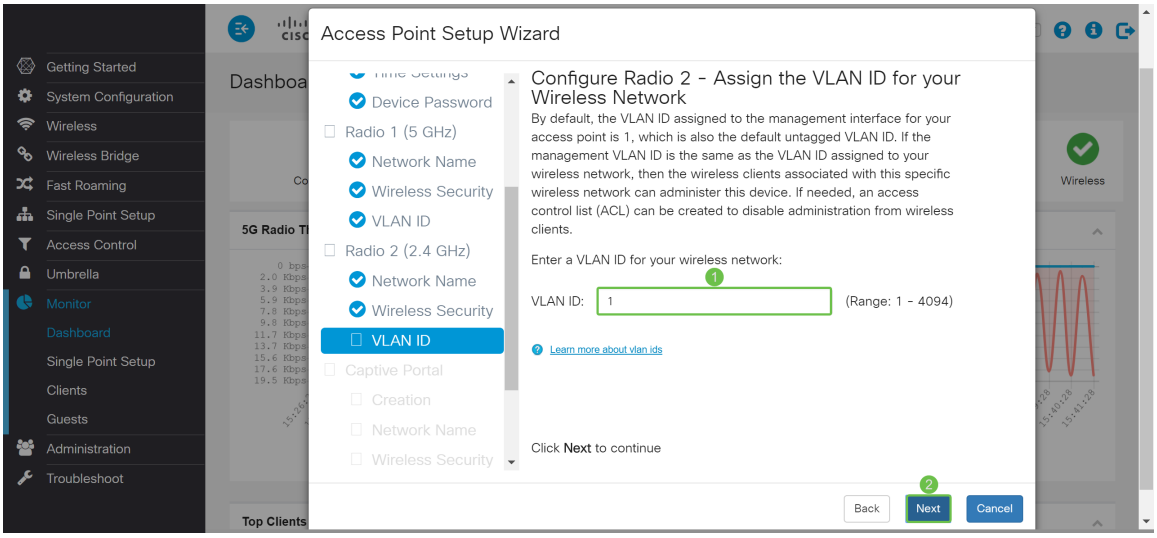
Alliance IEEE802.11i, che include la crittografia AES-CCMP e TKIP. Garantisce la sicurezza quando esistono dispositivi wireless meno recenti che supportano WPA originale ma non la nuova WPA2.

- Nessuna protezione (scelta non consigliata) La rete wireless non richiede una password e può essere utilizzata da chiunque.

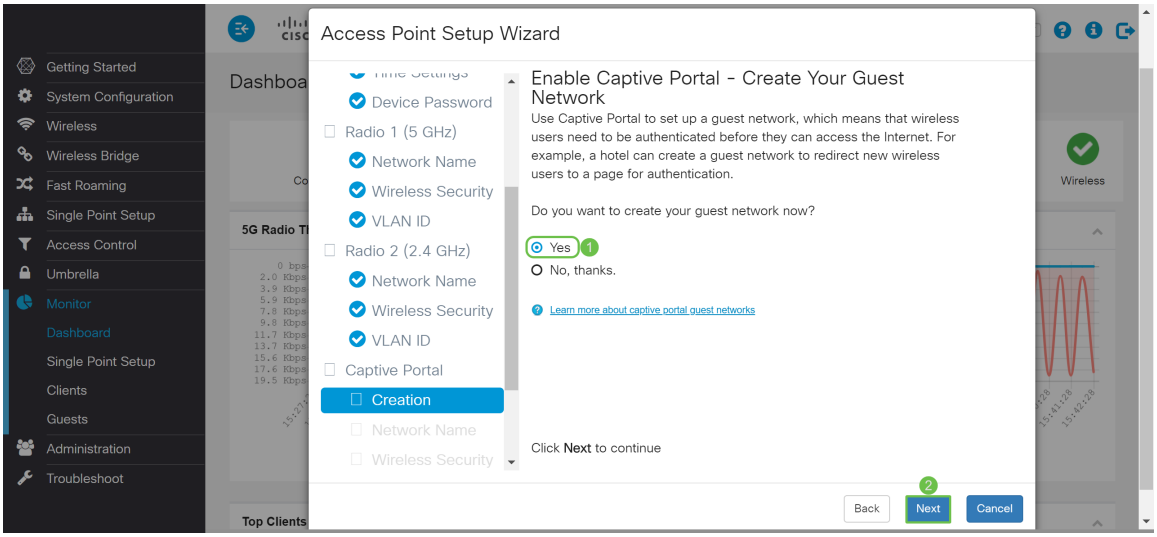


Passaggio 14. Nel campo *VLAN ID*, immettere il numero ID della VLAN a cui si desidera che la *radio 1 (2,4 GHz)* appartenga. Nell'esempio, verrà usato il valore predefinito 1 come *ID VLAN*. Fare clic su **Avanti** per configurare *Captive Portal*.

Nota: È consigliabile assegnare un ID VLAN diverso da quello predefinito (1) al traffico wireless, in modo da separarlo dal traffico di gestione sulla VLAN 1. Fare clic qui per ulteriori informazioni sui punti di accesso virtuali (VAP).

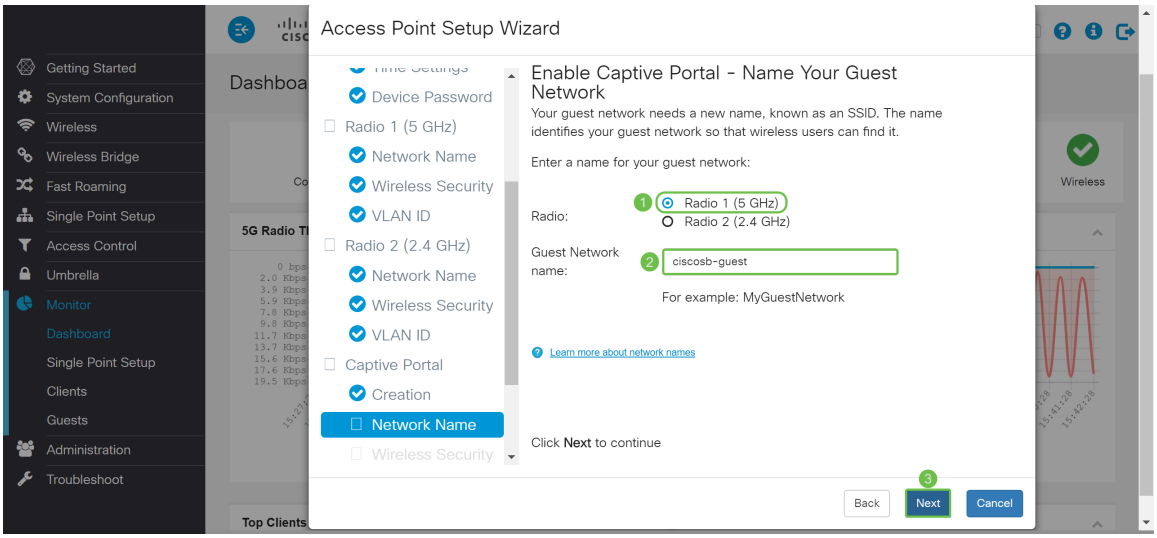


Passaggio 15. (Facoltativo) Non è necessaria una rete guest. Fare clic sul pulsante di opzione **Sì** per creare una rete guest. Fare clic sul pulsante di opzione **No** se non si desidera creare una rete guest e passare al passo 20. Fare clic sul pulsante **Avanti** per continuare.



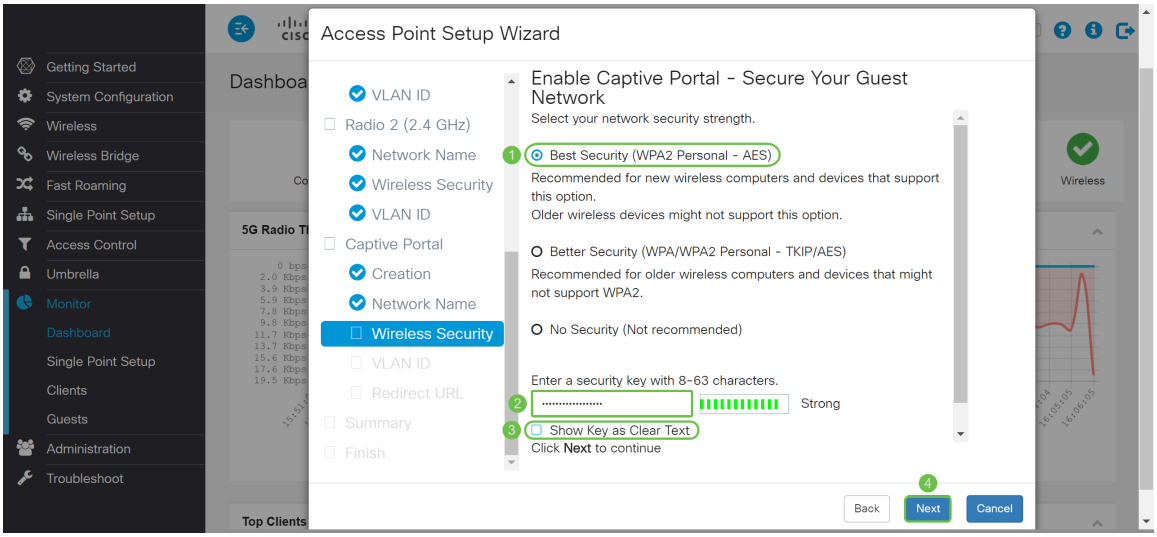
Passaggio 16. (Facoltativo) Selezionare il pulsante di opzione corrispondente alla *Radio* in cui si desidera posizionare la rete guest. Creare quindi un nome di rete nel campo *Nome rete guest*. Fare clic su **Avanti** per configurare le impostazioni di *protezione wireless* per la *rete guest*.

In questo esempio, sceglieremo **Radio 1 (5 GHz)** come *Radio* e lasceremo il nome di rete predefinito come **ciscosb-guest** in modo che gli utenti guest wireless possano trovare il nome di rete.

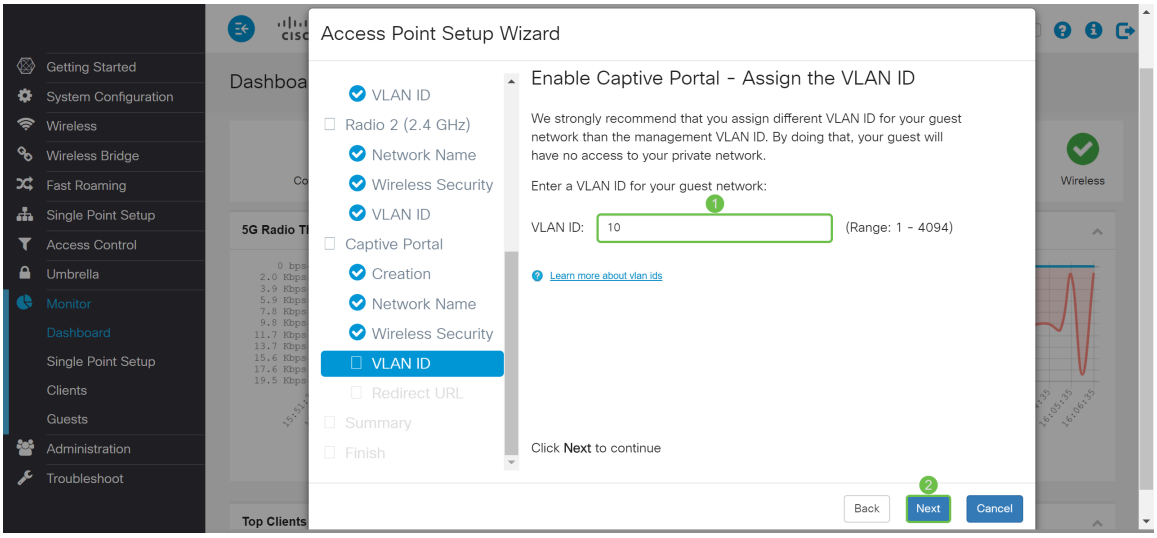


Passaggio 17. (Facoltativo) Selezionare il pulsante di opzione corrispondente alla sicurezza di rete che si desidera applicare alla rete guest. Immettere quindi una password per la rete guest nel campo *Chiave di protezione* se applicabile. Per **visualizzare la chiave come testo non crittografato** selezionare la casella di controllo per visualizzare la chiave di protezione come testo non crittografato. L'opzione è abilitata per impostazione predefinita. Fare clic su **Next** (Avanti) per continuare. Le opzioni di protezione di rete sono:

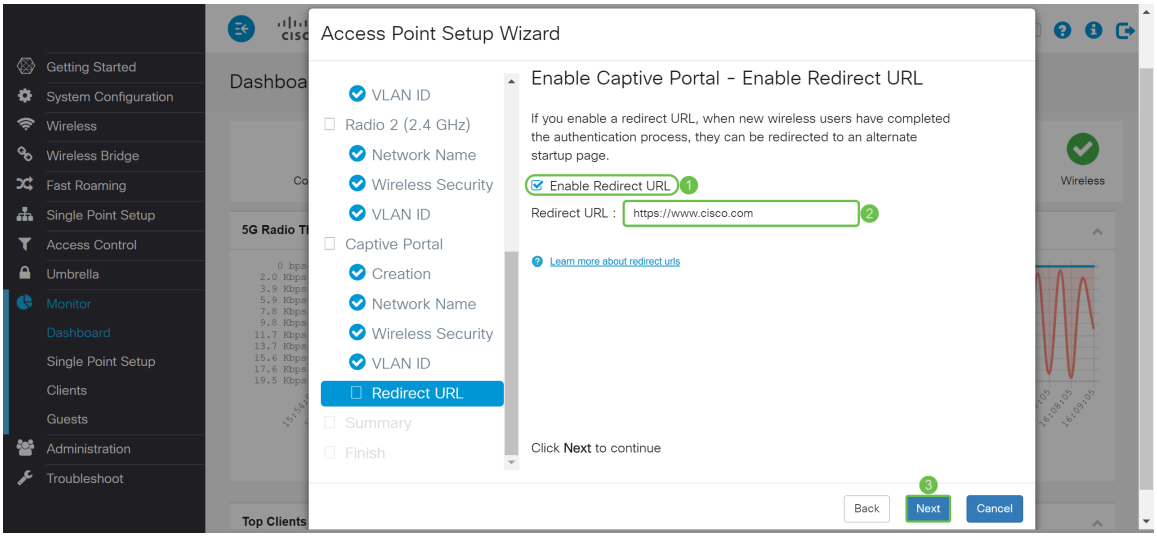
- Massima protezione (WPA2 Personal - AES): consigliata per i nuovi computer e dispositivi wireless che supportano questa opzione.
- Migliore protezione (WPA/WPA2 Personal - TKIP/AES) - Consigliata per i computer e i dispositivi wireless meno recenti che potrebbero non supportare WPA2.
- Nessuna protezione (scelta non consigliata) - Questa è la selezione predefinita.



Passaggio 18. (Facoltativo) Specificare un *ID VLAN* per la rete guest. L'ID della VLAN della rete guest deve essere diverso dall'ID della VLAN di gestione. Nell'esempio, viene usato l'*ID VLAN* **10** come ID VLAN per la rete guest. Fare clic su **Avanti** per configurare l'*URL di reindirizzamento* per la rete guest.

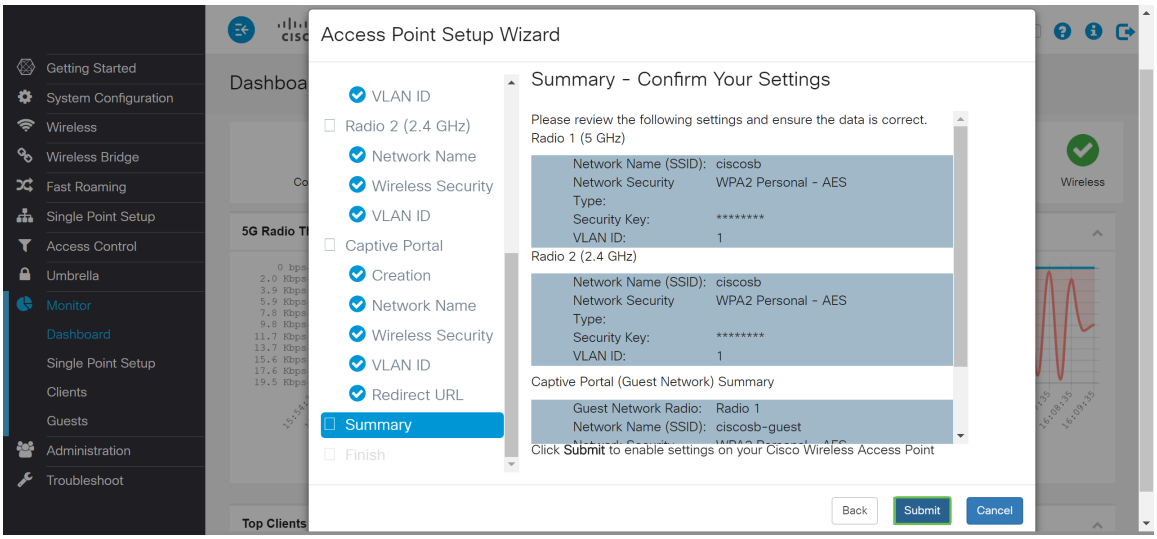


Passaggio 19. (Facoltativo) Selezionare la casella di controllo **Abilita URL di reindirizzamento** per reindirizzare i nuovi utenti wireless a una pagina di avvio alternativa. Immettere un nome di dominio completo (FQDN) o un indirizzo IP nel campo *Redirect URL* (incluso http:// o https://). Fare quindi clic su **Avanti** per passare alla pagina *Riepilogo*.

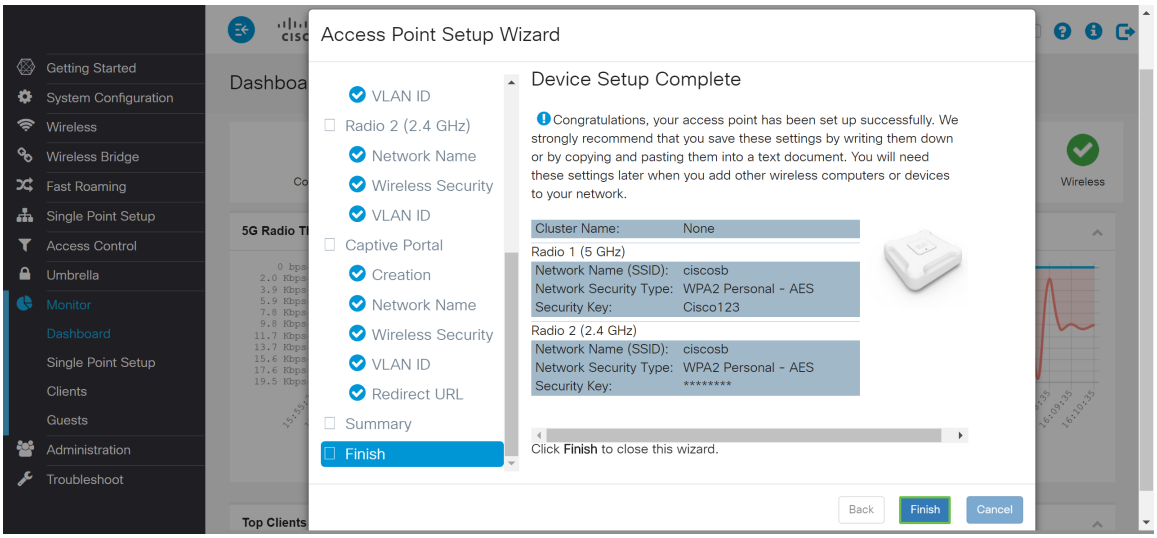


Passaggio 20. Nella pagina *Riepilogo - Conferma impostazioni*, rivedere le impostazioni configurate. Fare clic sul pulsante **Indietro** per riconfigurare una o più impostazioni. Se si fa clic su

Annulla, vengono ripristinati i valori precedenti o predefiniti di tutte le impostazioni. Se le configurazioni sono corrette, fare clic su **Invia**. Le impostazioni di configurazione vengono salvate e viene visualizzata una finestra di conferma.



Passaggio 21. Dopo aver configurato le impostazioni, viene visualizzata la pagina *Configurazione del dispositivo completata* per informare l'utente che il punto di accesso è stato configurato correttamente. Fare clic su **Finish** (Fine) per accedere di nuovo con la nuova password.



Conclusioni

Configurazione di WAP tramite l'Installazione guidata completata. Gli SSID appena configurati dovrebbero essere visualizzati nell'elenco delle reti Wi-Fi. Per configurare altre funzionalità in WAP, è necessario eseguire nuovamente l'accesso.