

Configurazione dell'installazione guidata su WAP551

Obiettivo

L'Impostazione guidata è costituita da una serie di istruzioni interattive che guidano l'utente nella configurazione iniziale di WAP551. Queste istruzioni riguardano le configurazioni di base necessarie per il funzionamento di WAP551. La finestra *Impostazione guidata Access Point* viene visualizzata automaticamente la prima volta che si accede a WAP, ma può essere utilizzata anche in qualsiasi momento.

In questo articolo viene illustrato come configurare WAP551 tramite l'installazione guidata.

Dispositivi interessati

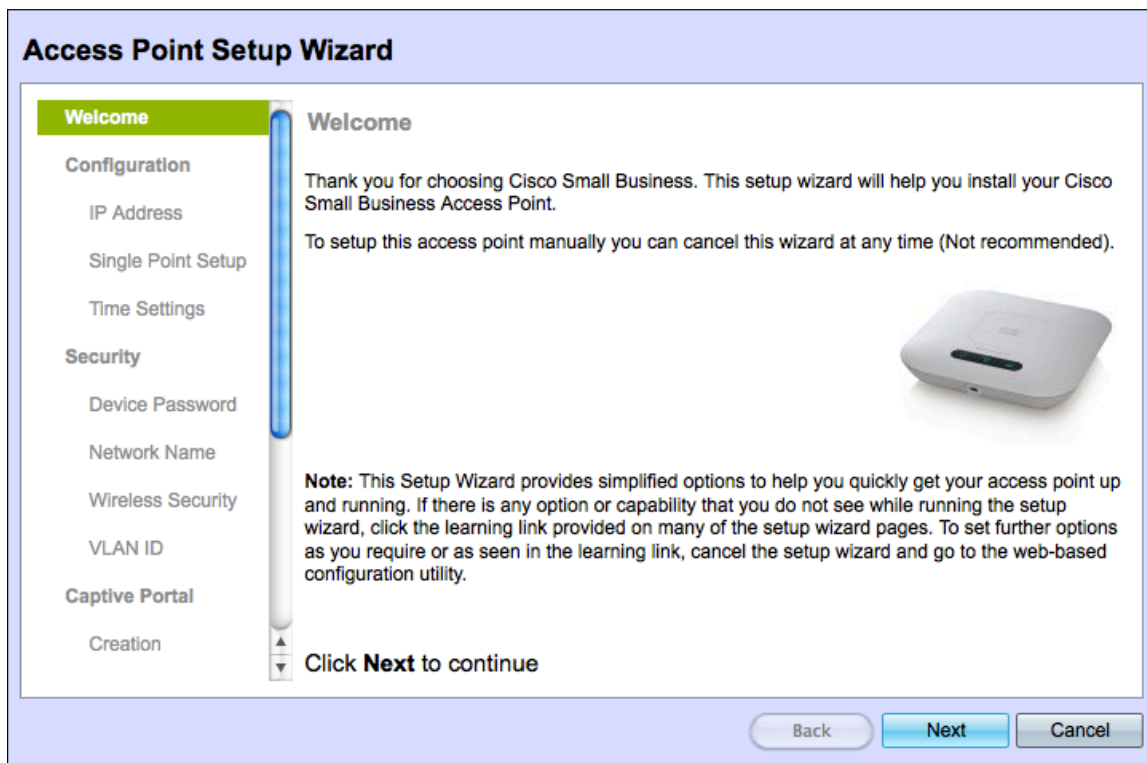
·WAP551

Versione del software

·v1.0.4.2

Configurazione guidata

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Esegui installazione guidata**. Verrà visualizzata la finestra *Configurazione guidata Access Point*.



Passaggio 2. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Configura dispositivo - indirizzo IP*:

Configure Device - IP Address

Select either Dynamic or Static IP address for your device.

Dynamic IP Address (DHCP) (Recommended)
 Static IP Address

Static IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

DNS: . . .

Secondary DNS (optional): . . .

[? Learn more about the different connection types](#)

Click **Next** to continue

Passaggio 3. Fare clic sul pulsante di opzione corrispondente al metodo che si desidera utilizzare per determinare l'indirizzo IP del WAP.

- Indirizzo IP dinamico (DHCP) (consigliato) - L'indirizzo IP del punto di accesso WAP viene assegnato da un server DHCP. Se si sceglie Indirizzo IP dinamico, andare al passo 9.

- Indirizzo IP statico: consente di creare un indirizzo IP fisso (statico) per il WAP. Un indirizzo IP statico non cambia.

Passaggio 4. Nel campo Indirizzo IP statico, immettere l'indirizzo IP del WAP. Questo indirizzo IP viene creato dall'utente e non deve essere utilizzato da un altro dispositivo nella rete.

Passaggio 5. Nel campo Subnet mask immettere la subnet mask dell'indirizzo IP.

Passaggio 6. Nel campo Gateway predefinito, immettere l'indirizzo IP del gateway predefinito per il WAP. Il gateway predefinito è in genere l'indirizzo IP privato assegnato al router.

Passaggio 7. Nel campo DNS immettere l'indirizzo IP del server DNS (Domain Name System) primario. Se si desidera accedere a pagine Web esterne alla rete, l'indirizzo IP del server DNS deve essere fornito dal provider di servizi Internet (ISP).

Passaggio 8. (Facoltativo) Nel campo *DNS secondario*, immettere l'indirizzo IP del DNS secondario.

Passaggio 9. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Configurazione punto singolo - Imposta cluster*.

Single Point Setup – Set A Cluster

A cluster provides a single point of administration and lets you view, deploy, configure, and secure the wireless network as a single entity, rather than as a series of separate wireless devices.

Create a New Cluster

Recommended for a new deployment environment.

New Cluster Name:

AP Location:

Join an Existing Cluster

Recommended for adding new wireless access points to the existing deployment environment.

Existing Cluster Name:

AP Location:

Do not Enable Single Point Setup

Recommended for single device deployments or if you prefer to configure each device individually.

Click **Next** to continue

Passaggio 10. Fare clic sul pulsante di opzione corrispondente alle impostazioni del cluster che si desidera utilizzare. Un cluster consente di configurare più punti di accesso come un unico dispositivo. Se si sceglie di non utilizzare un cluster, sarà necessario configurarlo singolarmente.

- Creare un nuovo cluster — Creare un nuovo cluster per i punti di accesso.
- Aggiungi a cluster esistente: consente di aggiungere un cluster AP esistente nella rete.
- Non abilitare Single Point Setup - Single Point Setup (cluster) non è consentito. Se si sceglie questa opzione, andare al passo 13.

Passaggio 11. Nel campo *Nome cluster*, immettere un nome cluster esistente o creare un nuovo nome cluster in base alla decisione presa nel passaggio 10.

Passaggio 12. Nel campo Ubicazione contabilità fornitori, immettere l'ubicazione fisica del conto WAP.

Timesaver: se si fa clic sul pulsante di opzione Aggiungi a cluster esistente, WAP configura le altre impostazioni in base al cluster. Fare clic su **Avanti**. Verrà visualizzata una pagina di conferma in cui viene richiesto se si desidera partecipare al cluster. Fare clic su **Invia** per unirsi al cluster. Al termine della configurazione, fare clic su **Fine** per uscire dall'installazione guidata.

Passaggio 13. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Configura dispositivo - Imposta data e ora di sistema*:

Configure Device - Set System Date And Time

Enter the time zone, date and time.

Time Zone:

Set System Time: Network Time Protocol (NTP)
 Manually

NTP Server:

[? Learn more about time settings](#)

Click **Next** to continue

Passaggio 14. Scegliere un fuso orario dall'elenco a discesa *Fuso orario*.

Passaggio 15. Fare clic sul pulsante di opzione corrispondente al metodo che si desidera utilizzare per impostare l'ora del WAP.

·Protocollo NTP (Network Time Protocol) - Il WAP riceve l'ora da un server NTP.

·Manualmente: l'ora viene immessa manualmente nel WAP. Se si sceglie manualmente, andare al passo 17.

Passaggio 16. Nel campo *Server NTP*, immettere l'URL del server NTP che fornisce la data e l'ora. Andare al passaggio 19.

Configure Device - Set System Date And Time

Enter the time zone, date and time.

Time Zone:

Set System Time: Network Time Protocol (NTP)
 Manually

NTP Server:

[? Learn more about time settings](#)

Click **Next** to continue

Passaggio 17. Dagli elenchi a discesa *Data sistema* scegliere rispettivamente il mese, il giorno e l'anno.

Passaggio 18. Dagli elenchi a discesa *Ora di sistema*, scegliere rispettivamente l'ora e i minuti.

Passaggio 19. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Abilita sicurezza - Imposta password*:

Enable Security - Set Password


The administrative password protects your access point from unauthorized access. For security reasons, you should change the access point password from its default settings. Please write this password down for future reference.

Enter a new device password:

New password needs at least 8 characters composed of lower and upper case letters as well as numbers/symbols by default.

New Password:

Confirm Password:

Password Strength Meter:  Strong

Password Complexity: Enable

[? Learn more about passwords](#)

Click **Next** to continue

Passaggio 20. Nel campo *Nuova password*, immettere una nuova password. Password che consente l'accesso amministrativo al WAP.

Passaggio 21. Nel campo *Conferma password*, immettere nuovamente la stessa password.

Nota: Quando si immette una password, il numero e il colore delle barre verticali cambiano per indicare l'intensità della password, come indicato di seguito:

- Rosso: la password non soddisfa i requisiti minimi di complessità.
- Arancione: la password soddisfa i requisiti minimi di complessità, ma la sua complessità è scarsa.
- Verde: la password è complessa.

Passaggio 22. (Facoltativo) Per abilitare la complessità della password, selezionare la casella di controllo **Abilita**. È quindi necessario che la password contenga almeno 8 caratteri e sia composta da lettere minuscole e maiuscole e numeri/simboli.

Passaggio 23. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Abilita sicurezza - Denominazione della rete wireless*:

Enable Security - Name Your Wireless Network

The name of your wireless network, known as an SSID, identifies your network so that wireless devices can find it.

Enter a name for your wireless network:

Network Name (SSID):

For example: MyNetwork

[? Learn more about network names](#)

Click **Next** to continue

Passaggio 24. Nel campo Nome rete (SSID), immettere l'SSID (Service Set Identification) della rete wireless. SSID è il nome della rete locale (LAN) wireless.

Passaggio 25. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Abilita sicurezza - Proteggi rete wireless*.

Enable Security - Secure Your Wireless Network

Select your network security strength.

- Best Security (WPA2 Personal - AES)
Recommended for new wireless computers and devices that support this option.
Older wireless devices might not support this option.
- Better Security (WPA Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.
- No Security (Not recommended)

Enter a security key with 8-63 characters.

 Strong

Show Key as Clear Text

[? Learn more about your network security options](#)

Click **Next** to continue

Passaggio 26. Fare clic sul pulsante di opzione corrispondente alla protezione di rete che si desidera applicare alla rete wireless.

·Massima sicurezza (WPA2 Personal - AES): WPA2 è la seconda versione della tecnologia di controllo degli accessi e della sicurezza WPA per le reti wireless Wi-Fi, che include la crittografia AES-CCMP. Questa versione del protocollo offre la migliore protezione dello

standard IEEE 802.11i. Tutte le stazioni client della rete dovranno essere in grado di supportare WPA2. WPA2 non consente l'utilizzo del protocollo TKIP (Temporal Key Integrity Protocol) con limitazioni note.

·Migliore sicurezza (WPA Personal - TKIP/AES): WPA Personal è uno standard Wi-Fi Alliance IEEE 802.11i, 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: la rete wireless non richiede una password e può essere utilizzata da chiunque. Se si sceglie Nessuna protezione, andare al passo 29.

Passaggio 27. Nel campo Chiave di accesso, immettere la password per la rete.

Passaggio 28. (Facoltativo) Per visualizzare la password durante la digitazione, selezionare la casella di controllo **Mostra chiave come testo non crittografato**.

Passaggio 29. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Abilita sicurezza - Assegna l'ID VLAN per la rete wireless*.

Enable Security - Assign The VLAN ID For Your Wireless Network

By default, the VLAN ID assigned to the management interface for your access point is 1, which is also the default untagged VLAN ID. If the management VLAN ID is the same as the VLAN ID assigned to your wireless network, then the wireless clients associated with this specific wireless network can administer this device. If needed, an access control list (ACL) can be created to disable administration from wireless clients.

Enter a VLAN ID for your wireless network:

VLAN ID: (Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Passaggio 30. Nel campo ID VLAN, immettere il numero ID della VLAN a cui si desidera che il WAP appartenga.

Nota: L'ID VLAN deve corrispondere a uno degli ID VLAN supportati sulla porta del dispositivo remoto connesso al WAP.

Passaggio 31. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Abilita Captive Portal - Crea rete guest*.

Enable Captive Portal - Create Your Guest Network

Use Captive Portal to set up a guest network, which means that wireless users need to be authenticated before they can access the Internet. For example, a hotel can create a guest network to redirect new wireless users to a page for authentication.

Do you want to create your guest network now?

- Yes
 No, thanks.

[? Learn more about captive portal guest networks](#)

Click **Next** to continue

Passaggio 32. Fare clic sul pulsante di opzione **Sì** per creare una rete guest. Una rete guest richiede l'autenticazione degli utenti prima di poter utilizzare Internet. Non è necessaria una rete guest. Fare clic sul pulsante di opzione **No** se non si desidera creare una rete guest e passare al passo 45.

Passaggio 3. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Abilita Captive Portal - Denominazione rete guest*.

Enable Captive Portal - Name Your Guest Network

Your guest network needs a new name, known as an SSID. The name identifies your guest network so that wireless users can find it.

Enter a name for your guest network:

Guest Network name:
For example: MyGuestNetwork

[? Learn more about network names](#)

Click **Next** to continue

Passaggio 34. Nel campo Nome rete guest, immettere il SSID della rete guest.

Passaggio 35. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Abilita Captive Portal - Proteggi la rete guest*.

Enable Captive Portal - Secure Your Guest Network

Select your guest network security strength.

- Best Security (WPA2 Personal - AES)
Recommended for new wireless computers and devices that support this option.
Older wireless devices might not support this option.
- Better Security (WPA Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.
- No Security (Not recommended)

Enter a security key with 8-63 characters.



Show Key as Clear Text

[Learn more about your network security options](#)

Click **Next** to continue

Passaggio 36. Fare clic sul pulsante di opzione corrispondente alla sicurezza di rete che si desidera applicare alla rete guest.

·Massima sicurezza (WPA2 Personal - AES): fornisce la massima sicurezza ed è consigliata se i dispositivi wireless supportano questa opzione.

·Maggiore sicurezza: fornisce sicurezza quando sono presenti periferiche wireless meno recenti che non supportano WPA2.

·Nessuna protezione: la rete wireless non richiede una password e può essere utilizzata da chiunque. Se si sceglie Nessuna protezione, andare al passo 39.

Passaggio 37. Nel campo Chiave di sicurezza, immettere la password per la rete guest.

Passaggio 38. (Facoltativo) Per visualizzare la password durante la digitazione, selezionare la casella di controllo **Mostra chiave come testo non crittografato**.

Passaggio 39. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Enable Captive Portal - Assign The VLAN ID*:

Enable Captive Portal - Assign The VLAN ID

We strongly recommend that you assign different VLAN ID for your guest network than the management VLAN ID. By doing that, your guest will have no access to your private network.

Enter a VLAN ID for your guest network:

VLAN ID: (Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Passaggio 40. Nel campo ID VLAN, immettere il numero ID della VLAN a cui si desidera che la rete guest appartenga.

Nota: L'ID VLAN deve corrispondere a uno degli ID VLAN supportati sulla porta del dispositivo remoto connesso al WAP.

Passaggio 41. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Abilita portale vincolato - Abilita URL di reindirizzamento*:

Enable Captive Portal - Enable Redirect URL

If you enable a redirect URL, when new wireless users have completed the authentication process, they can be redirected to an alternate startup page.

Enable Redirect URL

Redirect URL :

[? Learn more about redirect urls](#)

Click **Next** to continue

Passaggio 42. (Facoltativo) Per reindirizzare gli utenti wireless a una pagina Web dopo aver effettuato l'accesso alla rete guest, selezionare la casella di controllo **Abilita URL di reindirizzamento**.

Timesaver: Se non si seleziona la casella di controllo **Abilita**, andare al passo 44.

Passaggio 43. Nel campo Reindirizza URL, immettere la pagina Web a cui si desidera reindirizzare gli utenti dopo l'accesso alla rete guest.

Passaggio 4. Fare clic su **Avanti** per continuare. Viene visualizzata la pagina *Summary - Confirm Your Settings*:

Summary - Confirm Your Settings

Please review the following settings and ensure the data is correct.

Network Name (SSID):	cisco5b
Network Security Type:	plain-text
Security Key:	
VLAN ID:	1

Captive Portal (Guest Network) Summary

Network Name (SSID):	Guest
Network Security Type:	WPA2 Personal - AES
Security Key:	*****
Verification:	Guest
Redirect URL:	http://www.example.com
VLAN ID:	5

Note: The AP Radio will be enabled after clicking Submit.

Click **Submit** to enable settings on your Cisco Small Business Access Point

Back Submit Cancel

Passaggio 45. (Facoltativo) Per modificare un'impostazione, fare clic su **Indietro**.

Passaggio 46. (Facoltativo) Se si desidera uscire dall'Installazione guidata e annullare tutte le modifiche apportate, fare clic su **Annulla**.

Passaggio 47. Verificare le impostazioni della rete e della rete guest. Fare clic su **Submit** (Invia) per abilitare le impostazioni in WAP. Quando WAP abilita le impostazioni, viene visualizzata una barra di caricamento. Al termine dell'operazione, viene visualizzata la pagina *Fine*:

Nota: Il passo 48 è applicabile solo se si fa clic su **Submit** (Invia) nella pagina *Confirm Your Settings* (Conferma impostazioni).

Device Setup Complete



Congratulations, your access point has been set up successfully. We strongly recommend that you save these settings by writing them down or by copying and pasting them into a text document. You will need these settings later when you add other wireless computers or devices to your network.

Cluster Name:	ciscosb-cluster
Network Name (SSID):	ciscosb
Network Security Type:	plain-text
Security Key:	



Note: To configure WPS, Click "Run WPS" on the Getting Started page, under Initial Setup.

Click **Finish** to close this wizard.

Back

Finish

Cancel

Passaggio 48. Fare clic su **Fine** per uscire dall'Installazione guidata.