

# Configurazione iniziale dei punti di accesso wireless WAP150, WAP351, WAP361 e WAP371 tramite la procedura guidata di installazione

## Obiettivo

L'Installazione guidata è una funzionalità incorporata utilizzata per semplificare la configurazione iniziale dei punti di accesso wireless (WAP, Wireless Access Point). Semplifica la configurazione delle impostazioni di base. Il processo dettagliato dell'Installazione guidata consente di eseguire la configurazione iniziale del dispositivo WAP e di utilizzare rapidamente le funzionalità di base di tale dispositivo.

Lo scopo di questo documento è quello di mostrare come configurare i punti di accesso wireless WAP150, WAP351, WAP361 e WAP371 tramite l'Installazione guidata.

## Dispositivi interessati

- WAP150
- WAP351
- WAP361
- WAP371

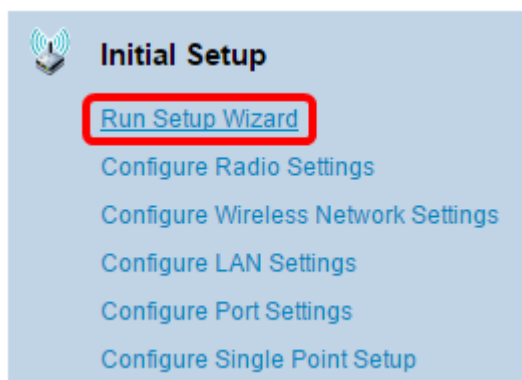
## Versione del software

- 1.0.1.7 - WAP150, WAP361
- 1.0.2.8 - WAP351
- 1.3.0.3 - WAP371

## Configurazione

**Nota:** Le immagini utilizzate di seguito sono tratte da WAP361.

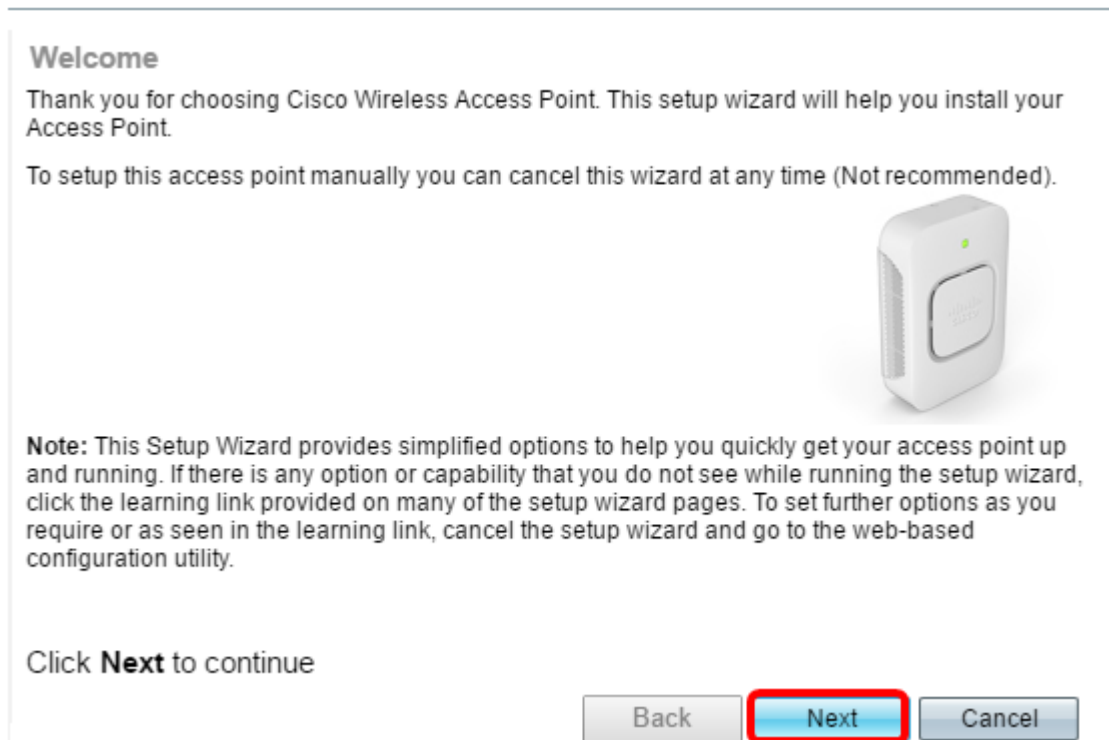
Passaggio 1. Accedere all'utility basata sul Web del punto di accesso. Nella pagina del menu Guida introduttiva, fare clic su **Esegui installazione guidata**.



**Nota:** se è la prima volta che si accede a WAP, l'Installazione guidata si aprirà

automaticamente.

Passaggio 2. Per continuare, fare clic su **Avanti** nella pagina iniziale della Configurazione guidata punto di accesso.



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

Le opzioni sono definite come segue:

- Indirizzo IP dinamico (DHCP) (consigliato) - Consente al server DHCP di assegnare un indirizzo IP dinamico per il WAP. Se si sceglie questa opzione, fare clic su **Next** (Avanti), quindi andare al [passaggio 9](#).
- Indirizzo IP statico — consente di creare un indirizzo IP fisso (statico) per il WAP. Un indirizzo IP statico non cambia.

**Nota:** Nell'esempio viene scelto DHCP (Dynamic IP Address).

### 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 4. Se nel passaggio precedente è stato scelto Indirizzo IP statico, immettere l'indirizzo IP del WAP nel campo *Indirizzo IP statico*. Questo indirizzo IP è univoco per il WAP e non deve essere utilizzato da un altro dispositivo nella rete.

Dynamic IP Address (DHCP) (Recommended)

Static IP Address

Static IP Address:  .  .  .

Subnet Mask:  .  .  .

Default Gateway:  .  .  .

DNS:  .  .  .

Secondary DNS (optional):  .  .  .

**Nota:** Nell'esempio, 192.168.1.121 viene usato come indirizzo IP statico.

Passaggio 5. Inserire la subnet mask nel campo *Subnet mask*.

Dynamic IP Address (DHCP) (Recommended)

Static IP Address

Static IP Address:  .  .  .

Subnet Mask:  .  .  .

Default Gateway:  .  .  .

DNS:  .  .  .

Secondary DNS (optional):  .  .  .

**Nota:** Nell'esempio, la subnet mask è 255.255.255.0.

Passaggio 6. Immettere il gateway predefinito per il WAP nel campo *Gateway predefinito*. Questo è l'indirizzo IP privato del router.

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

Static IP Address:  .  .  .   
 Subnet Mask:  .  .  .   
 Default Gateway:  .  .  .   
 DNS:  .  .  .   
 Secondary DNS (optional):  .  .  .

**Nota:** Nell'esempio, 192.168.1.1 è usato come gateway predefinito.

Passaggio 7. (Facoltativo) Se si desidera accedere all'utilità basata sul Web all'esterno della rete, immettere l'indirizzo DNS (Domain Name System) primario nel campo *DNS*. L'indirizzo del server DNS deve essere fornito dal provider di servizi Internet (ISP).

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

Static IP Address:  .  .  .   
 Subnet Mask:  .  .  .   
 Default Gateway:  .  .  .   
 DNS:  .  .  .   
 Secondary DNS (optional):  .  .  .

**Nota:** Nell'esempio, l'indirizzo DNS è 192.168.1.2.

Passaggio 8. (Facoltativo) Immettere un indirizzo DNS secondario nei campi *DNS secondario*, quindi fare clic su **Avanti**.

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

Static IP Address:  .  .  .   
 Subnet Mask:  .  .  .   
 Default Gateway:  .  .  .   
 DNS:  .  .  .   
 Secondary DNS (optional):  .  .  .

**Nota:** Nell'esempio, 192.168.1.3 viene utilizzato come indirizzo DNS secondario.

## Single Point Setup

Passaggio 9. Nella schermata Configurazione punto singolo - Imposta cluster, selezionare un pulsante di opzione corrispondente alla modalità di configurazione delle impostazioni cluster di WAP. Il clustering consente di gestire più punti di accesso da un singolo punto, anziché passare a ciascun dispositivo e modificare le impostazioni singolarmente.

Le opzioni sono definite come segue:

- Nuovo nome cluster: selezionare questa opzione se si desidera creare un nuovo cluster.

**Nota:** Per WAP351 e WAP371, l'opzione è Crea nuovo cluster.

- Aggiungi a cluster esistente: selezionare questa opzione se si desidera che WAP si unisca a un cluster esistente. Se si sceglie questa opzione, andare al [passaggio 11](#).
- Non abilitare Single Point Setup - Scegliere questa opzione se non si desidera che il punto di accesso Windows faccia parte di un cluster. Se si sceglie questa opzione, fare clic su **Avanti**, quindi andare al [passaggio 13](#).

**Nota:** In questo esempio, è stato scelto Non abilitare Single Point Setup.

**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.

New Cluster Name  
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.

[? Learn more about single point setup](#)

Click **Next** to continue

Back Next Cancel

Passaggio 10. Se nel passaggio precedente è stato scelto Nuovo nome cluster, immettere il nome del nuovo cluster e la relativa posizione nei *campi Nuovo nome cluster* e *Posizione punto di accesso* rispettivamente, quindi fare clic su **Avanti**. La posizione AP è la posizione fisica del punto di accesso definita dall'utente (ad esempio, Office). Andare al [Passaggio 13](#).

**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.

**New Cluster Name**  
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.

[? Learn more about single point setup](#)

Click **Next** to continue

Passaggio 11. Se si sceglie **Unisci a cluster esistente** nel passaggio 9, immettere il nome del cluster e la relativa posizione rispettivamente nei campi *Nome cluster esistente* e *Posizione AP*, quindi fare clic su **Avanti**.

**Nota:** Questa opzione è ideale se esiste già una rete wireless e tutte le impostazioni sono già state configurate.

**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.

**New Cluster Name**  
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.

[? Learn more about single point setup](#)

Click **Next** to continue

Passaggio 12. Controllare le impostazioni per verificare che i dati siano corretti, quindi fare clic su **Invia**.

**Summary - Confirm Your Settings**  
Please review the following settings and ensure the data is correct.

You are about to join this cluster:      Main Point

Click **Submit** to enable settings on your Cisco Wireless Access Point

Back    **Submit**    Cancel

## Impostazioni ora

Passaggio 13. Scegliere il fuso orario dall'elenco a discesa Fuso orario.

**Configure Device - Set System Date And Time**  
Enter the time zone, date and time.

Time Zone:      USA (Pacific) ▼

Set System Time:      USA (Aleutian Islands) ▲  
USA (Arizona)  
USA (Central)  
USA (Eastern)  
USA (Mountain)  
**USA (Pacific)**

NTP Server 1:      Uzbekistan  
NTP Server 2:      Vanuatu  
NTP Server 3:      Vatican City  
NTP Server 4:      Venezuela  
Vietnam  
Wake Islands  
Wallis & Futana Islands  
Western Samoa  
Windward Islands  
Yemen  
Zaire (Kasai)  
Zaire (Kinshasa)  
Zambia  
Zimbabwe

[? Learn more about t](#)

Click **Next** to continue

Back    **Next**    Cancel

**Nota:** Nell'esempio viene scelto USA (Pacifico).

Passaggio 14. Fare clic sul pulsante di opzione corrispondente al metodo che si desidera utilizzare per impostare l'ora del WAP.

Le opzioni sono le seguenti:

- Protocollo NTP (Network Time Protocol) - Il WAP ottiene l'ora da un server NTP.
- Manualmente - l'ora viene immessa manualmente in WAP. Se si sceglie questa opzione, andare al [passo 16](#).

**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 1:

NTP Server 2:

NTP Server 3:

NTP Server 4:

[? Learn more about time settings](#)

Click **Next** to continue

**Nota:** Nell'esempio viene utilizzato il protocollo NTP (Network Time Protocol).

Passaggio 15. Immettere il nome di dominio del server NTP che fornisce la data e l'ora nel campo *Server NTP 1*. È possibile aggiungere fino a quattro diversi server NTP immettendoli nei rispettivi campi e facendo clic su **Avanti**. Quindi, andare al [Passaggio 17](#).

**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 1:

NTP Server 2:

NTP Server 3:

NTP Server 4:

[? Learn more about time settings](#)

Click **Next** to continue

**Nota:** Nell'esempio vengono immessi quattro server NTP.

Passaggio 16. (Facoltativo) Se si sceglie Manualmente nel Passaggio 14, selezionare la data negli elenchi a discesa Data sistema per scegliere rispettivamente il mese, il giorno e l'anno. Selezionare l'ora e i minuti dagli elenchi a discesa Ora di sistema, quindi fare clic su **Avanti**.



**Configure Device - Set System Date And Time**  
 Enter the time zone, date and time.

Time Zone:

Set System Time:  Network Time Protocol (NTP)  
 Manually

System Date:

System Time:  :

[Learn more about time settings](#)

Click **Next** to continue

## Password dispositivo

Passaggio 17. Nella schermata Configure Device - Set Password (Configura dispositivo - Imposta password), immettere una nuova password per WAP nel campo *New Password* (Nuova password) e confermarla. Questa password viene utilizzata per ottenere l'accesso amministrativo all'utilità basata sul Web del punto di accesso wireless e non per la connessione alla rete wireless.

New Password:

Confirm Password:

Password Strength Meter:  Below Minimum

**Nota:** il campo *Misuratore dell'intensità della password* visualizza barre verticali che cambiano quando si immette la password.

I colori del misuratore dell'intensità della password sono definiti come segue:

- Rosso: il requisito minimo di complessità della password non è soddisfatto.
- Arancione: il requisito minimo di complessità della password è soddisfatto, ma la complessità della password è scarsa.
- Verde: il requisito minimo di complessità della password è soddisfatto e la complessità della password è elevata.

Passaggio 18. (Facoltativo) Abilitare la complessità della password selezionando la casella di controllo **Abilita** complessità password. È quindi necessario che la password contenga almeno 8 caratteri e sia composta da lettere minuscole e maiuscole e da numeri o simboli. La complessità della password è abilitata per impostazione predefinita.

New Password:

Confirm Password:

Password Strength Meter:  Below Minimum

Password Complexity:  Enable

[? Learn more about passwords](#)

Click **Next** to continue

Passaggio 19. Fare clic su **Avanti** per continuare.

## Configurazione delle radio 1 e 2 (2,4 e 5 GHz)

Le impostazioni della rete wireless devono essere configurate singolarmente per ogni canale radio. Il processo di configurazione della rete wireless è lo stesso per ogni canale.

**Nota:** Per il WAP371, Radio 1 è per la banda a 5 GHz e Radio 2 è per la banda a 2,4 GHz.

Passaggio 20. Nell'area Configura radio 1 - Denominazione rete wireless, immettere un nome per la rete wireless nel campo *Nome rete (SSID)*, quindi fare clic su **Avanti**.

**Configure Radio 1 - 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

**Nota:** Nell'esempio, il nome della rete è WAP361\_L2.

Passaggio 21. Nell'area Configura radio 1 - Proteggi la rete wireless, fare clic sul pulsante di opzione corrispondente alla sicurezza di rete che si desidera applicare alla rete wireless.

Le opzioni sono definite come segue:

- Massima protezione (WPA2 Personal - AES): offre la massima protezione ed è consigliata se le periferiche wireless supportano questa opzione. WPA2 Personal utilizza AES (Advanced Encryption Standard) e PSK (Pre-Shared Key) tra i client e il punto di accesso. Utilizza una

- nuova chiave di crittografia per ogni sessione, il che rende difficile la compromissione.
- Migliore protezione (WPA/WPA2 Personal - TKIP/AES): fornisce protezione quando sono presenti dispositivi wireless meno recenti che non supportano WPA2. WPA Personal utilizza AES e TKIP (Temporal Key Integrity Protocol). Utilizza lo standard Wi-Fi IEEE 802.11i.
  - Nessuna protezione (scelta non consigliata): la rete wireless non richiede una password e può essere utilizzata da chiunque. Se selezionato, viene visualizzata una finestra popup in cui viene chiesto se si desidera disattivare la protezione; fare clic su **Sì** per continuare. Se si sceglie questa opzione, andare al [passo 24](#).

### Configure Radio 1 - 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/WPA2 Personal - TKIP/AES)  
Recommended for older wireless computers and devices that might not support WPA2.
- No Security (Not recommended)

**Nota:** In questo esempio, viene scelto Protezione migliore (WPA2 Personal -AES).

Passaggio 2. Immettere la password per la rete nel campo *Chiave di accesso*. La barra colorata a destra di questo campo indica la complessità della password immessa.

### Configure Radio 1 - 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/WPA2 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.

..... |||| Session Key Refresh Rate

Show Key as Clear Text

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

Passaggio 23. (Facoltativo) Per visualizzare la password durante la digitazione, selezionare la casella di controllo **Mostra chiave come testo non crittografato** e fare clic su **Avanti**.

Enter a security key with 8-63 characters.

SecretKey1 ||||| Weak

Show Key as Clear Text

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

Click **Next** to continue

Back

Next

Cancel

Passaggio 24. Nell'elenco a discesa Configura radio 1 - Assegna l'ID VLAN per la rete wireless, scegliere un ID per la rete dall'elenco a discesa ID VLAN. Se la VLAN di gestione è la stessa assegnata alla rete wireless, i client wireless della rete possono amministrare il dispositivo. È inoltre possibile utilizzare Access Control Lists (ACL) per disattivare l'amministrazione dai client wireless.

**Nota:** Per i protocolli WAP371 e WAP150, è necessario immettere l'ID nel campo *ID VLAN* fornito. L'intervallo di ID della VLAN è compreso tra 1 e 4094.

---

**Configure Radio 1 - 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:

[? Learn more about vlan ids](#)

Click **Next** to continue

**Nota:** nell'esempio, viene usato l'ID VLAN 1.

Passaggio 25. Fare clic su **Avanti** per continuare l'installazione guidata e configurare Radio 2.

**Nota:** Il processo di configurazione delle impostazioni di rete wireless per Radio 2 è lo stesso di Radio 1.

## Captive Portal

Captive Portal consente di configurare una rete guest in cui gli utenti wireless devono essere autenticati prima di poter accedere a Internet. Per configurare Captive Portal, procedere come segue.

Passaggio 26. Nell'area Abilita portale vincolato - Crea rete guest, scegliere il pulsante di opzione **Sì**, quindi fare clic su **Avanti**.

**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 quest networks](#)

Click **Next** to continue

Back Next Cancel

**Nota:** Se si preferisce non abilitare Captive Portal, fare clic su No per visualizzare la pagina Riepilogo della procedura guidata di installazione. Quindi, andare al [passo 35](#).

Passaggio 27. Selezionare la frequenza radio desiderata per la rete guest. La banda a 2,4 GHz offre supporto per i dispositivi legacy e può propagare un segnale wireless più ampio attraverso più muri. La banda a 5 GHz, d'altra parte, è meno affollata e può fornire una maggiore velocità di trasmissione, assorbendo una frequenza di 40 MHz della banda invece dei 20 MHz standard nella banda a 2,4 GHz. Oltre alla gamma più breve, ci sono meno dispositivi che supportano la banda a 5 GHz rispetto a 2,4 GHz.

Radio:  Radio 1 (5 GHz)  
 Radio 2 (2.4 GHz)

Guest Network name:   
For example: MyGuestNetwork

**Nota:** Nell'esempio, viene scelto Radio 1 (5 GHz).

Passaggio 28. Immettere il nome del SSID guest nel campo *Nome rete guest*, quindi fare clic su **Avanti**.

**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:

Radio:  Radio 1 (5 GHz)  
 Radio 2 (2.4 GHz)

Guest Network name:   
For example: MyGuestNetwork

[? Learn more about network names](#)

Click **Next** to continue

**Nota:** In questo esempio, BeMyGuest! viene utilizzato come nome della rete guest.

Passaggio 29. Fare clic sul pulsante di opzione corrispondente alla protezione di rete che si desidera applicare alla rete wireless guest.

Le opzioni sono definite come segue:

- **Massima protezione (WPA2 Personal - AES):** offre la massima protezione ed è consigliata se le periferiche wireless supportano questa opzione. WPA2 Personal utilizza AES e PSK (Pre-Shared Key) tra i client e il punto di accesso. Utilizza una nuova chiave di crittografia per ogni sessione che rende difficile la compromissione.
- **Migliore protezione (WPA Personal - TKIP/AES):** fornisce protezione quando sono presenti dispositivi wireless meno recenti che non supportano WPA2. WPA Personal utilizza AES e TKIP. Utilizza lo standard Wi-Fi IEEE 802.11i.
- **Nessuna protezione (scelta non consigliata):** la rete wireless non richiede una password e può essere utilizzata da chiunque. Se selezionato, viene visualizzata una finestra popup in cui viene chiesto se si desidera disattivare la protezione; fare clic su **Sì** per continuare. Se si sceglie questa opzione, fare clic su **Next** (Avanti), quindi andare al [passo 35](#).

**Nota:** Nell'esempio viene scelto Better Security (WPA Personal - TKIP/AES).

### 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/WPA2 Personal - TKIP/AES)**  
Recommended for older wireless computers and devices that might not support WPA2.
- No Security (Not recommended)**

Passaggio 30. Immettere la password per la rete nel campo *Chiave di accesso*. La barra colorata a destra di questo campo indica la complessità della password immessa.

Enter a security key with 8-63 characters.

.....

Show Key as Clear Text

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

Click **Next** to continue

Back Next Cancel

Passaggio 31. (Facoltativo) Per visualizzare la password durante la digitazione, selezionare la casella di controllo **Mostra chiave come testo non crittografato** e fare clic su **Avanti**.

Enter a security key with 8-63 characters.

GuestPassw0rd

Show Key as Clear Text

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

Click **Next** to continue

Back Next Cancel

Passaggio 32. Nell'area Enable Captive Portal - Assegna l'ID VLAN, scegliere un ID per la rete guest dall'elenco a discesa VLAN ID, quindi fare clic su **Next** (Avanti).

**Nota:** Per i protocolli WAP371 e WAP150, è necessario immettere l'ID nel campo *ID VLAN* fornito. L'intervallo di ID della VLAN è compreso tra 1 e 4094.

**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:

[? Learn more about vlan ids](#)

Click **Next** to continue

Back Next Cancel

**Nota:** nell'esempio, viene scelto l'ID VLAN 2.

Passaggio 33. (Facoltativo) Se si desidera reindirizzare i nuovi utenti a una pagina di avvio alternativa, selezionare la casella di controllo **Abilita URL di reindirizzamento** nella schermata 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 :

Passaggio 34. (Facoltativo) Immettere l'URL per il reindirizzamento nel campo *URL reindirizzamento*, quindi fare clic su **Avanti**.

### 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

**Nota:** Nell'esempio, l'URL di reindirizzamento è <http://newuser.com>.

## Riepilogo

Passaggio 35. Esaminare le impostazioni mostrate e verificare che le informazioni siano corrette. Per modificare un'impostazione, fare clic sul pulsante **Indietro** fino a raggiungere la pagina desiderata. In caso contrario, fare clic su **Invia** per abilitare le impostazioni in WAP.



### Summary - Confirm Your Settings

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

#### Radio 1 (2.4 GHz)

Network Name (SSID):	WAP361_L2
Network Security Type:	WPA2 Personal - AES
Security Key:	SecretKey1
VLAN ID:	1

#### Radio 2 (5 GHz)

Network Name (SSID):	WAP361_L 2 _5ghz
Network Security Type:	WPA2 Personal - AES
Security Key:	SecretKey2
VLAN ID:	1

#### Captive Portal (Guest Network) Summary

Guest Network Radio:	Radio 1
Network Name (SSID):	BeMyGuest!
Network Security	WPA2 Personal - AES

Click **Submit** to enable settings on your Cisco Wireless Access Point

Passaggio 36. Viene visualizzata la schermata Device Setup Complete (Configurazione dispositivo completata) per confermare che il dispositivo è stato configurato correttamente. Fare clic su **Finish** (Fine).

### 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
Radio 1 (2.4 GHz)	
Network Name (SSID):	WAP361_L2
Network Security Type:	WPA2 Personal - AES
Security Key:	SecretKey1
Radio 2 (5 GHz)	
Network Name (SSID):	WAP361_L 2 _5ghz
Network Security Type:	WPA2 Personal - AES
Security Key:	SecretKey2



Click **Finish** to close this wizard.

A questo punto è necessario aver configurato correttamente il punto di accesso wireless utilizzando l'Installazione guidata.