

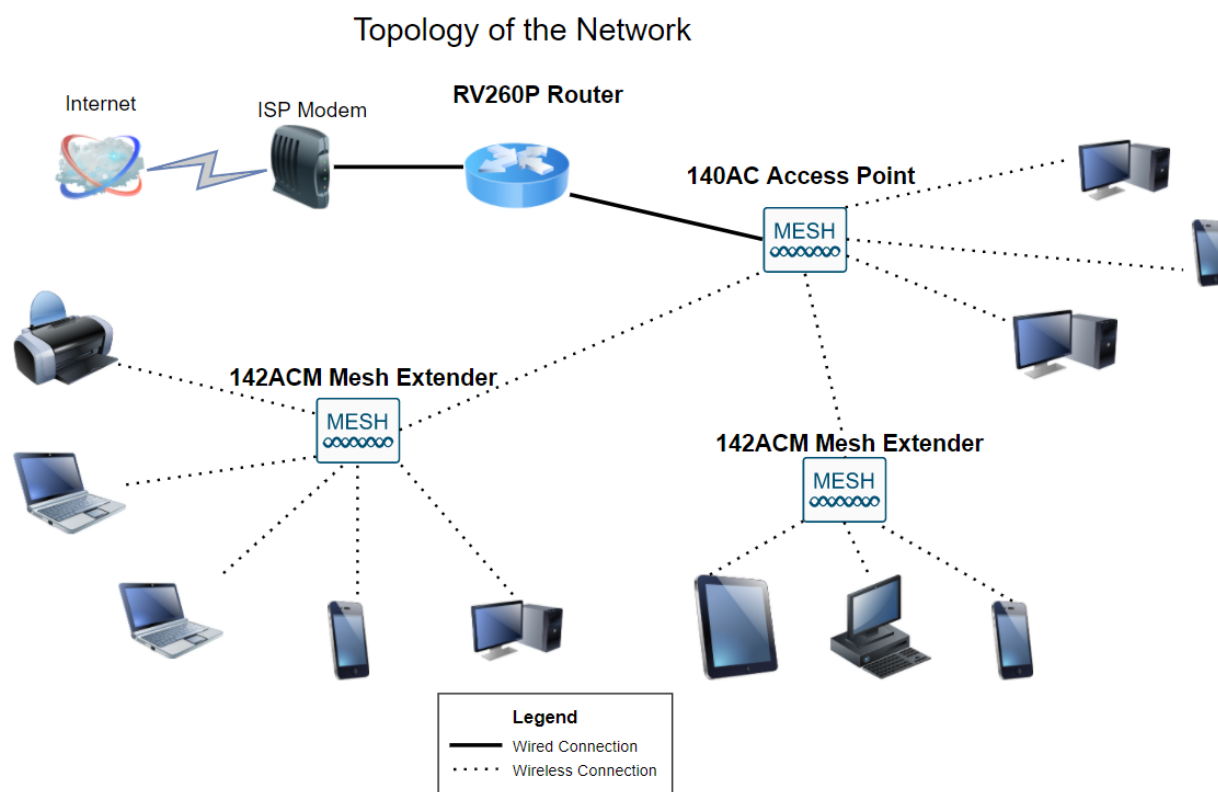
# Configurazione rete totale: RV260P con Cisco Business Wireless e interfaccia utente Web

## Obiettivo:

In questa guida viene illustrato come configurare una rete mesh wireless utilizzando un router RV260P, un punto di accesso CBW140AC e due estensori mesh CBW142ACM.

In questo articolo viene utilizzata l'interfaccia utente Web per impostare la rete wireless mesh. Se si preferisce utilizzare l'applicazione mobile, che è consigliata per una facile configurazione wireless, [fare clic per passare all'articolo che utilizza l'applicazione mobile](#). Se si desidera utilizzare l'interfaccia utente Web, continuare a leggere.

## Topologia:



## Introduzione

Ecco, pronto per configurare la nuova rete. È una giornata emozionante! In questo scenario, viene utilizzato un router RV260P. Questo router offre funzionalità Power over Ethernet (PoE) che consentono di collegare il CBW140AC al router anziché a uno switch. I dispositivi di estensione mesh CBW140AC e CBW142ACM verranno utilizzati per creare una rete mesh wireless.

Se non si conoscono alcuni dei termini utilizzati in questo documento o si desiderano ulteriori dettagli su Mesh Networking, controllare gli articoli seguenti:

- [Cisco Business: glossario dei nuovi termini](#)
- [Benvenuto in Cisco Business Wireless Mesh Networking](#)
- [Domande frequenti \(FAQ\) per una rete wireless aziendale Cisco](#)

Siete pronti? Andiamo!

## Dispositivi interessati | Versione software

- RV260P | 1.0.0.17
- CBW140AC | 10.3.1.0
- CBW142ACM | 10.3.1.0 (per la rete a maglie è necessaria almeno una rete a maglie)

## Sommario

- [Prima di iniziare](#)
- [Configurazione del router RV260P](#)
  - [RV260P integrato](#)
  - [Configurazione del router](#)
  - [Risoluzione dei problemi relativi alla connessione Internet](#)
  - [Configurazione iniziale](#)
  - [Aggiorna firmware se necessario](#)
  - [Configurazione delle VLAN \(opzionale\)](#)
  - [Modifica un indirizzo IP \(facoltativo\)](#)
  - [Aggiungi IP statico](#)
- [Configurazione di CBW140AC](#)
  - [CBW140AC](#)
  - [Configurazione del punto di accesso wireless primario 140AC sull'interfaccia utente Web](#)
- [Suggerimenti per la risoluzione dei problemi wireless](#)
- [Configurazione dei CBW142ACM Mesh Extender tramite l'interfaccia utente Web](#)
- [Controllo e aggiornamento del software tramite l'interfaccia utente Web](#)
- [Creazione di WLAN sull'interfaccia utente Web](#)
- [Creare una WLAN guest utilizzando l'interfaccia utente Web \(facoltativo\)](#)
- [Creazione profilo applicazione mediante interfaccia utente Web \(facoltativo\)](#)
- [Creazione profilo client tramite interfaccia utente Web \(facoltativo\)](#)

## Prima di iniziare

1. Verificare di disporre di una connessione Internet corrente per la configurazione.
2. Contattare il provider di servizi Internet per informazioni sulle istruzioni speciali disponibili per l'utilizzo del router RV260. Alcuni ISP offrono gateway con router integrati. Se si dispone di un gateway con un router integrato, potrebbe essere necessario disattivare il router e passare l'indirizzo IP WAN (Wide Area Network), ovvero l'indirizzo di protocollo Internet univoco assegnato dal provider Internet all'account, e tutto il traffico di rete attraverso il nuovo router.
3. Decidere dove posizionare il router. Se possibile, si desidera un'area aperta. Potrebbe non essere facile perché è necessario collegare il router al gateway a banda larga (modem) dal provider di servizi Internet (ISP).

# Configurazione del router RV260P

Un router è essenziale in una rete perché instrada i pacchetti. Consente a un computer di comunicare con altri computer che non si trovano sulla stessa rete o subnet. Un router accede a una tabella di routing per determinare dove inviare i pacchetti. La tabella di routing elenca gli indirizzi di destinazione. Le configurazioni statiche e dinamiche possono essere entrambe elencate nella tabella di routing per portare i pacchetti alla destinazione specifica.

La stampante RV260P è dotata di impostazioni predefinite ottimizzate per molte piccole aziende. È tuttavia possibile che le esigenze della rete o del provider di servizi Internet richiedano la modifica di alcune di queste impostazioni. Dopo aver contattato l'ISP per conoscere i requisiti necessari, è possibile apportare modifiche utilizzando l'interfaccia utente Web.

## RV260P integrato

### Passaggio 1

Collegare il cavo Ethernet di una delle porte LAN (Ethernet) RV260P alla porta Ethernet del computer. Se il computer non dispone di una porta Ethernet, sarà necessario disporre di un adattatore. Per eseguire la configurazione iniziale, il terminale deve trovarsi nella stessa sottorete cablata dell'RV260P.

### Passaggio 2

Assicurarsi di utilizzare l'adattatore di alimentazione in dotazione con la videocamera RV260P. L'utilizzo di un adattatore di alimentazione diverso potrebbe danneggiare la RV260P o causare il malfunzionamento dei dongle USB. L'interruttore di alimentazione è acceso per impostazione predefinita.

Collegare l'adattatore di alimentazione alla porta 12 V CC dell'RV260P, ma non collegarlo all'alimentazione.

### Passaggio 3

Assicurarsi che il modem sia spento.

### Passaggio 4

Utilizzare un cavo Ethernet per collegare il modem via cavo o DSL alla porta WAN dell'RV260P.

### Passaggio 5

Inserire l'altra estremità dell'adattatore RV260P in una presa elettrica. In questo modo si accende l'RV260. Collegare nuovamente il modem per accenderlo. La spia di alimentazione sul pannello anteriore è verde fisso quando l'adattatore di alimentazione

è collegato correttamente e l'avvio di RV260P è terminato.

## Configurazione del router

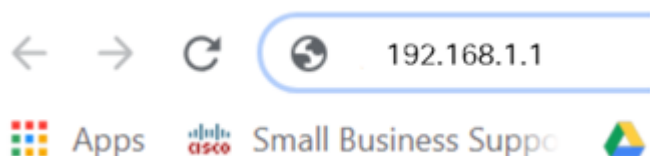
Il lavoro di preparazione è terminato, ora è il momento di fare alcune configurazioni!  
Per avviare l'interfaccia utente Web, eseguire la procedura seguente:

### Passaggio 1

Se il computer è configurato per diventare un client DHCP (Dynamic Host Configuration Protocol), al computer viene assegnato un indirizzo IP compreso nell'intervallo 192.168.1.x. DHCP automatizza il processo di assegnazione di indirizzi IP, subnet mask, gateway predefiniti e altre impostazioni ai computer. Per ottenere un indirizzo, i computer devono essere impostati in modo da poter partecipare al processo DHCP. A tale scopo, selezionare per ottenere automaticamente un indirizzo IP nelle proprietà di TCP/IP nel computer.

### Passaggio 2

Aprire un browser Web come Safari, Internet Explorer o Firefox. Nella barra degli indirizzi, immettere l'indirizzo IP predefinito dell'RV260P, ossia 192.168.1.1.



### Passaggio 3

È possibile che il browser invii un avviso per segnalare che il sito Web non è attendibile. Accedere al sito Web. Se non si è connessi, passare alla sezione [Risoluzione dei problemi di connessione Internet](#).



#### Your connection is not private

Attackers might be trying to steal your information from [ciscobusiness.cisco](#) (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. [Privacy policy](#)



### Passaggio 4

Quando viene visualizzata la pagina di accesso, immettere il nome utente predefinito cisco e la password predefinita *cisco*. Il nome utente e la password fanno distinzione

tra maiuscole e minuscole.

The image shows a login interface for a Cisco Router. It includes the Cisco logo, the word 'Router', and a form with three numbered steps: 1. Username field with 'cisco', 2. Password field with '....', 3. Language dropdown menu set to 'English'. A blue 'Login' button is at the bottom.

©2018 Cisco Systems, Inc. All Rights Reserved.  
Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

## Passaggio 5

Fare clic su **Login**. Viene visualizzata la pagina *Riquadro attività iniziale*. Dopo aver confermato la connessione e aver effettuato l'accesso al router, passare alla sezione [Configurazione iniziale](#) di questo articolo.

## Risoluzione dei problemi relativi alla connessione Internet

Se si sta leggendo il file, è probabile che si verifichino problemi di connessione a Internet o all'interfaccia utente Web. Una di queste soluzioni dovrebbe aiutare.

Sul sistema operativo Windows connesso è possibile verificare la connessione di rete aprendo il prompt dei comandi. Immettere ping 192.168.1.1 (indirizzo IP predefinito del router). Se la richiesta scade, non è possibile comunicare con il router.

Se la connettività non avviene, è possibile consultare la sezione [Risoluzione dei problemi sui router RV160 e RV260](#).

Altre cose da provare:

1. Verificare che il browser Web non sia impostato su Non in linea.
2. Verificare le impostazioni della connessione alla rete locale (LAN) per la scheda Ethernet. Il PC deve ottenere un indirizzo IP tramite DHCP. In alternativa, il PC può avere un indirizzo IP statico nell'intervallo 192.168.1.x con il gateway predefinito impostato su 192.168.1.1 (l'indirizzo IP predefinito dell'RV260P). Per connettersi, potrebbe essere necessario modificare le impostazioni di rete dell'RV260P. Se si utilizza Windows 10, controllare [le istruzioni di Windows 10 per modificare le impostazioni di rete](#).

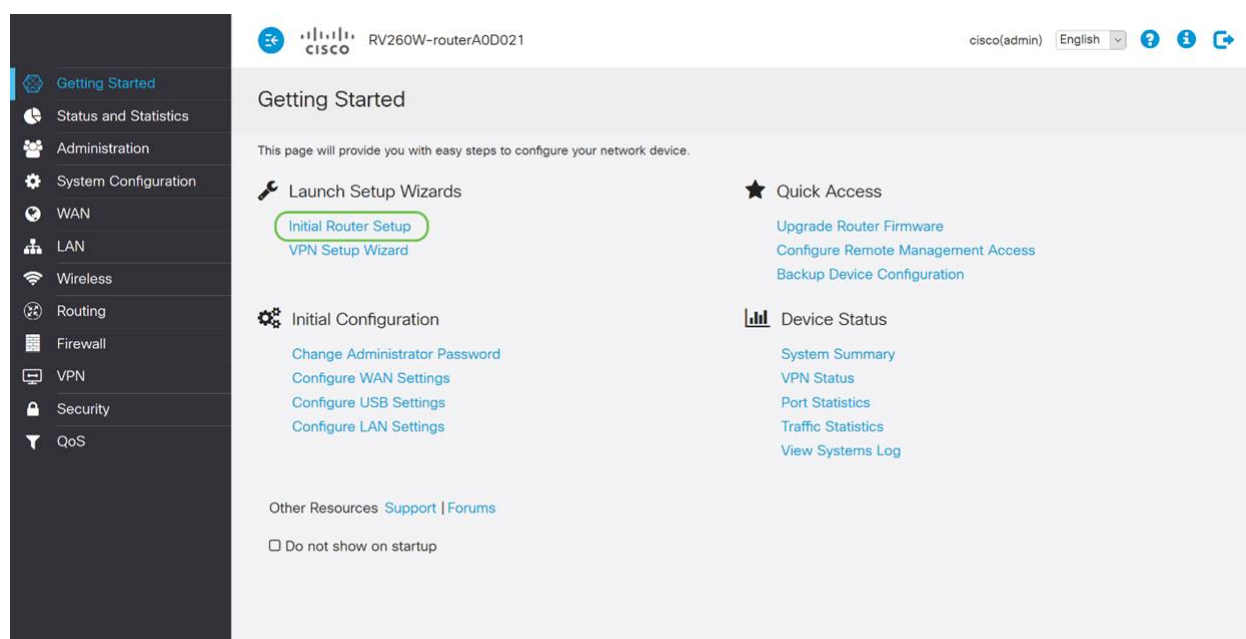
3. Se sono presenti apparecchiature che occupano l'indirizzo IP 192.168.1.1, sarà necessario risolvere il conflitto affinché la rete funzioni. Per maggiori informazioni, [fai clic qui](#) oppure [fai clic qui](#).
4. Reimpostare il modem e l'RV260P spegnendo entrambi i dispositivi. Accendere quindi il modem e lasciarlo inattivo per circa 2 minuti. Accendere quindi il modello RV260P. A questo punto, si dovrebbe ricevere un indirizzo IP WAN.
5. Se si dispone di un modem DSL, chiedere all'ISP di attivare la modalità bridge per il modem DSL.

## Configurazione iniziale

È consigliabile eseguire i passaggi dell'Installazione guidata iniziale elencati in questa sezione. È possibile modificare queste impostazioni in qualsiasi momento.

### Passaggio 1

Fare clic su **Installazione guidata iniziale** nella pagina *Introduzione*.



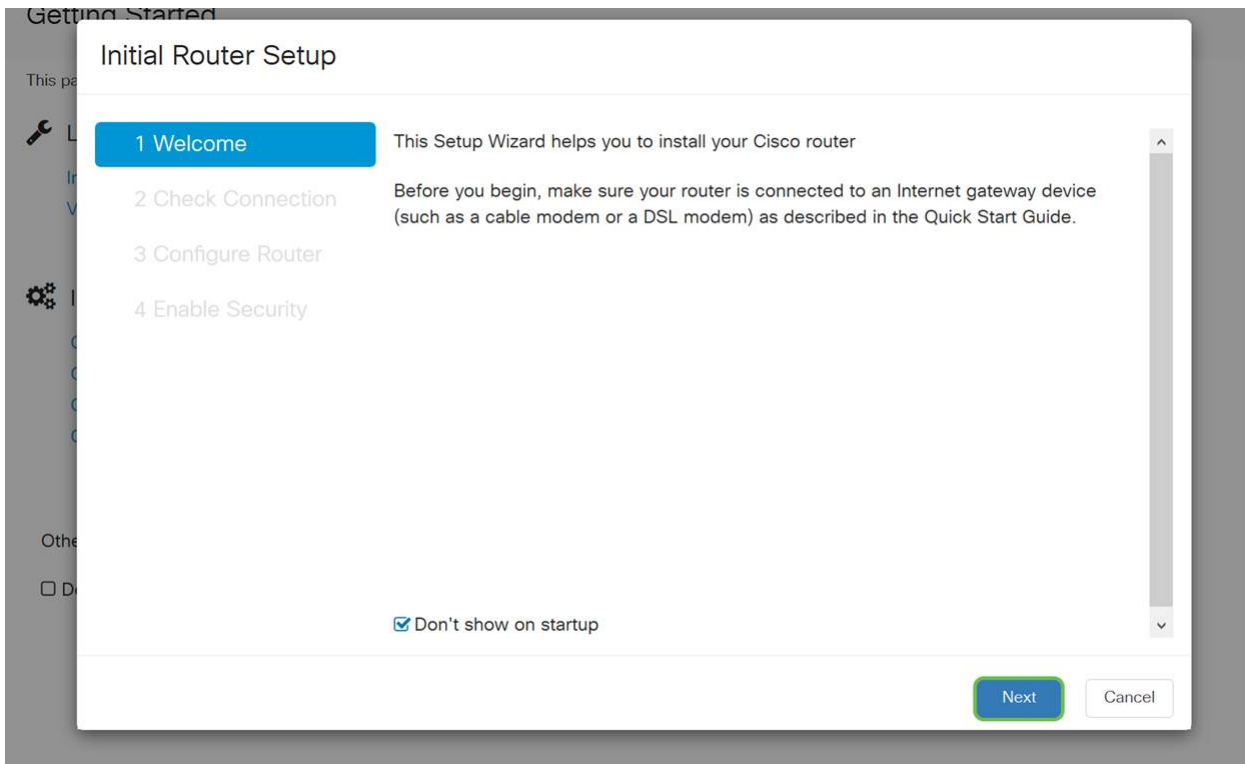
The screenshot shows the Cisco RV260W router's web interface. The top navigation bar includes the Cisco logo, the device name 'RV260W-routerA0D021', the user 'cisco(admin)', and the language 'English'. The main content area is titled 'Getting Started' and contains the following sections:

- Launch Setup Wizards:** Includes 'Initial Router Setup' (highlighted with a green circle) and 'VPN Setup Wizard'.
- Initial Configuration:** Includes links for 'Change Administrator Password', 'Configure WAN Settings', 'Configure USB Settings', and 'Configure LAN Settings'.
- Quick Access:** Includes links for 'Upgrade Router Firmware', 'Configure Remote Management Access', and 'Backup Device Configuration'.
- Device Status:** Includes links for 'System Summary', 'VPN Status', 'Port Statistics', 'Traffic Statistics', and 'View Systems Log'.

At the bottom, there are 'Other Resources' (Support | Forums) and a checkbox for 'Do not show on startup'.

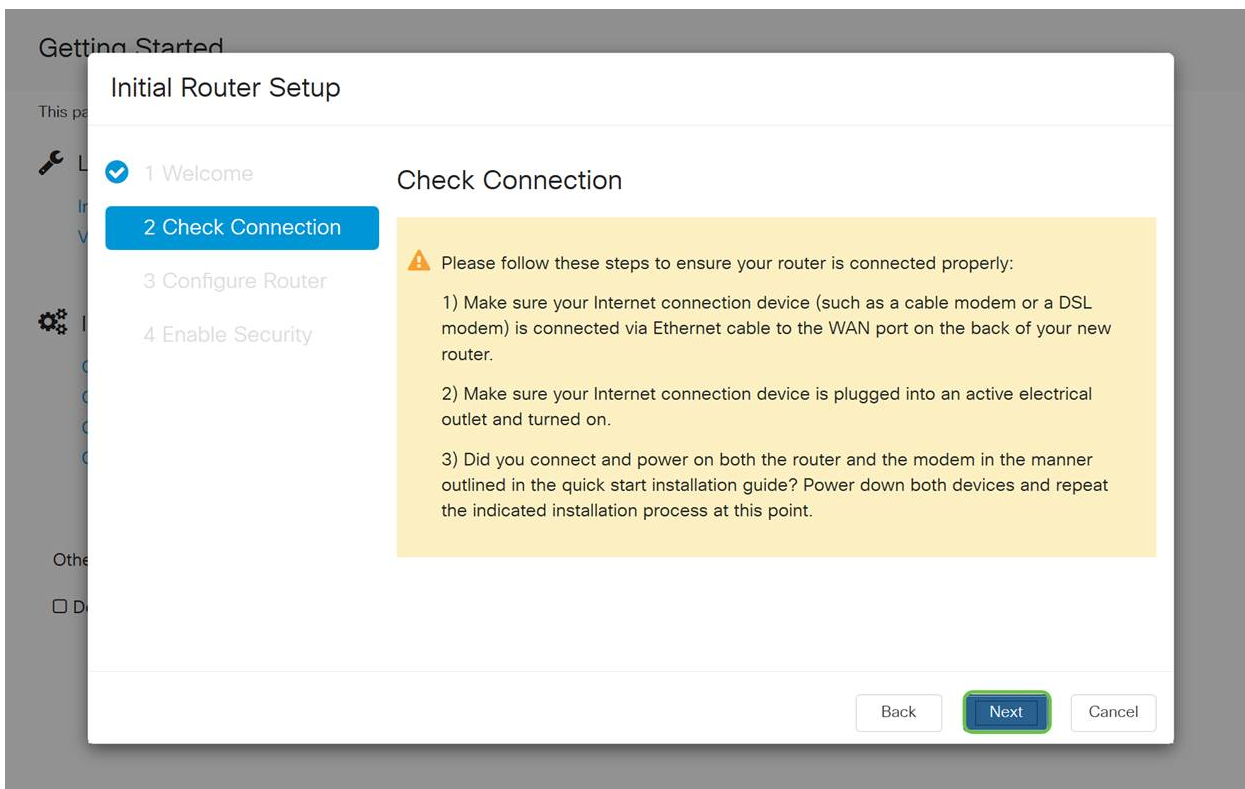
### Passaggio 2

Questa operazione conferma la connessione dei cavi. Poiché l'operazione è già stata confermata, fare clic su **Avanti**.



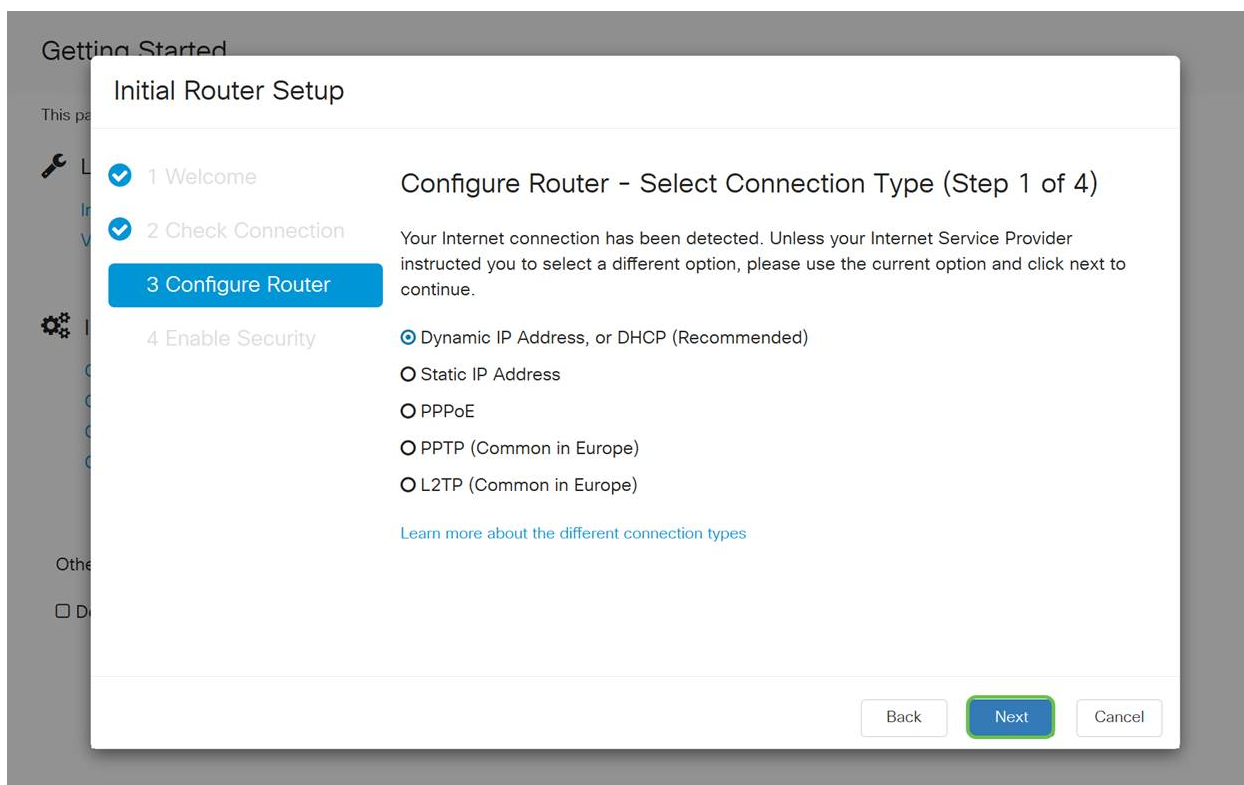
### Passaggio 3

In questo passaggio vengono illustrati i passaggi di base per verificare che il router sia connesso. Poiché l'operazione è già stata confermata, fare clic su **Avanti**.



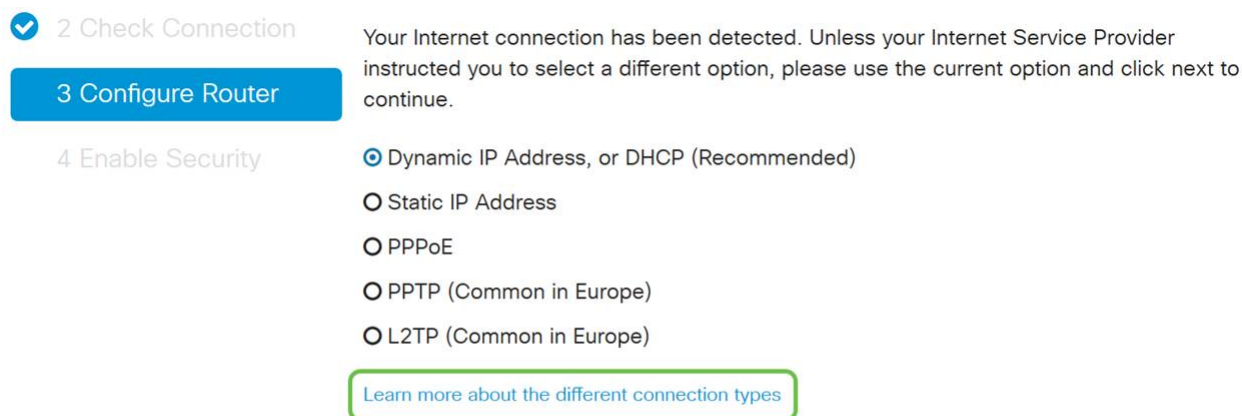
### Passaggio 4

Nella schermata successiva vengono visualizzate le opzioni per l'assegnazione degli indirizzi IP al router. In questo scenario è necessario selezionare DHCP. Fare clic su Next (Avanti).



Sebbene sia necessario utilizzare DHCP per questa configurazione iniziale, è possibile scegliere di *ottenere ulteriori informazioni sui diversi tipi di connessione* verso la parte inferiore dello schermo come riferimento futuro. Per ulteriori informazioni, consultare i seguenti articoli:

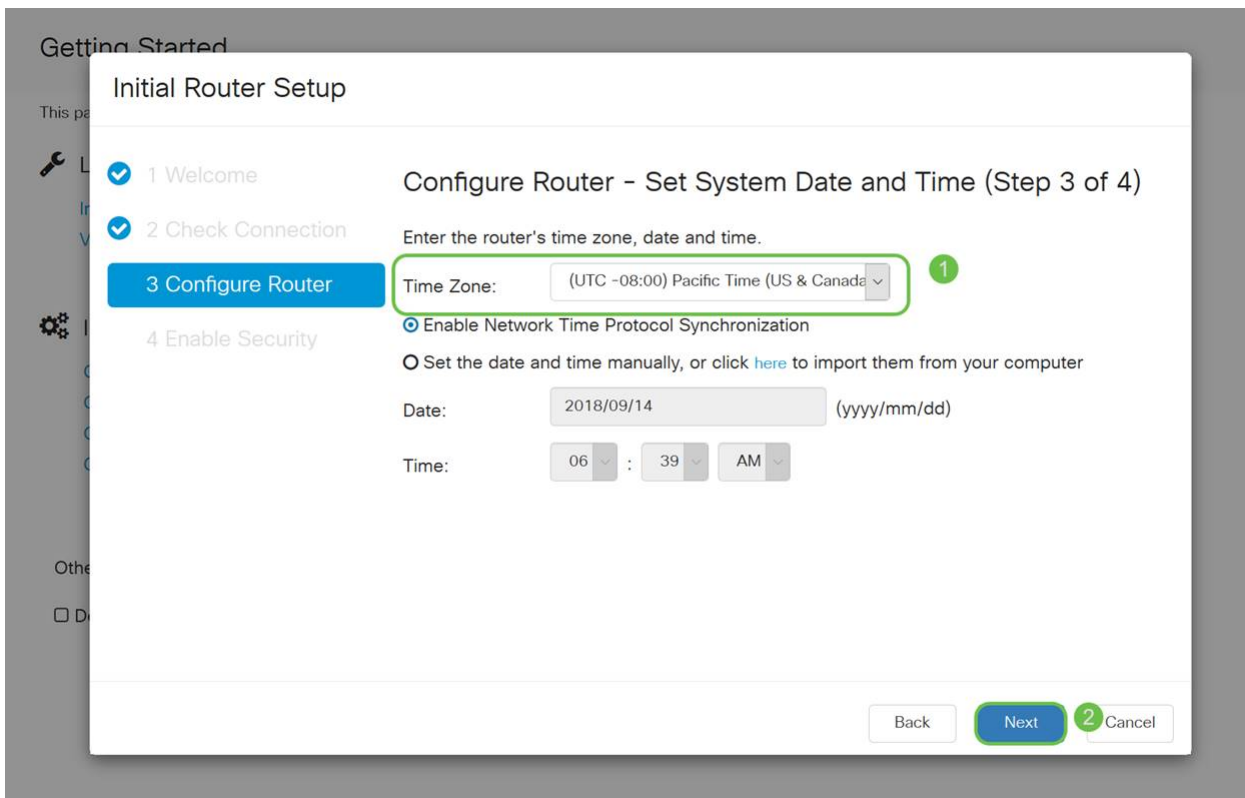
- [Configurazione WAN sui dispositivi RV160x e RV260x](#)
- [Configurazione del routing statico su RV160 e RV260](#)



## Passaggio 5

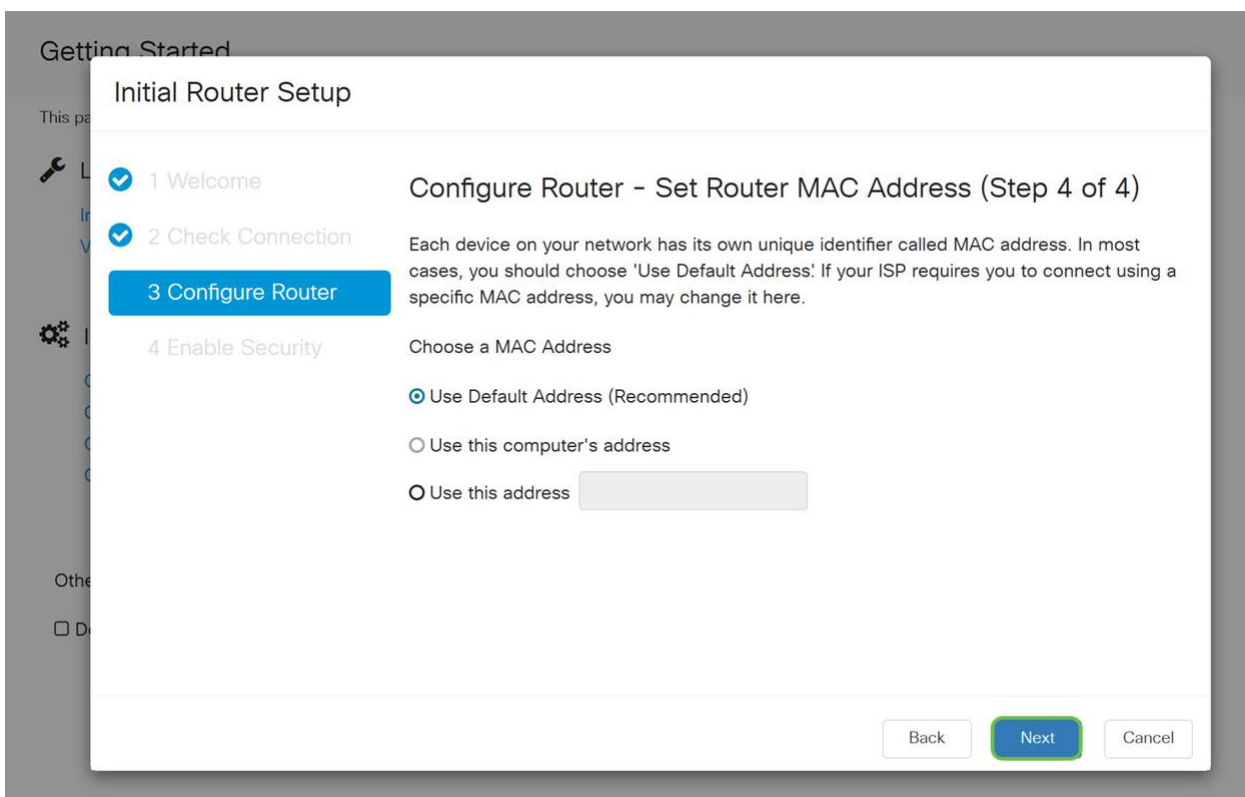
Verrà richiesto di configurare le impostazioni dell'ora del router. Questa operazione è importante perché consente di ottenere la precisione durante l'analisi dei registri o la risoluzione degli eventi. Selezionare il **fuso orario** e fare clic su **Avanti**.





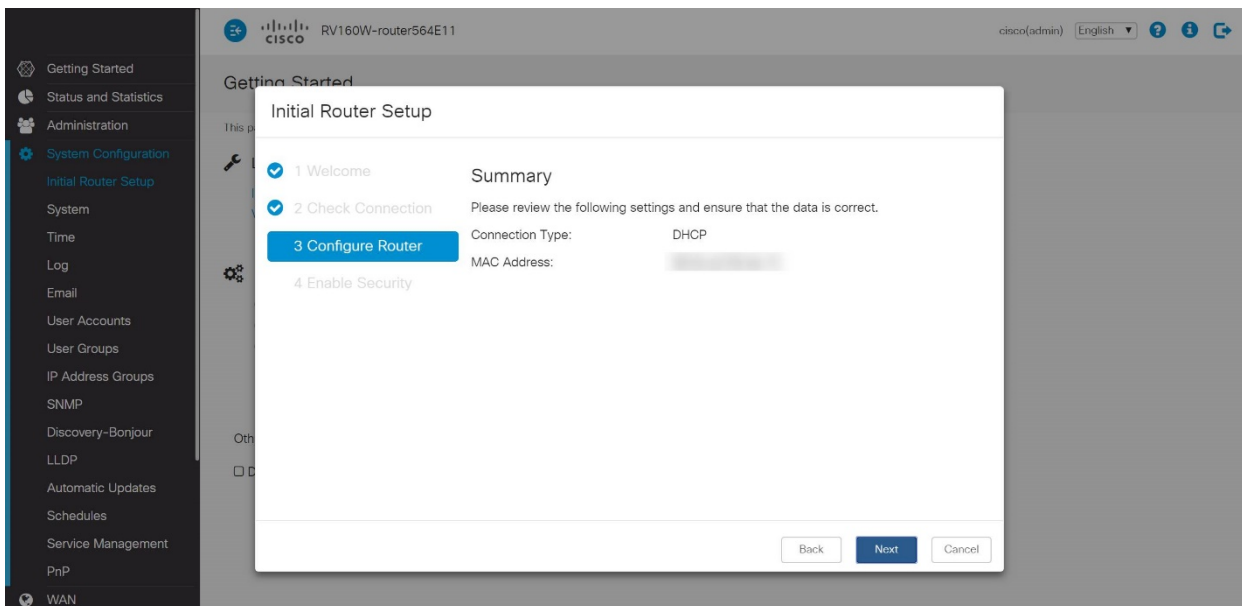
## Passaggio 6

In questa schermata, selezionare gli indirizzi MAC da assegnare ai dispositivi. Nella maggior parte dei casi, verrà utilizzato l'indirizzo predefinito. Fare clic su Next (Avanti).



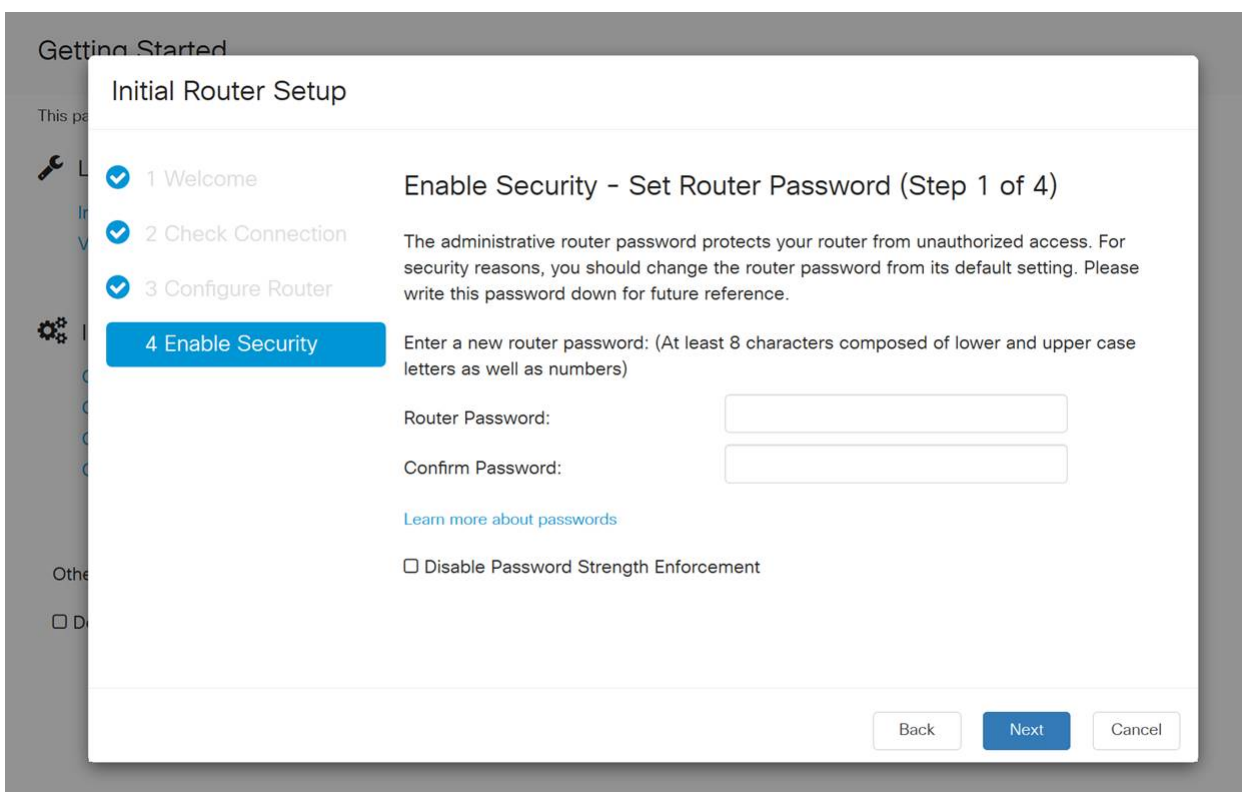
## Passaggio 7

La pagina seguente è un riepilogo delle opzioni selezionate. Rivedere e fare clic su Avanti se soddisfatto.



## Passaggio 8

Nel passaggio successivo, sarà necessario selezionare una password da utilizzare per accedere al router. Lo standard per le password deve contenere almeno 8 caratteri (maiuscoli e minuscoli) e includere numeri. **Immettere una password** conforme ai requisiti di protezione. Fare clic su Next (Avanti). Prendere nota della password per gli accessi futuri.



*Non è consigliabile selezionare Disabilita applicazione della forza della password. Questa opzione consente di selezionare una password semplice come 123.*

## Passaggio 9

Fare clic sull'icona **Salva**.

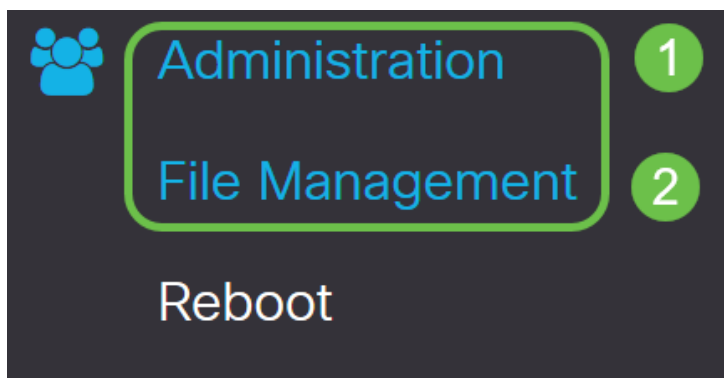


Aggiorna firmware se necessario

Questa è una sezione importante, non saltarla!

### Passaggio 1

Scegliere **Amministrazione > Gestione file**.



Nell'area *System Information* (Informazioni di sistema), le sottoaree seguenti descrivono:

- Modello dispositivo - Visualizza il modello del dispositivo.
- PID VID - ID prodotto e ID fornitore del router.
- Versione firmware corrente - Firmware attualmente in esecuzione sul dispositivo.
- Ultima versione Disponibile su Cisco.com - Ultima versione del software disponibile sul sito Web di Cisco.
- Ultimo aggiornamento firmware - Data e ora dell'ultimo aggiornamento firmware eseguito sul router.

## File Management

### System Information

Device Model: RV260P

PID VID: RV260P-K9 V01

Current Firmware Version: 1.0.00.15


Latest Version Available on Cisco.com: -

## Passaggio 2

Nella sezione *Aggiornamento manuale*, fare clic sul pulsante di opzione **Firmware Image** (Immagine firmware) per *File Type* (Tipo di file).

Manual Upgrade

File Type:  Firmware Image  Language File  USB Dongle Driver

Upgrade From:  cisco.com  PC  USB 

Firmware Image Format: \*.img (Maximum size: 100MB)

No file is selected

Reset all configurations/settings to factory defaults


The device will be automatically rebooted after the upgrade is complete.

## Passaggio 3

Nella pagina *Aggiornamento manuale*, fare clic su un pulsante di opzione per selezionare **cisco.com**. Sono disponibili altre opzioni, ma questo è il modo più semplice per eseguire un aggiornamento. Questo processo installa il file dell'aggiornamento più recente direttamente dalla pagina Web dei download di software Cisco.

Manual Upgrade

File Type:  Firmware Image  Language File  USB Dongle Driver

Upgrade From:  cisco.com  PC  USB 

Reset all configurations/settings to factory defaults

The device will be automatically rebooted after the upgrade is complete.

## Passaggio 4

Fare clic su **Aggiorna**.

## Manual Upgrade

File Type:  Firmware Image  Language File  USB Dongle Driver

Upgrade From:  cisco.com  PC  USB 

Reset all configurations/settings to factory defaults

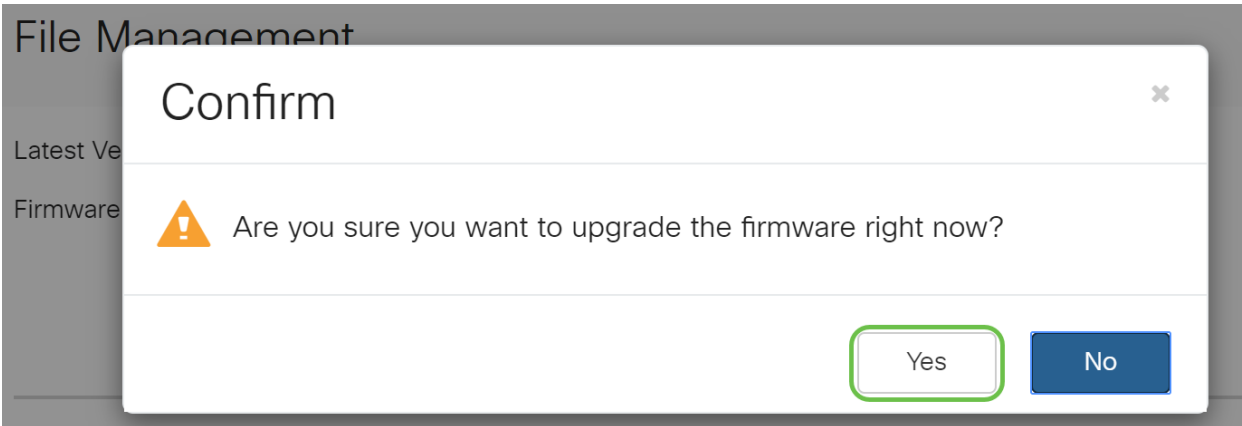
Upgrade

The device will be automatically rebooted after the upgrade is complete.

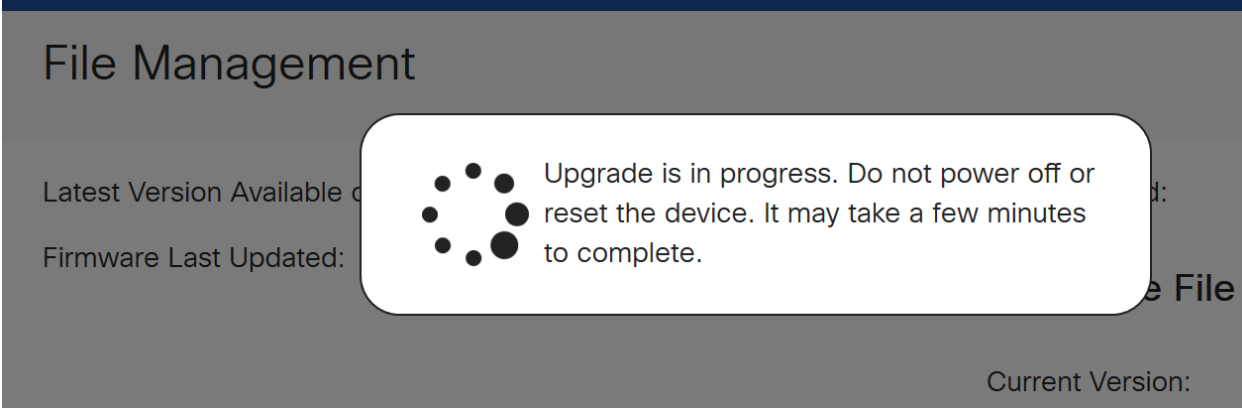
Download to USB

### Passaggio 5

Fare clic su **Sì** nella finestra di conferma per continuare.



Il processo di aggiornamento deve essere eseguito senza interruzione. Durante l'aggiornamento verrà visualizzato il seguente messaggio.



Al termine dell'aggiornamento, verrà visualizzata una finestra di notifica per informare che il router verrà *riavviato* con un conto alla rovescia del tempo stimato per il completamento del processo. In seguito, si verrà disconnessi.

## File Management

Latest Version Available

Firmware Last Updated



## Restarting

Please wait for 176 seconds...

### Passaggio 6

Accedere nuovamente all'utility basata sul Web per verificare che il firmware del router sia stato aggiornato, quindi scorrere fino a *System Information*. Nell'area *Current Firmware Version* dovrebbe essere visualizzata la versione del firmware aggiornata.

## File Management

### System Information

Device Model:

RV260P

PID VID:

RV260P-K9 V01

Current Firmware Version:

1.0.01.01

Latest Version Available on Cisco.com: -

Firmware Last Updated:

2020-Oct-  
26, 20:23:3  
2

### Language File

Current Version: 1.0.0.0

Le impostazioni di base sul router sono state completate. Sono disponibili alcune opzioni di configurazione.

Vi incoraggio a continuare a scorrere l'articolo per saperne di più su queste opzioni e se si applicano a voi. Se si preferisce, è possibile fare clic su uno dei collegamenti ipertestuali per passare a una sezione.

- [Configurazione delle VLAN \(opzionale\)](#)
- [Modifica indirizzo IP \(facoltativo\)](#)
- [Aggiungi indirizzi IP statici \(facoltativo\)](#)
- [Sono pronto per configurare la sezione Mesh Wireless della mia rete!](#)

### Configurazione delle VLAN (opzionale)

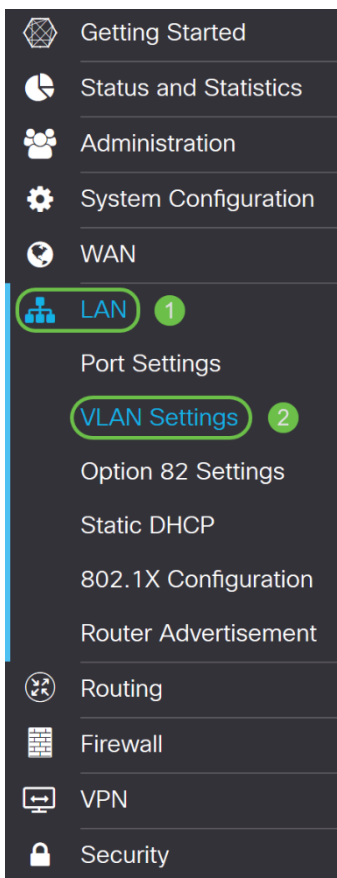
Una LAN virtuale o VLAN (Virtual Local Area Network) consente di segmentare logicamente una LAN (Local Area Network) in più domini di broadcast. Quando sulla rete vengono trasmessi anche dati sensibili, la creazione di VLAN offre una maggiore

sicurezza e il traffico viene quindi indirizzato a VLAN specifiche. L'uso delle VLAN inoltre può migliorare le prestazioni in quanto riduce la necessità di inviare pacchetti broadcast e multicast a destinazioni non necessarie. È possibile creare una VLAN, ma questa operazione non ha alcun effetto finché la VLAN non è collegata ad almeno una porta, in modo manuale o dinamico. Le porte devono sempre appartenere a una o più VLAN.

Se non si desidera creare le VLAN, andare alla [sezione successiva](#).

## Passaggio 1

Selezionare **LAN > Impostazioni VLAN**.



## Passaggio 2

Fare clic su **Add** per creare una nuova VLAN.

## VLAN Settings

Create new VLANs

<input type="checkbox"/>	VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149

### Passaggio 3

Immettere l'*ID VLAN* che si desidera creare e il *relativo nome*. L'intervallo degli *ID* della *VLAN* è compreso tra 1 e 4093.

Abbiamo scelto **200** come *ID VLAN* e **Engineering** come *nome* della *VLAN*.

## VLAN Settings

Create new VLANs

<input type="checkbox"/>	VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input type="checkbox"/>	200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

### Passaggio 4

Deselezionare la casella *Enabled* (Abilitato) per entrambe le opzioni *Routing tra VLAN* e *Gestione dispositivi*, se si desidera.

Il routing tra VLAN viene usato per indirizzare i pacchetti da una VLAN a un'altra VLAN. In generale, questa opzione non è consigliata per le reti guest in quanto si desidera isolare gli utenti guest e ridurre la protezione delle VLAN. In alcuni casi può essere necessario il routing tra le VLAN. In questo caso, controllare il [routing tra VLAN su un router RV34x con restrizioni ACL di destinazione](#) per configurare il traffico specifico consentito tra le VLAN.

Gestione dispositivi è il software che consente di utilizzare il browser per accedere all'interfaccia Web dell'RV260P dalla VLAN e gestire l'RV260P. Questa opzione deve essere disabilitata anche nelle reti guest.



Nell'esempio, non è stato abilitato né il *routing tra VLAN* né la *gestione dei dispositivi* per mantenere la VLAN più sicura.

RV160W-router564F71

### VLAN Settings

Create new VLANs

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
200	Engineering	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

## Passaggio 5

L'indirizzo IPv4 privato verrà popolato automaticamente nel campo *Indirizzo IP*. È possibile modificare questa impostazione se lo si desidera. Nell'esempio, la subnet ha 192.168.2.100-192.168.2.149 indirizzi IP disponibili per DHCP. 192.168.2.1-192.168.2.99 e 192.168.2.150-192.168.2.254 sono disponibili per gli indirizzi IP statici.

RV160W-router564F71

### VLAN Settings

Create new VLANs

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

## Passaggio 6

La subnet mask in *Subnet Mask* verrà popolata automaticamente. Se si apportano modifiche, il campo verrà regolato automaticamente.

Per questa dimostrazione, la *subnet mask* rimarrà impostata su **255.255.255.0** o su **/24**

## VLAN Settings

### Create new VLANs

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/> 1	Default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input type="checkbox"/> 200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

## Passaggio 7

Selezionare un *tipo DHCP (Dynamic Host Configuration Protocol)*. Le opzioni seguenti sono:

*Disabled*: disabilita il server IPv4 DHCP sulla VLAN. Questa operazione è consigliata in un ambiente di test. In questo scenario, tutti gli indirizzi IP dovranno essere configurati manualmente e tutte le comunicazioni interne.

*Server* - Opzione utilizzata con maggiore frequenza.

- Durata lease: immettere un valore temporale compreso tra 5 e 43.200 minuti. L'impostazione predefinita è 1440 minuti, ovvero 24 ore.
- Inizio intervallo e Fine intervallo: immettere l'inizio e la fine dell'intervallo di indirizzi IP che è possibile assegnare dinamicamente.
- Server DNS: selezionare questa opzione per utilizzare il server DNS come proxy o dall'elenco a discesa ISP.
- Server WINS - Immettere il nome del server WINS.
- Opzioni DHCP:
  - Opzione 6 - Immettere l'indirizzo IP del server TFTP.
  - Opzione 150: immettere l'indirizzo IP di un elenco di server TFTP.
  - Opzione 67 - Immettere il nome del file di configurazione.
- Relay - Immettere l'indirizzo IPv4 del server DHCP remoto per configurare l'agente di inoltro DHCP. Si tratta di una configurazione più avanzata.

## VLAN Settings

### Create new VLANs

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/> 1	Default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input type="checkbox"/> 200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

## Passaggio 8

Fare clic su **Apply** (Applica) per creare la nuova VLAN.



### Assegnazione delle VLAN alle porte

Sull'RV260 è possibile configurare 16 VLAN, con una VLAN per la WAN (Wide Area Network). Le VLAN che non sono su una porta devono essere *escluse*. In questo modo, il traffico su questa porta viene mantenuto esclusivamente per le VLAN/VLAN specificamente assegnate dall'utente. È considerata una buona pratica.

Le porte possono essere impostate come porte di accesso o porte trunk:

- Porta di accesso: assegnata una VLAN. Vengono passati frame senza tag.
- Porta trunk: può trasportare più di una VLAN. 802.1q. Il trunking consente di rimuovere il tag da una VLAN nativa. Le VLAN che non si desidera includere nel trunk devono essere escluse.

A una VLAN è stata assegnata una porta propria:

- Considerata una porta di accesso.
- La VLAN a cui è assegnata questa porta deve essere etichettata come Untagged.
- Tutte le altre VLAN devono essere etichettate come Escluse per quella porta.

Due o più VLAN che condividono una porta:

- Considerata una porta trunk.
- Una delle VLAN può essere etichettata come Senza tag.
- Le altre VLAN che fanno parte della porta trunk devono essere contrassegnate con tag.
- Le VLAN che non fanno parte della porta trunk devono essere etichettate come Escluse per quella porta.

**Nota:** nell'esempio non sono presenti trunk.

## Passaggio 9

Selezionare gli *ID VLAN* da modificare. Fare clic su **Modifica**.

Nell'esempio, sono state selezionate la *VLAN 1* e la *VLAN 200*.

#### Assign VLANs to ports

<input type="checkbox"/>	VLAN ID	LAN1	LAN2
<input checked="" type="checkbox"/>	1	Untagged	Excluded
<input checked="" type="checkbox"/>	200	Excluded	Untagged

### Passaggio 10

Fare clic su **Edit** per assegnare una VLAN a una porta LAN e specificare ciascuna impostazione come *Tagged*, *Untagged* o *Excluded*.

Nell'esempio, alla VLAN1 è stato assegnato il valore **Untagged** per la VLAN 1 e il valore **Excluded** per la VLAN 200. Alla VLAN 2 è stata assegnata la VLAN 1 come **Esclusa** e la VLAN 200 come **Senza tag**.

#### Assign VLANs to ports

<input type="checkbox"/>	VLAN ID	LAN1	LAN2
<input checked="" type="checkbox"/>	1	Untagged	Excluded
<input checked="" type="checkbox"/>	200	Excluded	Untagged

### Passaggio 11

Fare clic su **Apply** (Applica) per salvare la configurazione.

**Apply**

A questo punto, è necessario creare una nuova VLAN e configurare le VLAN sulle porte dell'RV260. Ripetere il processo per creare le altre VLAN. Ad esempio, la VLAN300 verrebbe creata per il reparto Marketing con una subnet di 192.168.3.x e la VLAN400 per il reparto Accounting con una subnet di 192.168.4.x.

Questi sono i principi base delle VLAN. Fare clic sul collegamento ipertestuale per ulteriori informazioni sulle [best practice e i suggerimenti sulla sicurezza delle VLAN per i router aziendali Cisco](#).

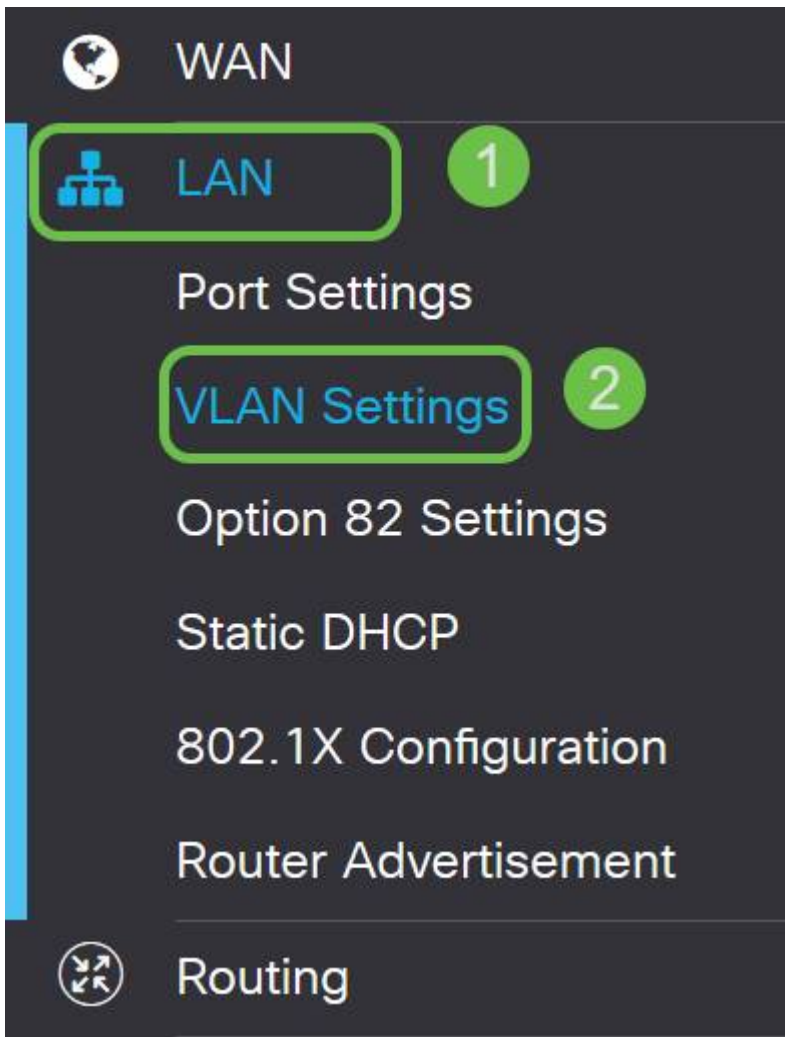
### Modifica un indirizzo IP (facoltativo)

Dopo aver completato la *Configurazione guidata iniziale*, è possibile impostare un indirizzo IP statico sul router modificando le impostazioni della VLAN. Ignorare la riesecuzione dell'installazione guidata iniziale. Per eseguire questa modifica, attenersi alla seguente procedura.

Se non occorre modificare un indirizzo IP, passare alla [sezione successiva](#) di questo articolo.

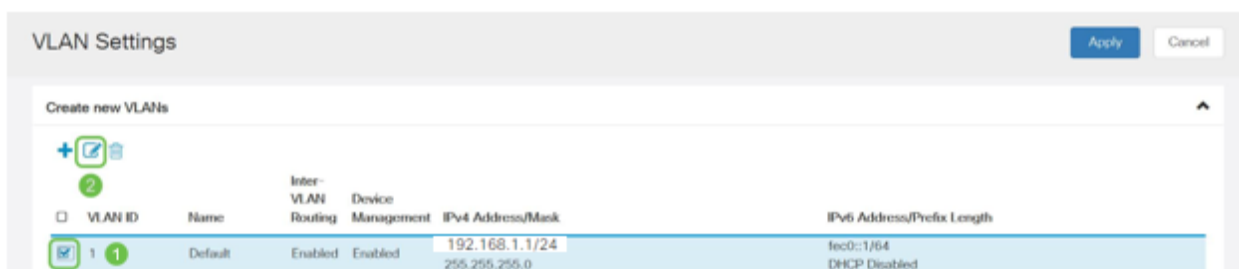
### Passaggio 1

Nella barra dei menu a sinistra, fare clic su **LAN > VLAN Settings**.



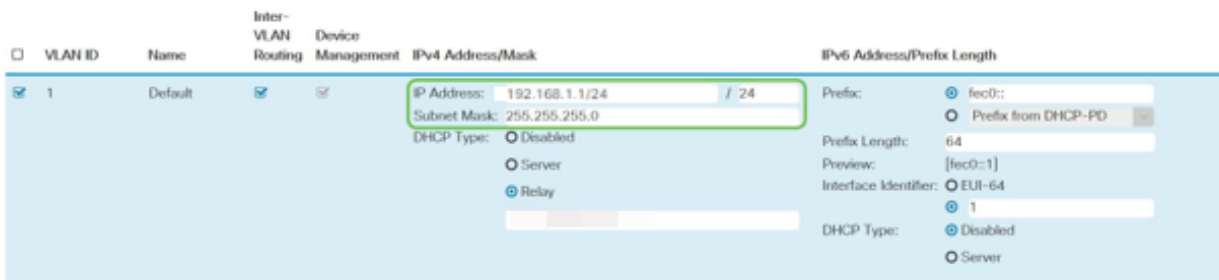
## Passaggio 2

Quindi selezionare la **VLAN** che contiene il dispositivo di routing e fare clic sull'icona di **modifica**.



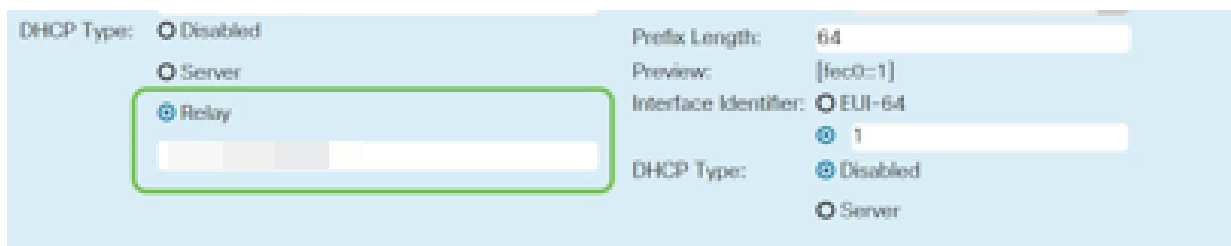
## Passaggio 3

Immettere l'**indirizzo IP statico** desiderato e fare clic su **Apply** (Applica) nell'angolo in alto a destra.



#### Passaggio 4 (facoltativo)

Se il router non è il server/dispositivo DHCP che assegna gli indirizzi IP, è possibile utilizzare la funzionalità di inoltro DHCP per indirizzare le richieste DHCP a un indirizzo IP specifico. È probabile che l'indirizzo IP sia il router connesso alla WAN o a Internet.



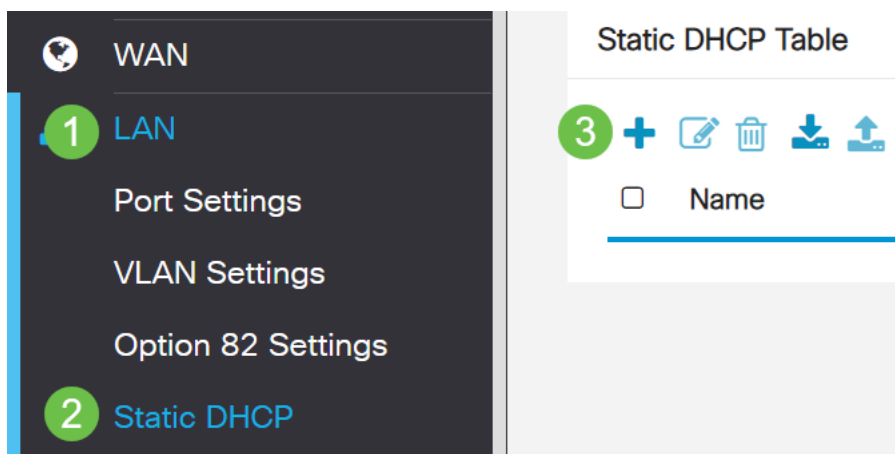
#### Aggiungi IP statico

Se si desidera che un determinato dispositivo sia raggiungibile da altre VLAN, è possibile assegnare a tale dispositivo un indirizzo IP locale statico e creare una regola di accesso per renderlo accessibile. Questa procedura funziona solo se è abilitato il routing tra VLAN. Ci sono altre situazioni in cui un indirizzo IP statico può essere utile. Per ulteriori informazioni sull'impostazione di indirizzi IP statici, vedere [Procedure consigliate per l'impostazione di indirizzi IP statici su hardware aziendale Cisco](#).

Se non è necessario aggiungere un indirizzo IP statico, è possibile passare alla [sezione successiva](#) di questo articolo per configurare i punti di accesso.

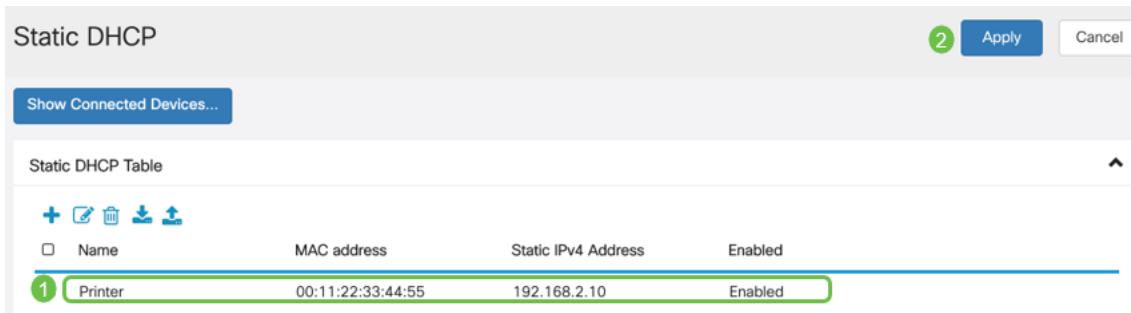
#### Passaggio 1

Selezionare LAN > DHCP statico. Fare clic sull'icona più.



#### Passaggio 2

Aggiungere le informazioni **DHCP statiche** per il dispositivo. In questo esempio, la periferica è una stampante.



Congratulazioni, la configurazione del router RV260P è stata completata. Ora configureremo i dispositivi Cisco Business Wireless.

## Configurazione di CBW140AC

### CBW140AC

Innanzitutto, collegare un cavo Ethernet dalla porta PoE del CBW140AC a una porta PoE dell'RV260P. Le prime 4 porte dell'RV260P possono fornire PoE, pertanto è possibile utilizzare qualsiasi porta.

Controllare lo stato delle spie. L'avvio del punto di accesso richiede circa 10 minuti. Il LED lampeggerà in verde a più tonalità, alternando rapidamente verde, rosso e giallo prima di tornare verde. Possono esserci piccole variazioni nell'intensità del colore dei LED e nella tonalità da un'unità all'altra. Quando la spia LED lampeggia in verde, procedere al passaggio successivo.

La porta uplink PoE Ethernet sull'access point primario può essere utilizzata SOLO per fornire un uplink alla LAN e NON per collegarsi ad altri dispositivi primari compatibili o di estensione mesh.

Se il punto di accesso non è nuovo, assicurarsi che sia ripristinato alle impostazioni predefinite di fabbrica per il SSID *Cisco Business-Setup* da visualizzare nelle opzioni Wi-Fi. Per assistenza, vedere [Come riavviare e ripristinare le impostazioni predefinite sui router RV260](#).

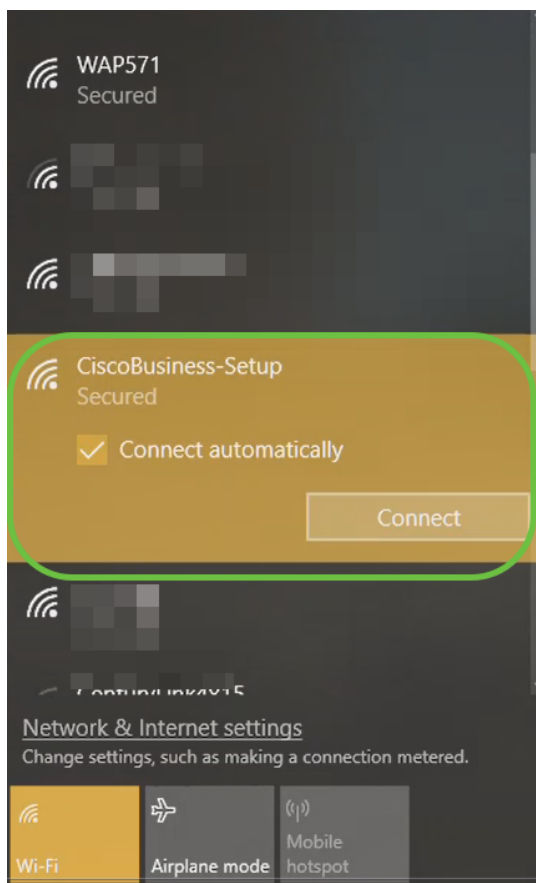
### Configurazione del punto di accesso wireless primario 140AC sull'interfaccia utente Web

È possibile configurare il punto di accesso utilizzando l'applicazione mobile o l'interfaccia utente Web. In questo articolo viene utilizzata l'interfaccia utente Web per l'installazione, che offre più opzioni di configurazione ma è un po' più complicata. Se si desidera utilizzare l'applicazione mobile per le sezioni successive, fare clic su per accedere alle [istruzioni](#) dell'[applicazione mobile](#).

In caso di problemi di connessione, fare riferimento alla sezione [Suggerimenti per la risoluzione dei problemi wireless](#) di questo articolo.

## Passaggio 1

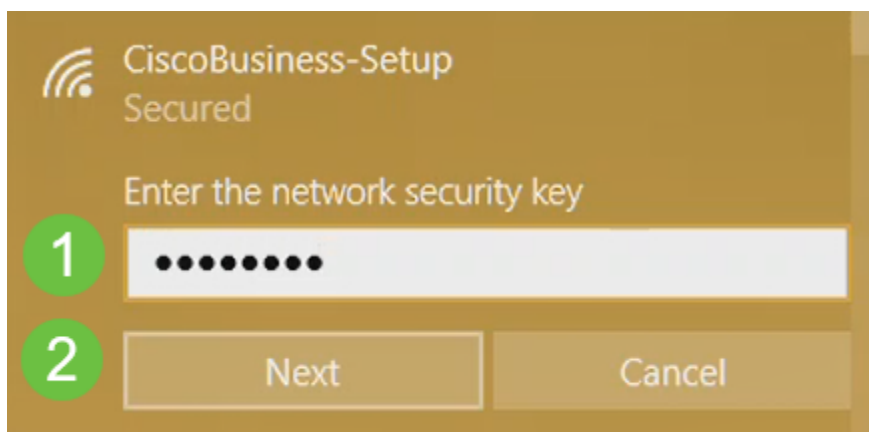
Sul PC, fare clic sull'icona **Wi-Fi** e scegliere *Cisco Business-Setup* rete wireless. Fare clic su **Connetti**.



Se il punto di accesso non è nuovo, assicurarsi che sia ripristinato alle impostazioni predefinite di fabbrica per il SSID *Cisco Business-Setup* da visualizzare nelle opzioni Wi-Fi.

## Passaggio 2

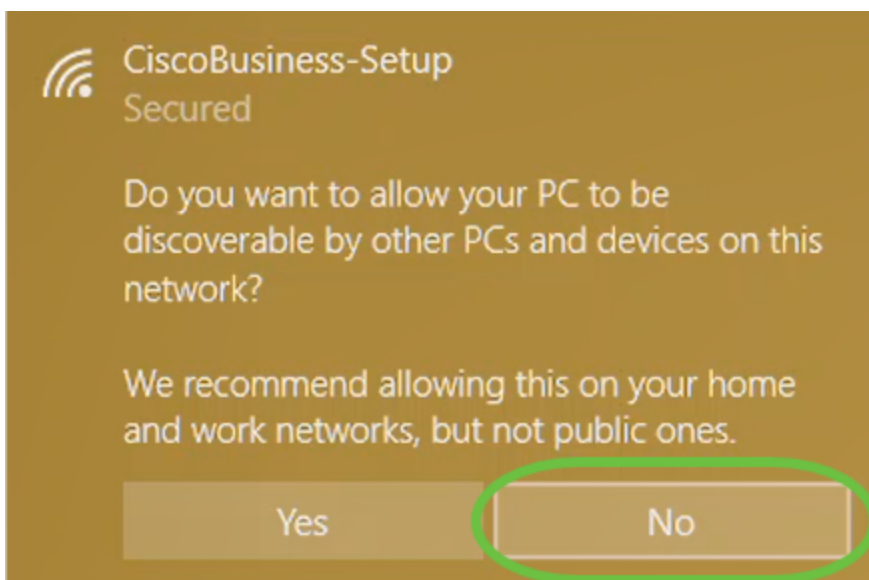
Immettere la passphrase **cisco123** e fare clic su **Avanti**.



## Passaggio 3

Viene visualizzata la seguente schermata. Poiché è possibile configurare un solo dispositivo alla volta, fare clic su **No**.

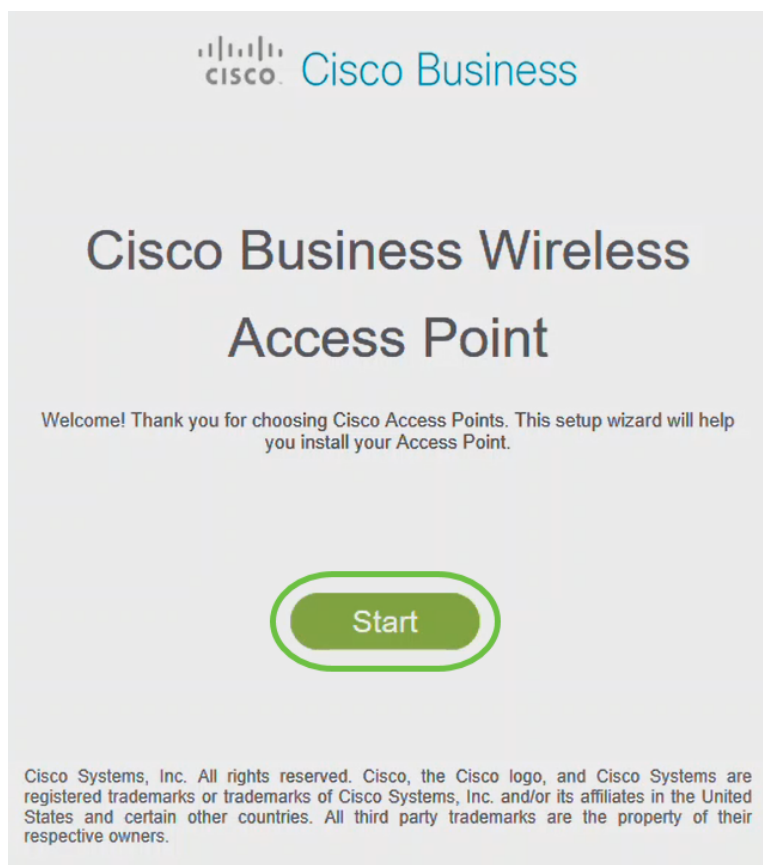




È possibile connettere un solo dispositivo all'SSID *Cisco Business-Setup*. Se un secondo dispositivo tenta di connettersi, non sarà in grado di connettersi. Se non è possibile connettersi all'SSID ed è stata convalidata la password, è possibile che la connessione sia stata stabilita da un'altra periferica. Riavviare il punto di accesso e riprovare.

#### Passaggio 4

Una volta connesso, il browser Web deve reindirizzare automaticamente alla procedura guidata CBW AP setup. In caso contrario, aprire un browser Web, ad esempio Internet Explorer, Firefox, Chrome o Safari. Nella barra degli indirizzi, digitare <http://ciscobusiness.cisco> e premere **Invio**. Fare clic su **Start** nella pagina Web.



Se la pagina Web non viene visualizzata, attendere qualche minuto o ricaricarla. Dopo

questa configurazione iniziale, utilizzare <https://ciscobusiness.cisco> per eseguire il login. Se il browser Web viene compilato automaticamente con <http://>, per ottenere l'accesso è necessario digitare manualmente il testo <https://>.

## Passaggio 5

Creare un *account admin* immettendo quanto segue:

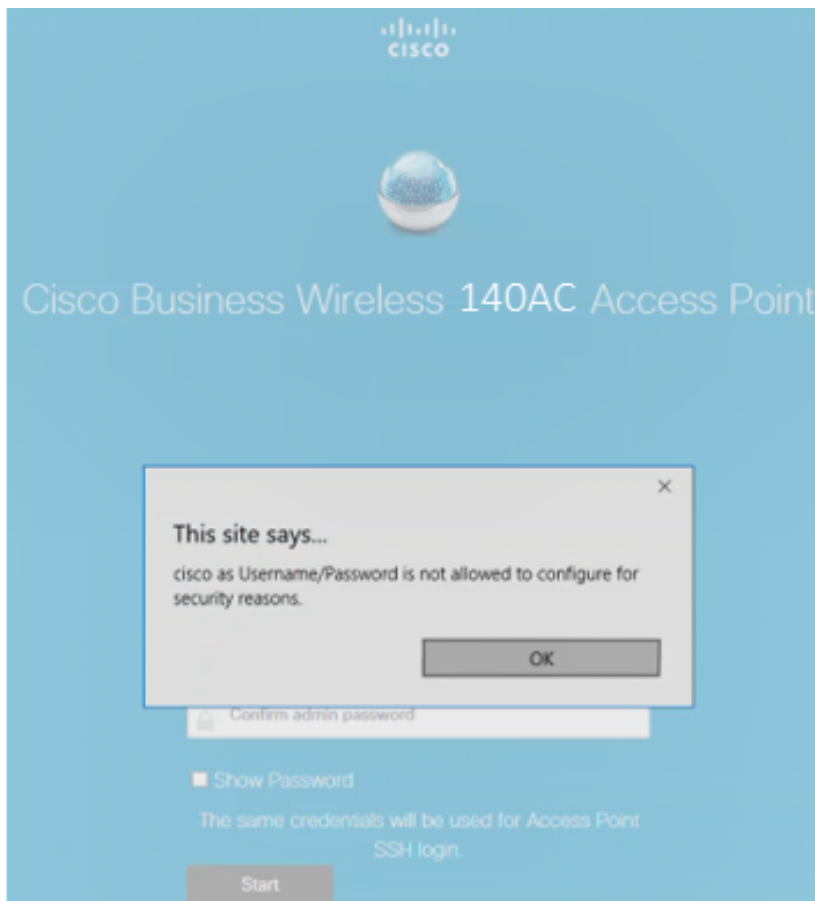
- Nome utente amministratore (massimo 24 caratteri)
- Password amministratore
- Conferma password amministratore

È possibile scegliere di visualizzare la password selezionando la casella di controllo accanto a *Mostra password*. Fare clic su **Start**.



The screenshot shows the Cisco Business Wireless 140AC Access Point configuration interface. At the top, the Cisco logo and the product name are displayed. Below, a message reads: "Welcome! Please start by creating an admin account." The form contains three input fields: the first is labeled "admin" (1), the second is labeled "P" (2), and the third is labeled "P" (3). A checkbox labeled "Show Password" (4) is located below the password fields. A "Start" button (5) is at the bottom. A note states: "Credentials will be used to manage the Access Point".

Non utilizzare *cisco* o sue varianti nei campi del nome utente o della password. In caso contrario, verrà visualizzato un messaggio di errore come illustrato di seguito.



## Passaggio 6

*Impostare l'access point principale immettendo quanto segue:*

- Nome AP primario
- Paese
- Data e ora
- Fuso orario
- Mesh

1 Set Up Your Primary AP

Primary AP Name

Test



1

Country

United States (US)



2

Date & Time

04/09/2021



9:11:17

3

Timezone

Central Time (US and Canada)



4

Mesh



5

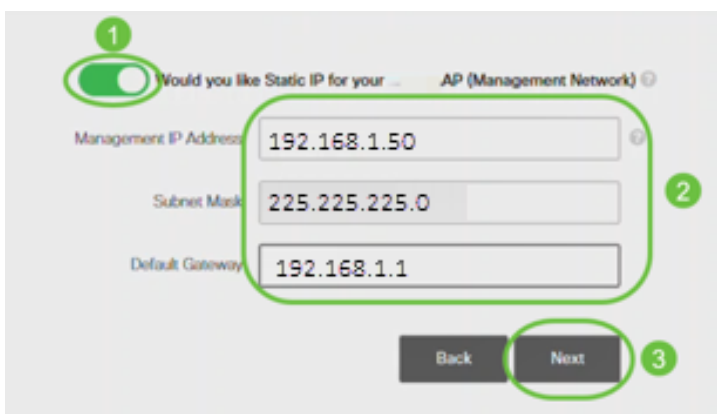
Mesh deve essere abilitato solo se si intende creare una rete mesh. Per impostazione predefinita, è disattivata.

### Passaggio 7

(Facoltativo) È possibile abilitare l'IP statico per il CBW140AC a scopo di gestione. In caso contrario, l'interfaccia riceve un indirizzo IP dal server DHCP. Per configurare un indirizzo IP statico, immettere quanto segue:

- Indirizzo IP di gestione
- Subnet mask
- Gateway predefinito

Fare clic su Next (Avanti).



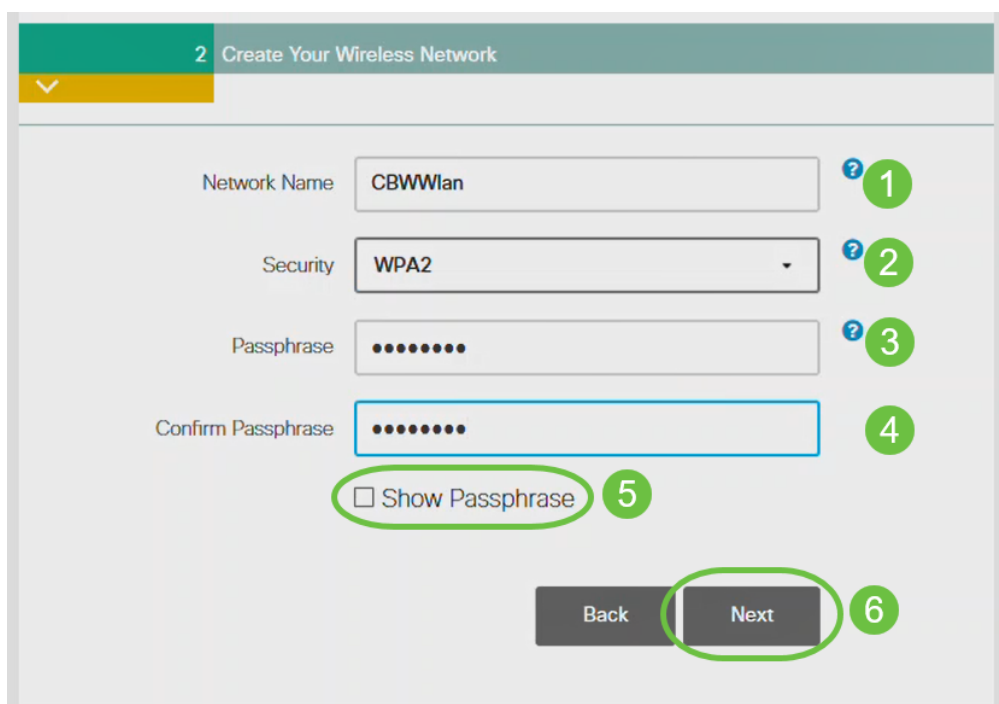
Per impostazione predefinita, questa opzione è disattivata.

## Passaggio 8

Creare le reti wireless immettendo quanto segue:

- Nome rete
- Scegli sicurezza
- Passphrase
- Conferma passphrase
- (Facoltativo) Selezionare la casella di controllo Mostra passphrase.

Fare clic su Next (Avanti).



The screenshot displays the '2 Create Your Wireless Network' configuration screen. It includes the following elements:

- Network Name:** A text input field containing 'CBWWlan' with a help icon (1).
- Security:** A dropdown menu set to 'WPA2' with a help icon (2).
- Passphrase:** A text input field with masked characters and a help icon (3).
- Confirm Passphrase:** A text input field with masked characters (4).
- Show Passphrase:** A checkbox labeled 'Show Passphrase' (5).
- Navigation:** 'Back' and 'Next' buttons at the bottom, with the 'Next' button highlighted (6).

Wi-Fi protected Access (WPA) versione 2 (WPA2) è lo standard corrente per la sicurezza Wi-Fi.

## Passaggio 9

Confermare le impostazioni e fare clic su **Applica**.



Please confirm the configurations and Apply

## 1 Primary AP Settings

Username **Admin**  
Primary AP Name **Test**  
Country **United States (US)**  
Date & Time **04/09/2021 9:14:16**  
Timezone **Central Time (US and Canada)**  
Mesh **No**  
Management IP Address **DHCP assigned IP Address**

## 2 Wireless Network Settings

Network Name **Test123**  
Security **WPA2 Personal**  
Passphrase: **\*\*\*\*\***

Back

Apply

### Passaggio 10

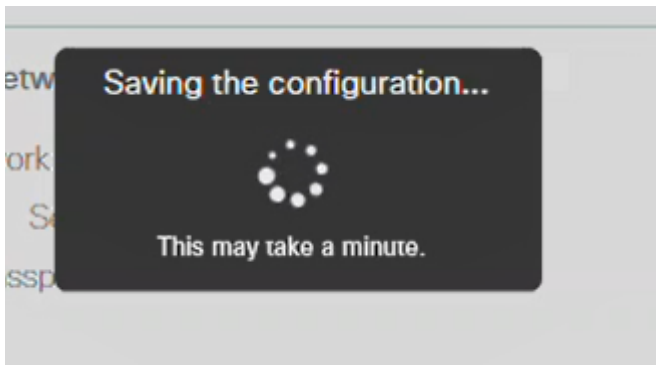
Fare clic su **OK** per applicare le impostazioni.

Primary AP will reboot after these configurations are applied. Click Ok to continue or click Cancel to return to the set up wizard.

OK

Cancel

Durante il salvataggio delle configurazioni e il riavvio del sistema viene visualizzata la seguente schermata. L'operazione potrebbe richiedere 10 minuti.

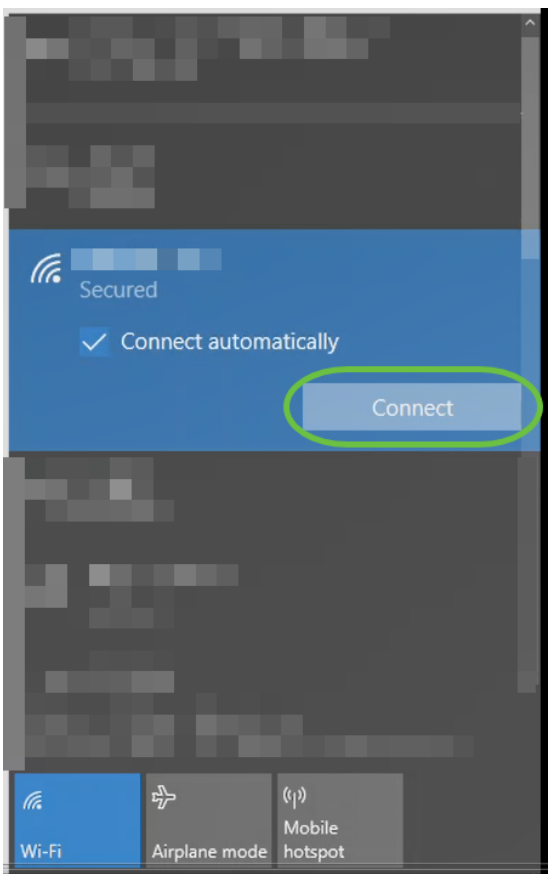


Durante il riavvio, il LED nel punto di accesso passa attraverso diversi modelli di colore. Quando il LED lampeggia in verde, procedere al passaggio successivo. Se il LED non supera il simbolo rosso, significa che nella rete non è presente alcun server DHCP. Verificare che l'access point sia collegato a uno switch o a un router con un server DHCP.

### Passaggio 11

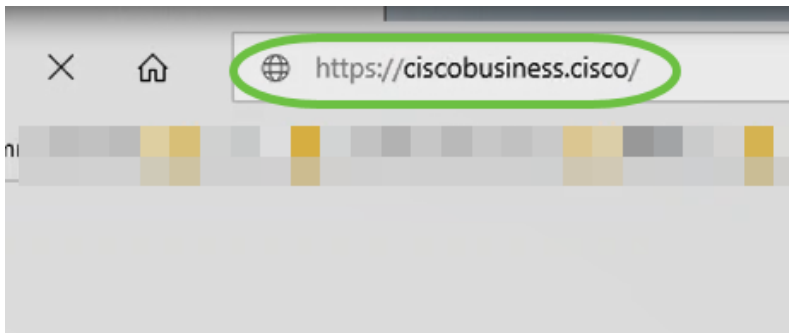
Accedere alle opzioni wireless del PC e scegliere la rete configurata. Fare clic su **Connetti**.

Il SSID *Cisco Business-Setup* scompare dopo il riavvio.



### Passaggio 12

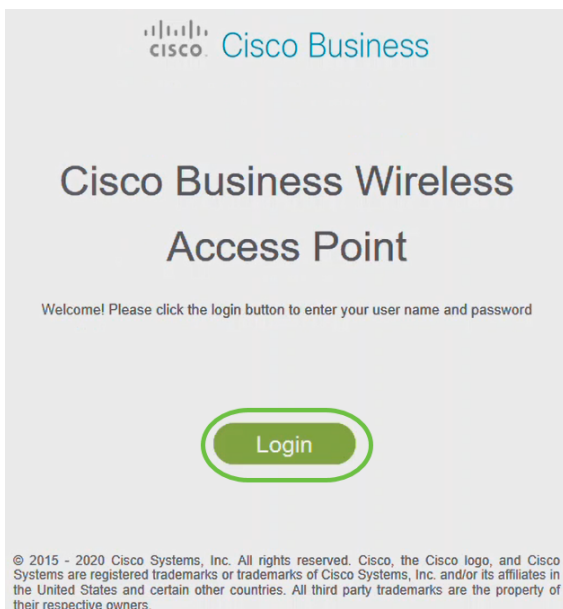
Aprire un browser Web e digitare *https://[indirizzo IP dell'access point CBW]*. In alternativa, digitare *https://ciscobusiness.cisco* nella barra degli indirizzi e premere Invio.



In questo passaggio, verificare di aver digitato *https* e non *http*.

### Passaggio 13

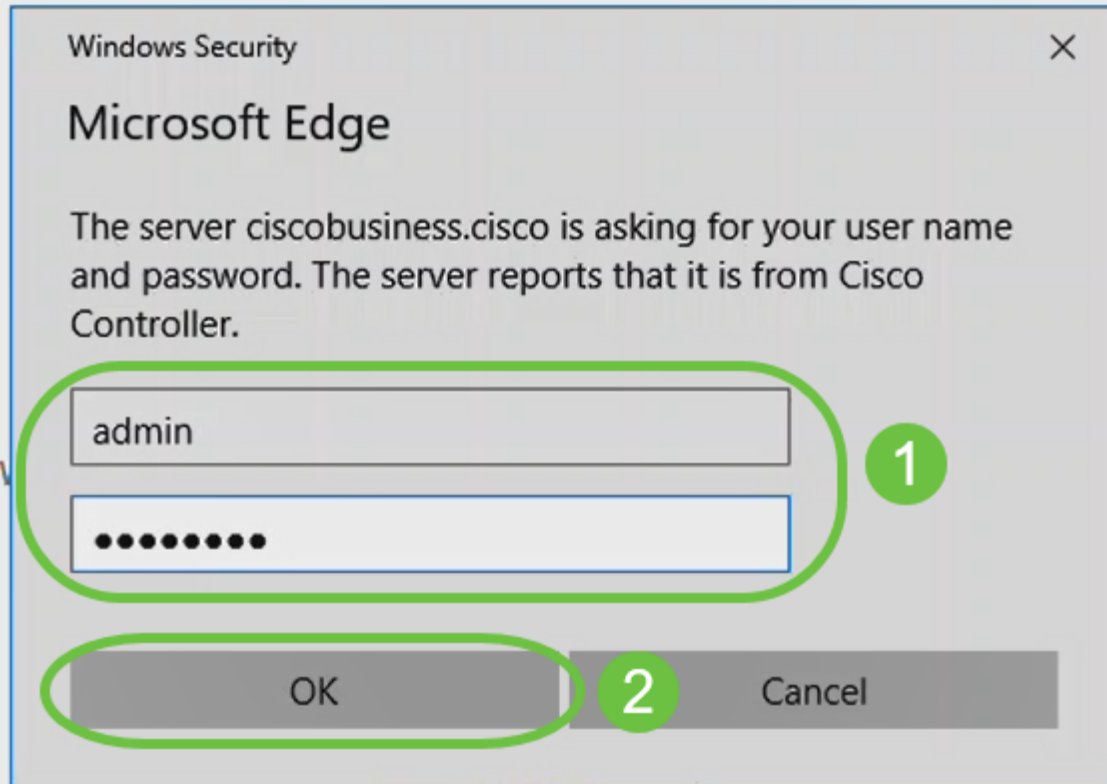
Fare clic su **Login**.



### Passaggio 14

Accedere utilizzando le credenziali configurate. Fare clic su OK.





© 2015 - 2020 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

## Passaggio 15

Sarà possibile accedere alla pagina dell'interfaccia utente Web dell'access point.



# Suggerimenti per la risoluzione dei problemi wireless

In caso di problemi, consultare i seguenti suggerimenti:

- Assicurarsi che sia selezionato l'SSID (Service Set Identifier) corretto. Questo è il nome creato per la rete wireless.
- Disconnetti qualsiasi VPN per l'app per dispositivi mobili o su un laptop. Potresti anche essere connesso a una VPN usata dal tuo provider di servizi mobili che potresti non conoscere. Ad esempio, un telefono Android (Pixel 3) con Google Fi come provider di servizi c'è una VPN integrata che si connette automaticamente senza notifica. Per trovare il punto di accesso primario, è necessario disattivare questa opzione.
- Accedere all'access point primario con <https://<indirizzo IP dell'access point primario>>.
- Dopo aver eseguito la configurazione iniziale, verificare che il sito [https:// is](https://is) venga utilizzato per accedere a *ciscobusiness.cisco* o per immettere l'indirizzo IP nel browser Web. A seconda delle impostazioni configurate, è possibile che nel computer sia stato inserito automaticamente [http:// since](http://since), che corrisponde a quello utilizzato al primo accesso.
- Per risolvere i problemi relativi all'accesso all'interfaccia utente Web o al browser durante l'uso dell'access point, nel browser Web (in questo caso Firefox) fare clic sul menu Apri, selezionare? > Informazioni per la risoluzione dei problemi e fare clic su Aggiorna Firefox.

## Configurazione dei CBW142ACM Mesh Extender tramite l'interfaccia utente Web

Sei nella fase iniziale di configurazione di questa rete, è sufficiente aggiungere le tue estensioni mesh!

### Passaggio 1

Collegare i due estensori di rete alla parete nelle posizioni selezionate. Annotare l'indirizzo MAC di ciascuna estensione di rete.

### Passaggio 2

Attendere circa 10 minuti l'avvio dei dispositivi Mesh Extender.

### Passaggio 3

Immettere l'indirizzo IP dei punti di accesso principali (AP) sul browser Web. Fare clic su **Login** per accedere all'access point primario.

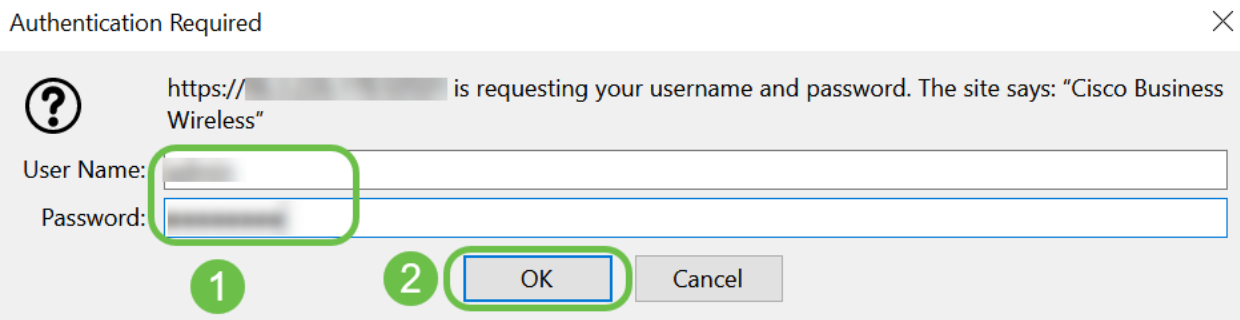
# Cisco Business Wireless Access Point

Welcome! Please click the login button to enter your user name and password



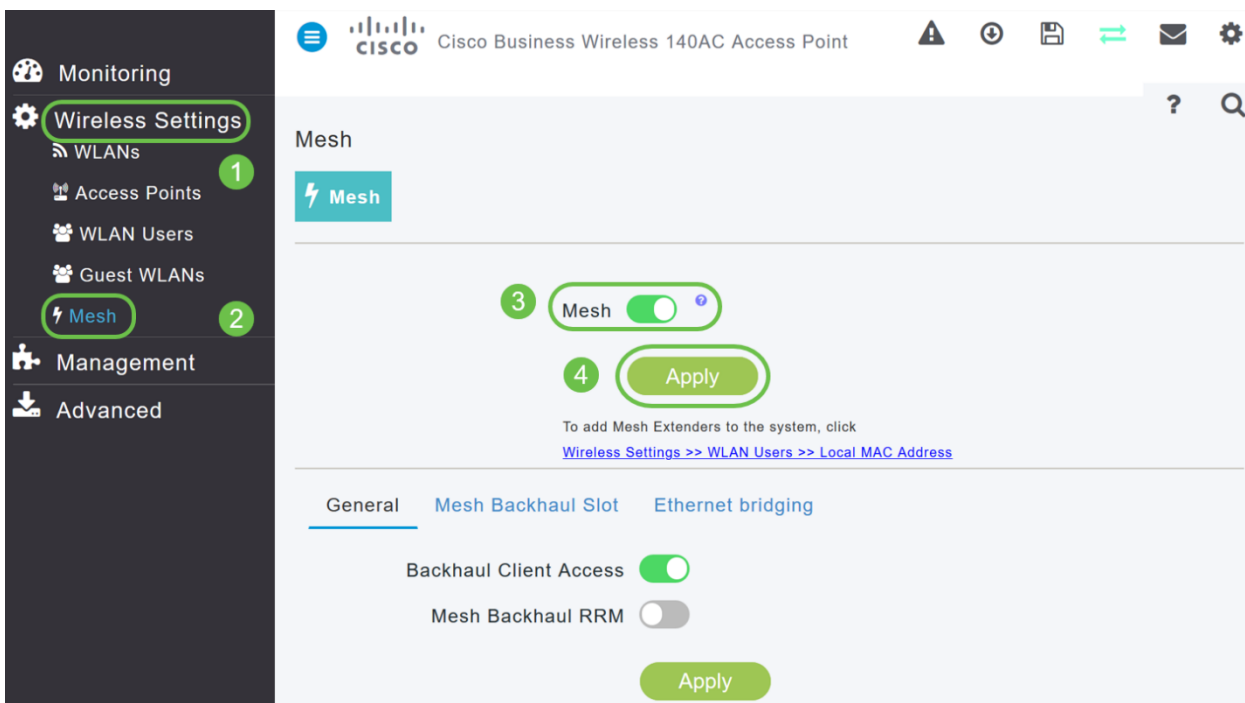
## Passaggio 4

Immettere il *nome utente* e la *password* per accedere all'access point primario. Fare clic su OK.



## Passaggio 5

Selezionare **Wireless Settings > Mesh** (Impostazioni wireless > Mesh). Assicurarsi che la *rete* sia attivata. Fare clic su Apply (Applica).



## Passaggio 6

Se Mesh non era già stato abilitato, il WAP potrebbe dover eseguire un riavvio. Viene visualizzato un popup per eseguire un riavvio. Conferma. L'operazione richiederà circa 10 minuti. Durante un riavvio, il LED lampeggia in verde in più schemi, alternando rapidamente verde, rosso e giallo prima di tornare verde. Possono esserci piccole variazioni nell'intensità del colore dei LED e nella tonalità da un'unità all'altra.

## Passaggio 7

Selezionare **Impostazioni wireless > Utenti WLAN > Indirizzi MAC locali**. Fare clic su **Aggiungi indirizzo MAC**.

The screenshot shows the Cisco Business Wireless 140AC Access Point configuration interface. The left sidebar is labeled 'Monitoring' and includes 'Wireless Settings' (1), 'WLANs', 'Access Points', 'WLAN Users' (2), 'Guest WLANs', 'DHCP Server', and 'Mesh'. The main area is titled 'WLAN Users' and shows 'Users 0'. Under 'WLAN Users', 'Local MAC Addresses' (3) is selected. A search bar (4) is present above the 'Add MAC Address' button. Below the search bar, there are 'Refresh' and 'Number of Blacklist:0 Number of Whitelist:2' indicators. A table lists MAC addresses and their types:

Action	MAC Address	Type	Profile Name	Description
	68:ca:e4:6e:15:58	AllowList	Any WLAN/RLAN	CBW142 Mesh Extender
	a4:53:0e:1f:e4:88	AllowList	Any WLAN/RLAN	CBW140AC-e488

## Passaggio 8

Immettere l'indirizzo MAC e la descrizione del dispositivo Mesh Extender. Selezionare l'elenco *Tipo* consentito. Selezionare *Nome profilo* dal menu a discesa. Fare clic su **Apply (Applica)**.

The 'Add MAC Address' dialog box contains the following fields and controls:

- MAC Address**: 68:ca:e4:6e:15:38 (1)
- Description**: CBW142 Mesh Extender (2)
- Type**:  Block list  Allow list (3)
- Profile Name**: Any WLAN/RLAN (4)
- Buttons**: **Apply** (5) and **Cancel**

## Passaggio 9

Accertarsi di salvare tutte le configurazioni premendo l'icona **Save (Salva)** nel riquadro in alto a destra dello schermo.



Ripetete la procedura per ogni estensione di mesh.

## Controllo e aggiornamento del software tramite l'interfaccia utente Web

Non saltare questo passaggio importante! Esistono alcuni modi per aggiornare il software, ma i passaggi elencati di seguito sono consigliati come i più semplici da eseguire quando si utilizza l'interfaccia utente Web.

Per visualizzare e aggiornare la versione software corrente dell'access point principale, effettuare le seguenti operazioni.

### Passaggio 1

Fare clic sull'icona **gear** nell'angolo superiore destro dell'interfaccia Web e quindi su **Primary AP Information**.

Primary AP Information	
Primary AP Name	Cisco Buisness Wireless
Model	CBW-145AC
Serial Number	ABC1415DEF1
Software Version	10.4.1.0
Up Time	2 days, 17 hours, 45 minutes
Primary AP Time	Sat Feb 27 10:05:15 2021
Timezone	San jose
Country	Multiple Countries : US
Management IP Address	10.10.10.7
Memory Usage	63%
Max Access Points Supported	50

### Passaggio 2

Confrontare la versione in esecuzione con l'ultima versione del software. Chiudere la

finestra una volta stabilito se è necessario aggiornare il software.

AP Information	
Primary AP Name	
Model	CBW140AC-B
Serial Number	
Software Version	10.0.251.24
Up Time	5 days, 1 hour, 57 minutes
Primary AP Time	Sun Mar 29 16:50:26 2020
Timezone	Central Time (US and Canada)
Country	US - United States
Management IP Address	192.168.1.125
Memory Usage	55%
Max Access Points Supported	50

Se si sta eseguendo la versione più recente del software, è possibile passare alla sezione [Creazione di WLAN](#).

### Passaggio 3

Scegliere **Gestione > Aggiornamento software** dal menu.

Viene visualizzata la finestra *Software Update* (Aggiornamento software) con il numero di versione del software corrente riportato nella parte superiore.

Software Update

Version 10.0.251.24

Transfer Mode TFTP

IP Address(IPv4)/Name \* 172.16.1.35

È possibile aggiornare il software CBW AP e le configurazioni correnti sull'access point principale non verranno eliminate.

Dall'elenco a discesa *Transfer Mode* (Modalità di trasferimento), selezionare **Cisco.com**.

Transfer Mode	Cisco.com
Automatically Check For Updates	HTTP
Last Software Check	TFTP
Latest Software Release	SFTP
	Cisco.com


#### Passaggio 4





Per impostare l'access point principale in modo che controlli automaticamente la disponibilità di aggiornamenti software, scegliere **Abilitato** dall'elenco a discesa *Controlla automaticamente disponibilità aggiornamenti*. L'opzione è abilitata per impostazione predefinita.

Transfer Mode	Cisco.com
Automatically Check For Updates	Enabled

Al termine di un controllo software e se è disponibile un aggiornamento software più recente o consigliato sul sito Cisco.com:

- L'icona dell'avviso di aggiornamento software nell'angolo superiore destro dell'interfaccia utente Web sarà di colore verde (o grigio). Se si fa clic sull'icona, viene visualizzata la pagina Aggiornamento software.
- Il pulsante Aggiorna nella parte inferiore della pagina *Aggiornamento software* è abilitato.

 Cisco Business Wireless 140AC Access Point

**Software Update**

Version 10.0.251.24

---

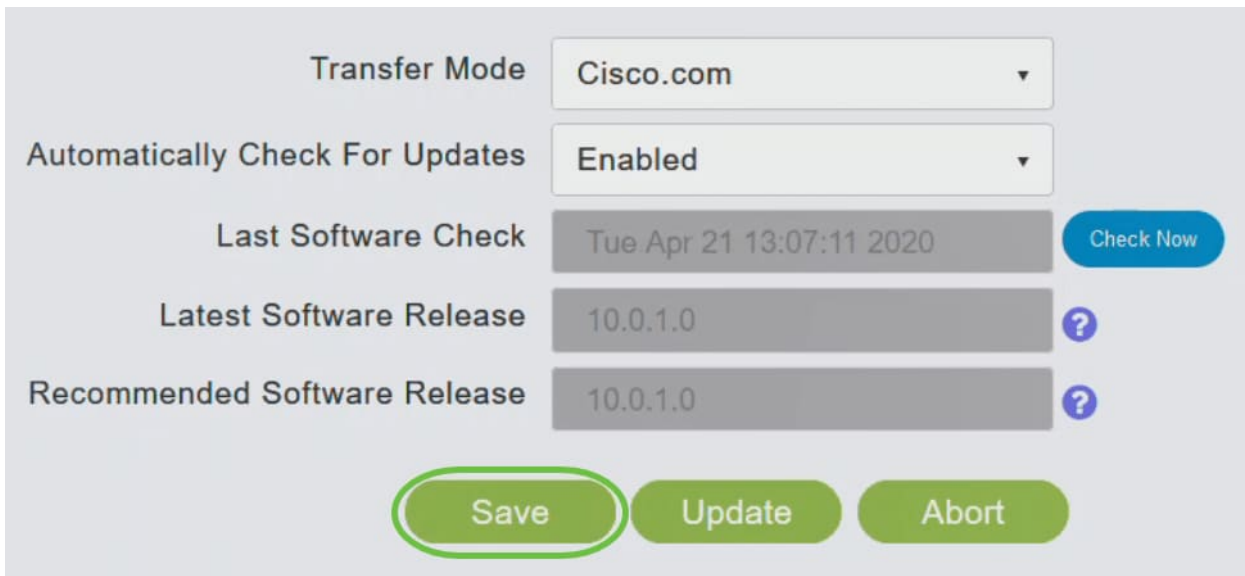
Transfer Mode	Cisco.com
Automatically Check For Updates	Enabled
Last Software Check	Fri Mar 27 10:44:29 2020 <span style="float: right; background-color: #00a651; color: white; padding: 2px 5px;">Check Now</span>
Latest Software Release	10.0.1.0 <span style="float: right; color: #00a651;">?</span>
Recommended Software Release	10.0.1.0 <span style="float: right; color: #00a651;">?</span>

Save
Update
Abort

Software update is available for your Cisco Business Wireless AP/APs on cisco.com

## Passaggio 5

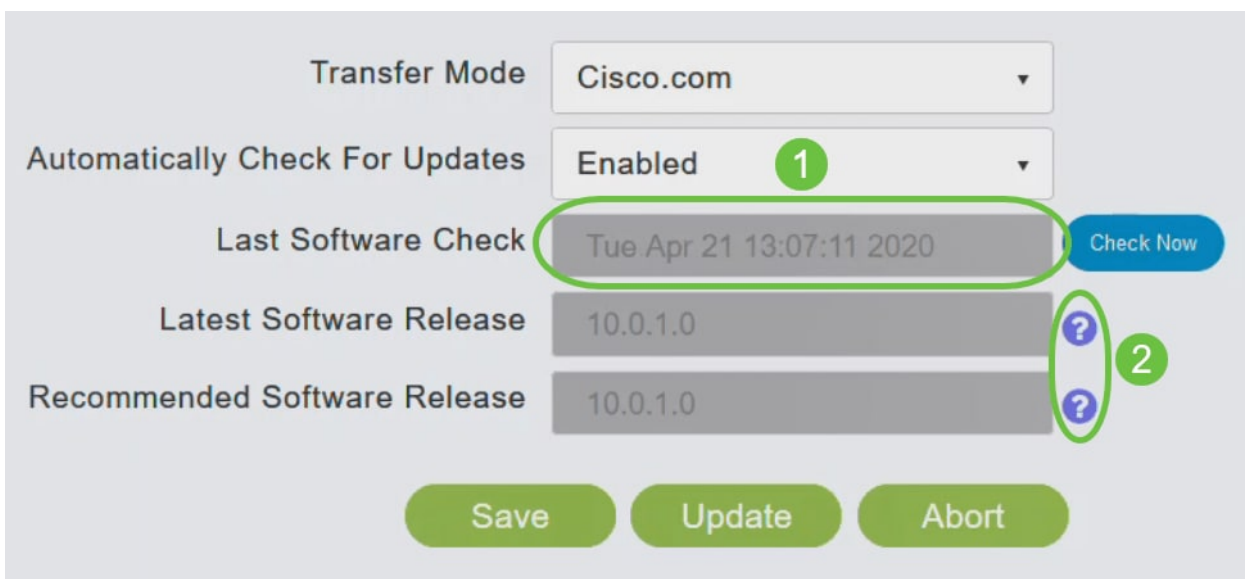
Fare clic su **Salva**. In questo modo vengono salvate le voci o le modifiche apportate sia in *modalità di trasferimento* che in *Controlla automaticamente aggiornamenti*.



Transfer Mode	Cisco.com	▼
Automatically Check For Updates	Enabled	▼
Last Software Check	Tue Apr 21 13:07:11 2020	Check Now
Latest Software Release	10.0.1.0	?
Recommended Software Release	10.0.1.0	?

Save Update Abort

Il campo *Ultimo controllo software* visualizza l'indicatore orario dell'ultimo controllo software automatico o manuale. È possibile visualizzare le note delle release visualizzate facendo clic sull'icona del **punto interrogativo** accanto ad esso.



Transfer Mode	Cisco.com	▼
Automatically Check For Updates	Enabled	▼ 1
Last Software Check	Tue Apr 21 13:07:11 2020	Check Now
Latest Software Release	10.0.1.0	? 2
Recommended Software Release	10.0.1.0	? 2

Save Update Abort

## Passaggio 6

È possibile eseguire manualmente un controllo software in qualsiasi momento facendo clic su *Esegui controllo*.



Transfer Mode	Cisco.com	▼
Automatically Check For Updates	Enabled	▼
Last Software Check	Tue Apr 21 13:07:11 2020	<a href="#">Check Now</a>
Latest Software Release	10.0.1.0	?
Recommended Software Release	10.0.1.0	?

[Save](#) [Update](#) [Abort](#)

### Passaggio 7

Per procedere con l'aggiornamento software, fare clic su **Aggiorna**.

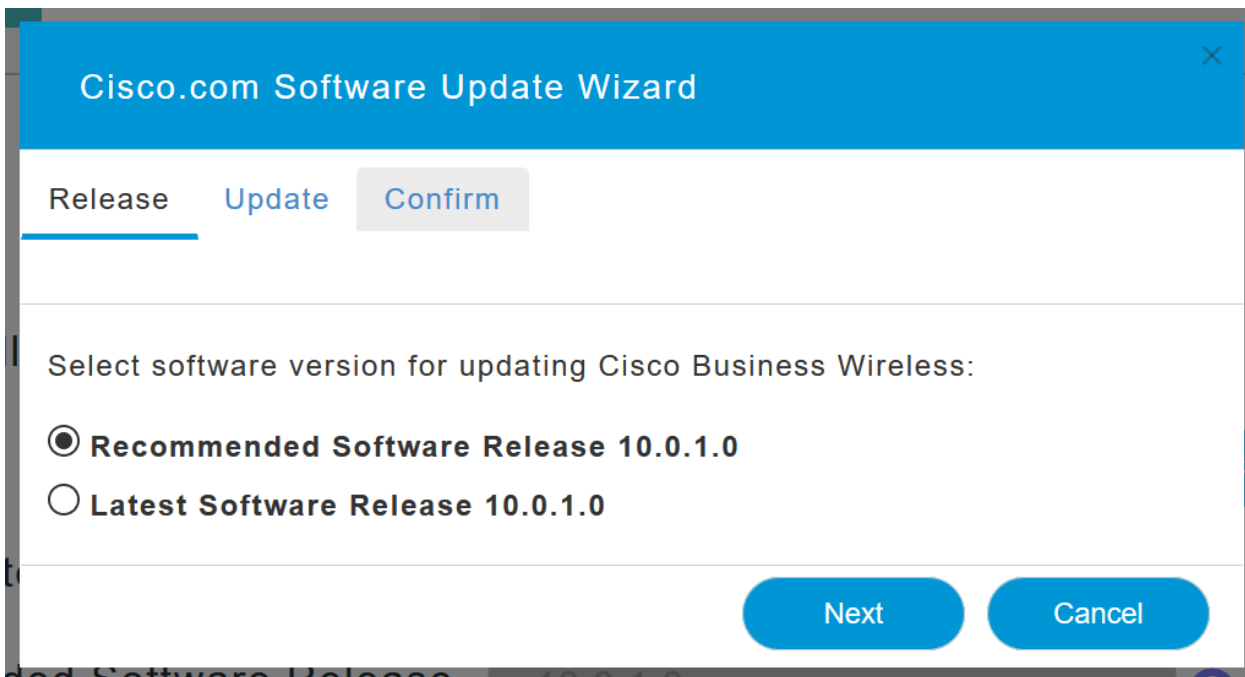
Transfer Mode	Cisco.com	▼
Automatically Check For Updates	Enabled	▼
Last Software Check	Tue Apr 21 13:07:11 2020	<a href="#">Check Now</a>
Latest Software Release	10.0.1.0	?
Recommended Software Release	10.0.1.0	?

[Save](#) [Update](#) [Abort](#)

Viene visualizzato l'*Aggiornamento guidato software*. La procedura guidata consente di visualizzare le tre schede seguenti in sequenza:

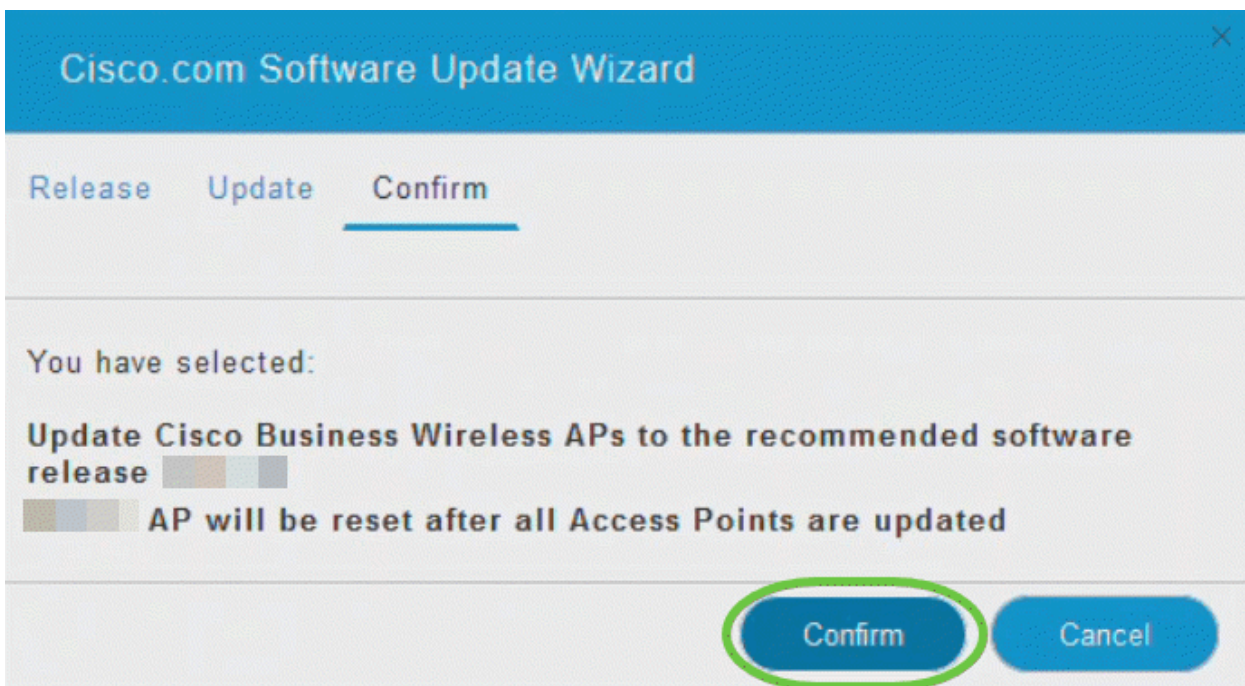
- Scheda Release (Versione) - Consente di specificare se si desidera eseguire l'aggiornamento alla versione software consigliata o alla versione più recente.
- Scheda Aggiorna: specificare quando reimpostare gli access point. È possibile scegliere di eseguirlo immediatamente o pianificarlo per un secondo momento. Per impostare il riavvio automatico dell'access point principale al termine del download preliminare dell'immagine, selezionare la casella di controllo Riavvio automatico.
- Scheda Conferma: conferma le selezioni.

Seguire le istruzioni della procedura guidata. È possibile tornare a qualsiasi scheda in qualsiasi momento prima di fare clic su *Conferma*.



### Passaggio 8

Fare clic su **Conferma**.

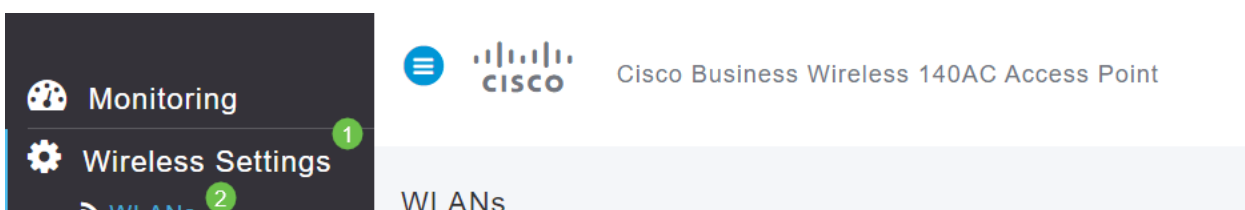


## Creazione di WLAN sull'interfaccia utente Web

In questa sezione è possibile creare reti WLAN (Wireless Local Area Network).

### Passaggio 1

È possibile creare una WLAN selezionando **Impostazioni wireless > WLAN**. Quindi selezionare **Add new WLAN/RLAN** (Aggiungi nuova WLAN/RLAN).



## Passaggio 2

Nella scheda *Generale*, immettere le seguenti informazioni:

- ID WLAN: selezionare un numero per la WLAN
- Tipo: selezione della **WLAN**
- Nome profilo: quando si immette un nome, il SSID viene inserito automaticamente con lo stesso nome. Il nome deve essere univoco e non deve superare i 31 caratteri.

I campi seguenti sono stati lasciati come predefiniti in questo esempio, ma sono elencate le spiegazioni nel caso si desideri configurarli diversamente.

- SSID - Il nome del profilo funge anche da SSID. Se lo desideri, puoi modificare questa impostazione. Il nome deve essere univoco e non deve superare i 31 caratteri.
- Enable - Questa opzione deve essere lasciata abilitata affinché la WLAN funzioni.
- Criteri radio: in genere si desidera lasciare **Tutto** questo in modo che i client a 2,4 e 5 GHz possano accedere alla rete.
- SSID di trasmissione: in genere si desidera che l'SSID venga individuato e quindi si desidera lasciarlo abilitato.
- Profilatura locale: questa opzione consente solo di visualizzare il sistema operativo in esecuzione sul client o di visualizzare il nome utente.

Fare clic su Apply (Applica).

The screenshot shows the 'Add new WLAN/RLAN' configuration window with the following settings:

- WLAN ID: 2 (marked with a green circle 1)
- Type: WLAN (marked with a green circle 2)
- Profile Name: Engineering (marked with a green circle 3)
- SSID: Engineering (marked with a green circle 3)
- Enable:
- Radio Policy: ALL (marked with a green circle 4)
- Broadcast SSID:
- Local Profiling:

Buttons: Apply (checked), Cancel (X)

## Passaggio 3

Viene visualizzata la scheda *Sicurezza WLAN*.

In questo esempio sono state lasciate come predefinite le opzioni seguenti:

- La rete guest, l'Assistente rete captive e il filtro MAC sono stati lasciati disabilitati. I dettagli per la configurazione di una rete guest sono descritti nella sezione successiva.
- WPA2 Personal - Accesso protetto Wi-Fi 2 con formato passphrase PSK (Pre-shared Key) - ASCII. Questa opzione indica Wi-Fi Protected Access 2 con chiave precondivisa (PSK).

WPA2 Personal è un metodo utilizzato per proteggere la rete tramite l'autenticazione PSK. La chiave PSK viene configurata separatamente sia sull'access point primario, in base ai criteri di sicurezza WLAN, sia sul client. WPA2 Personal non si basa su un server di autenticazione della rete.

- Formato passphrase: **ASCII viene lasciato come predefinito.**

In questo scenario sono stati immessi i campi seguenti:

- Mostra passphrase: fare clic sulla casella di controllo per visualizzare la passphrase immessa.
- Passphrase: immettere un nome per la passphrase (password).
- Conferma passphrase: immettere di nuovo la password per confermare.

Fare clic su Apply (Applica). La nuova WLAN verrà attivata automaticamente.

General WLAN Security VLAN & Firewall Traffic Shaping Scheduling

Guest Network

Captive Network Assistant

MAC Filtering  ?

Security Type

Passphrase Format

Passphrase \*  3

Confirm Passphrase \*  2

1  Show Passphrase

Password Expiry  ?

4

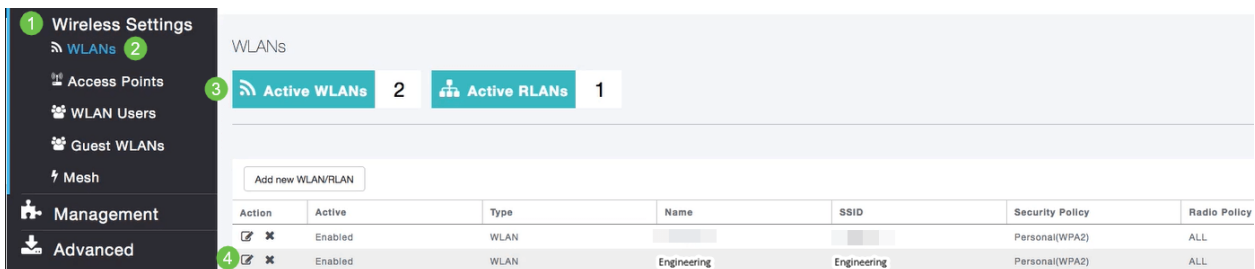
## Passaggio 4

Assicurarsi di salvare le configurazioni facendo clic sull'icona **Salva** nel pannello in alto a destra della schermata dell'interfaccia utente Web.



## Passaggio 5

Per visualizzare la WLAN creata, selezionare **Impostazioni wireless > WLAN**. Il numero di WLAN attive è aumentato a 2 e viene visualizzata la nuova WLAN.



Ripetere questi passaggi per le altre WLAN che si desidera creare.

## Configurazioni wireless opzionali

A questo punto sono state impostate tutte le configurazioni di base e si è pronti per l'uso. Sono disponibili alcune opzioni, pertanto è possibile passare a una delle sezioni seguenti:

- [Creare una WLAN guest utilizzando l'interfaccia utente Web \(facoltativo\)](#)
- [Creazione profilo applicazione \(facoltativo\)](#)
- [Creazione profilo client \(facoltativo\)](#)
- [Sono pronto per concludere e iniziare a usare la mia rete!](#)

### Creare una WLAN guest utilizzando l'interfaccia utente Web (facoltativo)

Una WLAN guest consente l'accesso guest alla rete wireless aziendale Cisco.

#### Passaggio 1

Accedere all'interfaccia utente Web dell'access point primario. Aprire un browser Web e immettere [www.https://ciscobusiness.cisco](https://ciscobusiness.cisco). È possibile che venga visualizzato un avviso prima di procedere. Immettere le credenziali. È inoltre possibile accedervi immettendo l'indirizzo IP dell'access point primario.

#### Passaggio 2

Per creare una rete WLAN (Wireless Local Area Network), selezionare **Impostazioni wireless > WLAN**. Quindi selezionare **Add new WLAN/RLAN** (Aggiungi nuova WLAN/RLAN).



## Passaggio 3

Nella scheda *Generale*, immettere le seguenti informazioni:

*ID WLAN*: selezionare un numero per la WLAN

*Type* - Seleziona **WLAN**

*Nome profilo*: quando si immette un nome, il SSID viene popolato automaticamente con lo stesso nome. Il nome deve essere univoco e non deve superare i 31 caratteri.

I campi seguenti sono stati lasciati come predefiniti in questo esempio, ma sono elencate le spiegazioni nel caso si desideri configurarli diversamente.

*SSID* - Il nome del profilo funge anche da SSID. Se lo desideri, puoi modificare questa impostazione. Il nome deve essere univoco e non deve superare i 31 caratteri.

*Enable* - Questa opzione deve essere lasciata abilitata affinché la WLAN funzioni.

*Criterio radio* - In genere si desidera lasciare **Tutto** questo in modo che i client 2,4 GHz e 5 GHz possano accedere alla rete.

*SSID trasmissione*: in genere si desidera che l'SSID venga individuato e quindi si desidera lasciarlo abilitato.

*Profilatura locale*: questa opzione consente solo di visualizzare il sistema operativo in esecuzione sul client o di visualizzare il nome utente.

Fare clic su **Apply** (Applica).

## Add new WLAN/RLAN

General **WLAN Security** VLAN & Firewall Traffic Shaping Scheduling

WLAN ID

1

Type

2

Profile Name \*

3

SSID \*

WLANs with same SSID can be configured, unless layer-2 security settings are different.

Enable

Radio Policy

?

Broadcast SSID

Local Profiling

?

4

Apply

Cancel

### Passaggio 4

Viene visualizzata la scheda *Sicurezza WLAN*. In questo esempio sono state selezionate le opzioni seguenti.

- Rete guest - Abilita
- Captive Network Assistant - Se si utilizza Mac o IOS, probabilmente si desidera attivare questa funzione. Questa funzionalità rileva la presenza di un portale vincolato inviando una richiesta Web alla connessione a una rete wireless. Questa richiesta viene indirizzata a un URL (Uniform Resource Locator) per i modelli iPhone e se si riceve una risposta, si presume che l'accesso a Internet sia disponibile e che non siano necessarie ulteriori interazioni. Se non viene ricevuta alcuna risposta, si presume che l'accesso a Internet sia bloccato dal portale in modalità di blocco e che l'Assistente alla rete in modalità di blocco di Apple (CNA) avvii automaticamente lo pseudo-browser per richiedere l'accesso al portale in una finestra controllata. La CNA potrebbe interrompersi durante il reindirizzamento a un portale separato di Identity Services Engine (ISE). L'access point primario impedisce la visualizzazione di questo pseudo-browser.
- Captive Portal - Questo campo è visibile solo quando l'opzione Rete guest è abilitata. Consente di specificare il tipo di portale Web che può essere utilizzato per l'autenticazione. Selezionare Pagina iniziale interna per utilizzare l'autenticazione basata sul portale Web Cisco predefinita. Scegliere Pagina iniziale esterna se si dispone

dell'autenticazione di portale vincolato, utilizzando un server Web esterno alla rete. Inoltre, specificare l'URL del server nel campo URL sito.

## Add new WLAN/RLAN

General WLAN Security VLAN & Firewall Traffic Shaping Scheduling

Guest Network

1

Captive Network Assistant

2

MAC Filtering

Captive Portal Internal Splash Page

3

Access Type Social Login

ACL Name(IPv4) None

?

ACL Name(IPv6) None

?

In questo esempio, verrà creata la WLAN guest con un tipo di accesso di accesso di social networking abilitato. Una volta connesso alla WLAN guest, l'utente verrà reindirizzato alla pagina di accesso predefinita di Cisco, dove potrà trovare i pulsanti di accesso per Google e Facebook. L'utente può accedere utilizzando il proprio account Google o Facebook per ottenere l'accesso a Internet.

### Passaggio 5

Nella stessa scheda selezionare un *tipo di accesso* dal menu a discesa. In questo esempio è stato selezionato *Accesso social*. Questa è l'opzione che consente agli ospiti di usare le loro credenziali Google o Facebook per autenticarsi e ottenere l'accesso alla rete.

Altre opzioni per *Tipo di accesso* sono:

*Account utente locale* - Opzione predefinita. Scegliere questa opzione per autenticare i guest utilizzando il nome utente e la password che è possibile specificare per gli utenti guest della WLAN, in **Impostazioni wireless > Utenti WLAN**. Questo è un esempio della pagina iniziale interna predefinita.



#### Welcome to the Cisco Business Wireless

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

User Name

Password



È possibile personalizzare questa impostazione selezionando **Impostazioni wireless > WLAN guest**. Da qui è possibile immettere un *titolo* e un *messaggio di pagina*. Fare clic su **Apply** (Applica). Fare clic su **Anteprima**.

*Web Consent*: consente agli utenti guest di accedere alla WLAN dopo aver accettato i termini e le condizioni visualizzati. Gli utenti guest possono accedere alla WLAN senza immettere un nome utente e una password.

*Indirizzo e-mail* - Gli utenti guest devono immettere il proprio indirizzo e-mail per accedere alla rete.

*RADIUS*: da utilizzare con un server di autenticazione esterno.

*WPA2 Personal* - Accesso protetto Wi-Fi 2 con chiave precondivisa (PSK)

Fare clic su **Apply** (Applica).

The screenshot shows the 'Add new WLAN/RLAN' configuration interface. The 'WLAN Security' tab is active. The 'Guest Network' and 'Captive Network Assistant' are turned on. The 'Access Type' dropdown menu is open, and the 'Web Consent' option is selected, indicated by a green circle with the number '1'. At the bottom right, the 'Apply' button is highlighted with a green circle with the number '2'.

## Passaggio 6

Assicurarsi di salvare le configurazioni facendo clic sull'icona **Salva** nel pannello in alto a destra della schermata dell'interfaccia utente Web.



È stata creata una rete guest disponibile nella rete CBW. I vostri ospiti apprezzeranno la comodità.

## Creazione profilo applicazione mediante interfaccia utente Web (facoltativo)

La profilatura è un sottoinsieme di funzionalità che consentono di applicare criteri organizzativi. Permette di associare e assegnare priorità ai tipi di traffico. Come le regole che decidono come classificare o eliminare il traffico. Il sistema Cisco Business Mesh Wireless prevede la profilatura di client e applicazioni. L'accesso a una rete come utente inizia con molti scambi di informazioni, tra cui il tipo di traffico. I criteri interrompono il flusso del traffico per indirizzare il percorso, in modo analogo a un diagramma di flusso. Altri tipi di funzionalità dei criteri includono: accesso guest, elenchi di controllo di accesso e QoS.

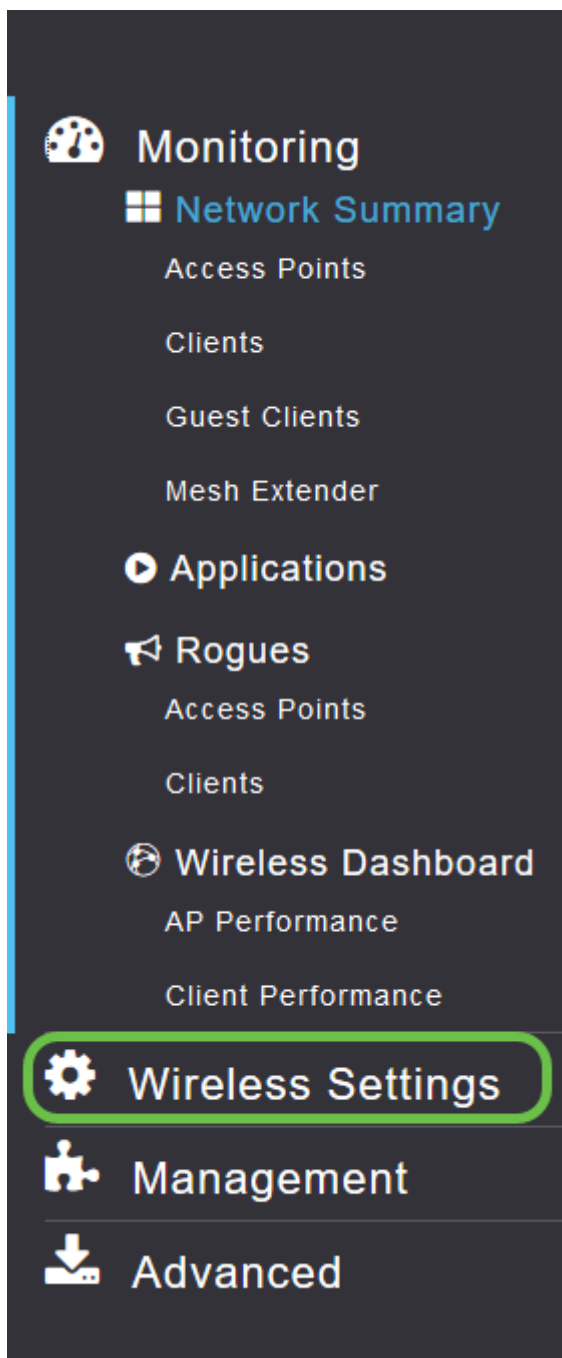
## Passaggio 1

Se la barra dei menu a sinistra non è visibile, spostarsi sul menu sul lato sinistro dello schermo.

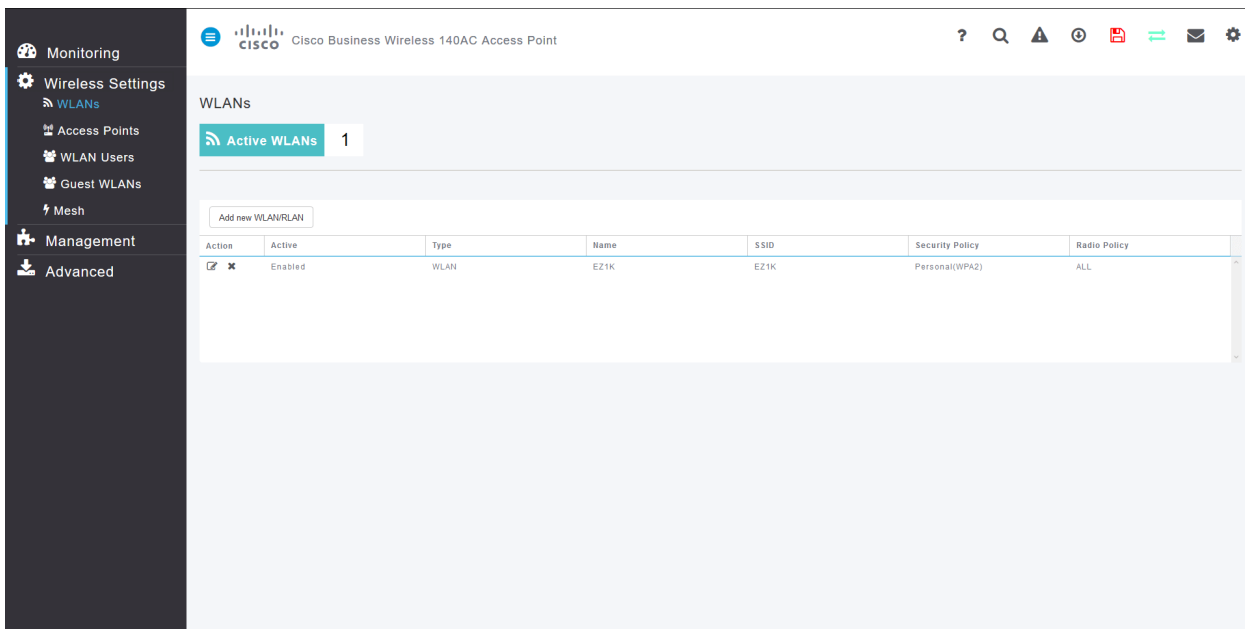


## Passaggio 2

Il menu Monitoraggio viene caricato per impostazione predefinita quando si accede al dispositivo. Sarà necessario fare clic su **Impostazioni wireless**.

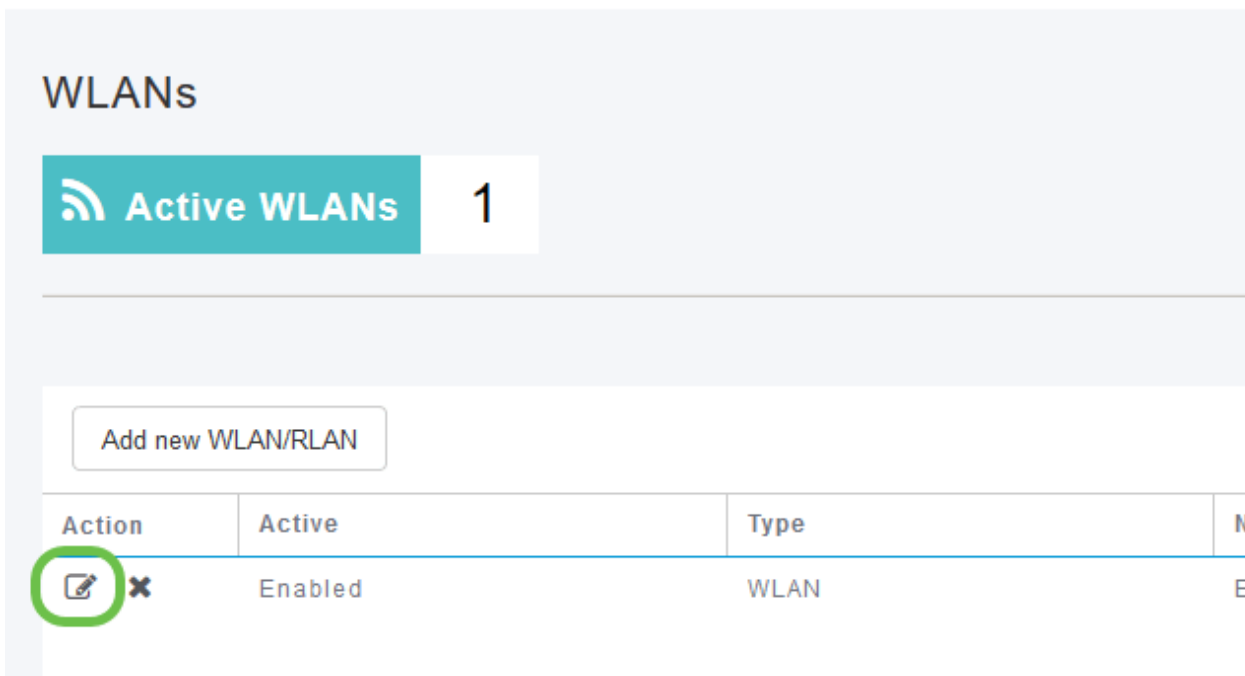
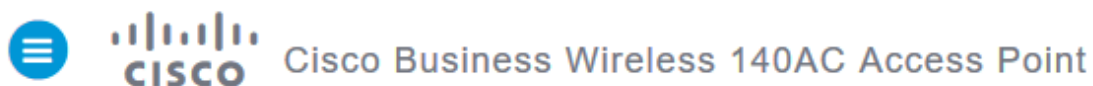


L'immagine seguente è simile a quella visualizzata quando si fa clic sul collegamento Impostazioni wireless.

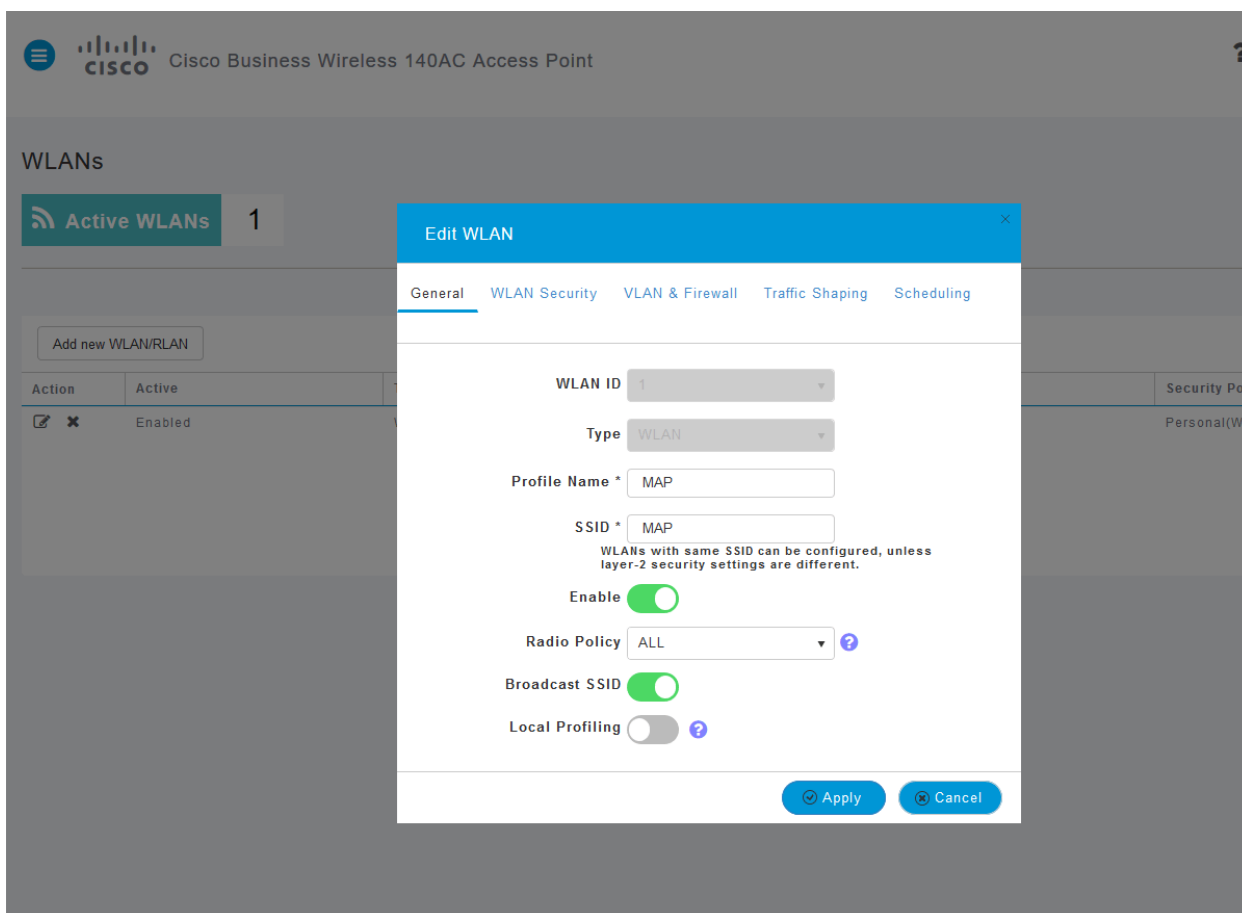


### Passaggio 3

Fare clic sull'icona di **modifica** a sinistra della rete locale wireless su cui si desidera attivare l'applicazione.

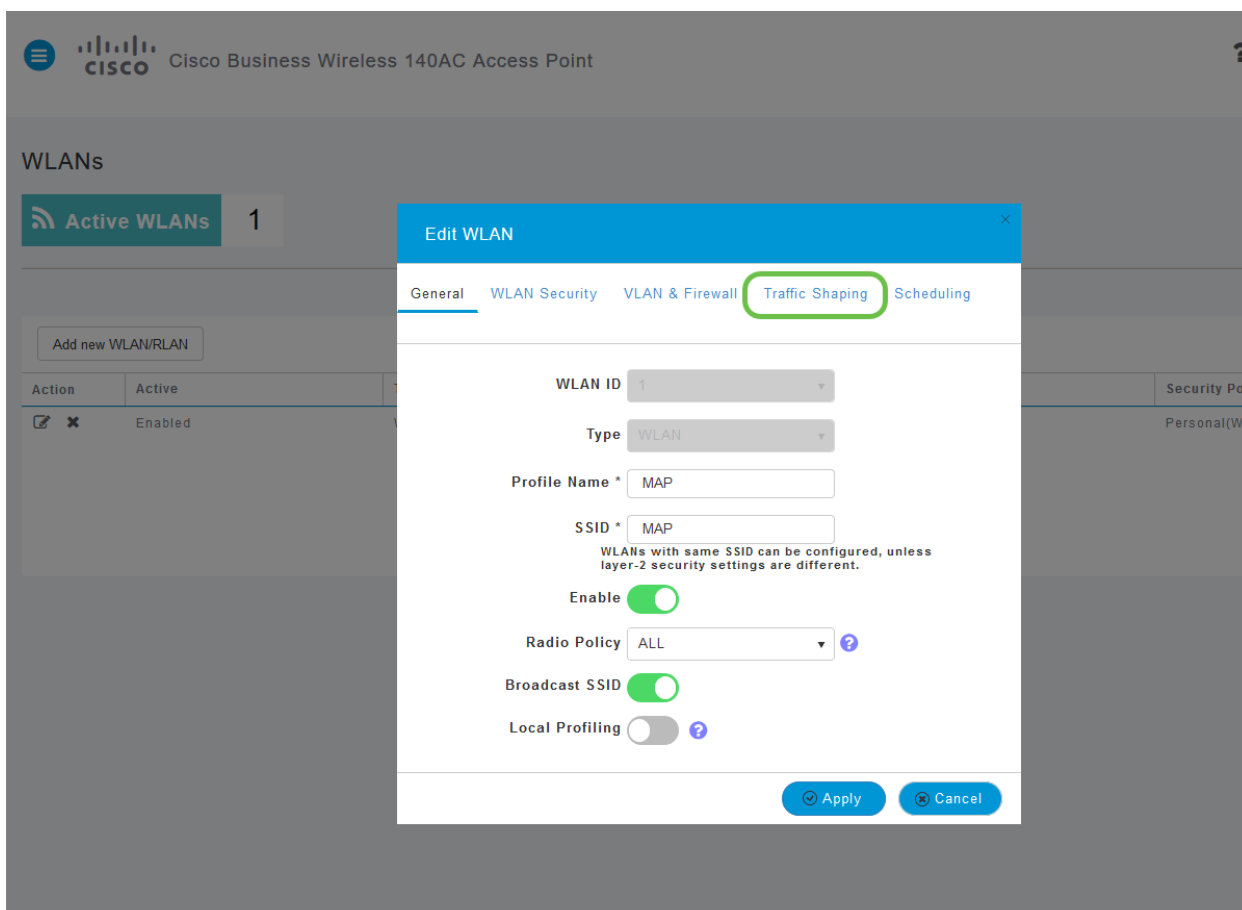


Poiché la WLAN è stata aggiunta di recente, la pagina *Modifica WLAN* potrebbe essere simile alla seguente:

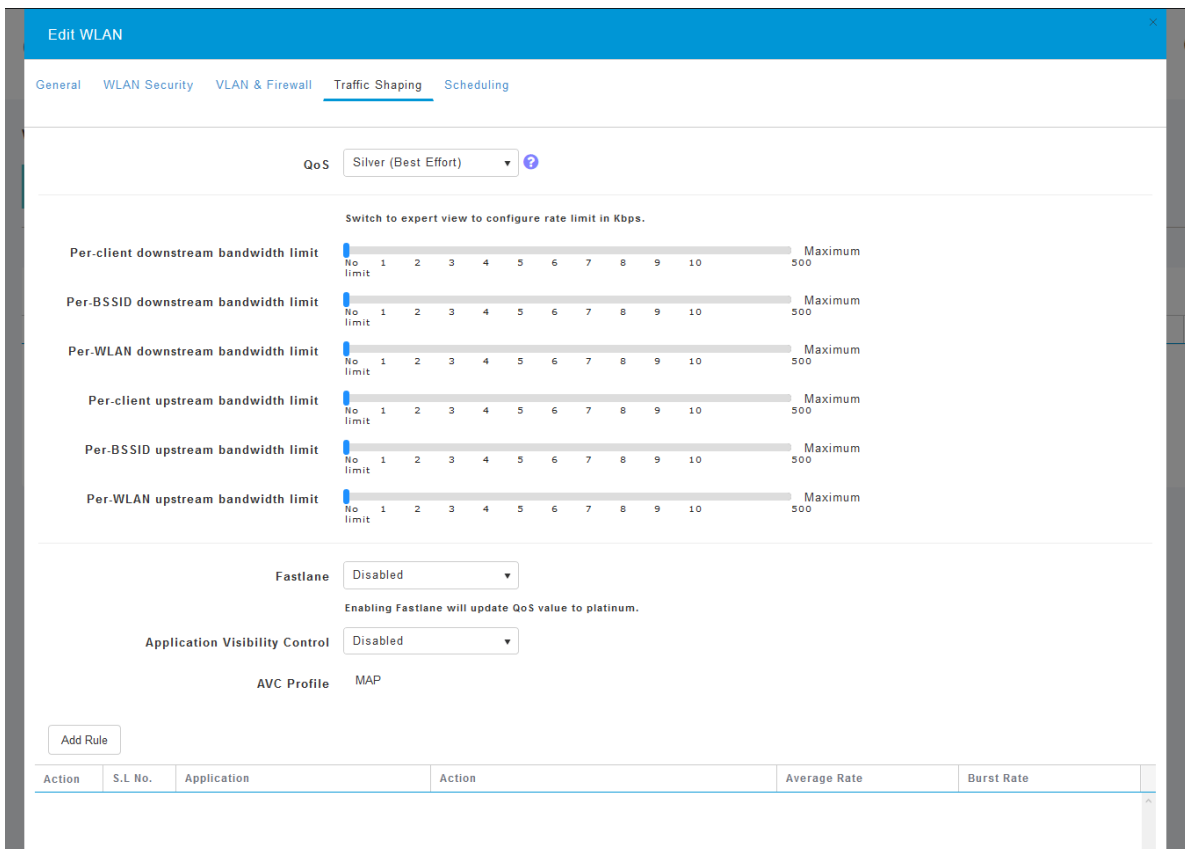


#### Passaggio 4

Passare alla scheda **Traffic Shaping** facendo clic su di essa.

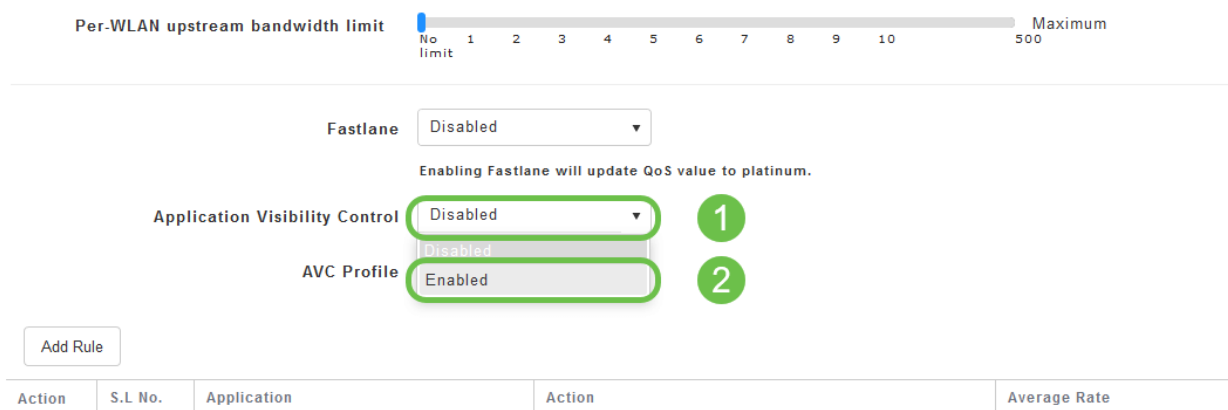


Lo schermo potrebbe apparire come segue:



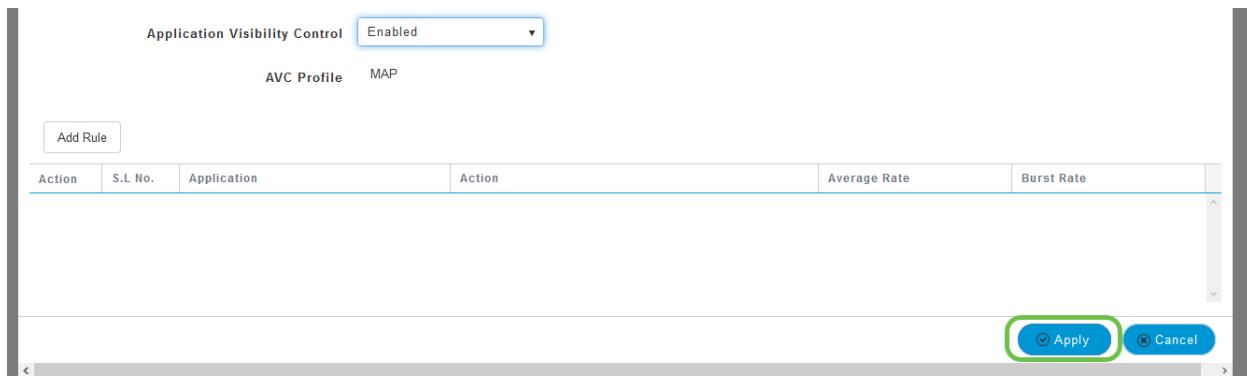
## Passaggio 5

Nella parte inferiore della pagina è disponibile la funzionalità *Controllo visibilità applicazioni*. Questa opzione è disabilitata per impostazione predefinita. Fare clic sull'elenco a discesa e selezionare **Abilitato**.



## Passaggio 6

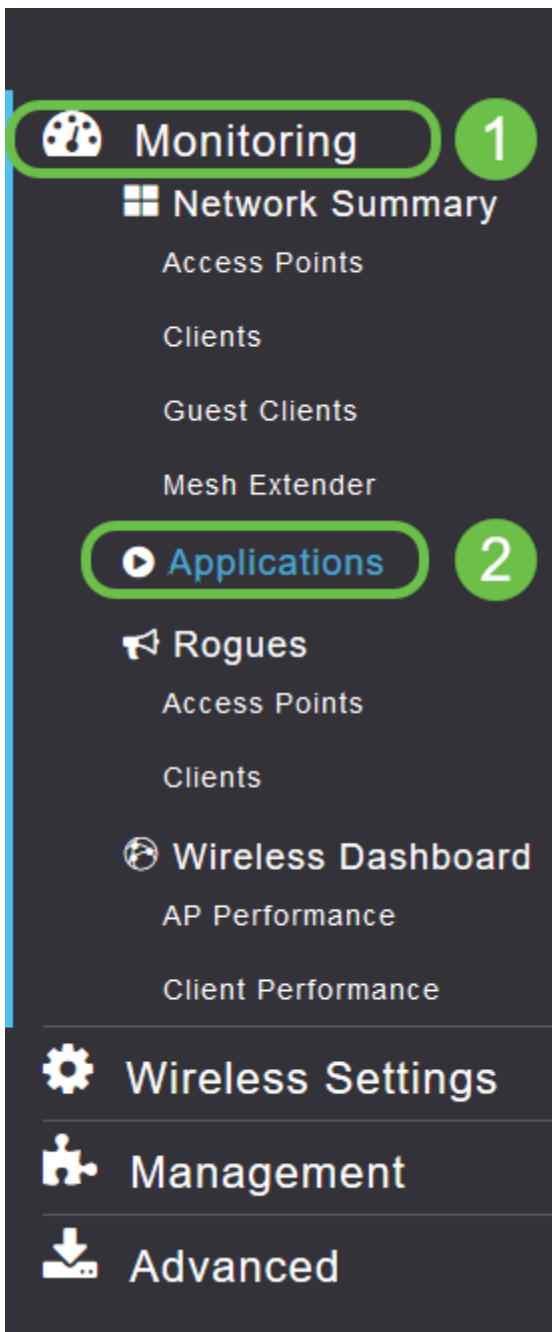
Fare clic sul pulsante **Applica**.



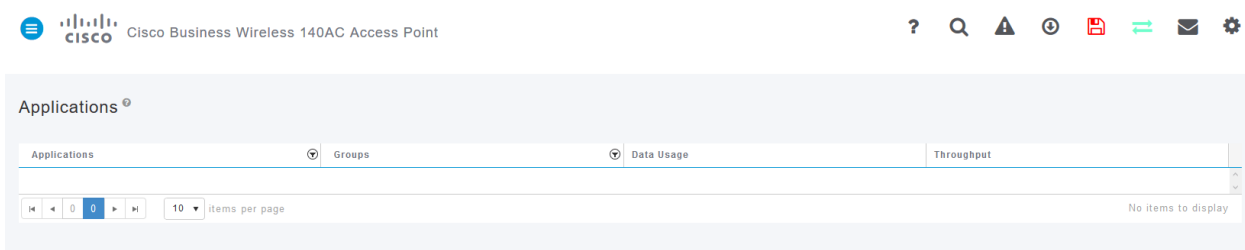
È necessario attivare questa impostazione, altrimenti la funzionalità non funzionerà.

## Passaggio 7

Fare clic sul pulsante Annulla per chiudere il sottomenu WLAN. Fare quindi clic sul menu **Monitoraggio** sulla barra dei menu a sinistra. Una volta completata l'operazione, fare clic sulla voce di menu **Applicazioni**.



Se non hai ricevuto traffico per nessuna fonte, la tua pagina sarà vuota come mostrato di seguito.



In questa pagina verranno visualizzate le informazioni seguenti:

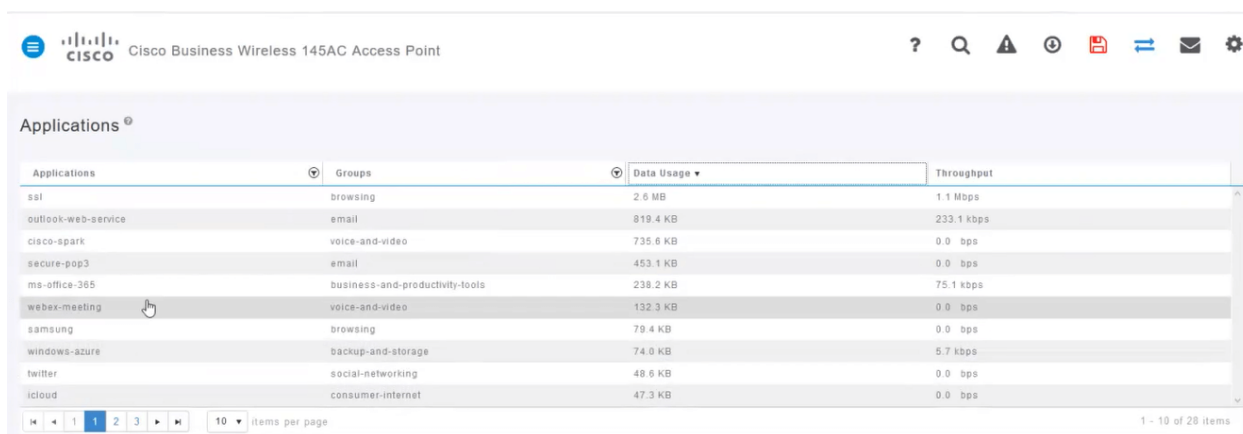
- Applicazione: include molti tipi diversi
- Gruppi: indica il tipo di gruppo di applicazioni per semplificare l'ordinamento
- Uso dati: la quantità di dati utilizzati da questo servizio nel complesso
- Throughput: quantità di larghezza di banda utilizzata dall'applicazione

È possibile fare clic sulle schede per eseguire l'ordinamento dal più grande al più piccolo, in modo da identificare gli utenti più grandi delle risorse di rete.

Questa funzionalità è molto potente per gestire le risorse WLAN a livello granulare. Di seguito sono riportati alcuni dei gruppi e dei tipi di applicazione più comuni. È probabile che l'elenco ne includa molti altri, inclusi i seguenti gruppi ed esempi:

- Esplorazione
  - ES: Specifico del client, SSL
- Email
  - ES: Outlook, Secure-pop3
- Voce e video
  - ES: WebEx, Cisco Spark,
- Strumenti per il business e la produttività
  - ES: Microsoft Office 365
- Backup e storage
  - ES: Windows-Azure
- Internet consumer
  - iCloud, Google Drive
- Social networking
  - ES: Twitter, Facebook
- Aggiornamenti software
  - ES: Google-Play, IOS
- Messaggistica immediata
  - ES: Hangouts, messaggi

Di seguito è riportato un esempio dell'aspetto della pagina quando viene compilata.



The screenshot shows the Cisco Business Wireless 145AC Access Point management interface. The page title is "Applications". Below the title is a table with the following columns: Applications, Groups, Data Usage, and Throughput. The table contains the following data:

Applications	Groups	Data Usage	Throughput
ssl	browsing	2.6 MB	1.1 Mbps
outlook-web-service	email	819.4 KB	233.1 kbps
cisco-spark	voice-and-video	735.6 KB	0.0 bps
secure-pop3	email	453.1 KB	0.0 bps
ms-office-365	business-and-productivity-tools	238.2 KB	75.1 kbps
webex-meeting	voice-and-video	132.3 KB	0.0 bps
samsung	browsing	79.4 KB	0.0 bps
windows-azure	backup-and-storage	74.0 KB	5.7 kbps
twitter	social-networking	48.6 KB	0.0 bps
icloud	consumer-internet	47.3 KB	0.0 bps

At the bottom of the table, there is a pagination control showing "10 items per page" and "1 - 10 of 28 items".

Ogni intestazione di tabella è selezionabile per l'ordinamento, il che è particolarmente utile per i campi *Use dati* e *Throughput*.

## Passaggio 8

Fare clic sulla riga relativa al tipo di traffico che si desidera gestire.



Cisco Business Wireless 145AC Access Point

Applications

Applications	Groups	Data Usage	Throughput
ssl	browsing	2.6 MB	1.1 Mbps
outlook-web-service	email	819.4 KB	233.1 kbps
cisco-spark	voice-and-video	735.6 KB	0.0 bps
secure-pop3	email	453.1 KB	0.0 bps
ms-office-365	business-and-productivity-tools	238.2 KB	75.1 kbps
webex-meeting	voice-and-video	132.3 KB	0.0 bps
samsung	browsing	79.4 KB	0.0 bps
windows-szure	backup-and-storage	74.0 KB	5.7 kbps
twitter	social-networking	48.6 KB	0.0 bps
icloud	consumer-internet	47.3 KB	0.0 bps

10 items per page 1 - 10 of 28 items

## Passaggio 9

Fare clic sulla casella a discesa **Azione** per selezionare la modalità di gestione del tipo di traffico.

Groups browsing Data Usage 2.6 MB

**Add AVC Rule**

Application icloud

Action **Mark**

DSCP Silver (Best Effort)

Select All

AVC Profile	WLAN SSID
<input type="checkbox"/> EZ1KWireless	EZ1KWireless
<input type="checkbox"/> CBWWireless	CBWWireless
<input type="checkbox"/> DEFAULT_RLAN	none

Apply Cancel

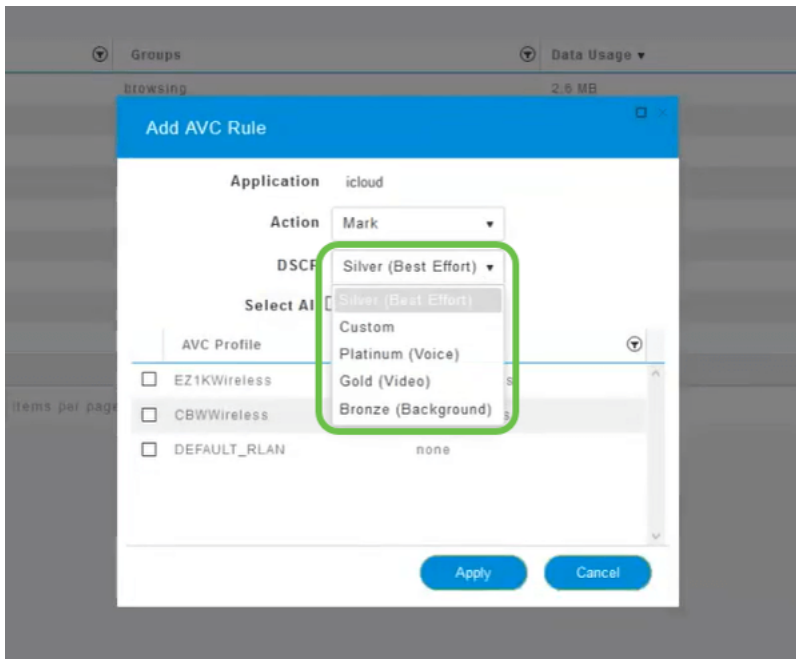
Nell'esempio, questa opzione viene lasciata a *Mark*.

Azione da intraprendere sul traffico

- Contrassegna: inserisce il tipo di traffico in uno dei 3 livelli DSCP (Differentiated Services Code Point), che definisce il numero di risorse disponibili per il tipo di applicazione
- Caduta: non fare altro che eliminare il traffico
- Limite velocità: consente di impostare la velocità media, burst rate in Kbps

## Passaggio 10

Fare clic sulla casella di riepilogo a discesa nel campo **DSCP** per selezionare una delle opzioni seguenti.



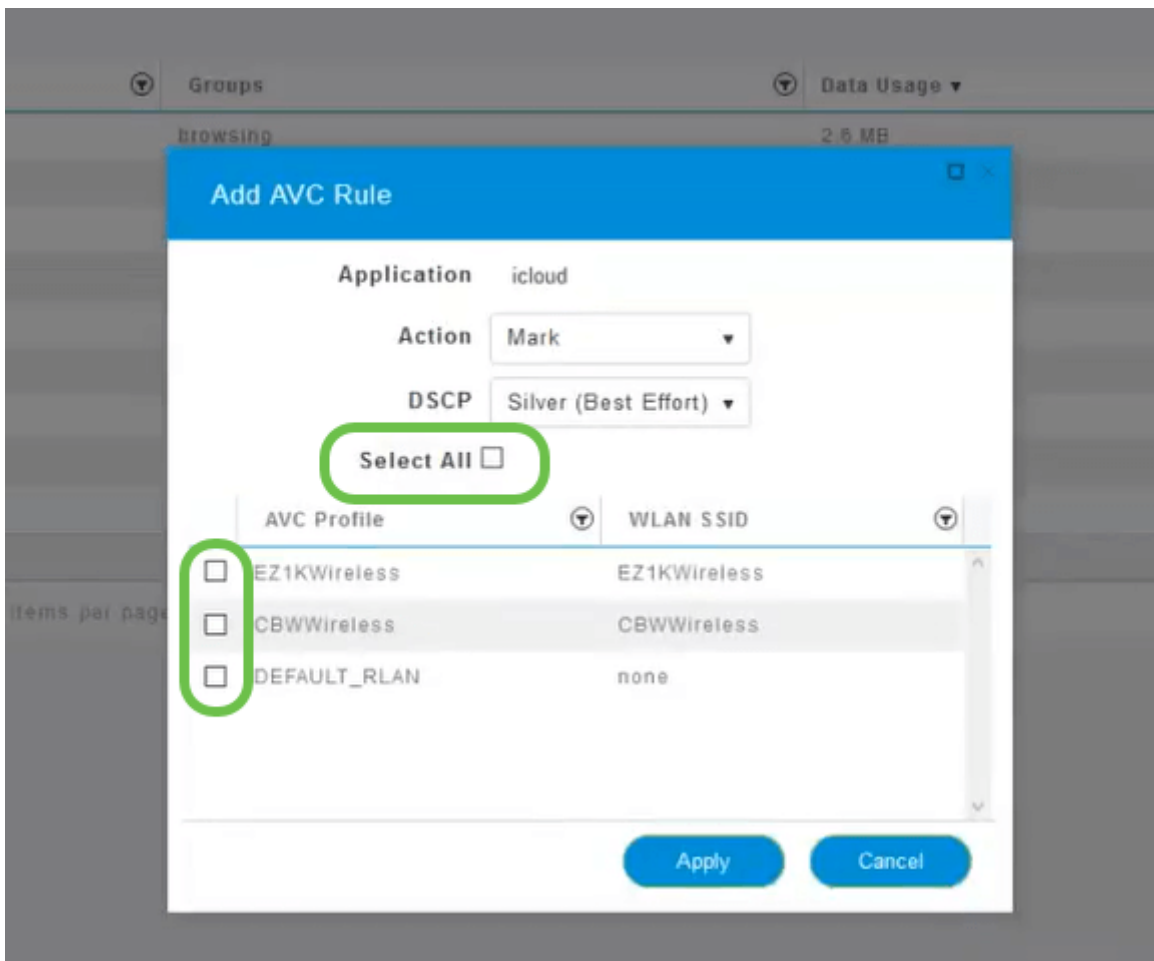
Di seguito sono riportate le opzioni DSCP per il traffico da contrassegnare. Queste opzioni consentono di passare da un numero inferiore di risorse a un numero maggiore di risorse disponibili per il tipo di traffico che si sta modificando.

- Bronzo (sfondo) - Meno
- Argento (massimo sforzo)
- Oro (video)
- Platinum (voce) - Altro
- Personalizzato - Set utenti

Per convenzione Web, il traffico è migrato verso l'esplorazione SSL, che impedisce di vedere il contenuto dei pacchetti quando vengono spostati dalla rete alla WAN. Pertanto, la maggior parte del traffico Web utilizzerà SSL. L'impostazione del traffico SSL per una priorità inferiore può influire sull'esplorazione.

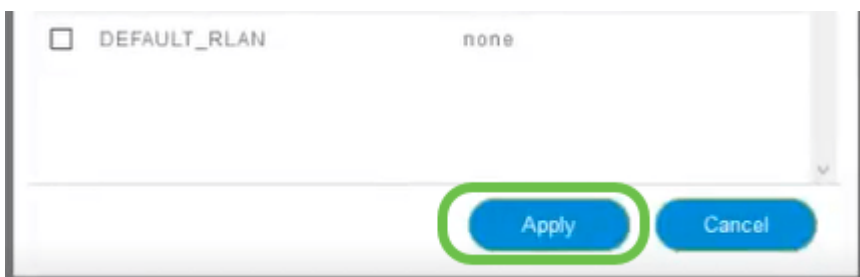
## Passaggio 11

Selezionare il singolo SSID che si desidera eseguire con questo criterio oppure fare clic su **Seleziona tutto**.



## Passaggio 12

Fare clic su **Applica** per iniziare il criterio.



Due casi in cui ciò potrebbe applicarsi:

- Guest/Utenti che gestiscono una grande quantità di traffico impedendo il passaggio del traffico mission-critical. Puoi aumentare la priorità per la voce, abbassare la priorità del traffico Netflix per migliorare le cose.
- Gli aggiornamenti software di grandi dimensioni che vengono scaricati durante l'orario di ufficio possono non essere considerati prioritari o avere una velocità limitata.

Ce l'hai fatta! La profilatura delle applicazioni è uno strumento molto potente che può essere ulteriormente abilitato attivando anche la profilatura client, come illustrato nella sezione successiva.

## Creazione profilo client tramite interfaccia utente Web (facoltativo)

Al momento della connessione a una rete, i dispositivi scambiano le informazioni di profilatura dei client. Per impostazione predefinita, la *profilatura client* è disabilitata. Tali informazioni possono includere:

- Nome host - o il nome del dispositivo
- Sistema operativo: il software principale del dispositivo
- Versione del sistema operativo: iterazione del software applicabile

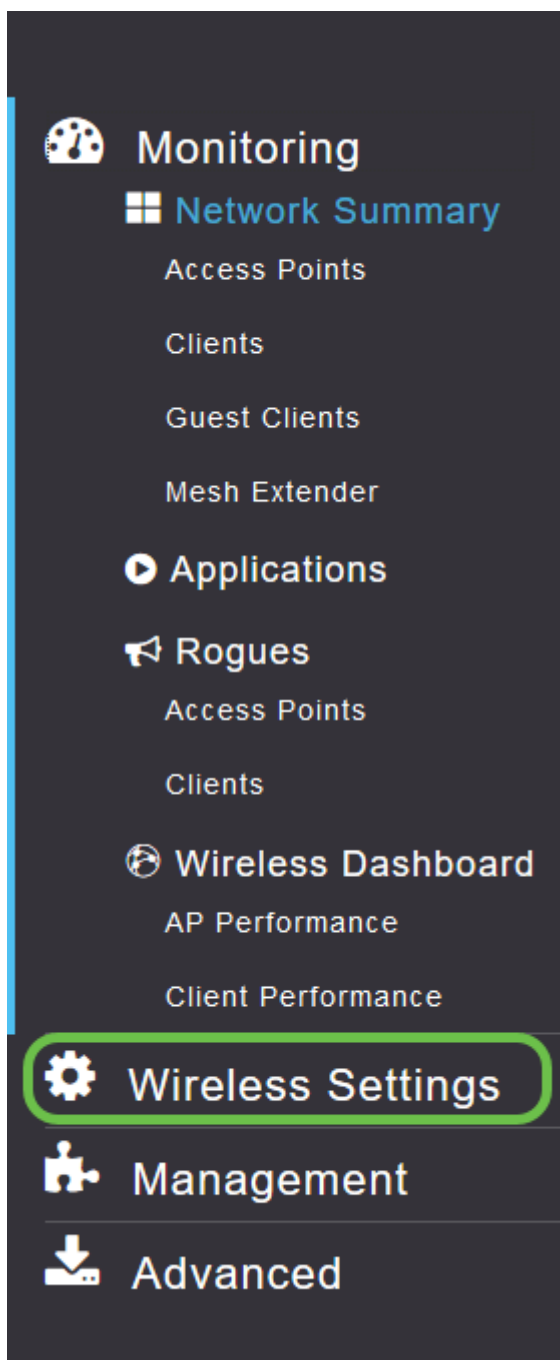
Le statistiche su questi client includono la quantità di dati utilizzati e il throughput.

La registrazione dei profili client consente un maggiore controllo sulla rete locale (LAN) wireless. Oppure potreste usarlo come funzione di un'altra feature. Ad esempio, utilizzando tipi di dispositivi di limitazione delle applicazioni che non contengono dati mission-critical per l'azienda.

Una volta abilitati, i dettagli client per la rete sono disponibili nella sezione Monitoraggio dell'interfaccia utente Web.

## Passaggio 1

Fare clic su **Impostazioni wireless**.



Le informazioni riportate di seguito sono simili a quelle visualizzate facendo clic sul collegamento Impostazioni wireless:

Monitoring  
Wireless Settings  
WLANs  
Access Points  
WLAN Users  
Guest WLANs  
Mesh  
Management  
Advanced

WLANs

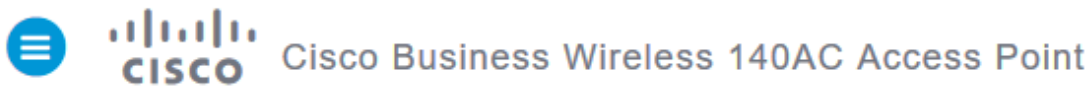
Active WLANs 1

Add new WLAN/RLAN

Action	Active	Type	Name	SSID	Security Policy	Radio Policy
	Enabled	WLAN	EZ1K	EZ1K	Personal(WPA2)	ALL

## Passaggio 2

Decidere quale WLAN usare per l'applicazione e fare clic sull'icona di modifica a sinistra di essa.



WLANs

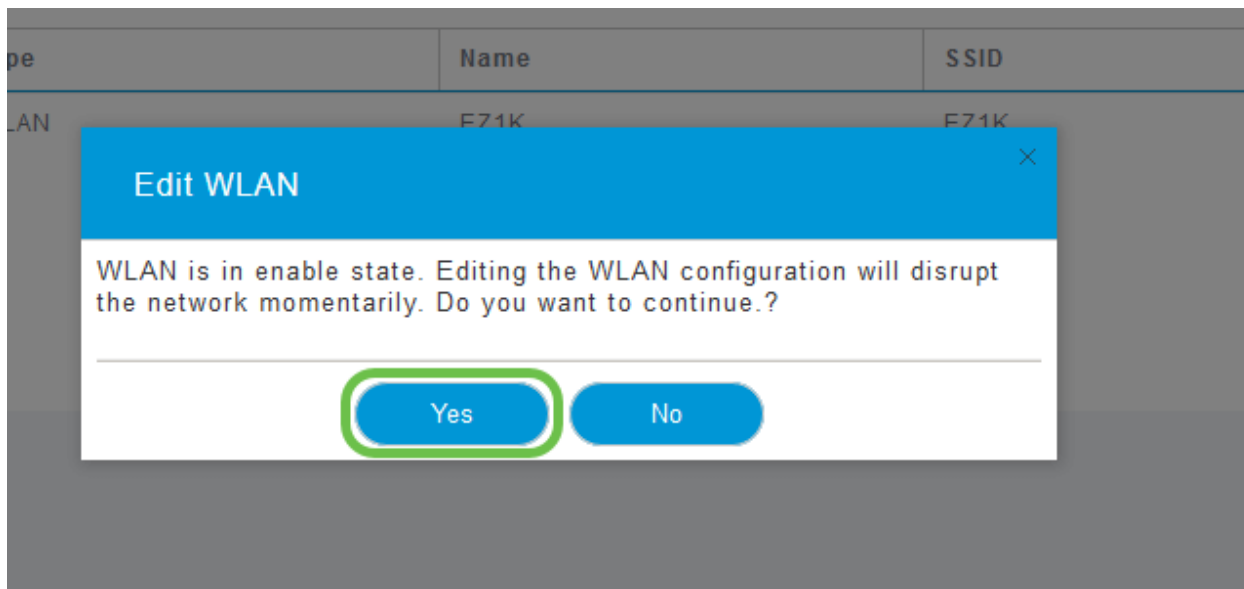
Active WLANs 1

Add new WLAN/RLAN

Action	Active	Type	Name	SSID	Security Policy	Radio Policy
	Enabled	WLAN	EZ1K	EZ1K	Personal(WPA2)	ALL

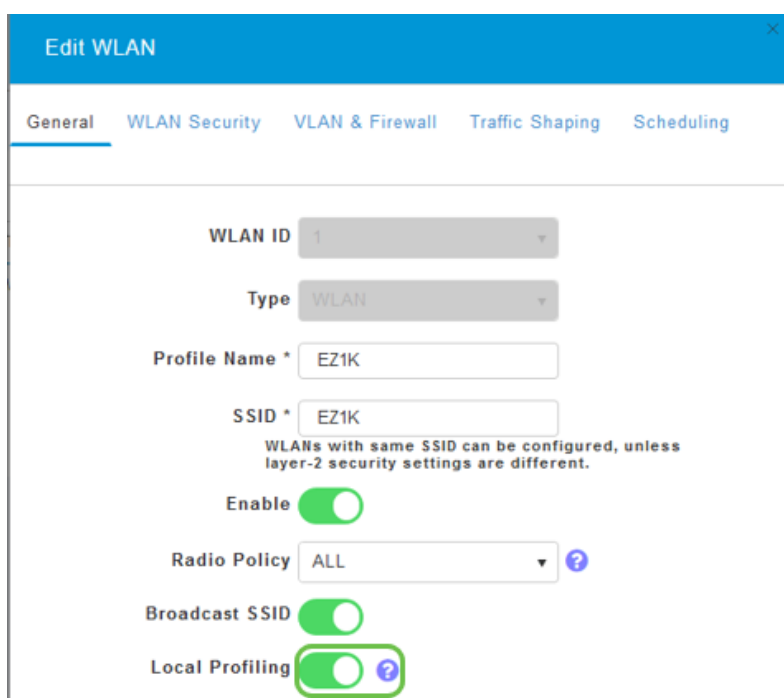
## Passaggio 3

È possibile che venga visualizzato un menu a comparsa simile al seguente. Questo messaggio importante può influire temporaneamente sul servizio di rete. Fare clic su **Sì** per procedere.



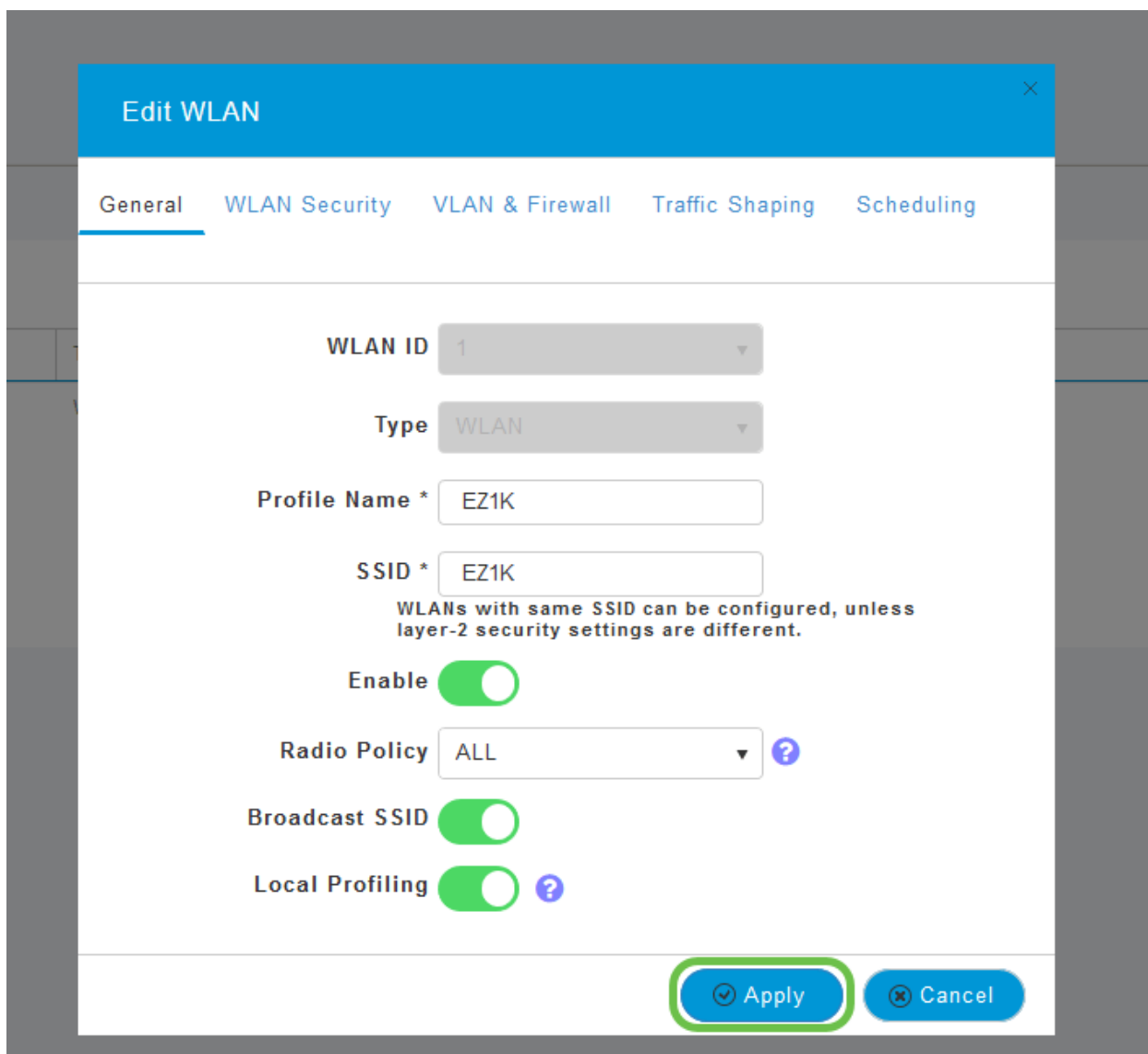
#### Passaggio 4

Attivare o disattivare la profilatura del client facendo clic sul pulsante **Profilatura locale**.



#### Passaggio 5

Fare clic su Apply (Applica).



## Passaggio 6

Fare clic sulla voce di menu della sezione **Monitoraggio** sul lato sinistro. I dati client verranno visualizzati nel dashboard della scheda *Monitoraggio*.

Client Identity	Device Type	Usage	Throughput
1 Anthony's-iPad	Apple-iPad	1.0 GB	260.3 bps
2 Galaxy-S9	Android-Samsung-Galax...	8.4 MB	1.2 kbps

## Conclusioni

La configurazione della rete protetta è stata completata. Che sensazione fantastica, ora prendi un minuto per festeggiare e poi vai al lavoro!

Vogliamo il meglio per i nostri clienti, quindi hai commenti o suggerimenti su questo argomento. Inviaci un'e-mail al [team dei contenuti Cisco](#).

Per leggere altri articoli e documentazione, consultare le pagine di supporto dell'hardware:



- [Cisco RV260P VPN Router con PoE](#)
- [Access point Cisco Business 140AC](#)
- [Cisco Business 142ACM Mesh Extender](#)