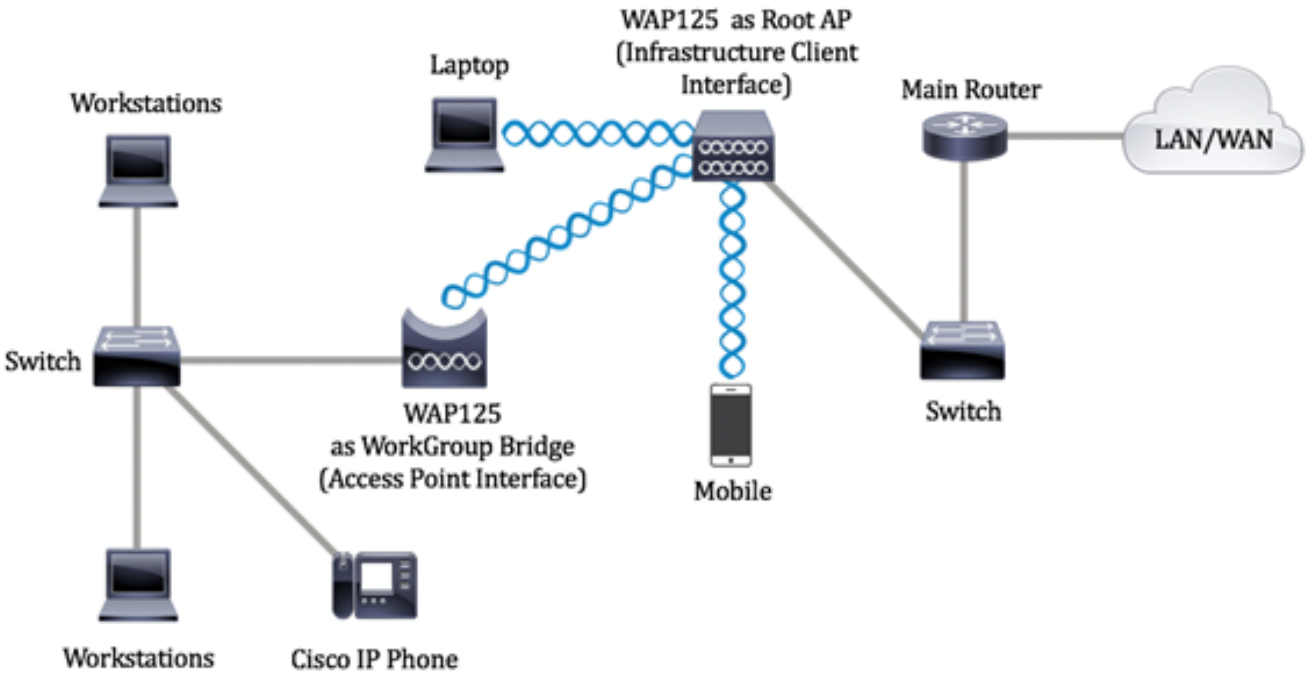
Configurazione delle impostazioni di WorkGroup Bridge sui punti di accesso WAP125 o WAP581

Obiettivo

La funzionalità Bridge per gruppi di lavoro consente al punto di accesso wireless (WAP) di collegare il traffico tra un client remoto e la LAN wireless connessa alla modalità Bridge per gruppi di lavoro. Il dispositivo WAP associato all'interfaccia remota è noto come interfaccia del punto di accesso, mentre il dispositivo WAP associato alla LAN wireless è noto come interfaccia dell'infrastruttura. WorkGroup Bridge consente ai dispositivi che dispongono solo di connessioni cablate di connettersi a una rete wireless. La modalità bridge per gruppi di lavoro è consigliata come alternativa quando la funzionalità WDS (Wireless Distribution System) non è disponibile.

La topologia riportata di seguito illustra un modello di esempio di WorkGroup Bridge. I dispositivi cablati sono collegati a uno switch che si connette all'interfaccia LAN del WAP. Nell'esempio seguente, il WAP125 funge da interfaccia di punto di accesso per la connessione all'interfaccia client dell'infrastruttura.



In questo documento viene spiegato come configurare le impostazioni di WorkGroup Bridge tra due punti di accesso wireless.

Dispositivi interessati

- WAP125
- WAP581

Versione del software

- 1.0.0.4 — WAP581

- 1.0.0.5 — WAP125

Configura impostazioni bridge gruppo di lavoro

Prima di configurare Work Group Bridge sul dispositivo WAP, tenere presenti le seguenti linee guida:

- Tutti i dispositivi WAP che partecipano a WorkGroup Bridge devono avere le seguenti impostazioni identiche:

-Radio

- Modalità IEEE 802.11

- Larghezza di banda del canale

- Canale (si sconsiglia l'impostazione automatica)

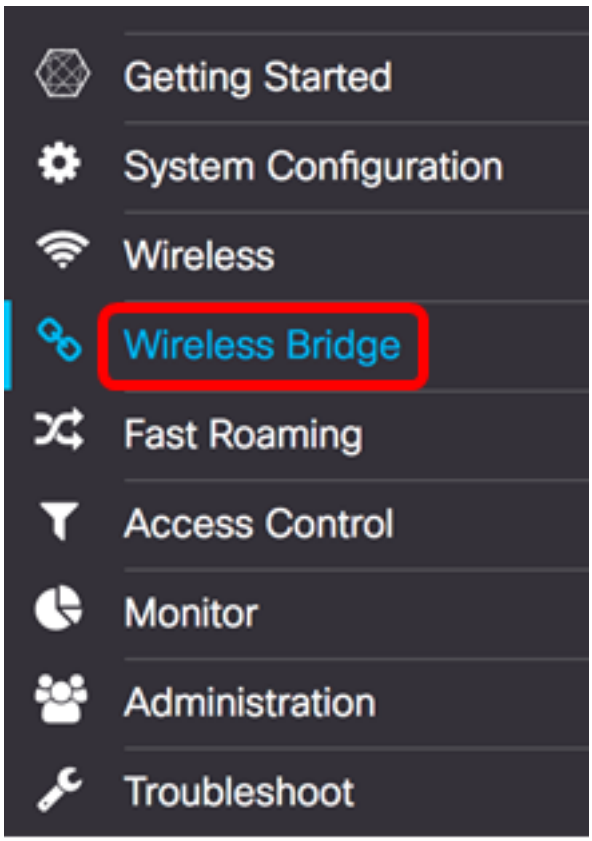
Nota: per informazioni su come configurare queste impostazioni in WAP125, fare clic qui per istruzioni. Per WAP581, fare clic qui.

- La modalità bridge per gruppi di lavoro attualmente supporta solo il traffico IPv4.
- La modalità bridge per gruppi di lavoro non è supportata in una configurazione con punto di accesso singolo. Se si dispone di punti di accesso WAP581, disabilitare SPS o il clustering prima di configurare le impostazioni di Bridge per gruppi di lavoro. Per istruzioni su come configurare le impostazioni dell'SPS sul WAP, fare clic qui.

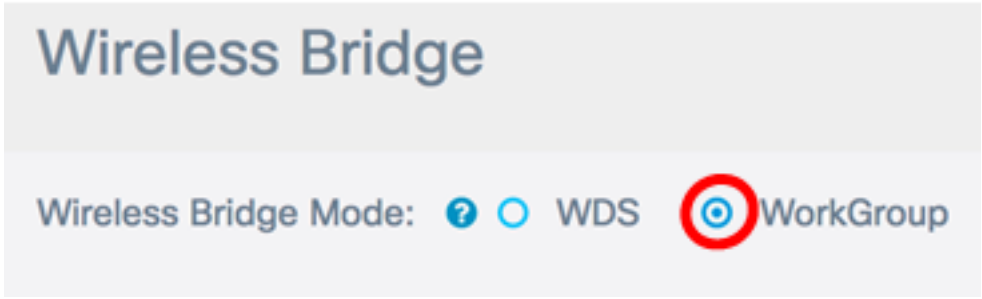
Configurazione interfaccia client infrastruttura

Passaggio 1. Accedere all'utilità basata sul Web di WAP, quindi scegliere **Wireless Bridge**.

Nota: Le opzioni disponibili possono variare a seconda del modello esatto del dispositivo. Nell'esempio viene utilizzato WAP125.



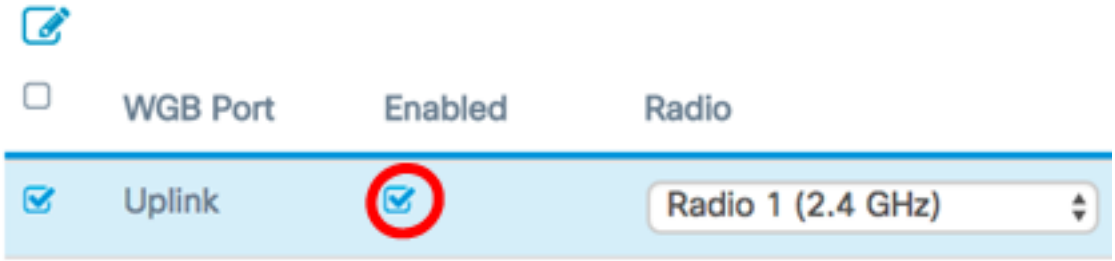
Passaggio 2. Fare clic sul pulsante di opzione **Gruppo di lavoro**.



Passaggio 3. Selezionare la casella di controllo **Uplink**.

Passaggio 4. Fare clic sull'icona **Modifica**.

Passaggio 5. Selezionare la casella di controllo **Abilitato** per abilitare l'interfaccia client dell'infrastruttura.



Passaggio 6. Scegliere l'interfaccia radio per WorkGroup Bridge. Quando si configura una radio come bridge per gruppi di lavoro, l'altra radio rimane operativa. Le interfacce radio corrispondono alle bande di radiofrequenza del WAP. Il WAP è in grado di trasmettere su due diverse interfacce radio. La configurazione delle impostazioni per un'interfaccia radio non influirà sull'altra.

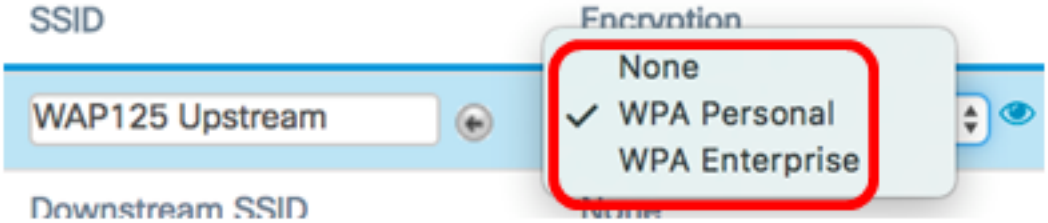
Nota: Nell'esempio, viene scelto Radio 2 (5 GHz).

Passaggio 7. Immettere il nome dell'identificatore del set di servizi (SSID) nel campo *SSID*. Questa funzione funge da connessione tra il dispositivo e il client remoto. È possibile immettere da 2 a 32 caratteri per l'SSID del client di infrastruttura.

Nota: Nell'esempio viene utilizzato WAP125 Upstream.

Nota: La freccia accanto a SSID è disponibile per la scansione SSID. Questa funzione è disabilitata per impostazione predefinita ed è abilitata solo se il rilevamento dei punti di accesso è abilitato in Rilevamento punti di accesso non autorizzati, anch'esso disabilitato per impostazione predefinita.

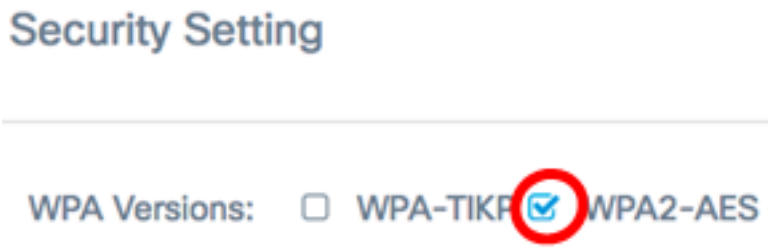
Passaggio 8. Selezionare il tipo di protezione da autenticare come stazione client sul dispositivo WAP upstream dall'elenco a discesa Crittografia. Le opzioni sono:



- Nessuno — Aprire o non impostare la protezione. Questa è l'impostazione predefinita. Se si sceglie questa opzione, andare al passo 22.
- WPA personale: WPA personale può supportare chiavi di lunghezza compresa tra 8 e 63 caratteri. Si consiglia WPA2 in quanto offre uno standard di crittografia più potente.
- WPA Enterprise: WPA Enterprise è più avanzato di WPA Personal e rappresenta la protezione consigliata per l'autenticazione. Utilizza PEAP (Protected Extensible Authentication Protocol) e TLS (Transport Layer Security). Andare al passo 12 per configurare. Questo tipo di protezione viene spesso utilizzato in un ambiente di ufficio e richiede la configurazione di un server RADIUS (Remote Authentication Dial-In User Service). Per ulteriori informazioni sui server RADIUS, fare clic qui.

Nota: In questo esempio viene scelto WPA Personal.

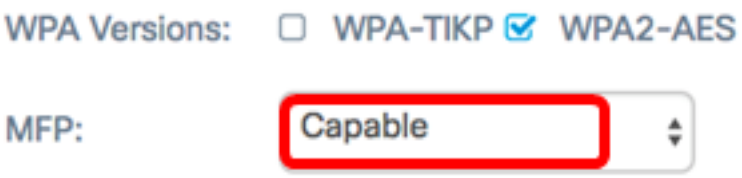
Passaggio 9. Fare clic sull' icona e selezionare la casella di controllo WPA-TKIP o WPA2-AES per determinare il tipo di crittografia WPA che verrà utilizzato dall'interfaccia client dell'infrastruttura.



Nota: Se tutte le apparecchiature wireless supportano WPA2, impostare la protezione del client dell'infrastruttura su WPA2-AES. Il metodo di crittografia è RC4 per WPA e AES (Advanced Encryption Standard) per WPA2. WPA2 è consigliato perché ha uno standard di crittografia più potente. Nell'esempio viene utilizzato WPA2-AES.

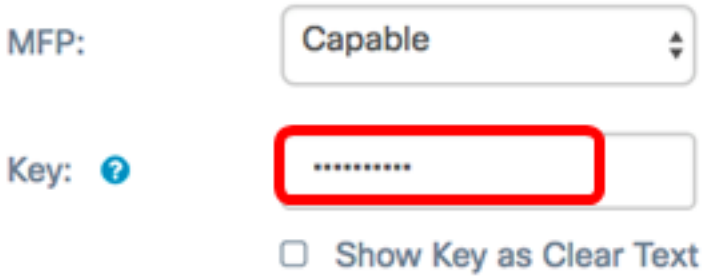
Passaggio 10. (Facoltativo) Se è stato selezionato WPA2-AES nel passaggio 9, scegliere un'opzione dall'elenco a discesa Management Frame Protection (MFP) per richiedere o meno che WAP abbia frame protetti. Per ulteriori informazioni sulla stampante multifunzione, fare clic qui. Le opzioni sono:

- Non richiesto: disabilita il supporto client per le stampanti multifunzione.
- Funzionalità: consente ai client che supportano le funzionalità MFP e a quelli che non le supportano di collegarsi alla rete. Si tratta dell'impostazione predefinita per le stampanti multifunzione in WAP.
- Obbligatorio: i client possono associarsi solo se viene negoziata l'interfaccia MFP. Se i dispositivi non supportano la funzionalità PMF, non potranno collegarsi alla rete.



Nota: Nell'esempio riportato di seguito, viene selezionato Capable.

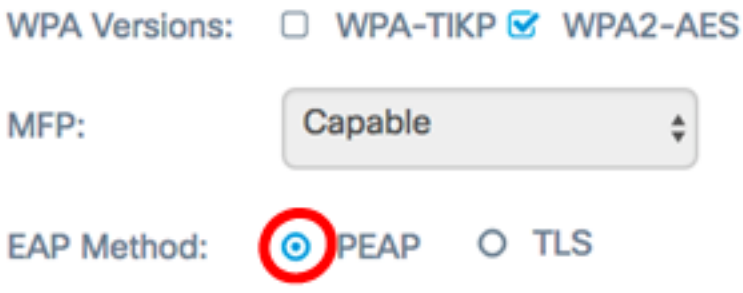
Passaggio 11. Immettere la chiave di crittografia WPA nel campo *Chiave*. La chiave deve avere una lunghezza compresa tra 8 e 63 caratteri. È una combinazione di lettere, numeri e caratteri speciali. Si tratta della password utilizzata per la prima connessione alla rete wireless. Quindi, andare al Passaggio 21.



Passaggio 12. Se nel passaggio 8 è stata scelta l'organizzazione WPA, fare clic su un pulsante di opzione per il metodo EAP.

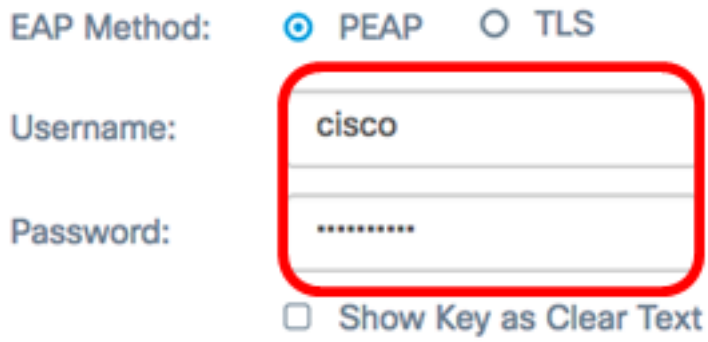
Le opzioni disponibili sono definite come segue:

- PEAP: questo protocollo fornisce a ciascun utente wireless i nomi utente e le password WAP individuali che supportano gli standard di crittografia AES. Poiché PEAP è un metodo di protezione basato su password, la protezione Wi-Fi si basa sulle credenziali della periferica del client. PEAP può rappresentare un rischio potenziale per la sicurezza se si dispone di password poco sicure o di client non protetti. Si basa su TLS ma evita l'installazione di certificati digitali su ogni client. Fornisce invece l'autenticazione tramite un nome utente e una password.
- TLS: ogni utente deve disporre di un certificato aggiuntivo per poter accedere. TLS è più sicuro se si dispone di server aggiuntivi e dell'infrastruttura necessaria per autenticare gli utenti nella rete. Se si sceglie questa opzione, andare al passo 14.

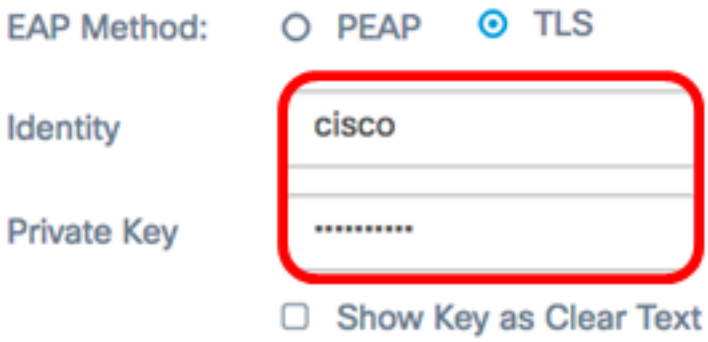


Nota: Per questo esempio, viene scelto PEAP.

Passaggio 13. Immettere il nome utente e la password per il client dell'infrastruttura nei campi Nome utente e Password. Si tratta delle informazioni di accesso utilizzate per connettersi all'interfaccia client dell'infrastruttura; per ulteriori informazioni, consultare l'interfaccia client dell'infrastruttura. Quindi, andare al Passaggio 21.

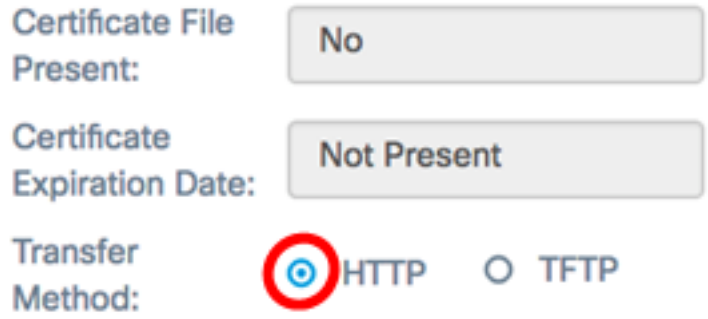


Passaggio 14. Se si è fatto clic su TLS nel passaggio 12, immettere l'identità e la chiave privata del client dell'infrastruttura nei campi Identità e Chiave privata.



Passaggio 15. Nell'area Metodo di trasferimento, fare clic su uno dei seguenti pulsanti di opzione:

- TFTP — Trivial File Transfer Protocol (TFTP) è una versione semplificata non protetta del protocollo FTP (File Transfer Protocol). Viene utilizzato principalmente per distribuire software o autenticare dispositivi tra le reti aziendali. Se è stato selezionato TFTP, andare al passo 18.
- HTTP: il protocollo HTTP (Hypertext Transfer Protocol) fornisce una semplice struttura di autenticazione in attesa/risposta che può essere utilizzata da un client per fornire la struttura di autenticazione.



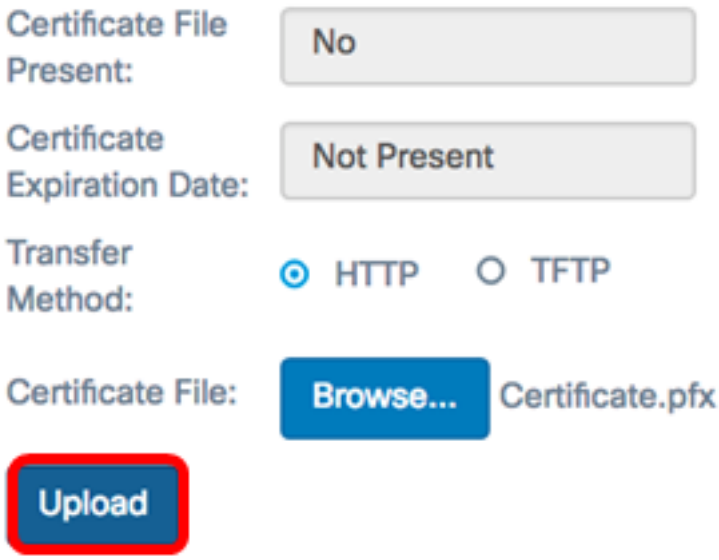
Nota: Se un file di certificato è già presente nel WAP, nei campi File di certificato presente e Data scadenza certificato verranno già inserite le informazioni pertinenti. In caso contrario, saranno vuote.

HTTP

Passaggio 16. Fare clic sul pulsante **Sfoglia** per individuare e selezionare un file di certificato. Il file deve avere l'estensione corretta (ad esempio, .pem o .pfx). In caso contrario, il file non verrà accettato.

Nota: In questo esempio viene scelto Certificate.pfx.

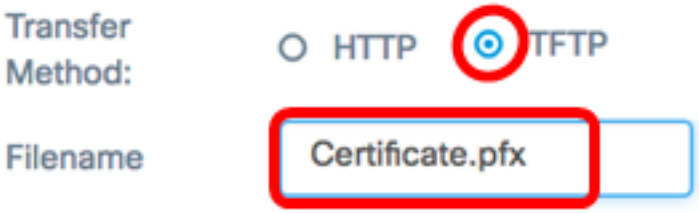
Passaggio 17. Fare clic su **Upload** per caricare il file di certificato selezionato. Andare al passo 21.



I campi File certificato presente e Data scadenza certificato verranno aggiornati automaticamente.

TFTP

Passaggio 18. (Facoltativo) Se si è fatto clic su TFTP al passaggio 15, immettere il nome del file del certificato nel campo *Nome file*.



Nota: Nell'esempio viene utilizzato Certificate.pfx.

Passaggio 19. Immettere l'indirizzo del server TFTP nel campo *Indirizzo IPv4 server TFTP*.

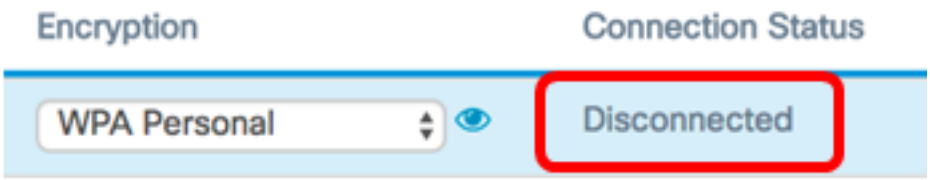
Nota: In questo esempio. 192.168.100.108 viene utilizzato come indirizzo del server TFTP.

Passaggio 20. Fare clic sul pulsante **Upload** per caricare il file di certificato specificato.

I campi File certificato presente e Data scadenza certificato verranno aggiornati automaticamente.

Passaggio 21. Fare clic su **OK** per chiudere la finestra Impostazioni protezione.

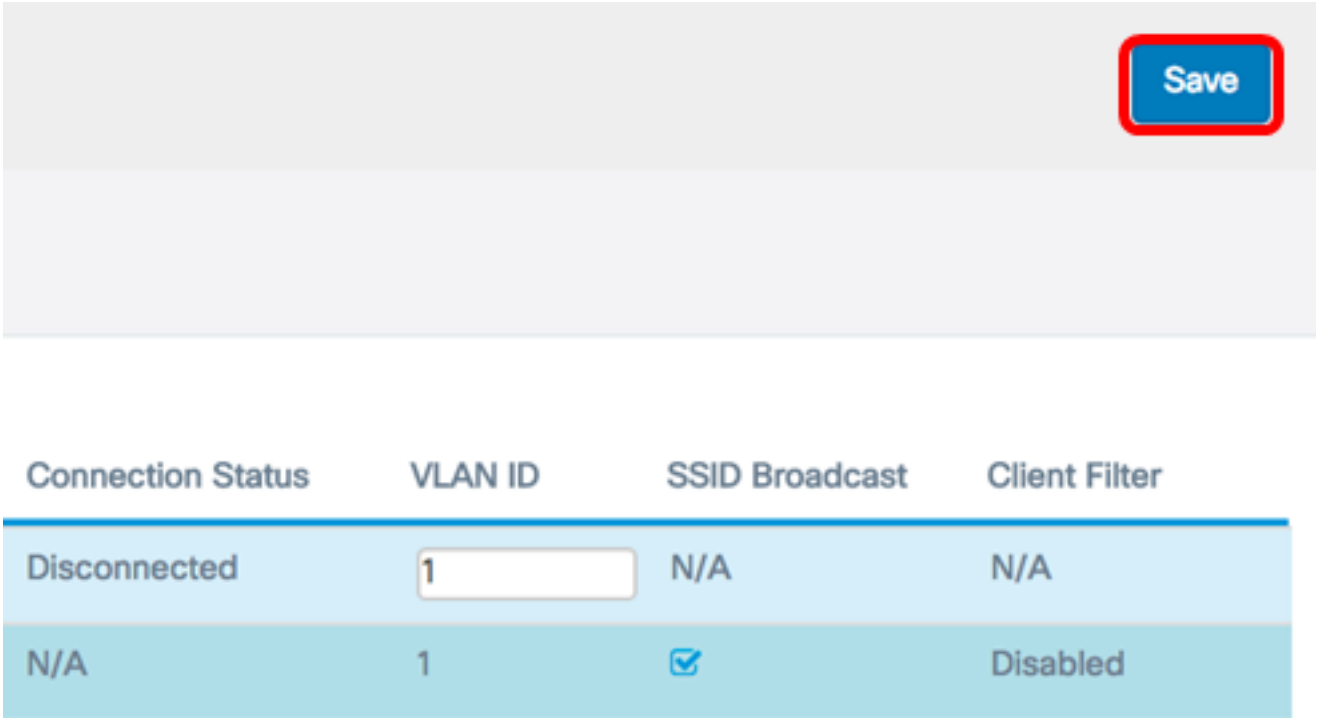
L'area Stato connessione indica se il dispositivo WAP è collegato al dispositivo WAP a monte.



Passaggio 22. Immettere l'ID VLAN per l'interfaccia client dell'infrastruttura. Il valore predefinito è 1.

Nota: Nell'esempio, viene usato l'ID VLAN predefinito.

Passaggio 23. Fare clic su **Save** per salvare le impostazioni configurate.

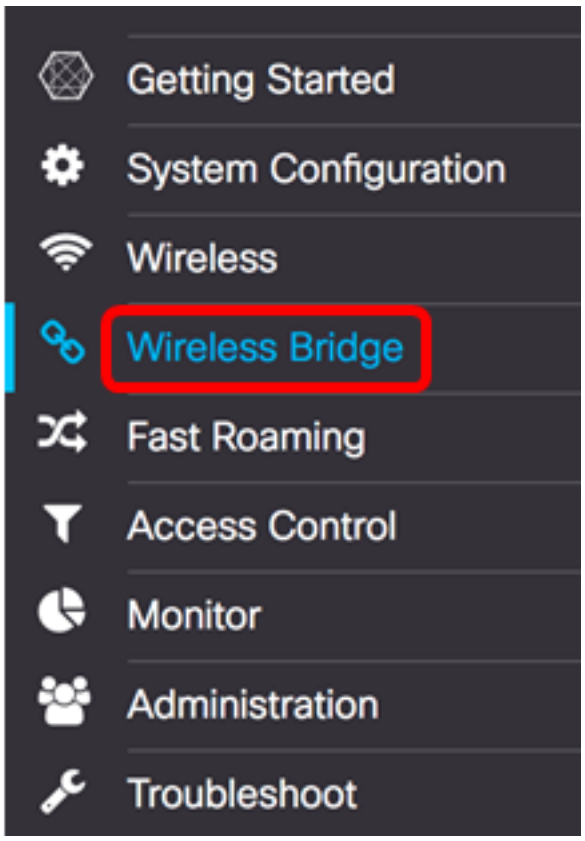


A questo punto, è necessario configurare correttamente le impostazioni dell'interfaccia client dell'infrastruttura sul WAP.

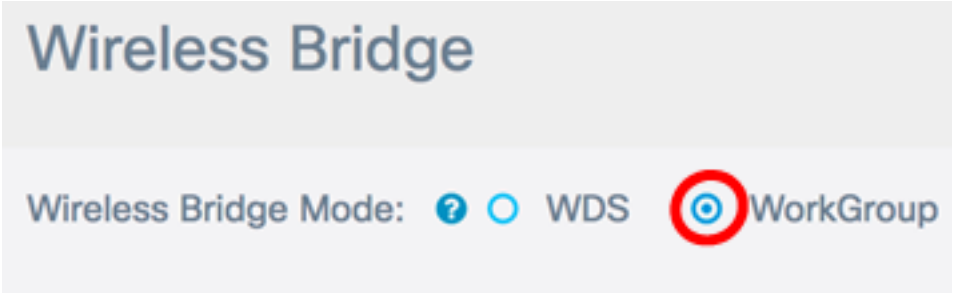
Configura interfaccia client Access Point

Passaggio 1. Accedere all'utilità basata sul Web di WAP, quindi scegliere **Wireless Bridge**.

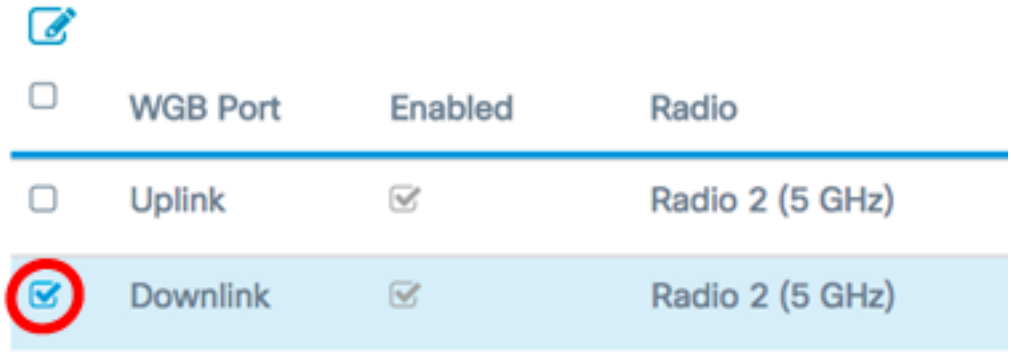
Nota: Le opzioni disponibili possono variare a seconda del modello esatto del dispositivo. Nell'esempio viene utilizzato WAP125.



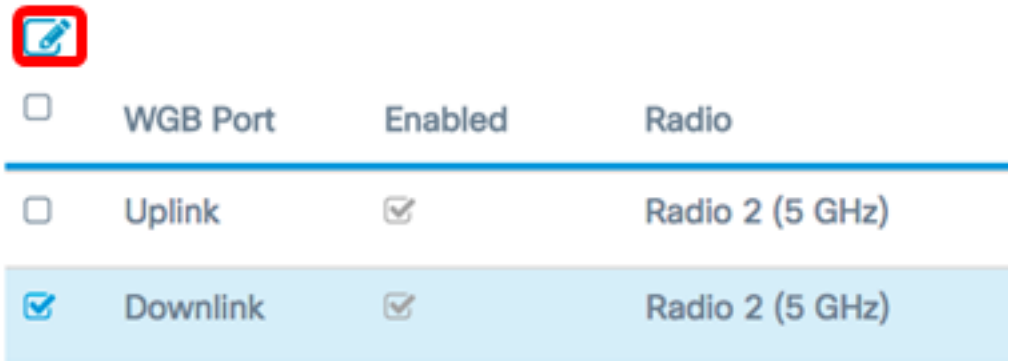
Passaggio 2. Fare clic sul pulsante di opzione **Gruppo di lavoro**.



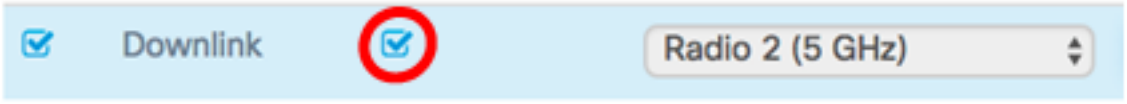
Passaggio 3. Selezionare la casella di controllo **Downlink**.



Passaggio 4. Fare clic sul pulsante **Modifica**.



Passaggio 5. Selezionare la casella di controllo **Abilitato** per abilitare il bridging sull'interfaccia del punto di accesso.



Passaggio 6. Immettere il SSID del punto di accesso nel campo *SSID*. La lunghezza SSID deve essere compresa tra 2 e 32 caratteri. Il valore predefinito è Downstream SSID.

Nota: Per questo esempio, l'SSID utilizzato è WAP125 Downstream.

Passaggio 7. Scegliere il tipo di sicurezza per autenticare le stazioni client downstream nel WAP dall'elenco a discesa Sicurezza.

Le opzioni disponibili sono definite come segue:

- Nessuno — Aprire o non proteggere. Questo è il valore predefinito. Se si sceglie questa opzione, andare al passo 13.
- WPA Personal — WPA (Wi-Fi Protected Access) Personal può supportare chiavi da 8 a 63 caratteri. Il metodo di crittografia è TKIP o la modalità Counter Cipher con il protocollo CCMP (Block Chaining Message Authentication Code Protocol). Si consiglia WPA2 con CCMP in quanto offre uno standard di crittografia più potente, AES (Advanced Encryption Standard), rispetto al protocollo TKIP (Temporal Key Integrity Protocol) che utilizza solo uno standard RC4 a 64 bit.

Passaggio 8. (Facoltativo) Selezionare la casella di controllo WPA-TKIP per determinare la crittografia WPA-TKIP che verrà utilizzata dall'interfaccia del punto di accesso. L'opzione è abilitata per impostazione predefinita.

Nota: WPA-AES è disattivato. Nell'esempio, WPA-TKIP è deselezionato.

Passaggio 9. Immettere la chiave WPA condivisa nel campo Chiave. La chiave deve contenere da 8 a 63 caratteri e può includere caratteri alfanumerici, maiuscoli e minuscoli e caratteri speciali.

Passaggio 10. Inserire il tasso nel campo Tasso di aggiornamento chiave trasmissione. La frequenza di aggiornamento della chiave di trasmissione specifica l'intervallo di aggiornamento della chiave di protezione per i client associati a questo punto di accesso. La velocità deve essere compresa tra 0 e 86400, con un valore pari a 0 per disattivare la funzionalità.

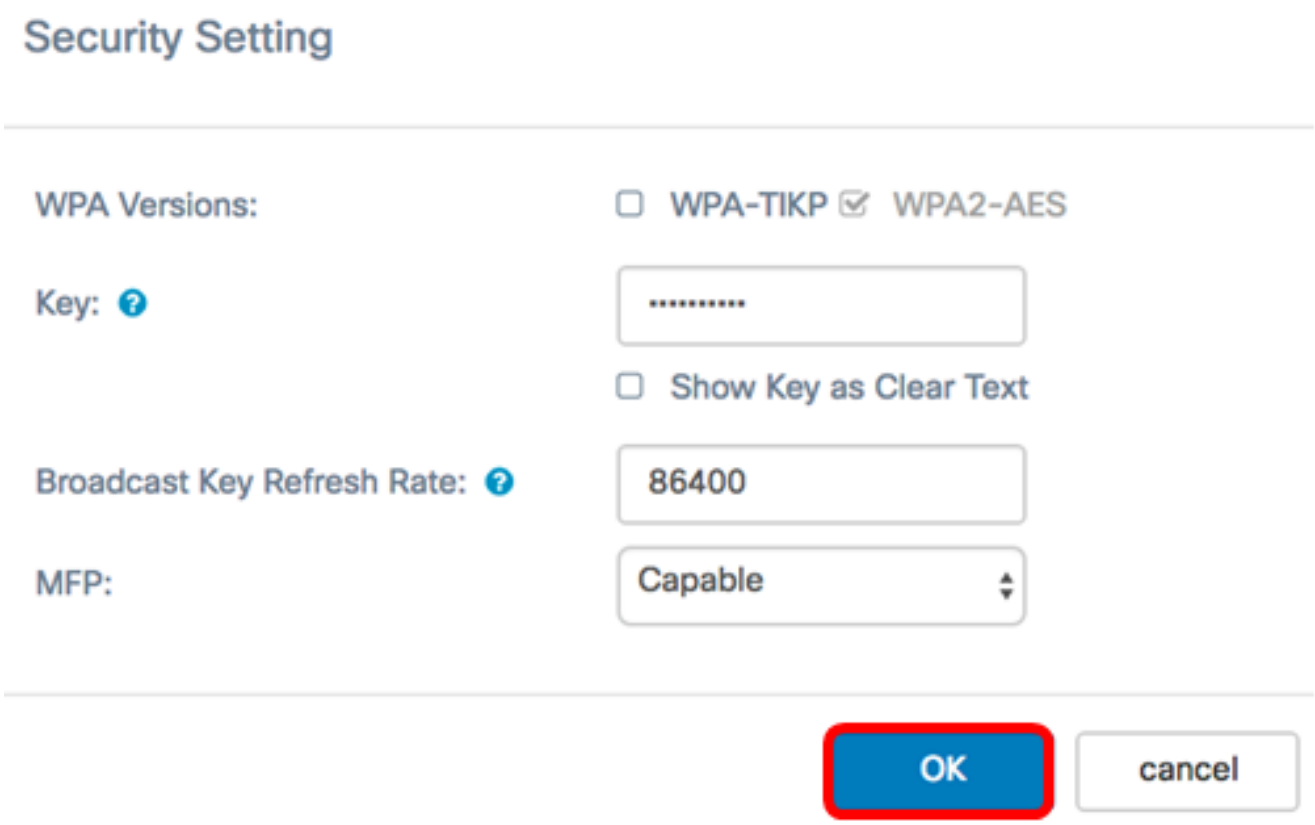
Nota: nell'esempio viene usato 86400.

Passaggio 11. Scegliere un'opzione dall'elenco a discesa Protezione file Windows per richiedere o meno la protezione dei frame. Per ulteriori informazioni sulla stampante multifunzione, fare clic qui. Le opzioni sono:

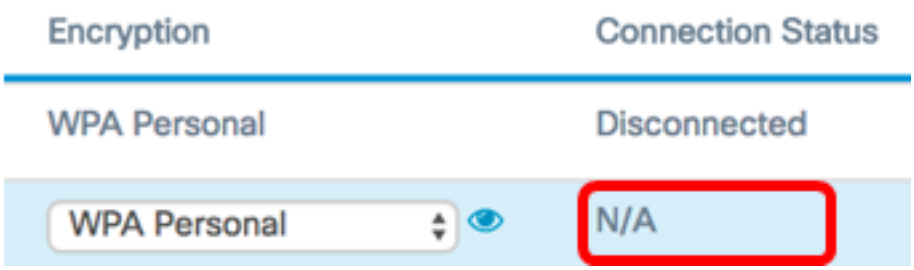
- Non richiesto: disabilita il supporto client per le stampanti multifunzione.
- Funzionalità: consente ai client che supportano le funzionalità MFP e a quelli che non le supportano di collegarsi alla rete. Si tratta dell'impostazione predefinita per le stampanti multifunzione in WAP.
- Obbligatorio: i client possono associarsi solo se viene negoziata l'interfaccia MFP. Se i dispositivi non supportano la funzionalità PMF, non potranno collegarsi alla rete.

Nota: Per questo esempio, viene scelto Capable.

Passaggio 12. Fare clic su **OK** per salvare le impostazioni di protezione.



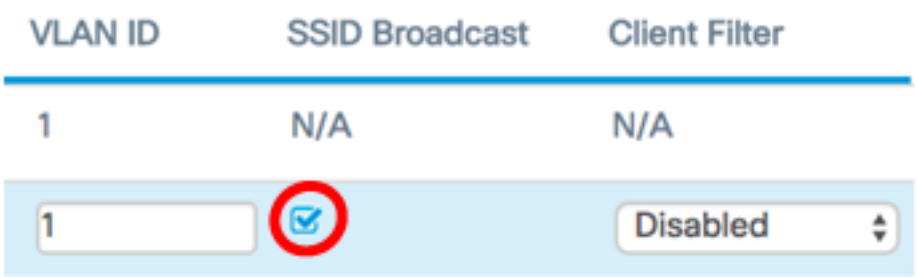
L'area Stato connessione indica Non applicabile o N/D.



Passaggio 13. Immettere l'ID VLAN nel campo VLAN ID per l'interfaccia del punto di accesso.

Nota: Per consentire il bridging dei pacchetti, la configurazione VLAN dell'interfaccia del punto di accesso e dell'interfaccia cablata deve corrispondere a quella dell'interfaccia del client dell'infrastruttura.

Passaggio 14. Selezionare la casella di controllo Trasmissione SSID se si desidera trasmettere il SSID downstream. La trasmissione SSID è abilitata per impostazione predefinita.



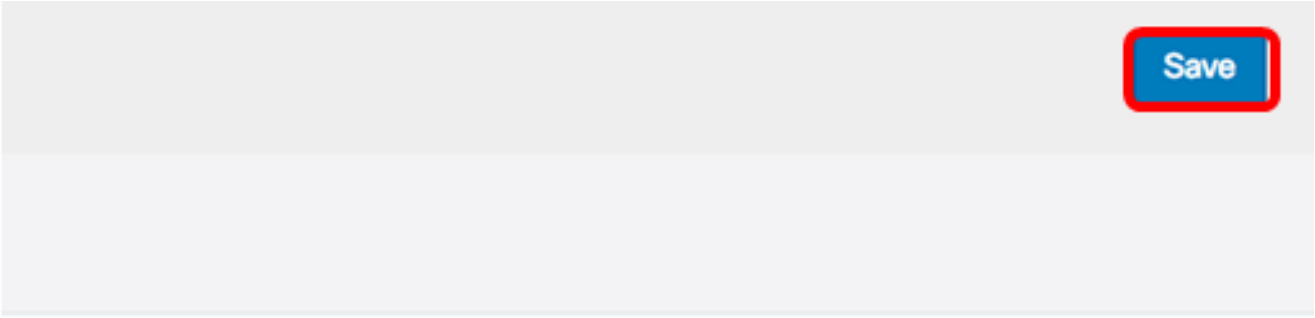
Passaggio 15. Selezionare il tipo di filtro MAC che si desidera configurare per l'interfaccia del punto di accesso dall'elenco a discesa Filtro MAC. Quando questa opzione è abilitata, agli utenti viene concesso o negato l'accesso al WAP in base all'indirizzo MAC del client utilizzato.

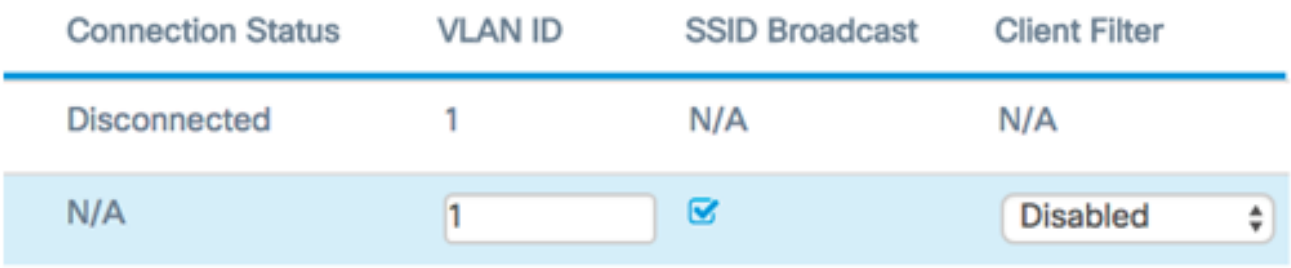
Le opzioni disponibili sono definite come segue:

- Disabilitato: tutti i client possono accedere alla rete a monte. Questo è il valore predefinito.
- Locale: l'insieme di client che possono accedere alla rete a monte è limitato ai client specificati in un elenco indirizzi MAC definito localmente.
- RADIUS: l'insieme di client che possono accedere alla rete upstream è limitato ai client specificati in un elenco indirizzi MAC su un server RADIUS.

Nota: Nell'esempio riportato di seguito, viene selezionato Disabilitato.

Passaggio 16. Fare clic su **Salva** per salvare le modifiche.





Èora necessario configurare correttamente le impostazioni di WorkGroup Bridge nei punti di accesso wireless.