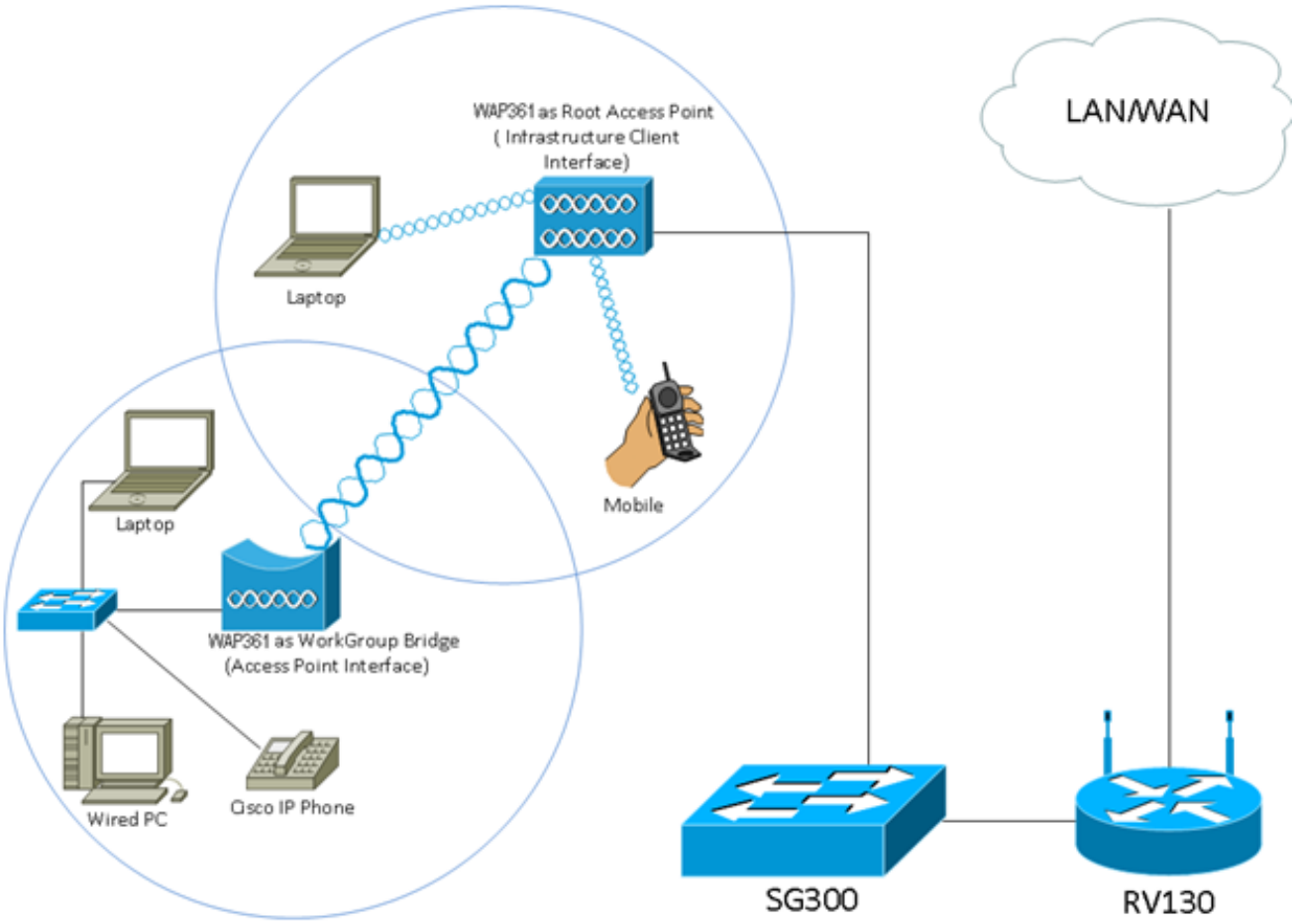
Configurare Workgroup Bridge su un punto di accesso wireless (WAP)

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 rete 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 non è disponibile.



Nota: la topologia sopra riportata illustra un modello di esempio di WorkGroup Bridge. I dispositivi cablati sono collegati a uno switch, che si connette all'interfaccia LAN del WAP. Il WAP agisce come interfaccia di un punto di accesso e si connette all'interfaccia dell'infrastruttura.

In questo articolo viene illustrato come configurare il bridge per gruppi di lavoro tra due punti di accesso WAP.

Dispositivi interessati

- Serie WAP100
- Serie WAP300
- Serie WAP500

Versione del software

- 1.0.0.17 — WAP571, WAP571E
- 1.0.1.7 — WAP150, WAP361
- 1.0.2.5 — WAP131, WAP351
- 1.0.6.5 — WAP121, WAP321
- 1.2.1.3 — WAP551, WAP561
- 1.3.0.3 — WAP371

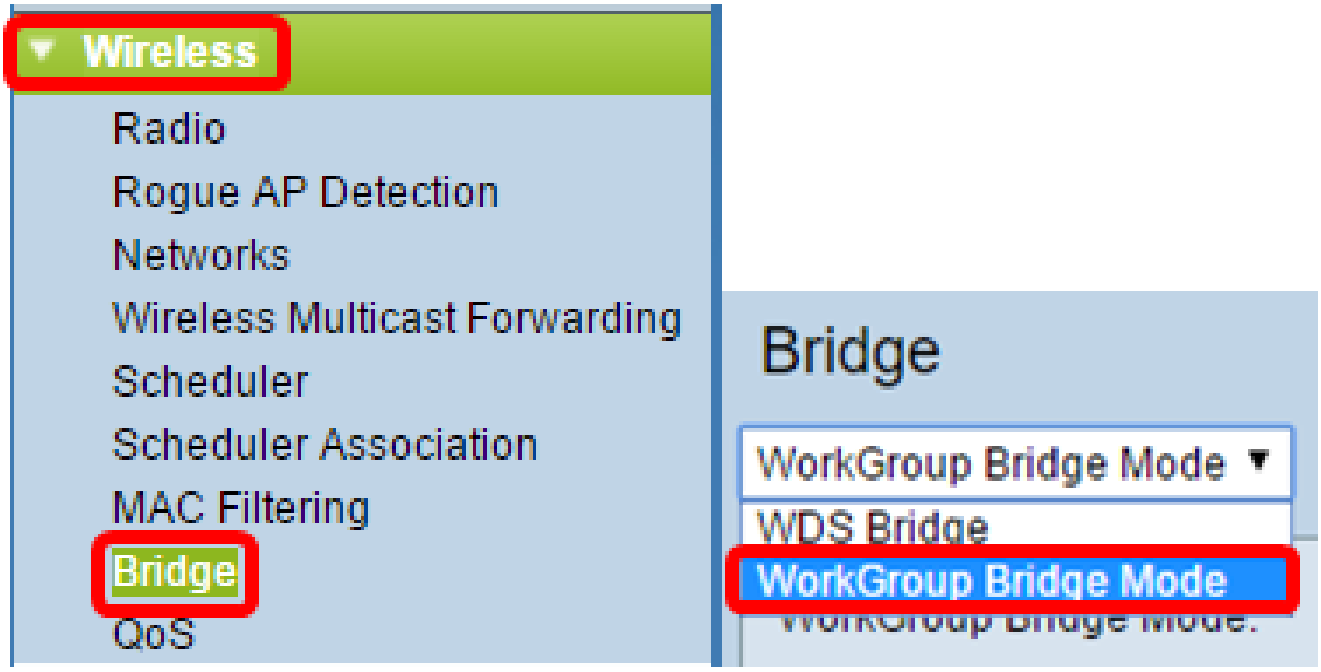
Configura bridge gruppo di lavoro

Interfaccia client dell'infrastruttura

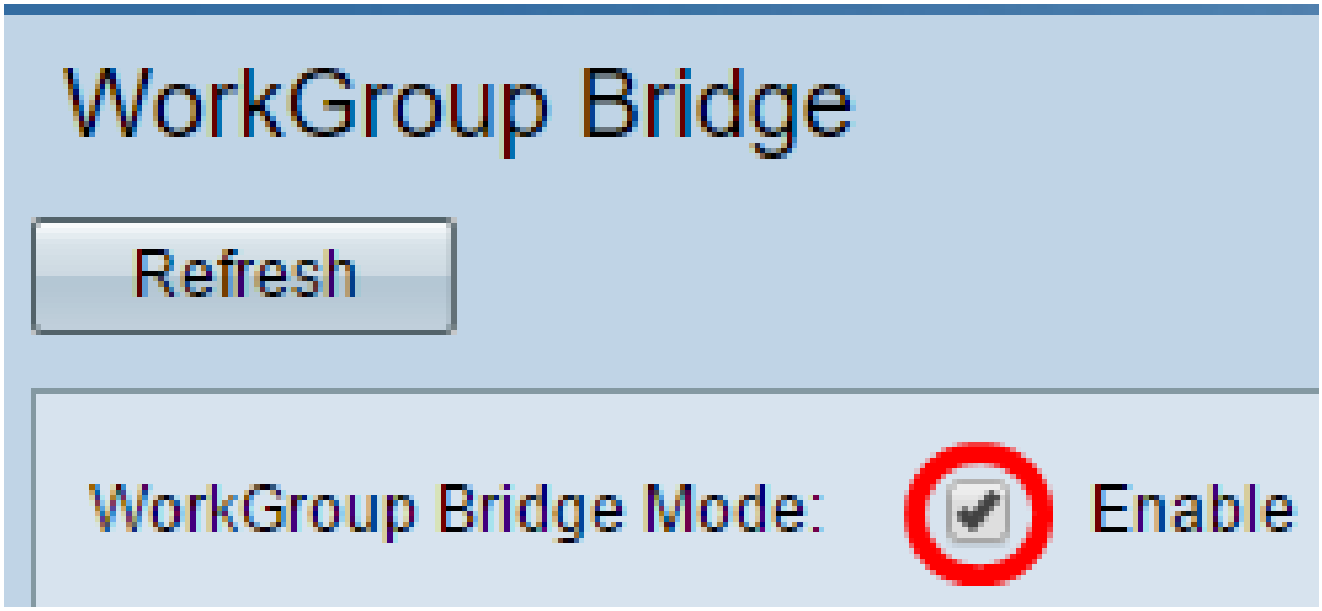
Passaggio 1. Accedere all'utility basata sul Web di WAP e scegliere Wireless > WorkGroup Bridge.

Nota: le opzioni di menu possono variare a seconda del modello del dispositivo in uso. Le immagini seguenti sono tratte da WAP361, se non diversamente specificato.

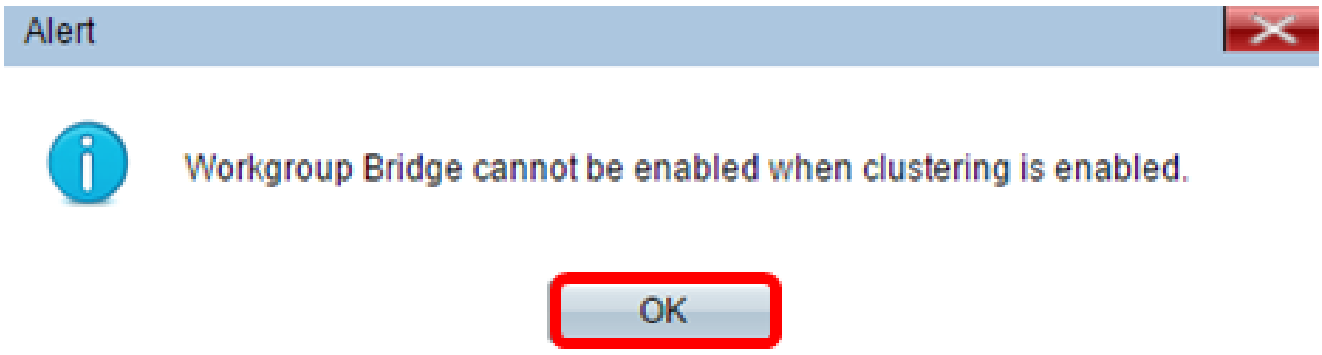
Per WAP571 e WAP571E, scegliete Wireless > Bridge > Modalità bridge gruppo di lavoro.



Passaggio 2. Selezionare la casella di controllo Attiva modalità bridge per gruppi di lavoro.

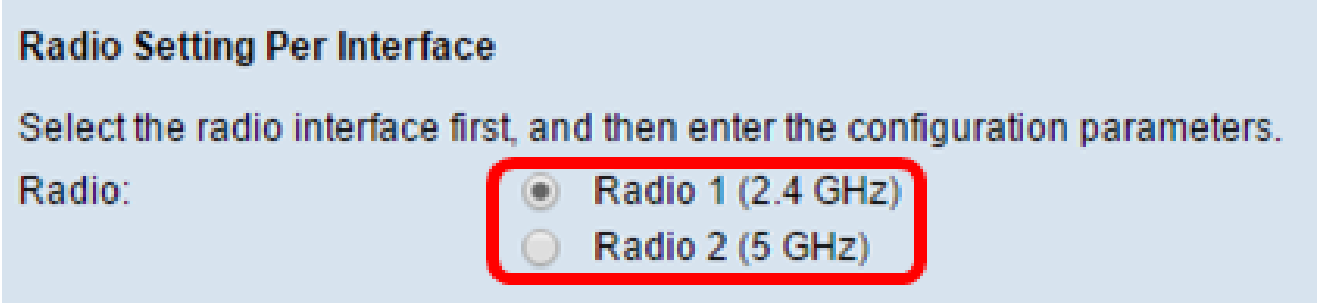


Nota: se il clustering è abilitato in WAP, verrà visualizzato un messaggio per informare l'utente della disabilitazione del clustering affinché WorkGroup Bridge funzioni. Fare clic su OK per continuare. Per disabilitare il clustering, scegliere Configurazione punto singolo dal pannello di navigazione, quindi scegliere Access Point > Disabilita configurazione punto singolo.



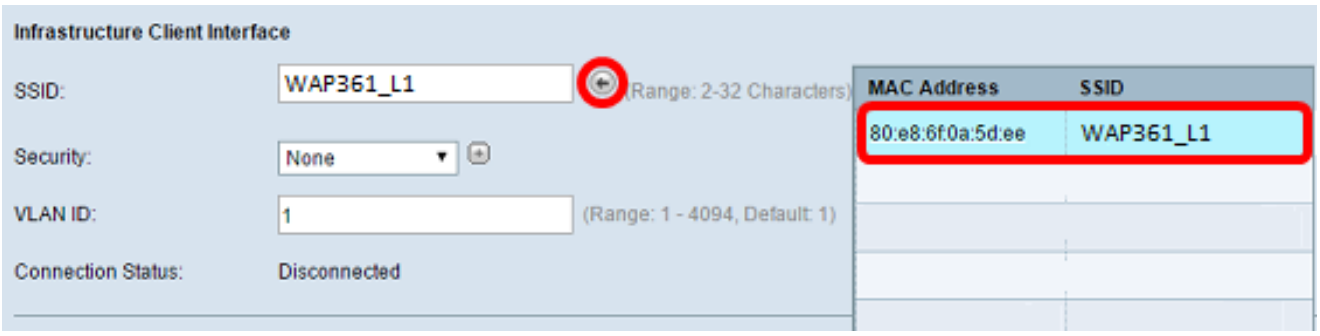
Passaggio 3. Fare clic sull'interfaccia radio di WorkGroup Bridge. Quando si configura una radio come bridge per gruppi di lavoro, l'altra radio rimane operativa. Le interfacce radio corrispondono alle bande di radiofrequenza del WAP. Il WAP è in grado di trasmettere su due diverse interfacce radio. La configurazione delle impostazioni per un'interfaccia radio non influirà sull'altra. Le opzioni dell'interfaccia radio possono variare a seconda del modello WAP. Alcuni WAP visualizzano Radio 1 a 2,4 GHz, mentre altri hanno Radio 2 a 2,4 GHz.

Nota: questo passaggio riguarda solo i seguenti WAP con dual-band: WAP131, WAP150, WAP351, WAP361, WAP371, WAP561, WAP571, WAP571E. Per questo esempio, viene scelta Radio 1.



Passaggio 4. Immettere il nome SSID (Service Set Identifier) nel campo SSID oppure fare clic sul pulsante freccia accanto al campo per cercare i vicini. 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.

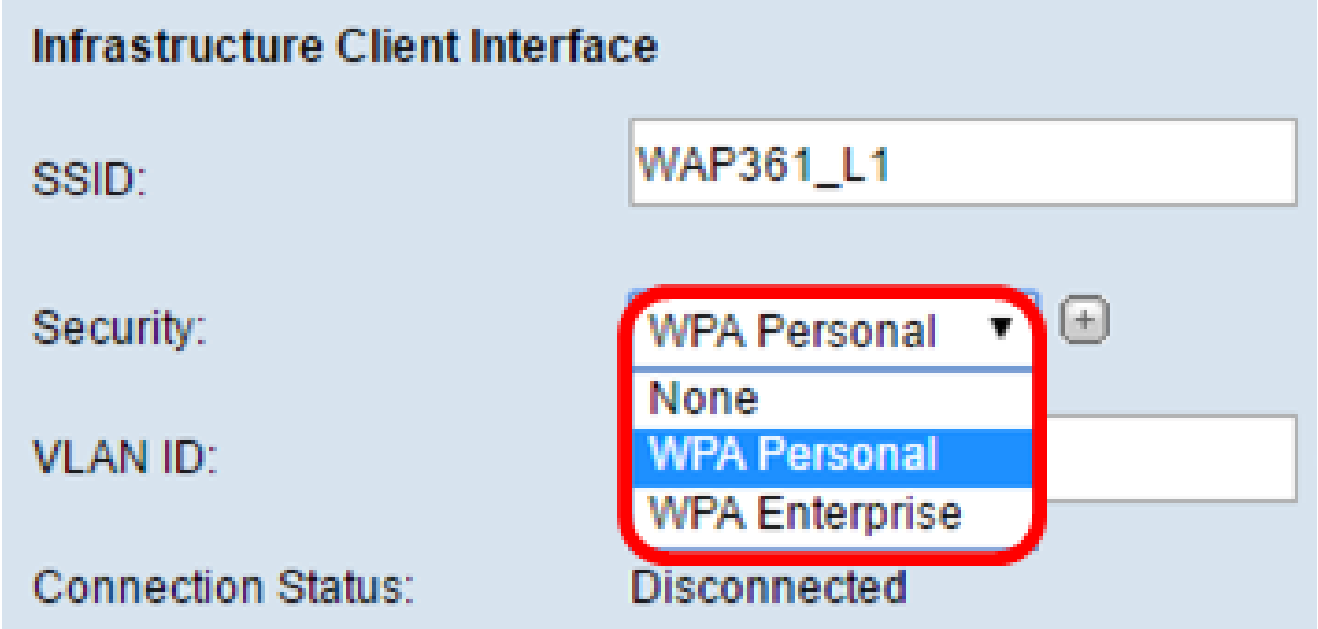
Nota: è importante abilitare il rilevamento dei punti di accesso non autorizzati. Per ulteriori informazioni su come attivare la suddetta funzione, fare clic qui. In questo esempio, viene fatto clic sul pulsante freccia per scegliere WAP361_L1 come SSID dell'interfaccia client dell'infrastruttura.



Passaggio 5. Nell'area Interfaccia client infrastruttura, scegliere il tipo di protezione da autenticare come stazione client sul dispositivo WAP upstream dall'elenco a discesa Protezione. Le opzioni sono:

- Nessuno — Aprire o non impostare la protezione. Questa è l'impostazione predefinita. Se si sceglie questa opzione, andare al passaggio 18.
- WPA personale: WPA personale può supportare chiavi di lunghezza compresa tra 8 e 63 caratteri. WPA2 è consigliato in quanto offre uno standard di crittografia più potente. Andare al passo 6 per configurare.
- WPA Enterprise: WPA Enterprise è più avanzato di WPA Personal e rappresenta la

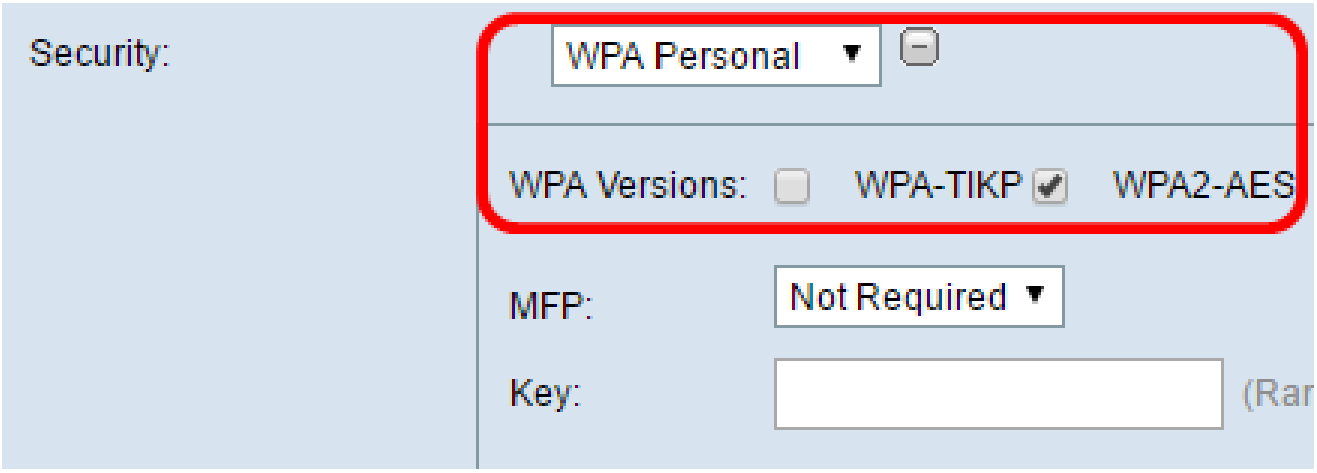
protezione consigliata per l'autenticazione. Utilizza PEAP (Protected Extensible Authentication Protocol) e TLS (Transport Layer Security). Andare al passaggio 9 per configurare. Questo tipo di protezione viene spesso utilizzato in un ambiente di ufficio e richiede la configurazione di un server RADIUS (Remote Authentication Dial-In User Service). Per ulteriori informazioni sui server RADIUS, fare clic qui.



Nota: in questo esempio viene scelto WPA Personal.

Passaggio 6. Fare clic sul segno + 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 sicurezza 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 in quanto offre uno standard di crittografia più potente. Nell'esempio viene utilizzato WPA2-AES.

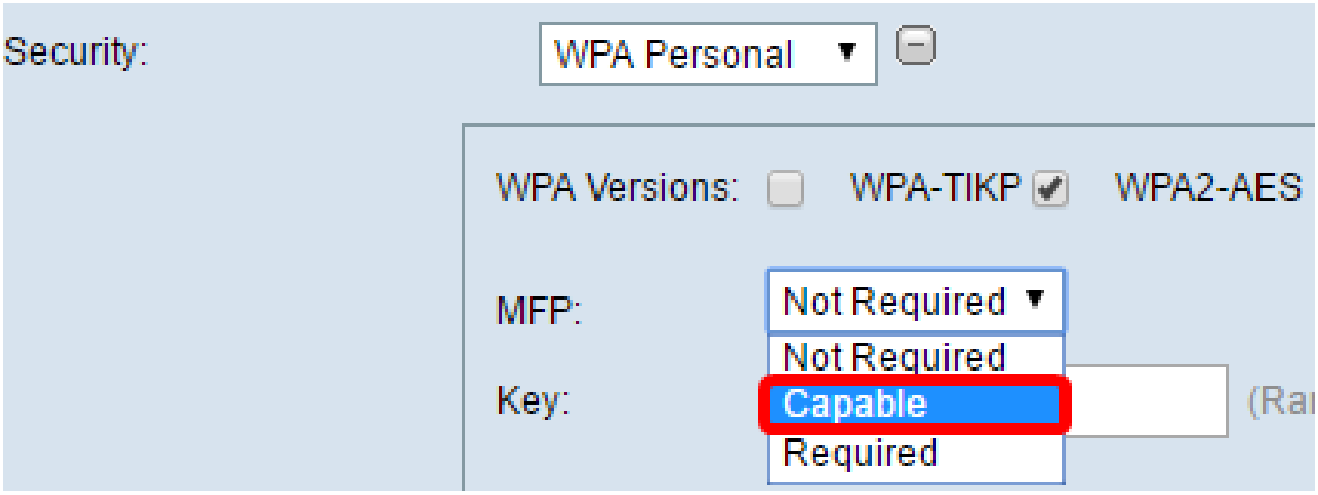


Passaggio 7. (Facoltativo) Se è stato selezionato WPA2-AES nel passaggio 6, scegliere un'opzione dall'elenco a discesa Management Frame Protection (MFP) per richiedere o meno che WAP abbia frame protetti. Per ulteriori informazioni sulla stampante multifunzione,

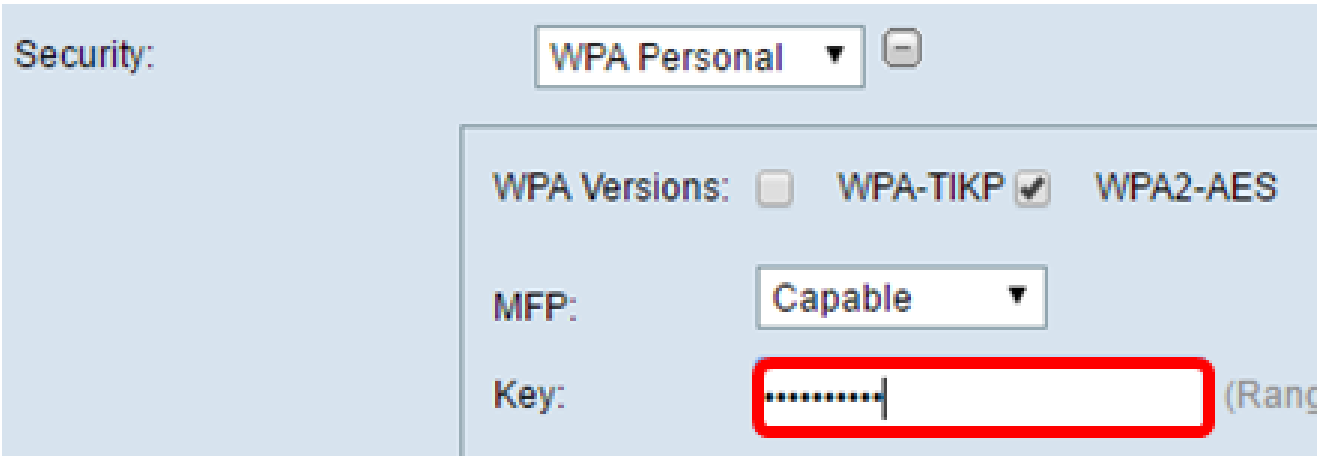
fare clic qui. Le opzioni sono:

- Non richiesto: disabilita il supporto client per le stampanti multifunzione.
- Funzionalità: consente ai client che supportano le funzionalità MFP e a quelli che non supportano le funzionalità MFP 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, è stato scelto Capable.



Passaggio 8. Immettere la chiave di crittografia WPA nel campo Chiave. La chiave deve contenere da 8 a 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 18.



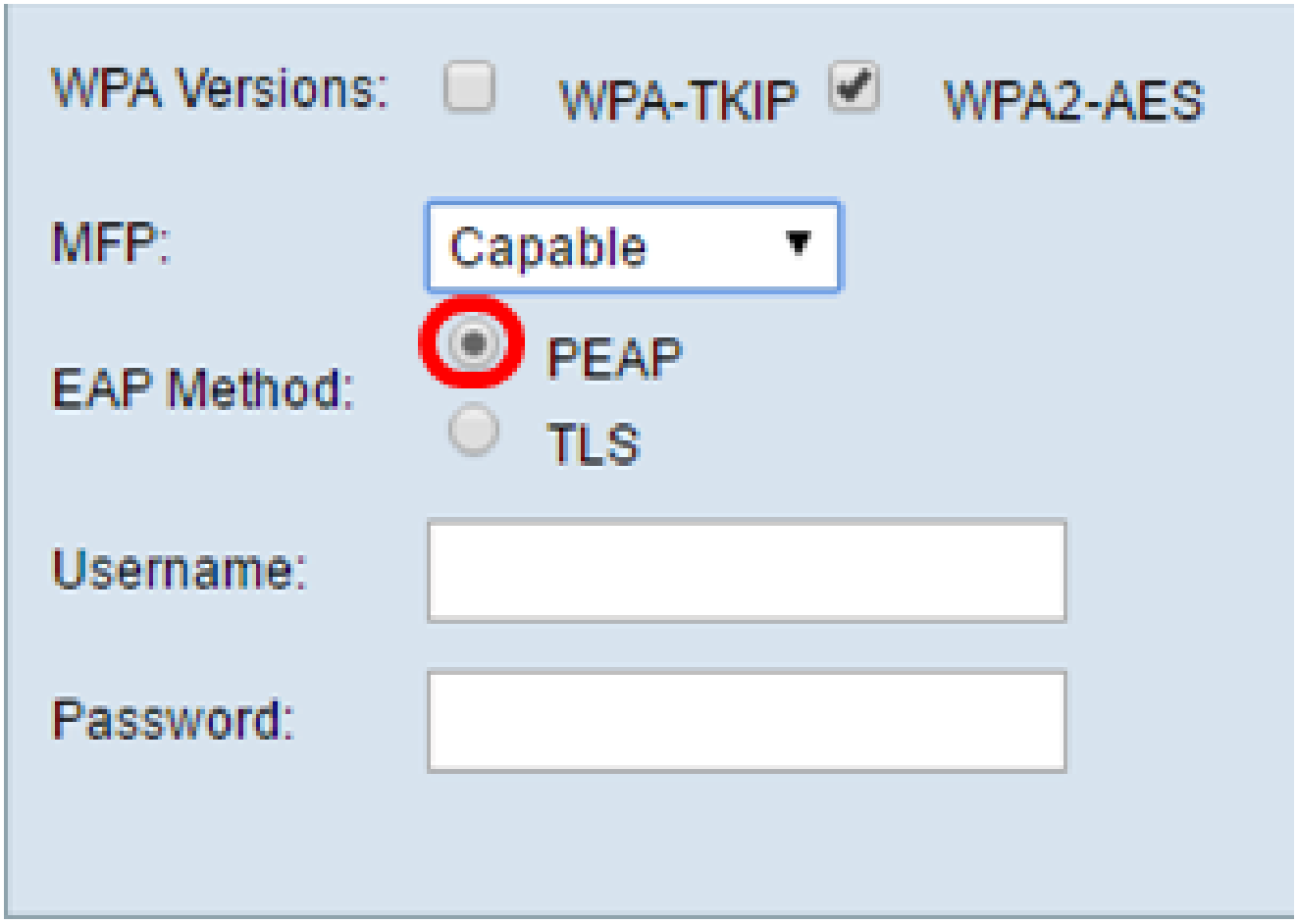
Passaggio 9. Se nel passaggio 5 è stata scelta l'organizzazione WPA, fare clic su un pulsante di opzione per il metodo EAP.

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

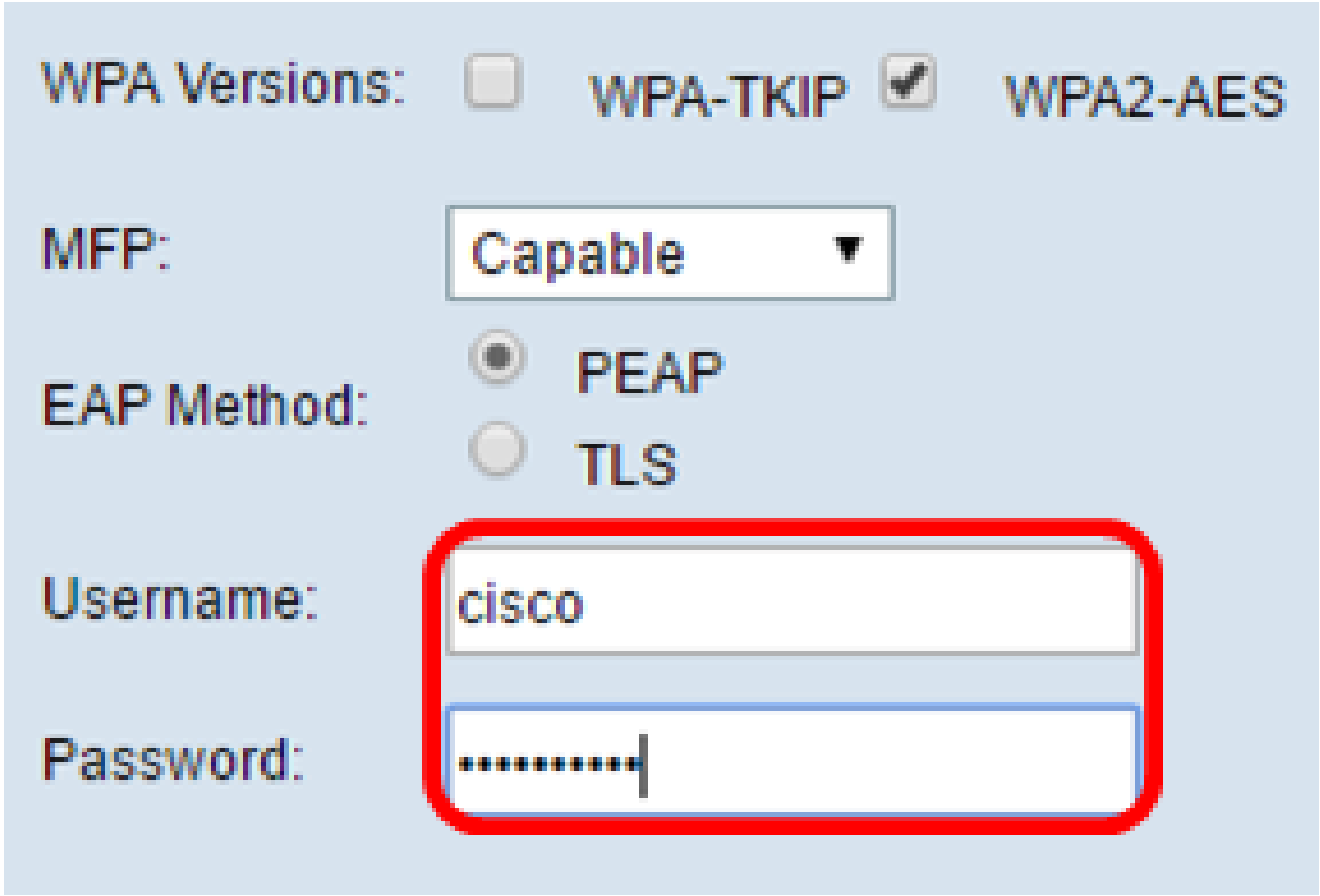
della periferica del client. PEAP può rappresentare un rischio potenziale per la sicurezza se si dispone di password poco sicure o di client non protetti. Si basa su TLS ma evita l'installazione di certificati digitali su ogni client. Fornisce invece l'autenticazione tramite nome utente e password.

- TLS — TLS richiede che ogni utente disponga 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.

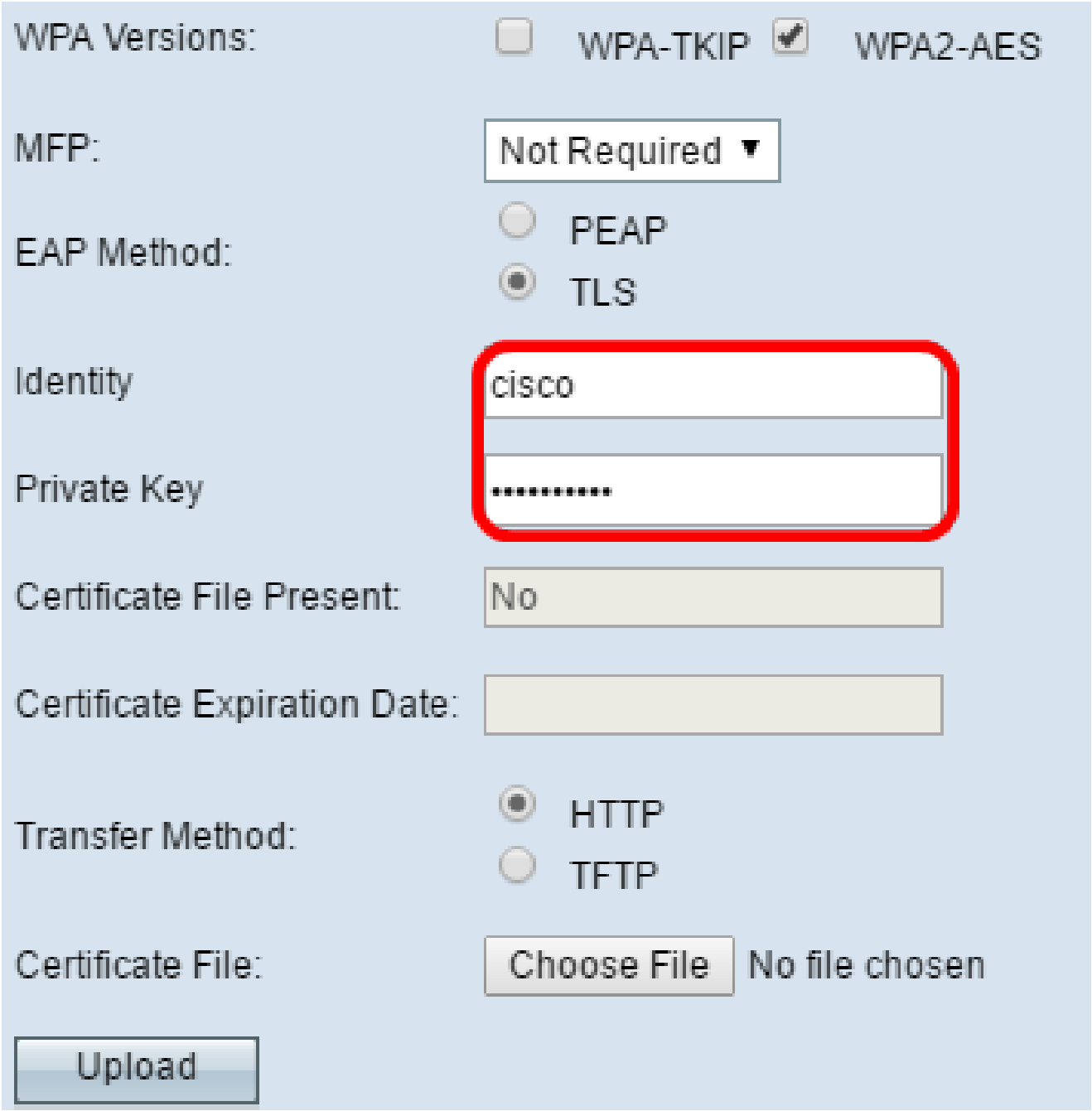


Nota: per questo esempio, viene scelto PEAP.

Passaggio 10. Immettere il nome utente e la password per il client dell'infrastruttura nei campi Nome utente e Password. Queste sono le informazioni di accesso utilizzate per la connessione all'interfaccia client dell'infrastruttura. Per ulteriori informazioni, fare riferimento all'interfaccia client dell'infrastruttura. Quindi, andare al Passaggio 18.

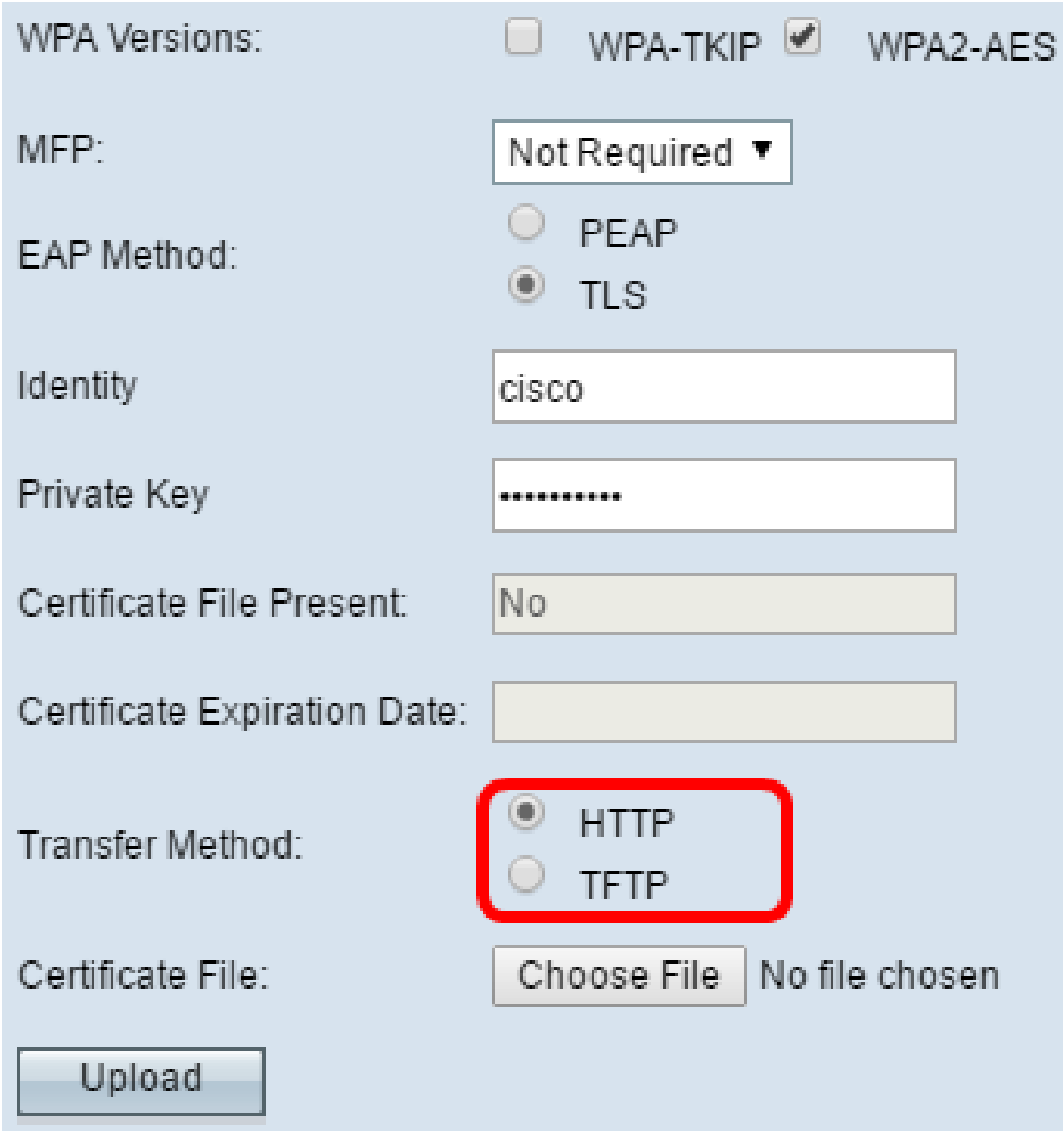


Passaggio 11. Se si è fatto clic su TLS nel passaggio 9, immettere l'identità e la chiave privata del client dell'infrastruttura nei campi Identità e Chiave privata.



Passaggio 12. Nell'area Metodo di trasferimento fare clic su uno dei pulsanti di opzione seguenti:

- TFTP - Il protocollo TFTP (Trivial File Transfer Protocol) 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 15.
- 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.



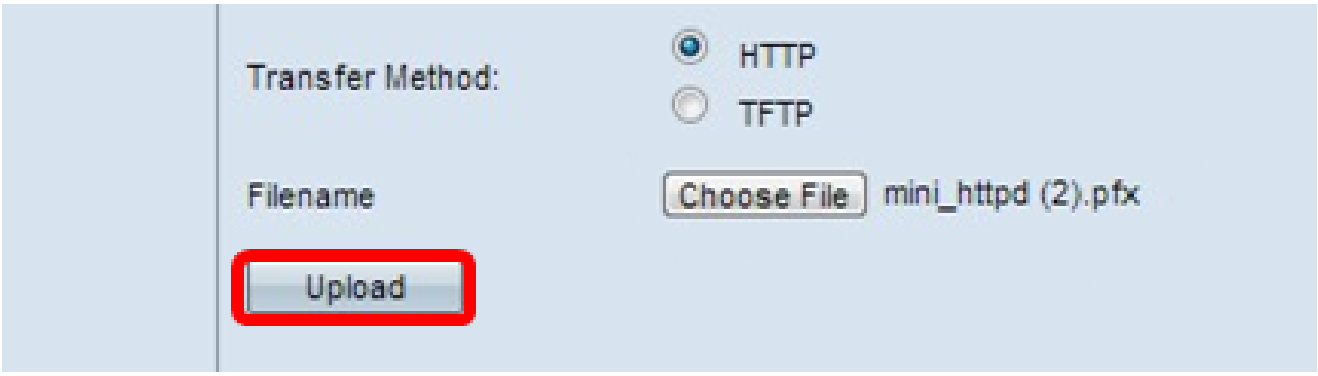
Nota: se un file di certificato è già presente nel WAP, nei campi File certificato presente e Data scadenza verranno già inserite le informazioni pertinenti. In caso contrario, saranno vuote.

HTTP

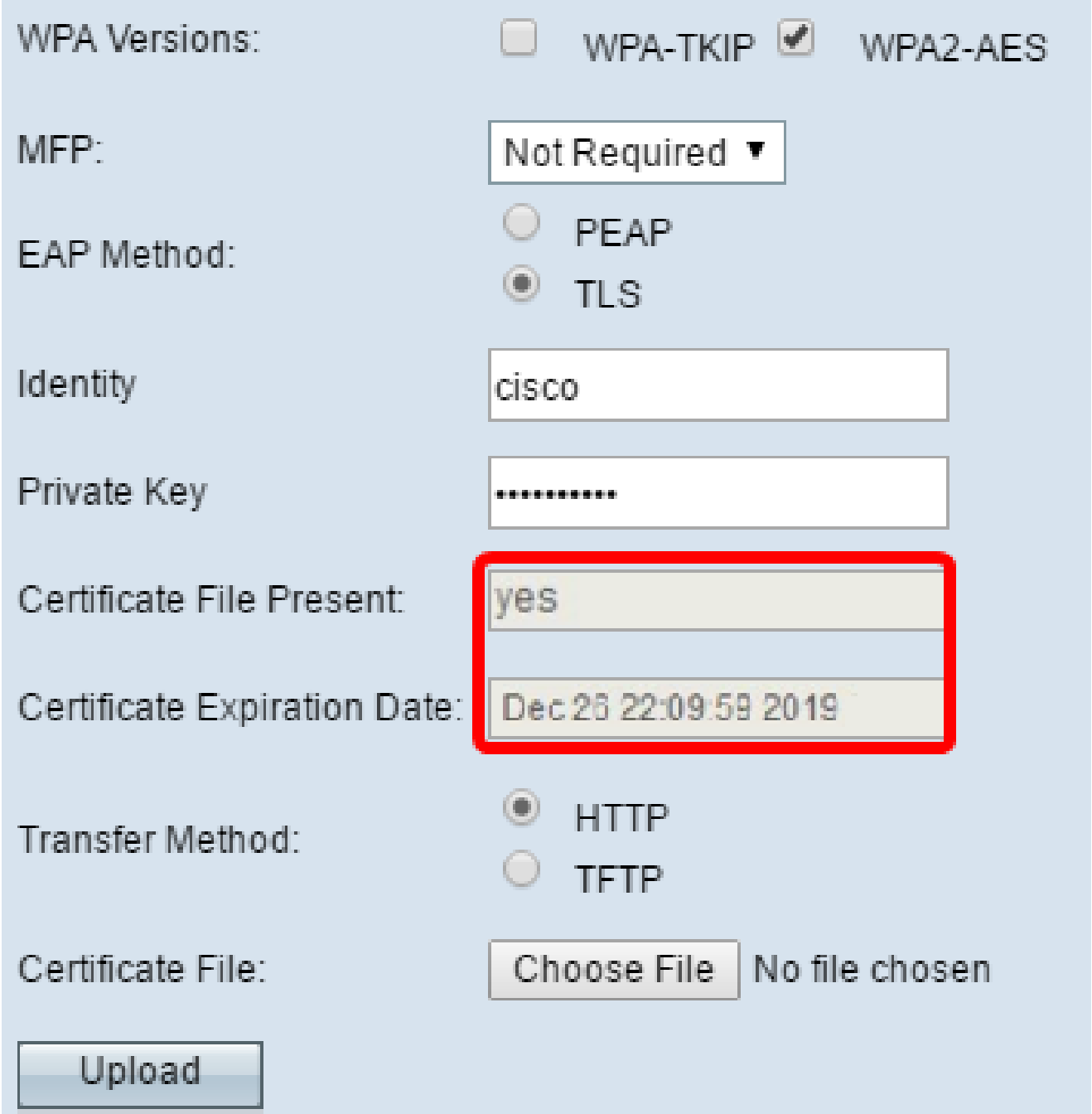
Passaggio 13. Fare clic sul pulsante Scegli file per individuare e selezionare un file di certificato. Il file deve avere l'estensione corretta (ad esempio, .pem o .pfx). In caso contrario, il file non verrà accettato.

Nota: in questo esempio, viene scelto mini_httpd(2).pfx.

Passaggio 14. Fare clic su Upload (Carica) per caricare il file di certificato selezionato. Andare al passo 18.



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



TFTP

Passaggio 15. Se si è fatto clic su TFTP nel passaggio 12, immettere il nome del file del certificato nel campo Nome file.

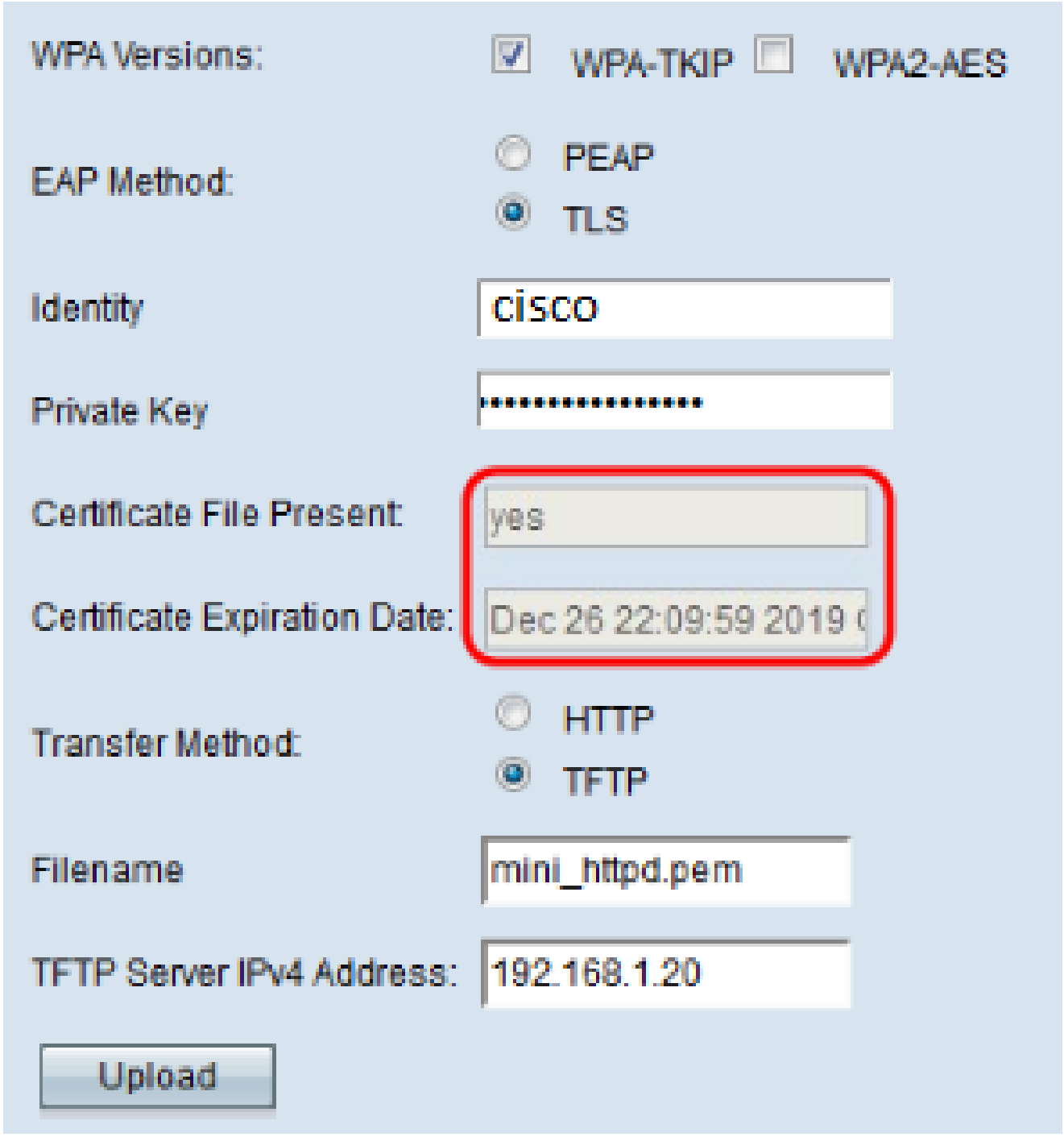
Nota: nell'esempio viene utilizzato il file mini_httpd.pem.

Passaggio 16. Immettere l'indirizzo del server TFTP nel campo Indirizzo IPv4 server TFTP.

Nota: in questo esempio. 192.168.1.20 viene utilizzato come indirizzo del server TFTP.

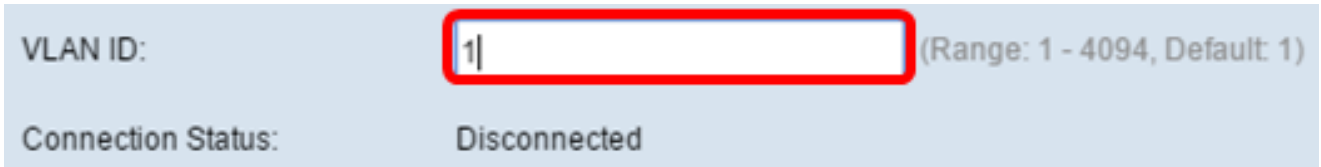
Passaggio 17. Fare clic sul pulsante Upload per caricare il file di certificato specificato.

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



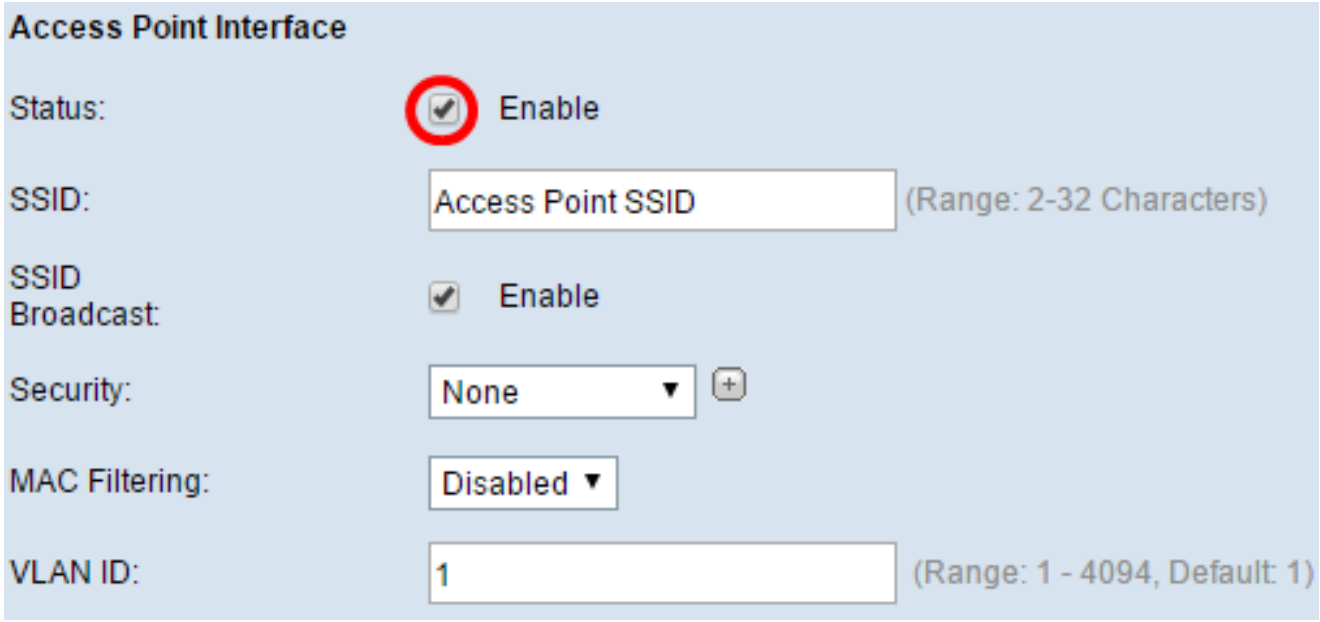
Passaggio 18. Immettere l'ID VLAN per l'interfaccia client dell'infrastruttura. Il valore predefinito è 1.

Nota: nell'esempio viene usato l'ID VLAN predefinito.



Access Point Interface

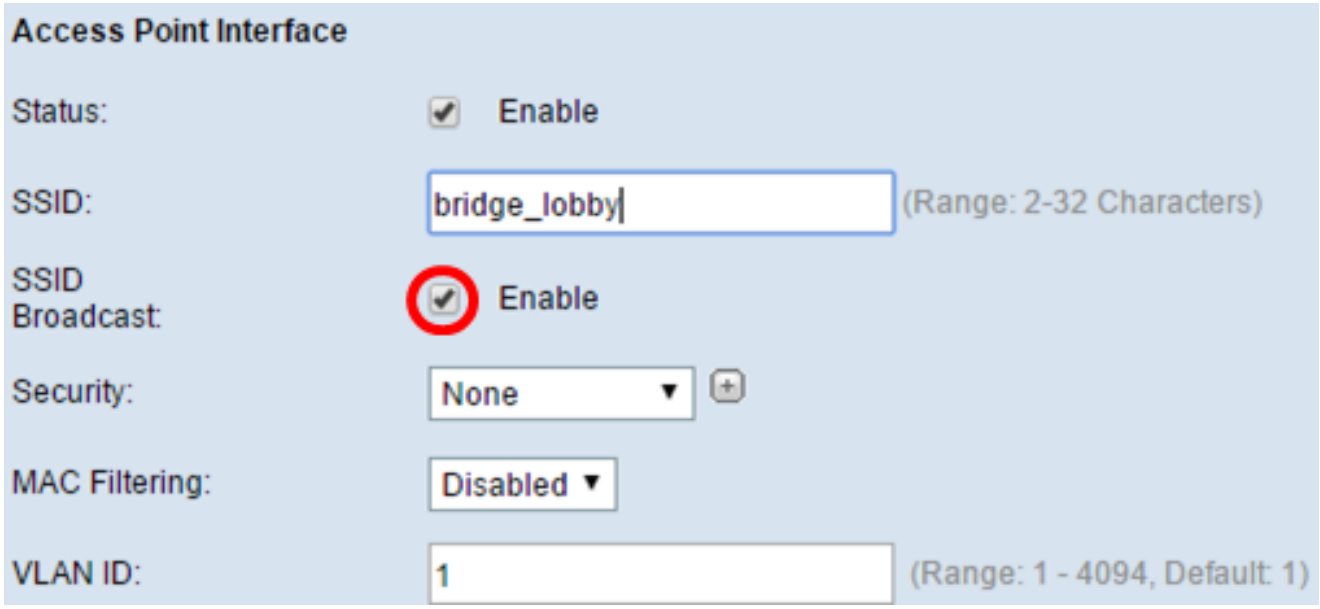
Passaggio 1. Selezionare la casella di controllo Attiva stato per attivare il bridging sull'interfaccia del punto di accesso.



Passaggio 2. 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 Access Point SSID.

Nota: per questo esempio, il SSID utilizzato è bridge_lobby.

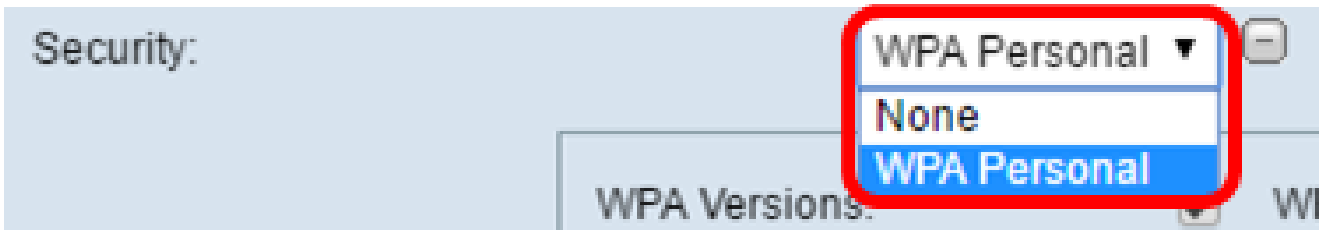
Passaggio 3. (Facoltativo) Se non si desidera trasmettere il SSID, deselezionare la casella di controllo Abilita trasmissione SSID. In questo modo il punto di accesso non sarà visibile a chi cerca punti di accesso wireless e potrà essere connesso solo da chi conosce già il SSID. La trasmissione SSID è abilitata per impostazione predefinita.



Passaggio 4. Selezionare il tipo di protezione per l'autenticazione delle stazioni client downstream in WAP dall'elenco a discesa Protezione.

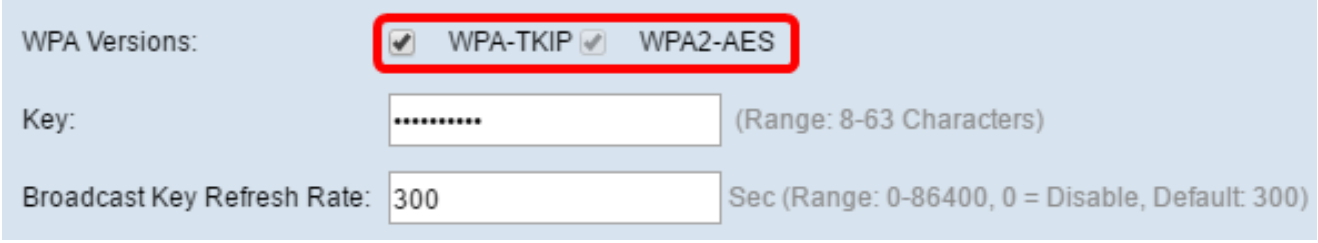
Le opzioni disponibili sono definite come segue:

- Nessuno — Aprire o non impostare alcuna protezione. Questo è il valore predefinito. Se si sceglie questa opzione, andare al Passaggio 10.
- 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.

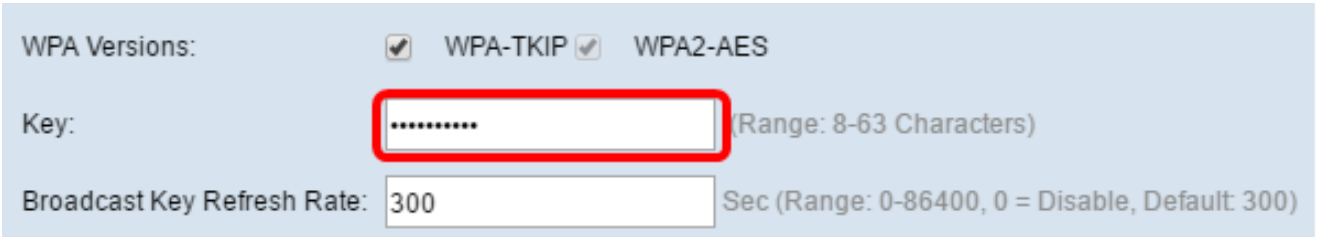


Passaggio 5. Selezionare la casella di controllo WPA-TKIP o WPA2-AES per determinare il tipo di crittografia WPA che verrà utilizzata dall'interfaccia del punto di accesso. Questi sono attivati per impostazione predefinita.

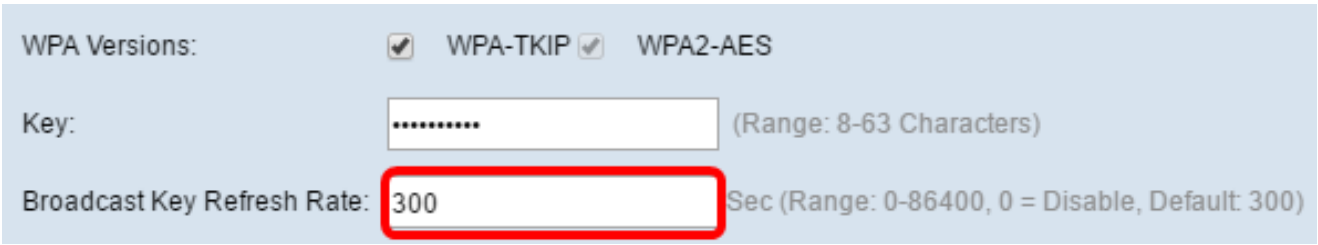
Nota: se tutte le apparecchiature wireless supportano WPA2, impostare la sicurezza del client dell'infrastruttura su WPA2-AES. Il metodo di crittografia è RC4 per WPA e AES (Advanced Encryption Standard) per WPA2. WPA2 è consigliato in quanto offre uno standard di crittografia più potente. Nell'esempio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



Passaggio 6. 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.



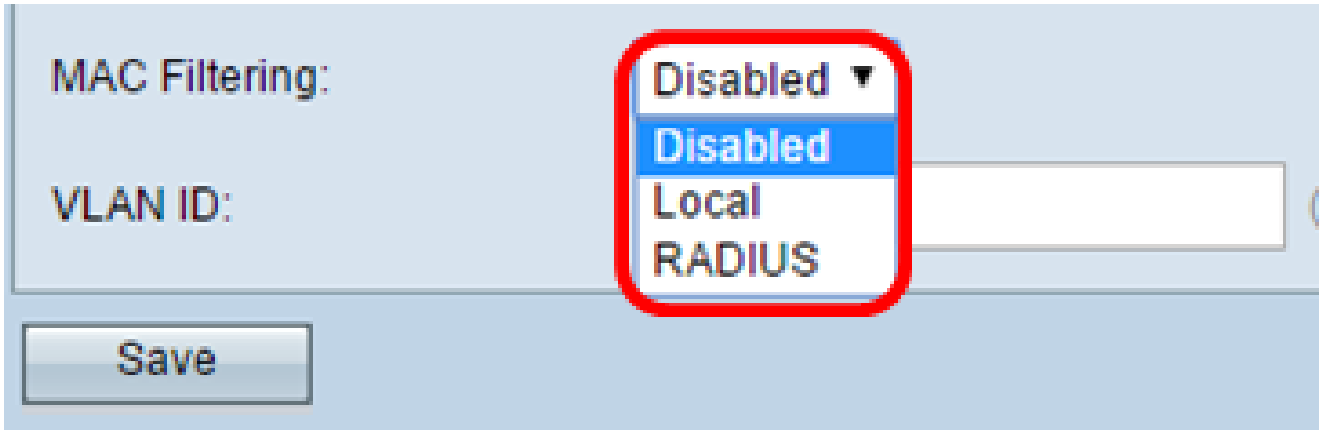
Passaggio 7. Immettere la velocità nel campo Velocità di aggiornamento chiave trasmissione. La frequenza di aggiornamento della chiave di trasmissione specifica l'intervallo di aggiornamento della chiave di protezione per i client associati a questo punto di accesso. La velocità deve essere compresa tra 0 e 86400, con un valore pari a 0 per disattivare la funzionalità. Il valore predefinito è 300.



Passaggio 8. 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 che utilizzano.

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 di 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.

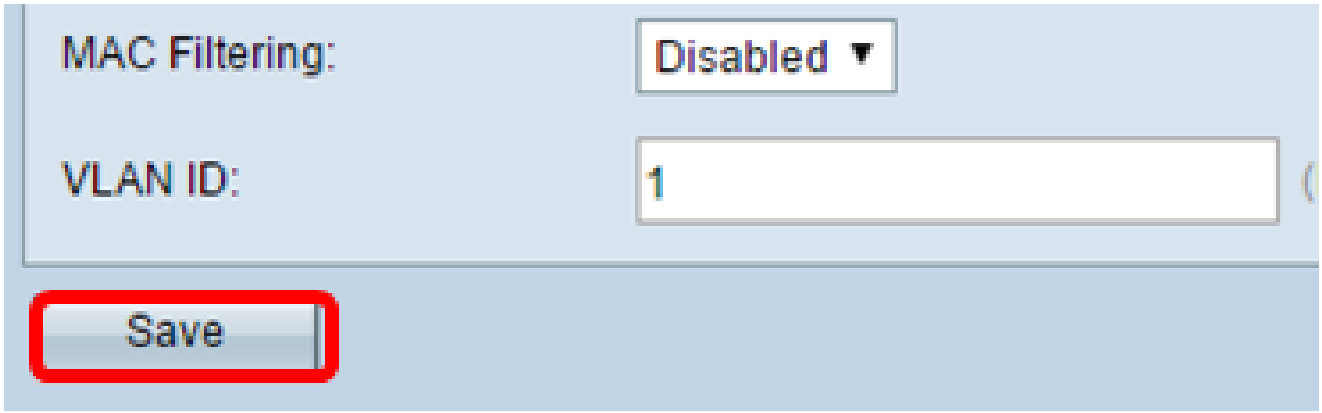


Nota: per questo esempio, è stato scelto Disabilitato.

Passaggio 9. Immettere l'ID VLAN nel campo VLAN ID dell'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 10. Fare clic su Salva per salvare le modifiche.



È ora necessario aver configurato correttamente un bridge per gruppi di lavoro su un punto di accesso wireless.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).