Configurazione di Work Group Bridge sui punti di accesso WAP551 e WAP561

Obiettivo

In questo articolo viene spiegato come configurare il bridge di gruppi di lavoro sui punti di accesso WAP551 e WAP561.

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 quello associato alla LAN wireless è definito interfaccia di infrastruttura. È consigliabile utilizzare questa funzionalità quando non è possibile utilizzare la funzionalità Servizi di distribuzione Windows, in quanto si tratta di una soluzione di bridge preferita per WAP551 e WAP561. Quando la funzionalità di bridge per gruppi di lavoro è abilitata, la funzionalità di bridge Servizi di distribuzione Windows non funziona. Per informazioni sulla configurazione di WDS Bridge, vedere l'articolo *Configurazione di WDS (Wireless Distribution System) sui punti di accesso WAP551 e WAP561* .

Dispositivi interessati

·WAP551
· WAP561

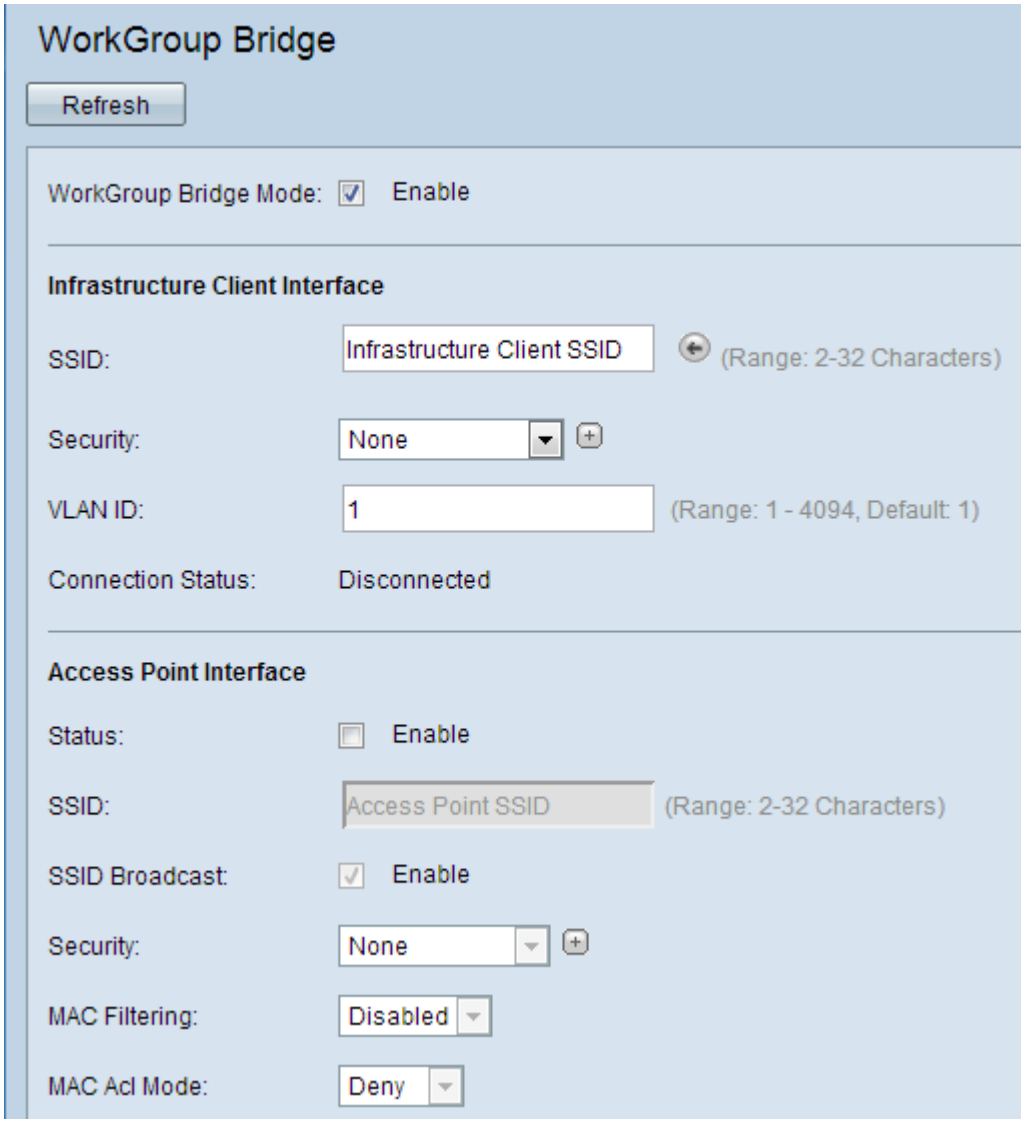
Versione del software

·v1.0.4.2

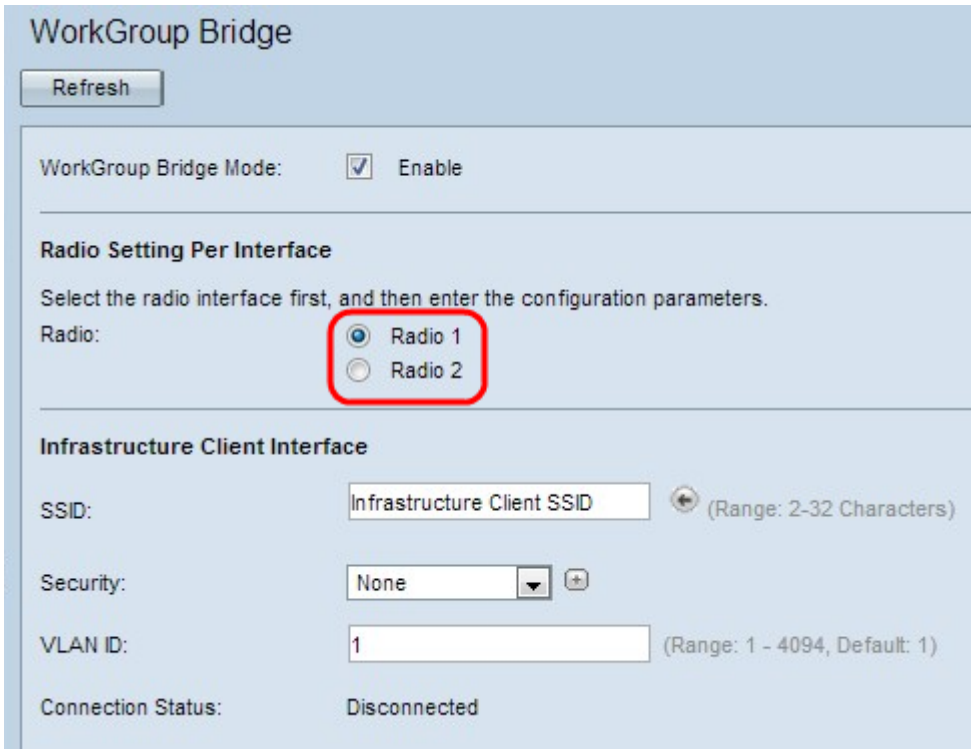
Configura bridge per gruppi di lavoro

Nota: Per abilitare il clustering del bridge di gruppi di lavoro, è necessario abilitarlo in WAP. Se è disattivata, è necessario disattivare Single Point Setup che a sua volta attiva il clustering. Tutti i dispositivi WAP che fanno parte del bridge di gruppi di lavoro devono avere impostazioni comuni per radio, modalità IEEE 802.11, larghezza di banda del canale e canale (audio non consigliato). Per assicurarsi che queste impostazioni siano uguali in tutte le periferiche, cercare le impostazioni radio. Per configurare queste impostazioni, consultare l'articolo *Impostazioni radio su WAP551/WAP561*.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Wireless > Bridge per gruppi di lavoro**. Viene visualizzata la pagina *Gruppo di lavoro: Bridge.*

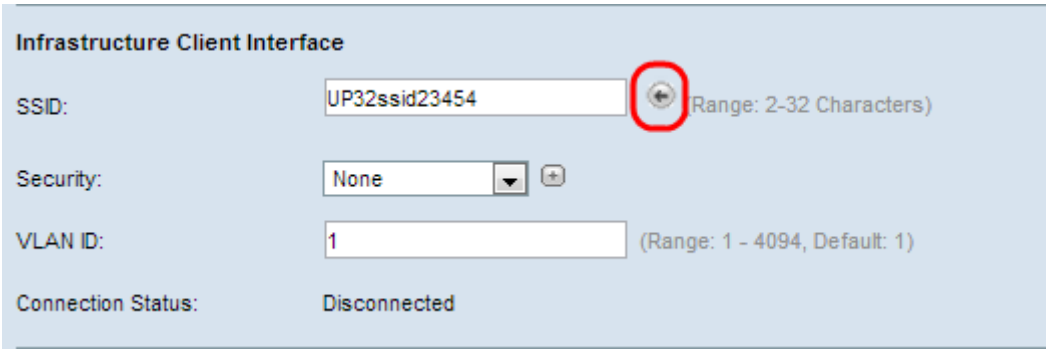


Passaggio 2. Nel campo Modalità bridge gruppo di lavoro, selezionare **Abilita** per abilitare la funzionalità bridge gruppo di lavoro.

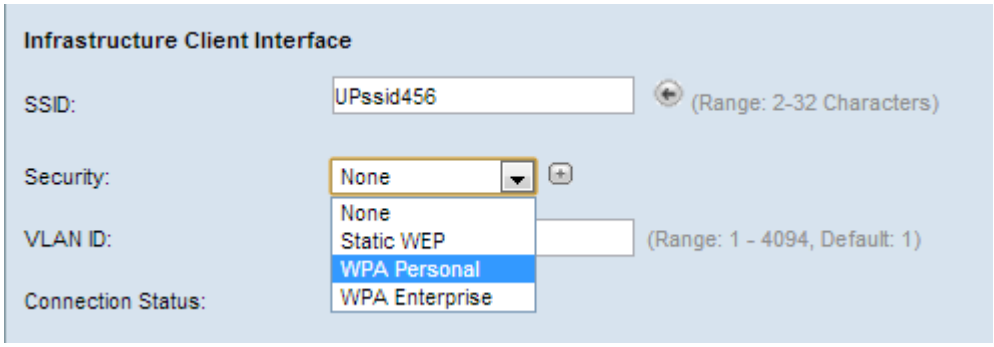


Passaggio 3. Questo passaggio è necessario solo per WAP561. Fare clic sul pulsante di scelta **Radio1** o **Radio 2** per scegliere una delle interfacce radio. Ignorare questo passaggio per WAP551 che ha una sola interfaccia radio. Per individuare la radio configurata e i parametri che consentono di cercare le impostazioni radio. Per configurare queste impostazioni, vedere l'articolo *Impostazioni radio su WAP551/WAP561*.

Passaggio 4. Nel campo SSID, immettere il nome SSID (Service Set Identifier) per l'interfaccia client dell'infrastruttura o il punto di accesso upstream.



Suggerimento: È inoltre possibile fare clic sull'icona **Arrow** accanto al campo SSID per analizzare SSID adiacenti simili. Questa opzione è attivata solo se il rilevamento dei punti di accesso è attivato nel rilevamento dei punti di accesso non autorizzati (è disattivato per impostazione predefinita). Per abilitare il rilevamento dei punti di accesso non autorizzati, consultare l'articolo *Rilevamento punti di accesso non autorizzati su WAP561 e WAP551*.



Passaggio 5. Scegliere il tipo di protezione da autenticare come stazione client sul dispositivo WAP a monte (Interfaccia client infrastruttura) dall'elenco a discesa nel campo Protezione della sezione Interfaccia client infrastruttura. Le scelte possibili sono riportate di seguito.

·Nessuno — Aperto o senza protezione. Questo è il valore predefinito. Se si sceglie questo comando, passare alla sezione *Configurazione dell'ID VLAN e dell'interfaccia del punto di accesso*.

·Static WEP: il protocollo WEP statico offre una sicurezza minima e può supportare fino a 4 chiavi di lunghezza compresa tra 64 e 128 bit. La stessa chiave deve essere utilizzata in tutti i nodi.

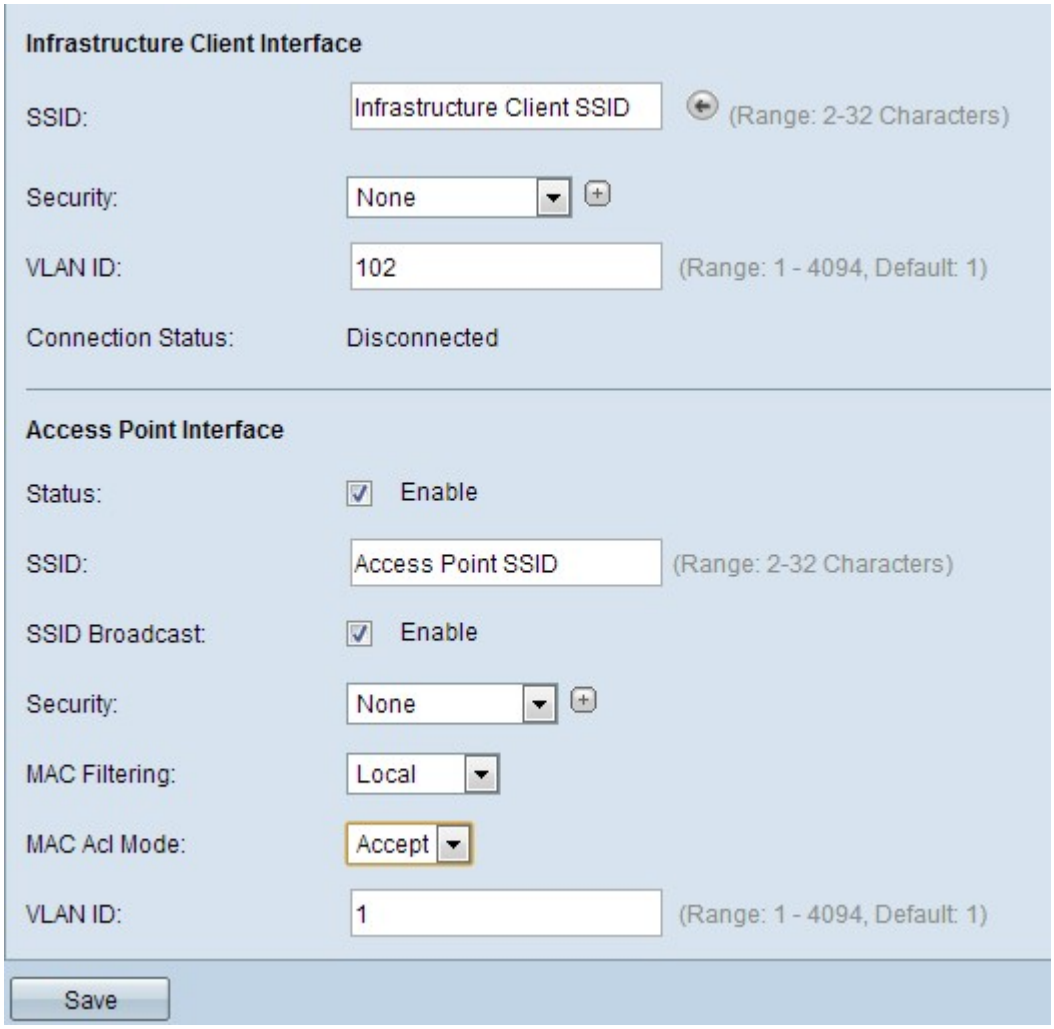
·WPA Personal: WPA Personal è più avanzato rispetto a WEP e può supportare chiavi di lunghezza compresa tra 8 e 63 caratteri. Il metodo di crittografia è RC4 per WPA e AES (Advanced Encryption Standard) per WPA2. WPA2 è consigliato perché ha uno standard di crittografia più potente.

·WPA Enterprise — WPA Enterprise è la protezione più avanzata e consigliata. Utilizza il protocollo PEAP (Protected Extensible Authentication Protocol), in cui ogni singolo utente

wireless in WAP è autorizzato con nomi utente e password individuali che supportano persino gli standard di crittografia AES. Utilizza anche Transport Layer Security (TLS) oltre a PEAP, in cui ogni utente deve fornire un certificato aggiuntivo per ottenere l'accesso. Il metodo di crittografia è RC4 per WPA e AES (Advanced Encryption Standard) per WPA2.

Nota: A seconda della modalità scelta per IEEE 802.11, la disponibilità delle opzioni precedenti può variare.

Passaggio 6. In base all'opzione scelta nel passaggio 5, fare clic su uno dei collegamenti alle opzioni e seguire la procedura appropriata. Se si sceglie Nessuno, non è necessario configurare alcuna di queste procedure.



Passaggio 7. Nel campo ID VLAN, immettere l'ID VLAN per l'interfaccia client dell'infrastruttura.

Passaggio 8. Nel campo Stato, selezionare **Abilita** per abilitare il bridging sull'interfaccia del punto di accesso.

Passaggio 9. Nel campo SSID, immettere il nome SSID (Service Set Identifier) dell'interfaccia del punto di accesso.

Passaggio 10. (Facoltativo) Se si desidera trasmettere il SSID (Access Point Interface SSID) downstream, selezionare **Abilita** nel campo Trasmissione SSID. È attivata per impostazione predefinita.

Passaggio 11. Selezionare il tipo di protezione per autenticare le stazioni client downstream sul dispositivo WAP (Access Point Interface) dall'elenco a discesa Protezione. I valori

possibili sono:

·Nessuno — Aperto o senza protezione. Questo è il valore predefinito. Se si sceglie questa opzione, ignorare i passaggi da 12 a 15. Passare al punto 16.

·WEP statico: WEP statico è la sicurezza minima e può supportare fino a 4 chiavi di lunghezza compresa tra 64 e 128 bit. Fare riferimento alla sezione *Configurazione WEP statico*. Andare al passo 16.

·WPA Personal: WPA Personal è più avanzato rispetto a WEP e può supportare chiavi di lunghezza compresa tra 8 e 63 caratteri. Il metodo di crittografia è TKIP (Temporal Key Integrity Protocol) o CCMP (Counter Cipher Mode with 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 TKIP che utilizza solo uno standard RC4 a 64 bit.

Timesaver: Eseguire i passi da 12 a 15 solo se è stata scelta l'opzione WPA personale nei passi 11.

Passaggio 12. Selezionare le caselle appropriate per scegliere la versione WPA. È possibile selezionare sia WPA che WAP2 in client WAP diversi con versioni WPA diverse.

Passaggio 13. Selezionare le caselle appropriate per scegliere le suite di cifratura. È possibile selezionare sia TKIP che CCMP(AES).

Passaggio 14. Immettere la chiave WPA condivisa nel campo Chiave. La chiave può includere caratteri alfanumerici, caratteri maiuscoli e minuscoli e caratteri speciali.

Passaggio 15. Immettere l'intervallo di aggiornamento della chiave desiderato nel campo Velocità aggiornamento chiave trasmissione. Intervallo di aggiornamento della chiave di gruppo per tutti i client WAP.

Passaggio 16. 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. I valori possibili sono:

·Disattivato: tutti i client possono accedere alla rete upstream. Questo è il valore predefinito.

·Locale: l'insieme di client che possono accedere alla rete upstream 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.

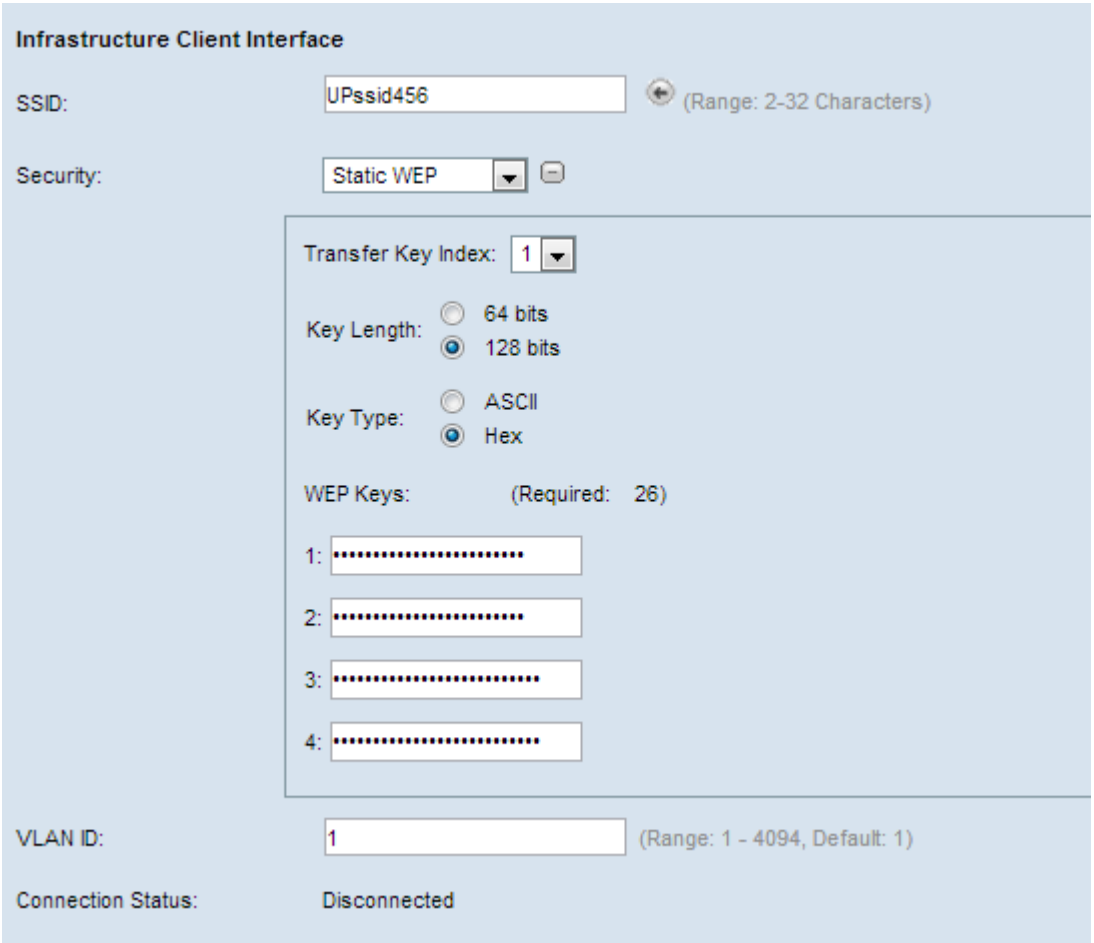
Passaggio 17. Nel campo VLAN ID, immettere l'ID VLAN per l'interfaccia client del punto di accesso.

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 18. Fare clic su **Save** per salvare le impostazioni.

Configura WEP statico

Se si è scelto di configurare WEP statico come tipo di protezione per l'autenticazione, effettuare le seguenti operazioni.

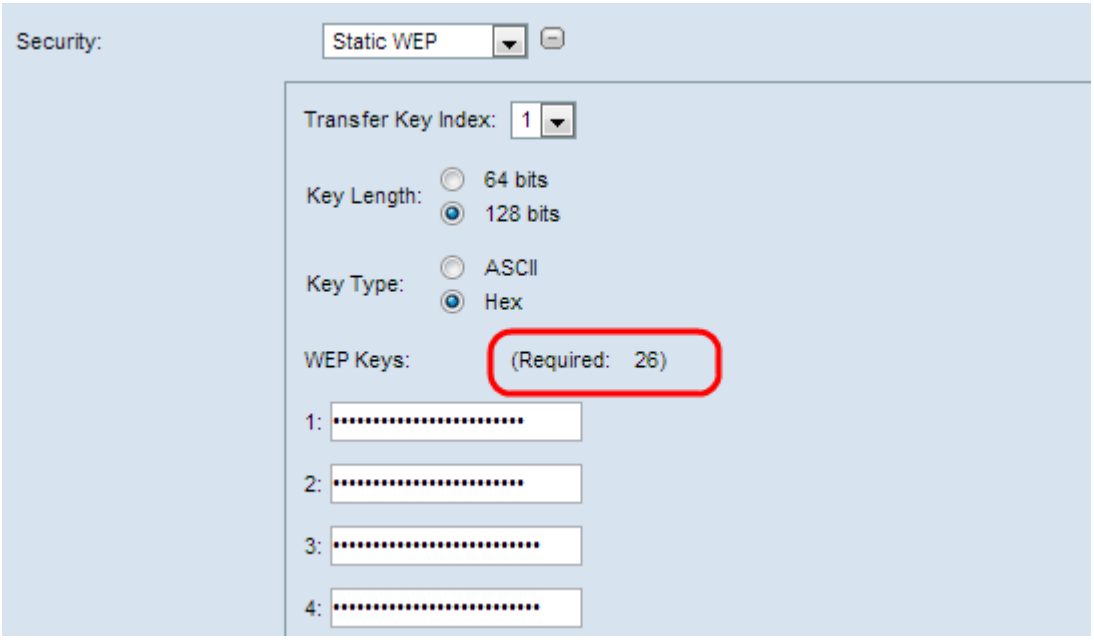


Passaggio 1. Quando si sceglie WEP statico, vengono visualizzati alcuni campi aggiuntivi. Nell'elenco a discesa del campo Indice chiave di trasferimento scegliere un indice di chiave.

I valori disponibili sono 1, 2, 3 e 4. Il valore predefinito è 1. L'indice della chiave è diverso per le diverse WLAN. I dispositivi collegati a una particolare WLAN devono avere lo stesso indice di chiave. Questa chiave viene utilizzata per crittografare i dati per la comunicazione.

Passaggio 2. Nel campo Lunghezza chiave, scegliere il pulsante di opzione **64 bit** o il pulsante di opzione **128 bit**. Specifica la lunghezza della chiave utilizzata.

Passaggio 3. Fare clic sul pulsante di scelta **ASCII** o **HEX** per scegliere il tipo di chiave nel campo Tipo di chiave. Le chiavi WEP sono in genere in formato esadecimale.

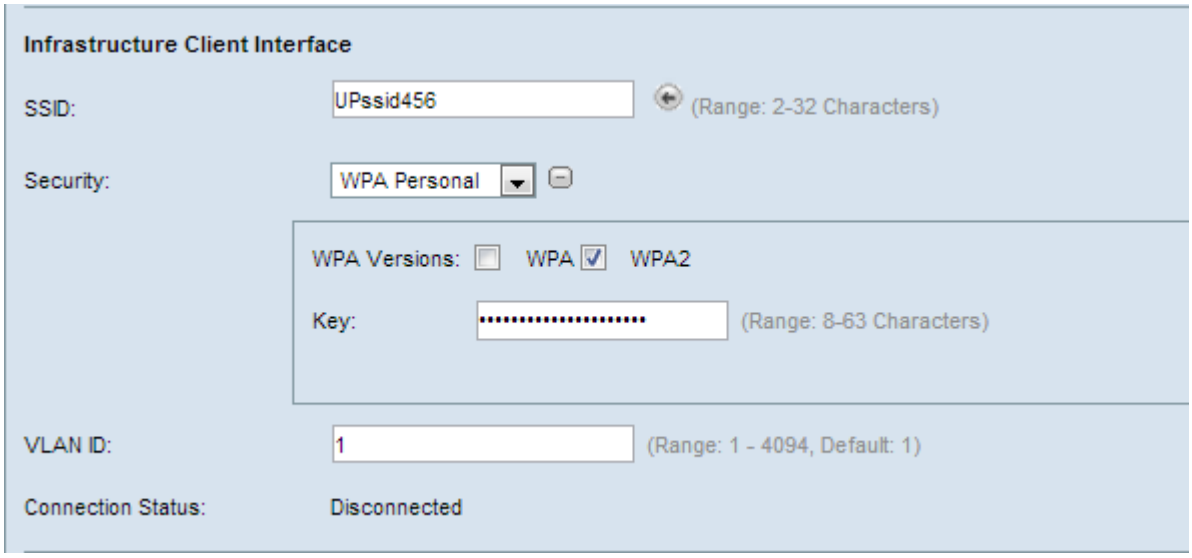


Passaggio 4. Inserire fino a quattro chiavi WEP nei quattro campi successivi contrassegnati come 1, 2, 3 e 4 sotto il campo Chiave WEP. Si tratta di una stringa immessa come chiave. La lunghezza della chiave varia in base alla lunghezza e al tipo della chiave. La lunghezza richiesta è indicata accanto al campo Chiave WEP. Le stringhe della chiave WEP devono corrispondere in tutti i nodi WAP (AP e Client) e devono trovarsi nello stesso campo. Ciò significa che se la stringa 1 è la chiave 1 in un dispositivo, la stringa 1 deve essere la chiave 1 anche negli altri dispositivi del bridge per gruppi di lavoro.

Fare clic qui per continuare con la configurazione.

Configura WPA personale

Se si è scelto di configurare WPA Personal come tipo di protezione per l'autenticazione, eseguire la procedura seguente.



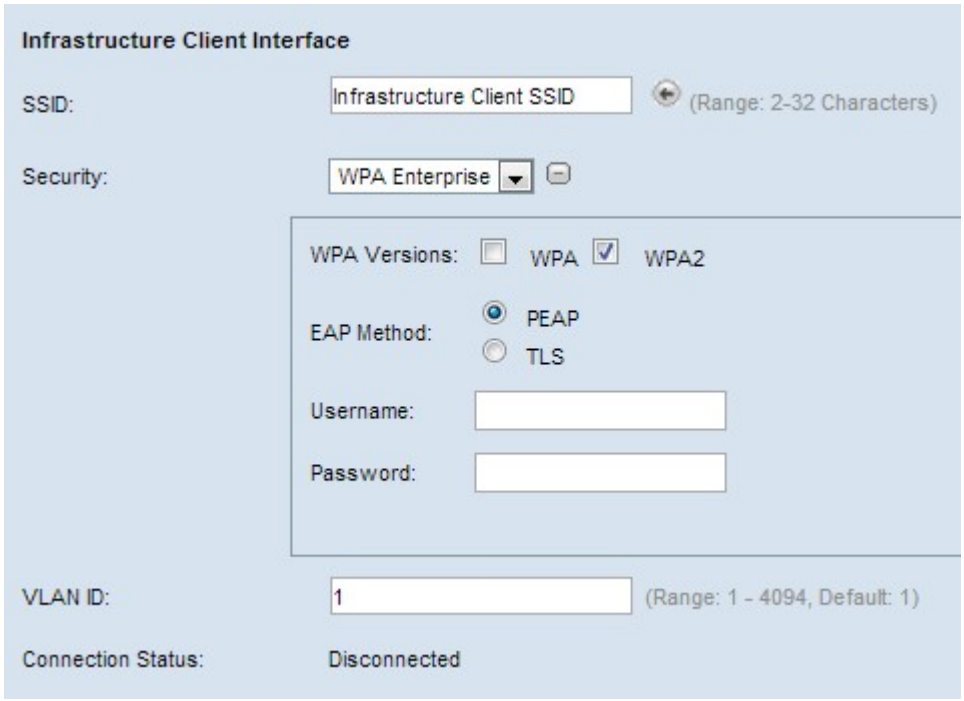
Passaggio 1. Selezionare **WPA** o **WPA2** per scegliere la versione di WPA. In genere, la scelta di WPA viene effettuata solo se nessuno dei WAP interessati supporta WPA2. In caso contrario, si consiglia WPA 2.

Passaggio 2. Immettere la chiave WPA condivisa nel campo Chiave. La chiave può includere caratteri alfanumerici, maiuscoli e minuscoli e caratteri speciali.

Fare clic qui per continuare con la configurazione.

Configura WPA Enterprise

Se si è scelto di configurare WPA Enterprise come tipo di protezione per l'autenticazione, eseguire la procedura seguente.

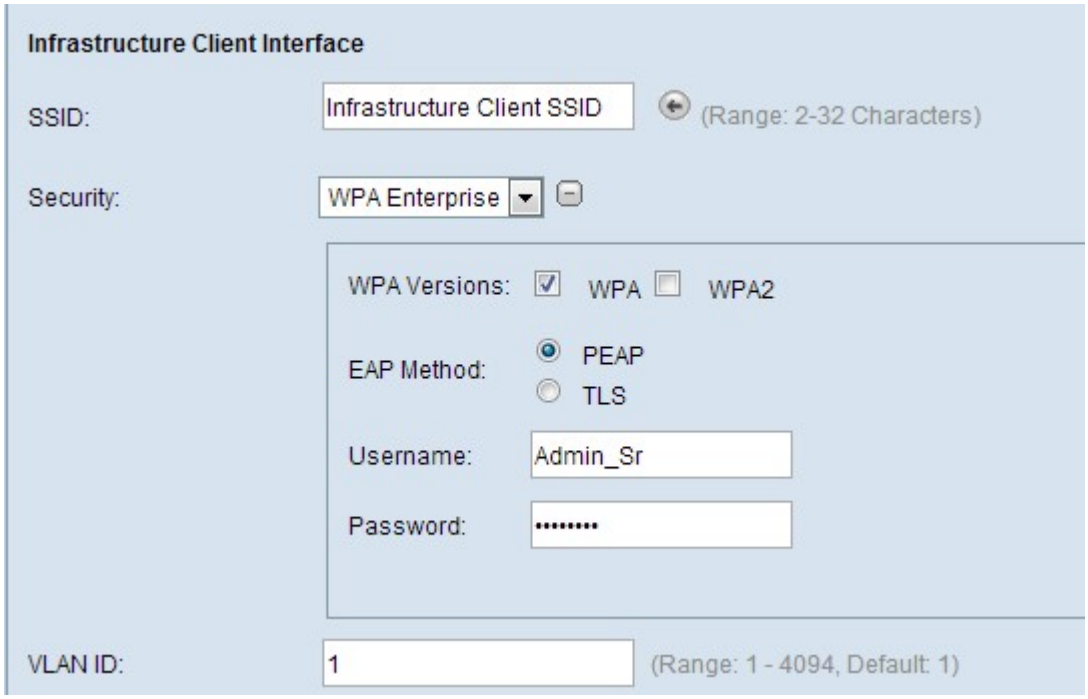


Passaggio 1. Se si sceglie WPA Enterprise, selezionare **WPA** o **WPA2** per scegliere la versione di WPA. Di solito WPA viene scelto solo se nessuno dei WAP nel sistema di bridge supporta WPA2. WPA 2 è il più avanzato e consigliato.

Passaggio 2. Fare clic sul pulsante di opzione appropriato per scegliere tra i due metodi EAP.

·PEAP — Protected EAP. 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. Eseguire i passi da 3 a 5.

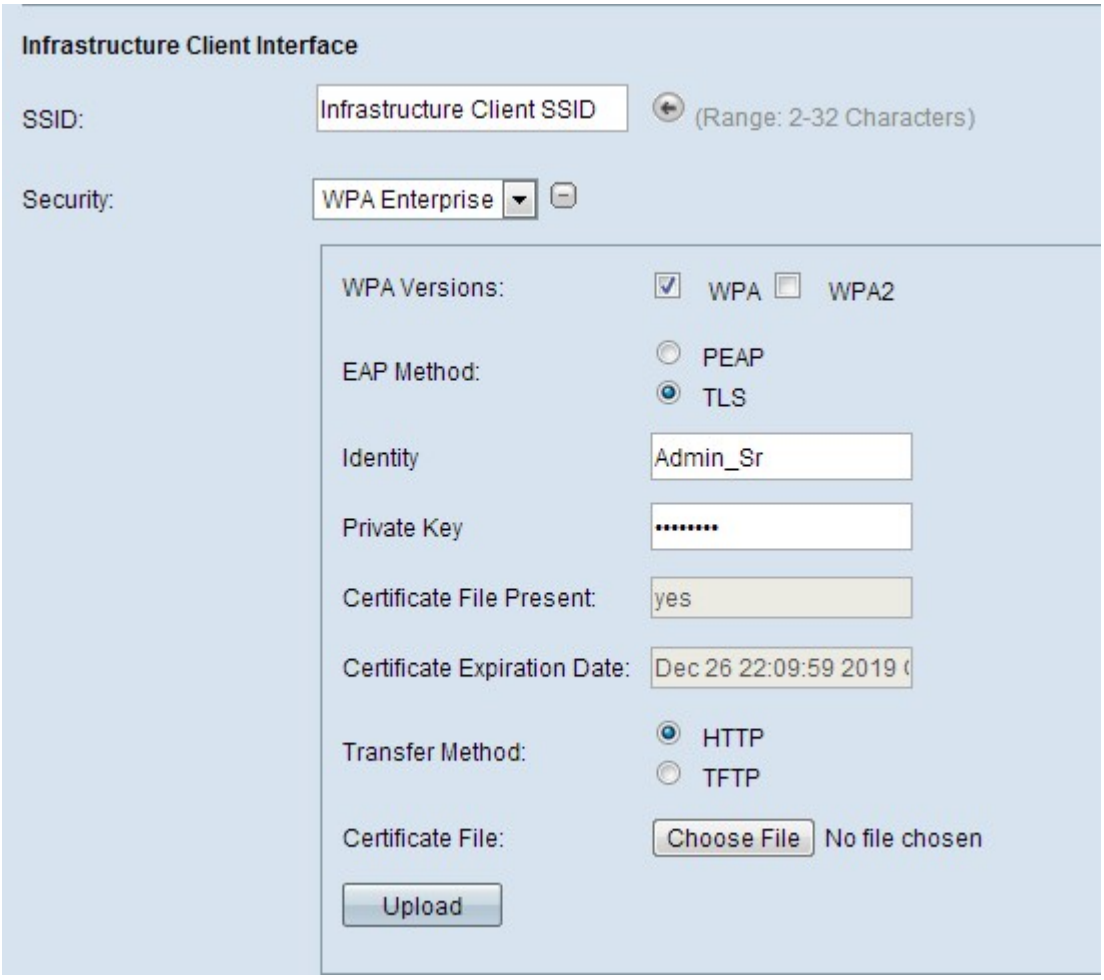
·TLS: autenticazione tramite scambio di certificati digitali. Richiede l'esecuzione dei passi da 3 a 7.



Passaggio 3. Indipendentemente dal metodo scelto nel Passaggio 1, immettere un nome utente nel campo Nome utente.

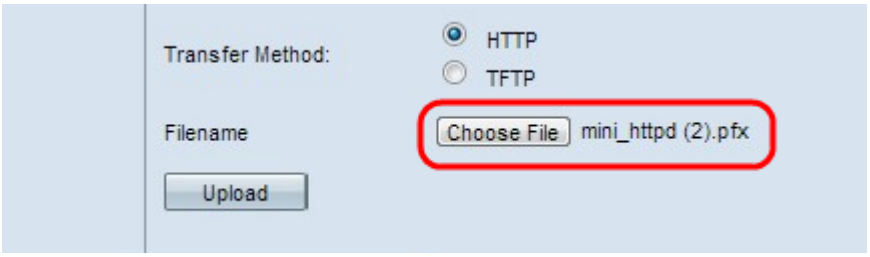
Passaggio 4. Indipendentemente dal metodo scelto nel passaggio 1, immettere una password nel campo Password.

Passaggio 5. Se è stato scelto PEAP, fare clic qui per continuare la configurazione. Se è stato scelto TLS, andare al passo 6.



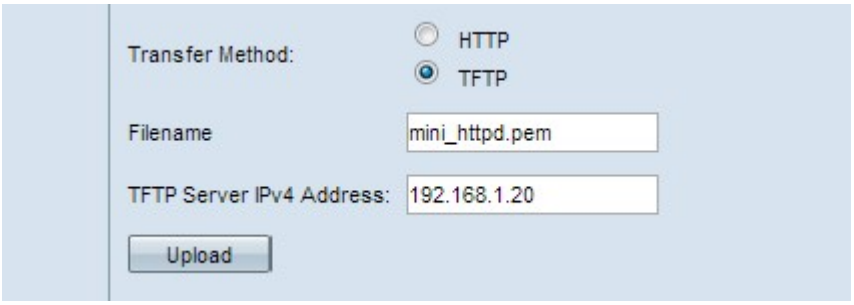
Passaggio 6. Se si sceglie TLS, fare clic sul pulsante di opzione **HTTP** o **TFTP** per scegliere tra le due modalità di trasferimento per scaricare un file di certificato per l'autenticazione TLS.

·HTTP: download tramite server Web o da PC.



- Scegli file - Fare clic per selezionare un file di certificato. Deve essere un file di tipo certificato con estensione .pem, .pfx, ecc. In caso contrario, il caricamento del file non riuscirà.

·TFTP: download da un file server. È necessario eseguire azioni.



- Nome file - Immettere il nome del file di certificato nel campo Nome file.

- Indirizzo IPv4 server TFTP - Immettere l'indirizzo IP del server TFTP.

Nota: nel campo Trasferimento file certificato viene indicato se nel WAP è presente un certificato e nel campo Data scadenza certificato viene visualizzata la data di scadenza del certificato corrente.

Passaggio 7. Fare clic su **Upload**.

Fare clic qui per continuare con la configurazione.