Risoluzione dei problemi di una rete Mesh wireless Cisco Business

Obiettivo

Questo documento copre diverse aree da analizzare quando si risolvono i problemi delle reti mesh Cisco Business Wireless (CBW).

Se si dispone di una rete wireless tradizionale, è consigliabile consultare la sezione Risoluzione dei problemi di una rete wireless aziendale Cisco tradizionale.

Dispositivi interessati | Versione firmware

- 140AC (Scheda tecnica) | 10.1.1.0 (scarica la versione più recente)
- 141ACM (scheda tecnica) | 10.1.1.0 (scarica la versione più recente)
- 142ACM (scheda tecnica) | 10.1.1.0 (scarica la versione più recente)
- 143ACM (scheda tecnica) | 10.1.1.0 (scarica la versione più recente)
- 145AC (Scheda tecnica) | 10.1.1.0 (scarica la versione più recente)
- 240AC (Scheda tecnica) | 10.1.1.0 (scarica la versione più recente)

Sommario

Introduzione

Le reti wireless a mesh sono fantastiche, ma ammettiamolo, le cose succedono! Proprio come qualsiasi rete wireless, un certo numero di cose può causare problemi. A volte c'è una soluzione semplice, mentre altre potrebbero essere più complicate.

Se non conosci i termini di questo documento, controlla Cisco Business: glossario dei nuovi termini.

Per prestazioni e affidabilità ottimali, tenetele a mente!

1. Accertarsi che l'area abbia copertura completa per il numero previsto di client e le relative applicazioni. Per ottimizzare le prestazioni dell'intera infrastruttura wireless, potrebbe essere necessario aggiungere ulteriori punti di accesso wireless.
2. Tenere presente i tipi di applicazioni che potrebbero utilizzare (o come amministratore, i tipi di applicazioni consentiti).
3. I client che eseguono applicazioni di streaming video utilizzano una maggiore larghezza di banda rispetto a quelli che utilizzano programmi di solo audio in streaming. Le applicazioni video si affidano al buffering per fornire un'esperienza decente.
4. I client che eseguono applicazioni vocali richiedono un servizio immediato senza ritardi e con un utilizzo ridotto della larghezza di banda. Poiché non è possibile memorizzare una chiamata vocale nel buffer, è molto importante che i pacchetti non vengano scartati.

Sei pronto per la risoluzione dei problemi? Scaviamo dentro!

In questa sezione attivata/disattivata vengono evidenziati i suggerimenti per i principianti.

Accesso

Accedere all'interfaccia utente Web dell'access point primario. A tale scopo, aprire un browser Web e immettere https://ciscobusiness.cisco.com Prima di procedere, è possibile che venga visualizzato un messaggio di avviso. Immettere le credenziali.È inoltre possibile accedere all'access point primario immettendo https://[ipaddress] (dell'access point primario) in un browser Web.

Descrizione comandi

In caso di domande su un campo nell'interfaccia utente, cercare una descrizione comando simile alla seguente: 

Impossibile individuare l'icona Espandi menu principale.

Passare al menu sul lato sinistro dello schermo. Se il pulsante del menu non è visibile, fare clic su

questa icona per aprire il menu della barra laterale. 

Cisco Business App

Questi dispositivi dispongono di app complementari che condividono alcune funzionalità di gestione con l'interfaccia utente Web. Non tutte le funzionalità nell'interfaccia utente Web saranno disponibili nell'app.

Scarica app iOS Scarica l'app Android

Domande frequenti

Se hai ancora domande a cui non hai risposto, puoi controllare il nostro documento delle domande frequenti. Domande frequenti

Per iniziare la risoluzione dei problemi, consultare le nozioni di base.

Verifica delle condizioni fisiche e ambientali

Questo è il modo più semplice per risolvere i problemi, ma viene spesso ignorato. Anche se possono sembrare ovvi, è bene iniziare con le basi.

1. Tutte le apparecchiature sono accese?
2. C'è potere in tutto?
3. La luce del collegamento è costantemente accesa? Le luci verdi sono un buon segno!
4. I cavi sono collegati correttamente?
5. Potrebbe essere un cavo non valido?
6. Qualche apparecchiatura è surriscaldata?
7. Vi possono essere fattori ambientali come la sua ubicazione?
8. Sono presenti pareti di metallo o spesse tra l'access point e il dispositivo wireless?
9. Se il client non è in grado di connettersi, potrebbe non essere compreso nell'intervallo consentito?

Altri elementi da considerare

1. Riavviare il punto di accesso
2. Per i punti di accesso che si connettono a uno switch, controllare la configurazione dello switch e verificare che lo switch funzioni correttamente. L'utilizzo della CPU, della temperatura e della memoria deve essere inferiore ai livelli di soglia specificati.
3. Nell'interfaccia utente Web, in *Monitoraggio*, controllare il *dashboard wireless* per raccogliere informazioni sulle prestazioni e altri problemi.
4. Abilitare *Bonjour* e *Link Layer Discovery Protocol (LLDP)* sul router, se disponibile.
5. Abilita *inoltro multicast wireless* quando disponibile per le applicazioni di gioco e streaming.
6. Verificare che tutti gli access point primari compatibili si trovino sulla stessa VLAN.
7. Se è stato eseguito l'accesso all'access point principale tramite wireless e si modificano alcune impostazioni, ad esempio la VLAN, è possibile che la connessione venga interrotta. La connessione all'access point principale via cavo consente di mantenere la connessione

stabile.

Number of SSIDs

Ogni SSID richiede l'invio di un frame beacon ogni 100 millisecondi (ms), che può occupare molto spazio nell'utilizzo dei canali.

Èconsigliabile limitare il numero totale di SSID nell'access point a 1-2 SSID per radio o per access point, anche se la rete mesh può supportare fino a un limite fisico di 16 SSID per radio.

Si verificano problemi durante l'accesso all'access point primario?

Probabilmente hai provato ad accedere a *ciscobusiness.cisco* e stai riscontrando un problema. Ecco alcuni semplici suggerimenti:

- Se le configurazioni del giorno zero sono appena state completate, chiudere l'app e riavviarla.
- Assicurarsi che sia selezionato l'SSID (Service Set Identifier) corretto. Questo è il nome creato per la rete wireless.
- Accedere all'access point primario con *https://<indirizzo IP dell'access point primario>*. L'indirizzo AP principale è l'indirizzo IP assegnato utilizzato nella procedura di configurazione iniziale. Se in quel momento si è deciso di non assegnare un indirizzo manuale, controllare sul router l'indirizzo IP DHCP assegnato alla pagina di gestione del punto di accesso primario. L'indirizzo di gestione verrà assegnato all'indirizzo MAC 00:00:5e:00:01:01.
- Una volta eseguita la configurazione iniziale, verificare che *https://* sia utilizzato per accedere a *ciscobusiness.cisco* o per immettere l'indirizzo di gestione IP nel browser Web. A seconda delle impostazioni configurate, è possibile che nel browser sia stato inserito automaticamente *http://* poiché è stato utilizzato il primo accesso.
- Il problema potrebbe riguardare il browser. Ad esempio, in Firefox si dovrebbe fare clic sul menu in alto a destra dello schermo. Selezionare **Guida > Informazioni sulla risoluzione dei problemi** e fare clic su **Aggiorna Firefox**.
- Disconnetti qualsiasi rete privata virtuale (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.
- Se si dispone di un telefono Android, è possibile che si stia utilizzando un DNS (Domain Name Server) privato e che sia necessario disattivare questa funzionalità per la connettività. Per verificare questa condizione, in genere è possibile trovarla in Impostazioni > Rete e Internet > Avanzate > DNS privato.

Sui punti di accesso è in esecuzione la versione più recente?

Perché è importante

Il firmware, noto anche come software, è incorporato nel punto di accesso. L'aggiornamento del firmware migliora le prestazioni e la stabilità del punto di accesso. Gli aggiornamenti possono includere nuove funzionalità o correggere una vulnerabilità rilevata nella versione precedente del software. È davvero così importante? Assolutamente! È fondamentale che tutti i link per gli aggiornamenti siano stati aggiunti nella sezione Versione firmware di questo articolo. Questa

potrebbe essere una soluzione semplice da provare in caso di problemi di rete. Se la versione del firmware non corrisponde, è possibile che si verifichino dei problemi durante l'aggiunta del primo dispositivo Mesh Extender a una rete. Perché non aggiornarli immediatamente?

Èestremamente importante aggiornare tutti i dispositivi Mesh Extender prima di aggiornare i punti di accesso primari.

Sebbene sia possibile aggiornare il firmware in diversi modi, si consiglia di utilizzare *Cisco.com* per l'aggiornamento. Per assistenza nell'aggiornamento del firmware, consultare il documento sull' aggiornamento del software di un Cisco Business Wireless Access Point.

Risoluzione dei problemi di aggiornamento

A volte l'aggiornamento non avviene senza problemi. È possibile provare a eseguire alcune semplici operazioni:

1. Aggiornare o chiudere il browser Web.
2. Cancellare la cache del browser e accedere nuovamente all'access point primario. Il processo varia in base al browser Web utilizzato.
3. Fare clic su una pagina o scheda alternativa nell'interfaccia utente Web del punto di accesso principale, quindi tornare alla pagina Aggiornamento software e provare a scaricare di nuovo l'immagine del firmware.
4. Prova un nuovo browser Web. Se ad esempio si utilizza Chrome e non funziona, provare Firefox.
5. In rari casi, se la pagina di gestione non è riuscita ad avviare l'aggiornamento del firmware o non risponde (nessun cambiamento di stato dopo l'avvio dell'aggiornamento), potrebbe essere necessario spegnere/accendere tutti i punti di accesso e le estensioni mesh della rete e ripetere l'aggiornamento del firmware.

Vi si applica una di queste situazioni?

- Se si utilizza la porta Ethernet downstream sul CBW240, passare a un'altra porta.
- Se si utilizza un portale vincolato, evitare di utilizzare browser basati su Chrome, incluso Microsoft Edge. A volte potrebbe non essere possibile collegarsi alla rete. Potrebbe essere semplice come utilizzare Firefox come il browser.
- Se un client utilizza una connessione VPN senza split tunneling/split DNS, la pagina di gestione CBW potrebbe non essere accessibile e l'app mobile potrebbe non funzionare. Provare a disabilitare temporaneamente la VPN sul client per accedere alle funzioni di gestione CBW.
- Se nel client è abilitato il DNS privato, le query DNS vengono crittografate e non possono essere intercettate dalla CBW. Ciò impedirà il funzionamento dell'app mobile Cisco Business e la risoluzione di ciscobusiness.cisco. Si consiglia di gestire la connessione CBW da un client aggiunto alla rete senza DNS privato oppure di gestire la connessione CBW utilizzando l'interfaccia utente Web tramite l'indirizzo IP di gestione.
- Verificare che i dispositivi CBW non siano configurati nella stessa VLAN di un controller Cisco Wireless LAN.

Potrebbe trattarsi di un problema di connettività?

Esegui test di connettività dall'interfaccia utente Web

Per essere efficace, l'access point deve essere in grado di comunicare con altri dispositivi. Per verificare questa condizione, è possibile eseguire un ping.

Eseguire il ping dell'access point da almeno due client connessi (associati) a quel particolare punto di accesso.

Eseguire il ping tra il router e l'indirizzo IP del punto di accesso per verificare se è disponibile una connettività end-to-end. Eseguire il ping tra il router e i client wireless associati all'access point per verificare se sono raggiungibili dalla rete principale.

Potenziali problemi DHCP

Anche se probabilmente è stato assegnato un indirizzo IP statico all'access point primario, questo deve comunque avere accesso a un server DHCP. Il server DHCP deve essere operativo e raggiungibile dalla porta LAN Ethernet dell'access point. Questa operazione è necessaria affinché l'access point primario possa fornire indirizzi IP per tutti gli access point e i client che si uniscono alla rete. Se dopo un riavvio sul sistema principale lampeggia una luce rossa, è possibile che si tratti di un problema.

Sebbene sia possibile scegliere un indirizzo IP statico per la gestione della larghezza di banda, si applica solo all'indirizzo IP di gestione. Ogni punto di accesso, incluse le estensioni mesh, necessita di un indirizzo IP separato per la sua funzionalità. L'indirizzo MAC di gestione è 00:00:5e:00:01:01.

Anche se tutti gli indirizzi CBW sono configurati come statici, l'aggiunta di un nuovo punto di accesso o di un'estensione mesh richiede comunque un server DHCP per l'installazione iniziale del nuovo dispositivo, anche se in seguito si prevede di passare a un indirizzo IP statico.

Èpossibile che vi siano più client che necessitano di un indirizzo IP di quanti non siano disponibili nel pool DHCP. Per ulteriori informazioni, vedere la sezione *Come visualizzare o modificare il pool di indirizzi IP per DHCP* nell'articolo Best Practices for Setting Static IP Addresses on Cisco Business Hardware.

In alcuni casi nella cache vengono memorizzati troppi indirizzi DHCP, il che può impedire ai client di ottenere un indirizzo IP. Per ulteriori informazioni, vedere Suggerimenti per mantenere la tabella ARP disponibile per gli indirizzi IP DHCP. Se lo si desidera, è possibile riavviare il router.

Supporto Windows

Se si utilizza Windows, selezionare la connessione wireless dal pannello Connessioni di rete e verificare che lo stato sia *Abilitato*.

Per ulteriori informazioni, visitare il forum del supporto Microsoft per la risoluzione dei problemi relativi alla connettività di rete wireless, facendo clic sul collegamento seguente: Risolvere i problemi di connessione Wi-Fi in Windows.

Èpossibile che sia necessario regolare le impostazioni della larghezza di banda

Alcune impostazioni predefinite potrebbero causare problemi di connessione in alcuni dispositivi meno recenti. È possibile provare a modificare le impostazioni seguenti.

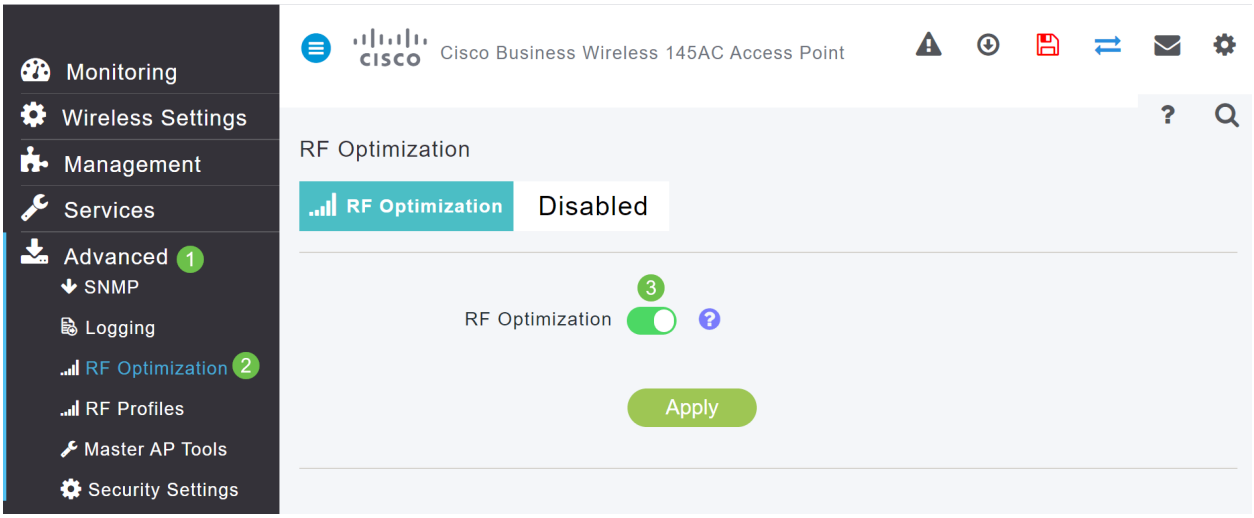
Ottimizzazione RF

Passaggio 1

Accertarsi di utilizzare la *visualizzazione avanzata* per queste impostazioni.

Passaggio 2

Passare a **Avanzate > Ottimizzazione RF**. Attiva *Ottimizzazione RF*.

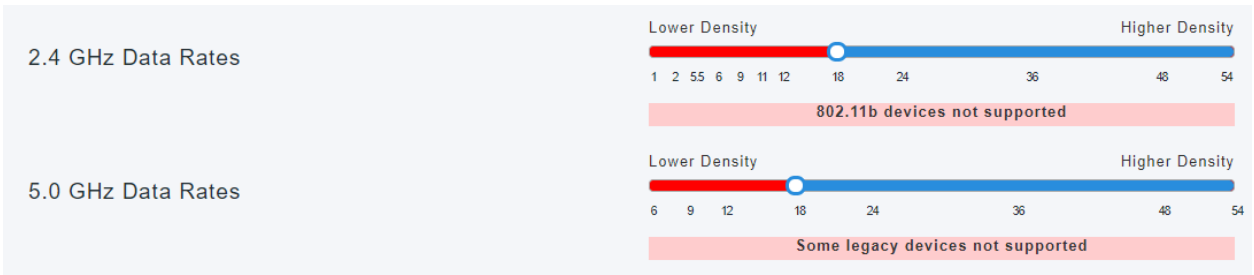


Passaggio 3

Scorrere verso il basso fino alla parte inferiore della schermata. All'interno di ciascuna velocità dati radio, rimuovere il supporto per velocità di controllo inferiori per rimuovere i client della modalità wireless legacy meno recenti, ad esempio i client 802.11b.

Passaggio 4

Verrà visualizzato un messaggio che informa che i dispositivi meno recenti non sono supportati. Più a destra scorrete, meno possono collegarsi.



Nomi gruppi bridge

Se la rete è stata configurata con tutti gli access point in base alle impostazioni predefinite

Quando avete eseguito le configurazioni del giorno zero per la rete mesh, è stato creato automaticamente un BGN. Corrisponde al primo SSID (Service Set Identifier) immesso, fino ai primi 10 caratteri. Questo BGN viene utilizzato nei punti di accesso per associare e verificare che rimangano connessi correttamente. Se si configura l'access point principale e quindi si uniscono gli access point subordinati, il BGN deve corrispondere automaticamente senza ulteriori configurazioni necessarie.

Se si reimposta un punto di accesso primario o si sposta un punto di accesso configurato su una nuova rete

Se si ripristina il valore predefinito sull'access point primario o si spostano gli access point da una rete configurata a un'altra, è possibile che i BGN non corrispondano.

Quando un access point tenta di connettersi a una rete in uno scenario in cui il BGN non corrisponde ad alcuna rete disponibile, l'access point subordinato tenterà comunque di connettersi temporaneamente alla rete con il segnale più forte. L'access point potrà unirsi alla rete se è elencato e approvato.

Una volta che l'access point si è unito alla rete, poiché il BGN non corrisponde, l'access point subordinato continuerà a cercare un BGN corrispondente ogni 10-15 minuti. In questo modo la connessione verrà interrotta e la connessione verrà nuovamente stabilita se non viene trovato un BGN corrispondente. Ciò può causare molti problemi di connettività nella rete wireless, in particolare quando potrebbe essere presente un segnale wireless più forte proveniente da un'altra rete wireless.

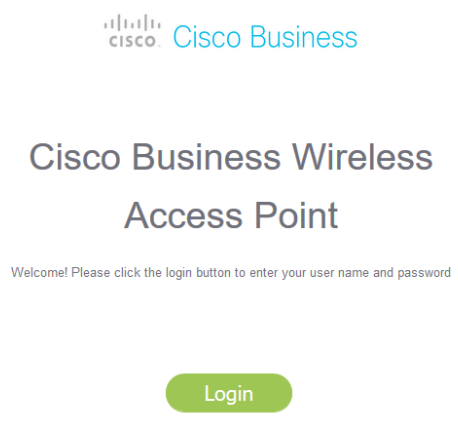
Come soluzione semplice, affinché tutti i punti di accesso possano funzionare insieme, è necessario verificare che il valore BGN di tutti i punti di accesso corrisponda esattamente. Per cancellare il valore BGN sugli altri access point, è possibile eseguire un reset di fabbrica su di essi o modificare manualmente ciascuno di essi in modo che corrisponda.

Se si desidera visualizzare o modificare il nome di un gruppo di bridge (BGN) in un punto di accesso

Si consiglia di assegnare i BGN alle estensioni mesh con il maggior numero di hop, in modo da ridurre il numero di hop. Quindi, assegnare i BGN degli access point primari compatibili. Il BGN dell'access point primario deve essere configurato per ultimo. È possibile visualizzarli e modificarli uno alla volta eseguendo la procedura seguente.

Passaggio 1

Accedere all'access point e immettere le credenziali.

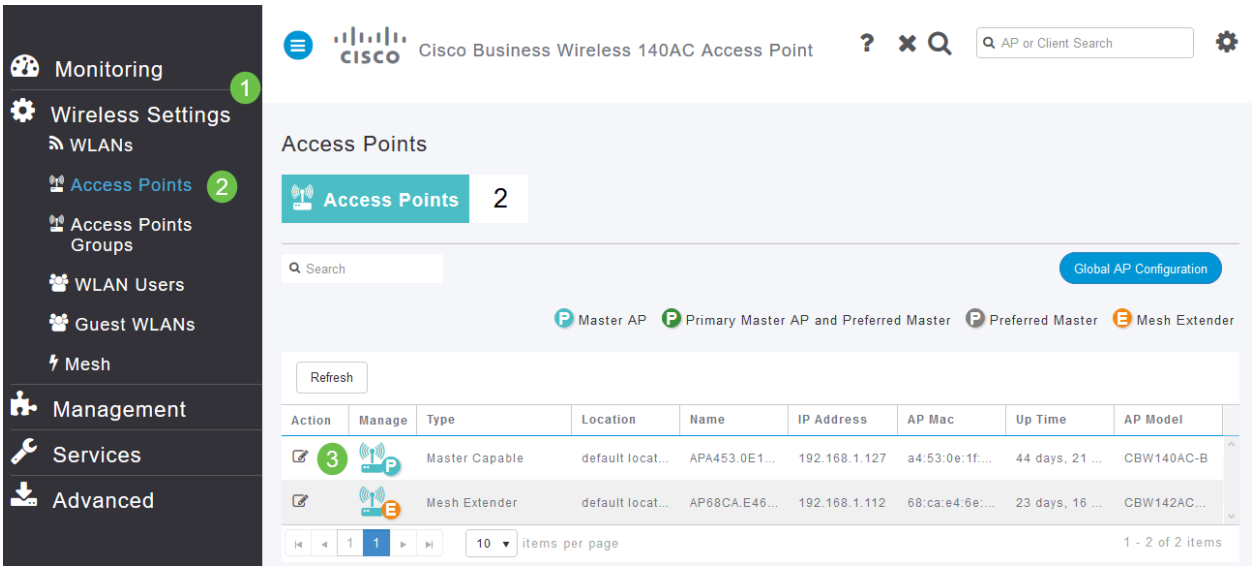


Passaggio 2

Passare alla *visualizzazione Esperti* facendo clic sull'**icona** della **freccia**.

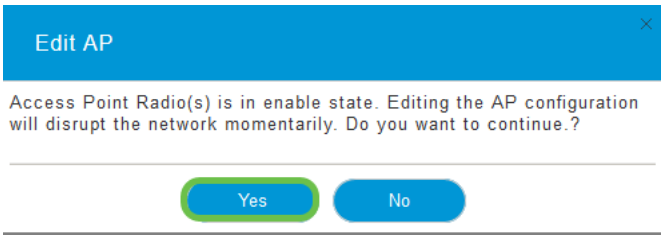
Passaggio 3

Selezionare **Impostazioni wireless > Access Point**. Fare clic sull'**icona Modifica** dell'access point che si desidera modificare o visualizzare.



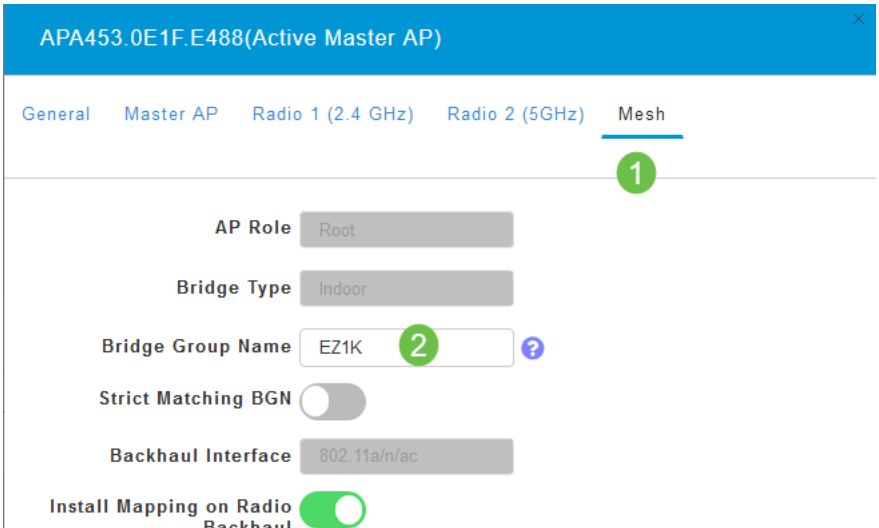
Passaggio 4

Viene visualizzata una schermata di popup in cui viene richiesto di confermare la modifica della configurazione AP. Selezionare **Sì**.



Passaggio 5

Fare clic sulla scheda *Rete*. Qui è possibile visualizzare e modificare il *nome* del *gruppo di bridge*. Se si apportano modifiche, fare clic su **Applica**.



Passaggio 6

Ripetere i passaggi per ogni access point della rete che si desidera controllare. Fare clic sull'**icona Salva** per salvare definitivamente le modifiche. Tenere presente che quando viene assegnato il nome di un gruppo bridge, il dispositivo esegue un riavvio. Dal momento che un riavvio interrompe il Wi-Fi, non è consigliabile durante l'orario di lavoro.

Consenti elenchi

Per collegare altri punti di accesso primari ed estensori di rete, è necessario creare un elenco di indirizzi consentiti in un punto di accesso primario che includa l'indirizzo MAC (Media Access Control) di tutti i punti di accesso.

Inoltre, gli access point subordinati devono essere elencati in modo che l'access point primario possa accedere e aggiornare gli altri access point, il che è essenziale per mantenere la rete funzionante.

L'elenco Consenti, insieme a tutti gli access point con lo stesso nome BGN, consente una connessione efficiente e coerente. La procedura seguente illustra come aggiungere un indirizzo MAC (Media Access Control) e etichettarlo come elenco Consenti.

Passaggio 1

Ènecessario conoscere l'indirizzo MAC dell'access point. Se si conosce l'indirizzo MAC dell'access point, è possibile andare al passaggio 4.

Un indirizzo MAC include numeri e lettere in coppie, separati da due punti.

Passaggio 2

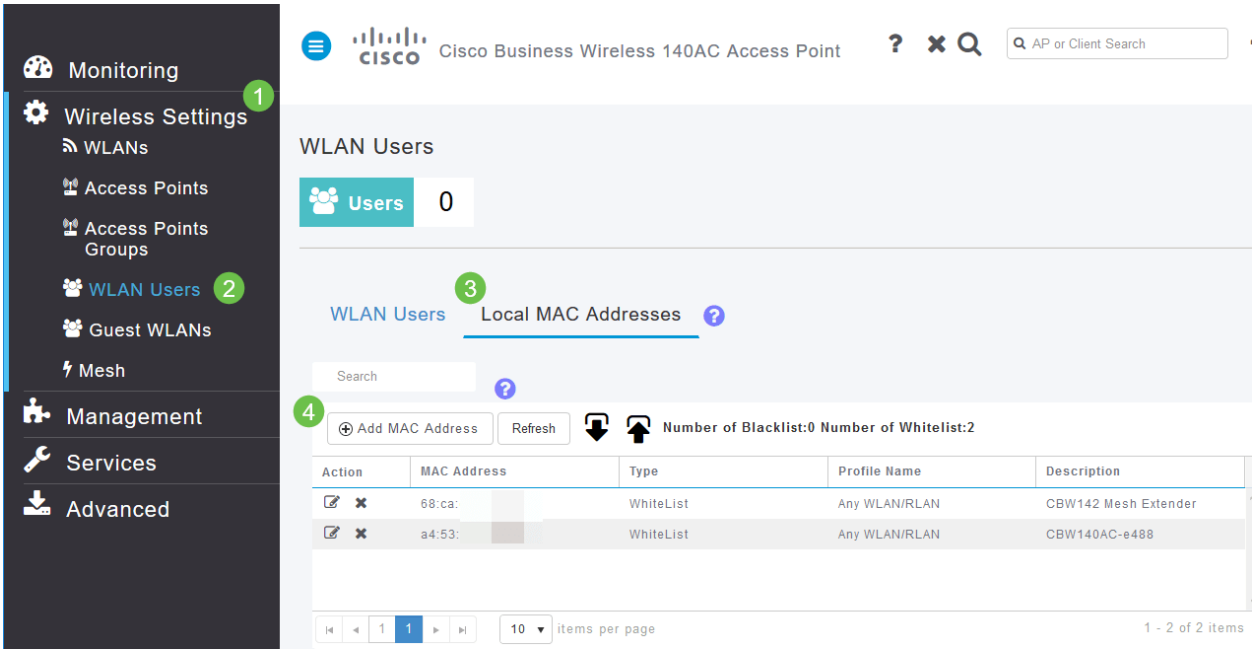
Nella maggior parte dei punti di accesso, l'indirizzo MAC è indicato all'esterno del punto di accesso effettivo. Sui modelli 142ACM e 143ACM è necessario far scorrere l'apparato di alimentazione per visualizzare l'indirizzo MAC. A tale scopo, applicare una leggera pressione sull'access point quando le frecce indicano. Far scorrere e sollevare il componente di alimentazione.

Passaggio 3

Sui modelli 142ACM e 143ACM, l'indirizzo MAC sarà visibile nelle posizioni indicate di seguito.

Passaggio 4

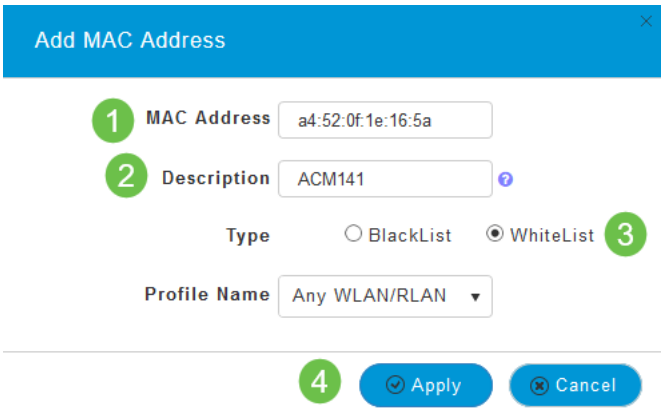
1. Seleziona **impostazioni wireless**
2. Selezione **utenti WLAN**
3. Seleziona **indirizzi MAC locali**
4. Selezionare **Aggiungi indirizzo MAC**



Passaggio 5

Immettere le seguenti informazioni:

1. *Indirizzo MAC*
2. *Descrizione* (fino a 32 caratteri)
3. Selezionare il pulsante di opzione *Consenti elenco*
4. Fare clic su **Applica**



Considerazioni sulle interferenze e sulla spaziatura

Nemici, interferenti e canali RF...oh mio!

Le interferenze possono causare problemi alle reti wireless e possono provenire da un numero di fonti mai raggiunto prima. Microonde, telecamere di sicurezza, smartwatch, rilevatori di movimento o lampadine fluorescenti possono causare interferenze.

L'impatto sulla rete può dipendere da molti fattori, tra cui la quantità di energia emessa se l'oggetto è costantemente acceso o se è intermittente. Più forte è il segnale, più frequentemente è sui problemi che possono sorgere.

I punti di accesso non autorizzati e i client non autorizzati possono causare problemi se sono presenti troppi punti di accesso nello stesso canale.

Le interferenze possono essere un importante inibitore delle prestazioni wireless, creando vulnerabilità della sicurezza e instabilità della rete wireless.

Sono disponibili strumenti per monitorare **i canali attualmente in uso**. Potete anche cambiare canale. Per ulteriori informazioni, consultare i seguenti articoli.

- Identificazione dei client non autorizzati
- Identificazione degli interferenti
- Modifica dei canali RF

Suggerimenti per la spaziatura e la distribuzione

1. Collocare gli estensori di rete nella linea di sito dei punti di accesso primari.
2. Estensori di rete a valle nella linea del sito dell'estensione di rete padre.
3. Gli estensori di rete a valle richiedono un'ottima/eccellente potenza del segnale SSID sul backhaul dai punti di accesso primari a monte.
4. Gli estensori di rete devono avere un valore del rapporto segnale/rumore (SNR) minimo di 30.
5. Evitare di posizionare i dispositivi Mesh Extender troppo vicino ad altri dispositivi Mesh Extender o ad altri punti di accesso primari.

Il grafico seguente elenca le aree di copertura previste in uno spazio aperto. Se si distribuisce la rete in un'area non aperta, ridurre questi valori del 20-30%.

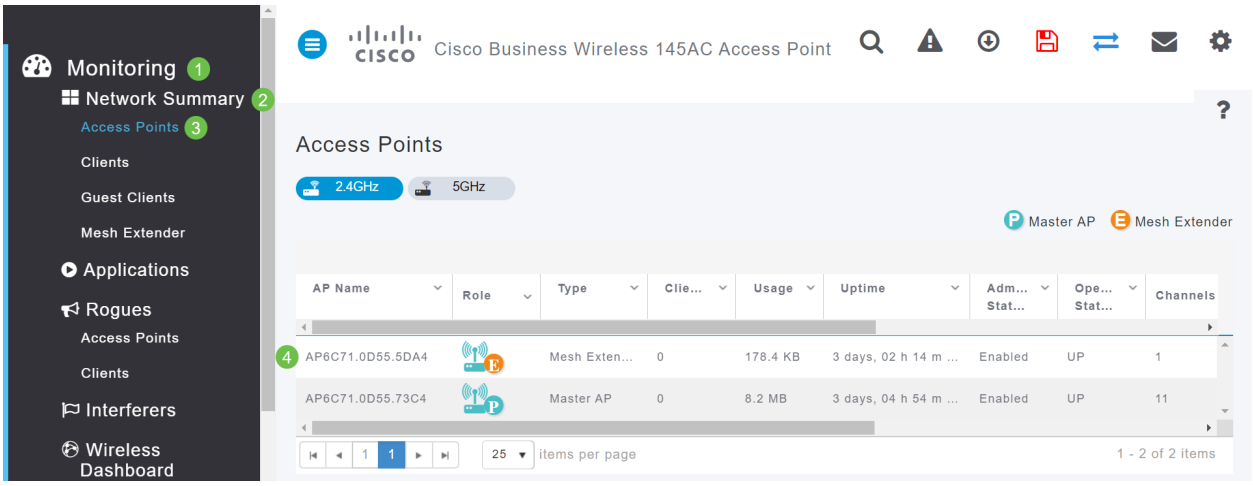
Model	Recommended Distance (Meters)	Recommended Distance (Feet)
CBW240AC	18 - 21	60 - 70
CBW140AC	15 - 18	50 - 60
CBW145AC	15 - 18	50 - 60
CBW141ACM	15 - 18	50 - 60
CBW142ACM	10 - 13	32 - 42
CBW143ACM	10 - 13	32 - 42

Rapporto segnale/rumore tra "hop"

In tutte le reti è necessario utilizzare un segnale forte tra i client e gli access point. In una rete mesh, è inoltre necessario verificare che tra i vari access point sia presente un segnale forte. Se uno degli "hop" non ha un ottimo segnale, un rapporto segnale/rumore più elevato, sarà necessario risolvere il problema. Potrebbe essere necessario regolare la posizione o controllare la causa dell'interferenza.

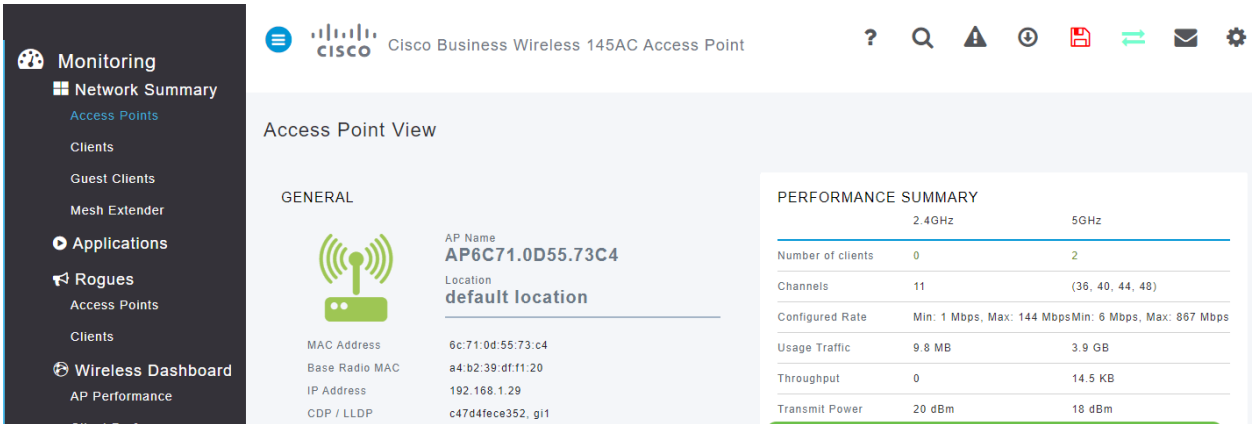
Passaggio 1

Passare a **Monitoraggio > Riepilogo rete > Access Point** e fare clic su un punto di accesso qualsiasi nella tabella per verificare la potenza del segnale client associato.



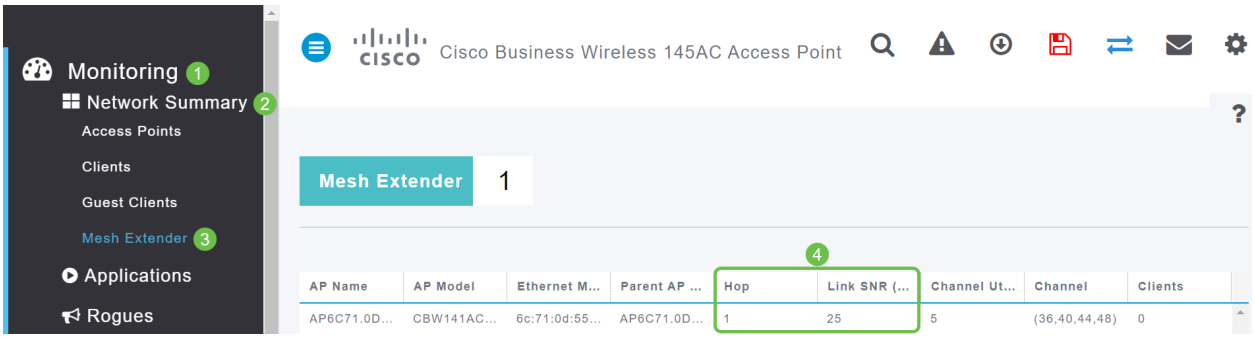
Passaggio 2

Dopo aver aperto *Access Point View*, controllare le informazioni in *Riepilogo prestazioni*.



Passaggio 3

Potete anche raccogliere informazioni su tutti i conteggi *hop* delle estensioni di mesh e sul *rapporto segnale/rumore*. Passare a **Monitoraggio > Sintetico rete > Mesh Extender**.



Date un'occhiata dietro la tenda

Syslog

Il rilevamento degli eventi consente di garantire il corretto funzionamento della rete e di evitare errori. I syslog sono utili per la risoluzione dei problemi di rete, il debug del flusso di pacchetti e il monitoraggio degli eventi.

Questi registri possono essere visualizzati nell'interfaccia utente Web dell'access point primario e, se configurati, nei server di registro remoti. Gli eventi in genere vengono cancellati dal sistema al riavvio se non vengono salvati su un server remoto.

Per ulteriori informazioni, vedere Impostazione dei log dei messaggi di sistema (syslog) su una rete CBW.

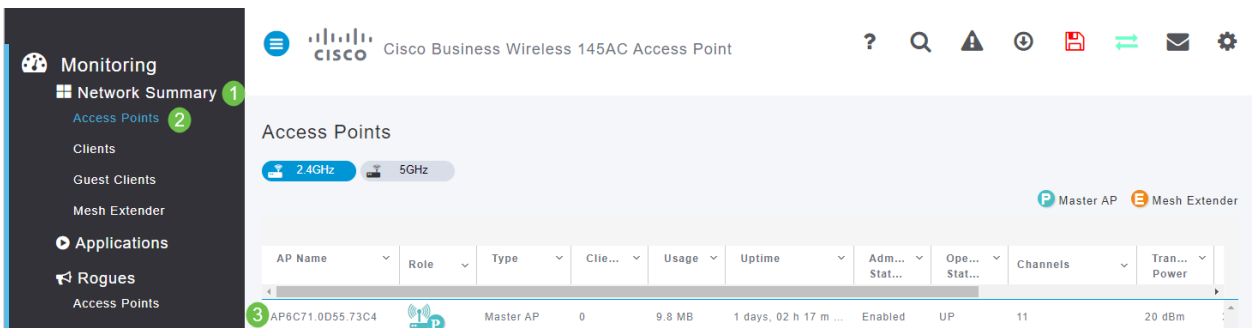
Pacchetto di supporto

Una funzione disponibile su questa apparecchiatura CBW è di scaricare un pacchetto di supporto. Un pacchetto di supporto è uno strumento utile per la risoluzione dei problemi. Fornisce i log di avvio dell'access point e specifica le configurazioni applicate. Per avere un quadro completo, potrebbe essere necessario farlo su ogni punto di accesso.

Prima di scaricare il pacchetto di supporto sull'access point principale, accertarsi di eseguire la versione più aggiornata del firmware. Per aggiornare il firmware, selezionare il collegamento corretto in Periferiche applicabili | Versione firmware. Per assistenza nell'aggiornamento del firmware, consultare il documento sull'aggiornamento del software di un Cisco Business Wireless Access Point.

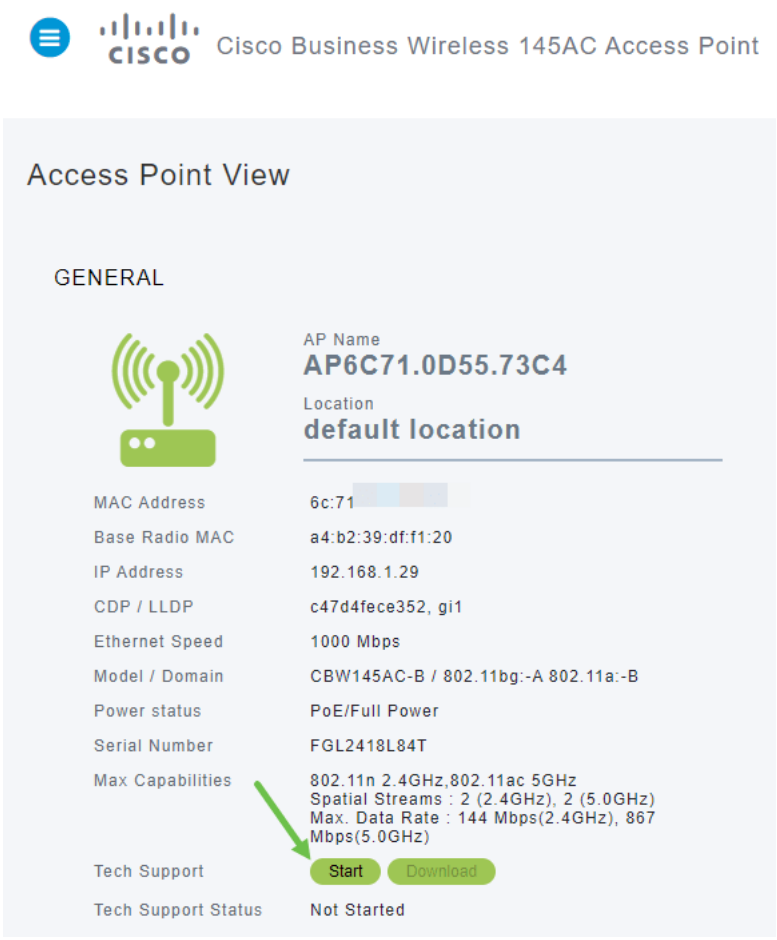
Passaggio 1

Per scaricare il pacchetto di supporto tecnico specifico per la funzionalità dei punti di accesso, selezionare **Monitoraggio > Access Point**. Selezionare l'access point a cui si desidera accedere.



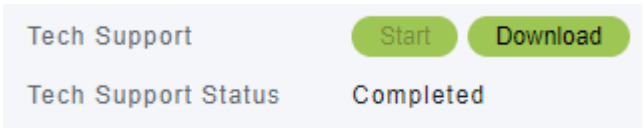
Passaggio 2

Nella sezione *Assistenza tecnica*, selezionare **Start**.



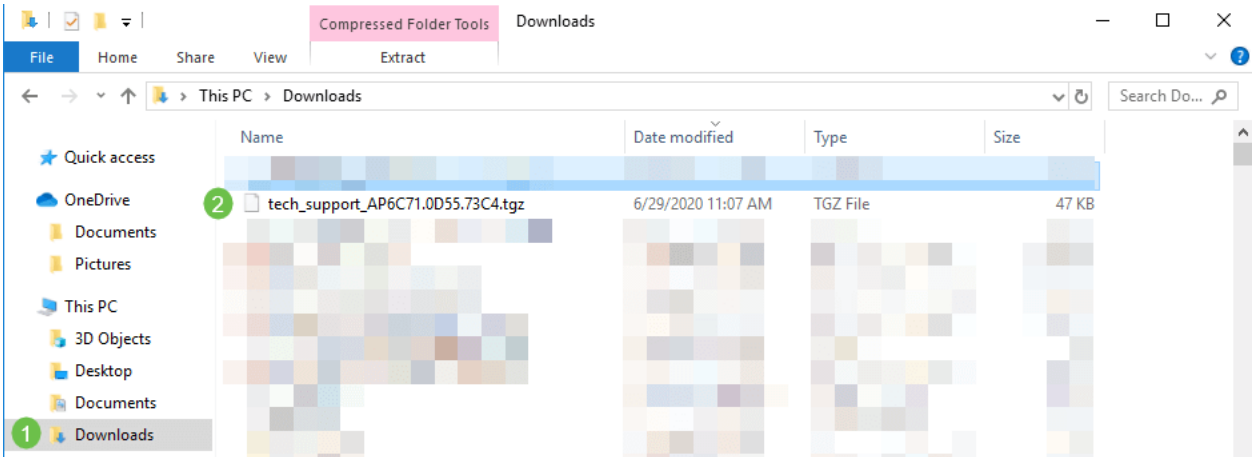
Passaggio 3

Una volta completato il download, verrà visualizzato il messaggio *Stato supporto tecnico* è *completato*. Selezionare il pulsante **Download** per scaricare i file. A questo punto, anche se il download non riesce, viene eliminato dalla memoria dell'access point. Ciò accade se non si consentono i popup.



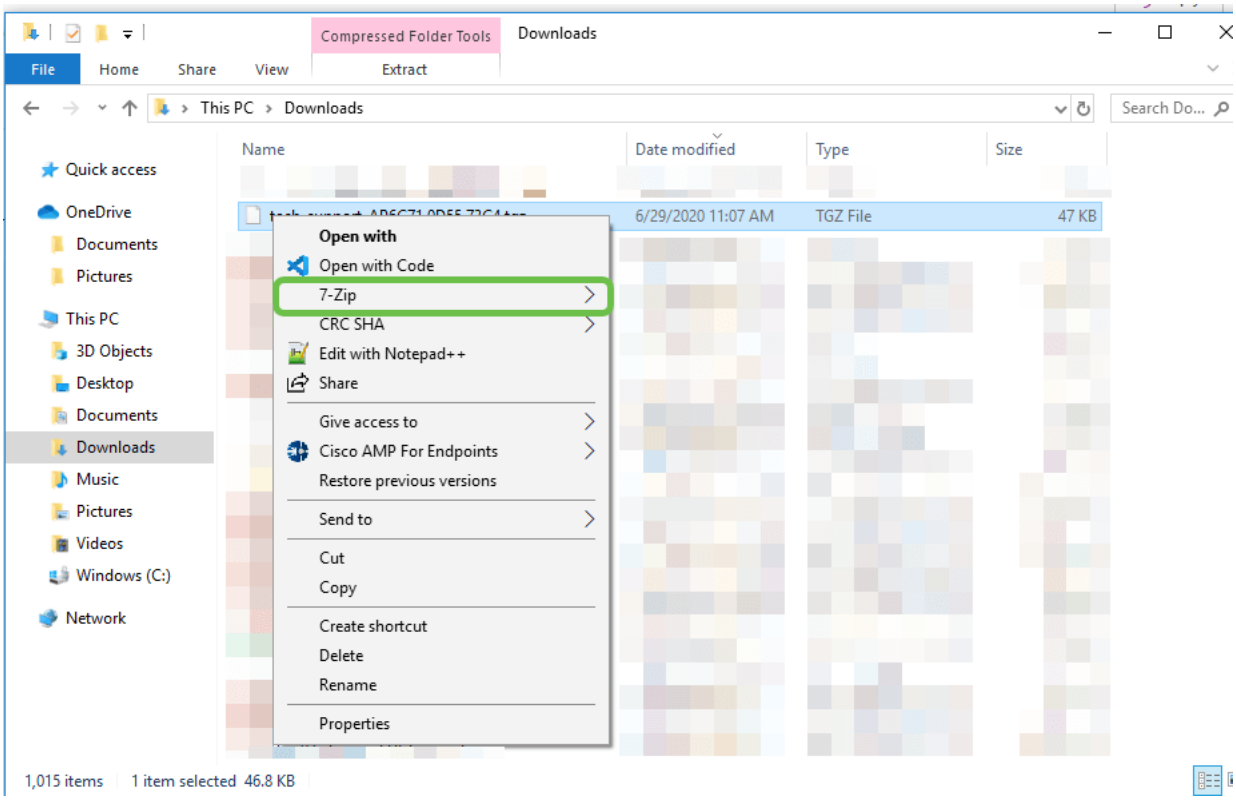
Passaggio 4

Nella cartella *Download* dei file del computer verrà visualizzato un file tech support *.tgz*. I file all'interno di questa cartella devono essere estratti.

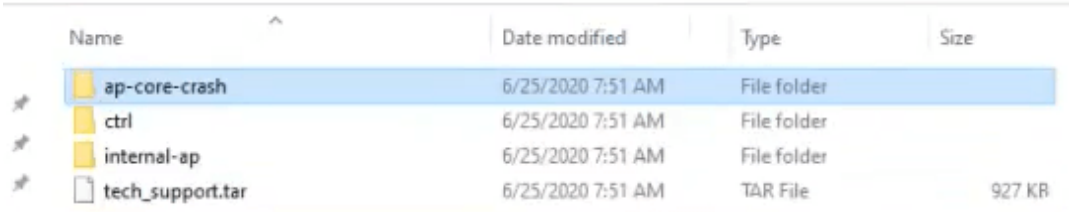


Passaggio 5

Fare clic con il pulsante destro del mouse e selezionare l'applicazione di decompressione da utilizzare. Nell'esempio, è stato usato *7-Zip*. Selezionare per estrarre i file nel percorso selezionato. Per impostazione predefinita, i file vengono inviati alla cartella *Download*.

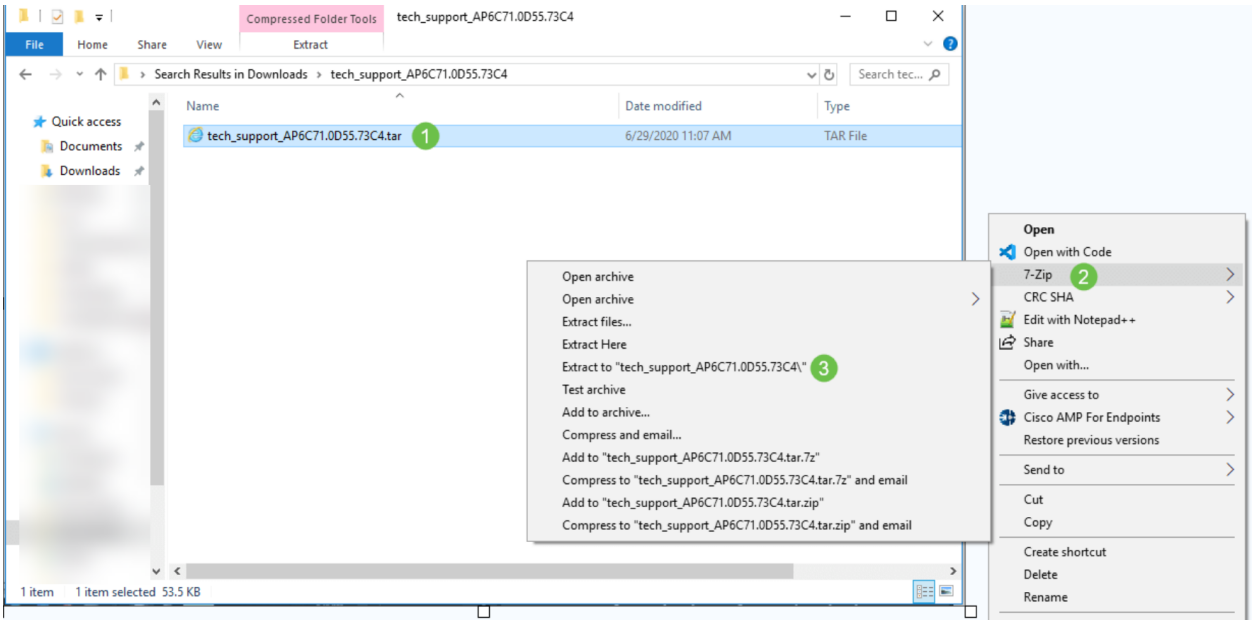


(Visualizzazione alternativa) Se si verifica un arresto anomalo del core, è possibile che vengano visualizzate queste cartelle.



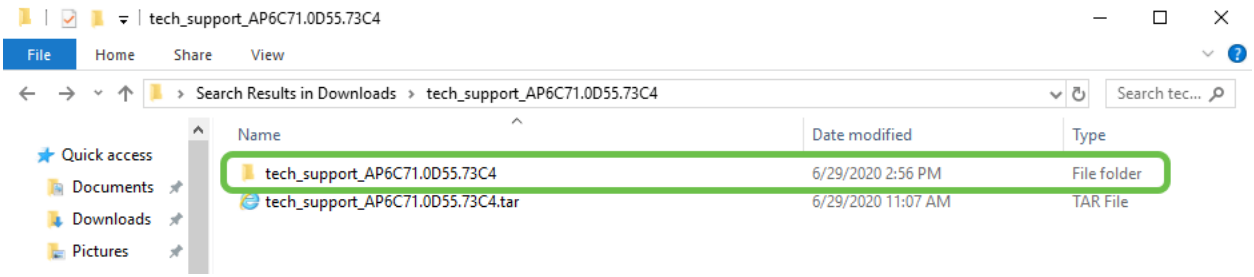
Passaggio 6

Una volta estratti i file dal file *.tgz*, saranno in un file *.tar*. Sarà necessario estrarre nuovamente il file.



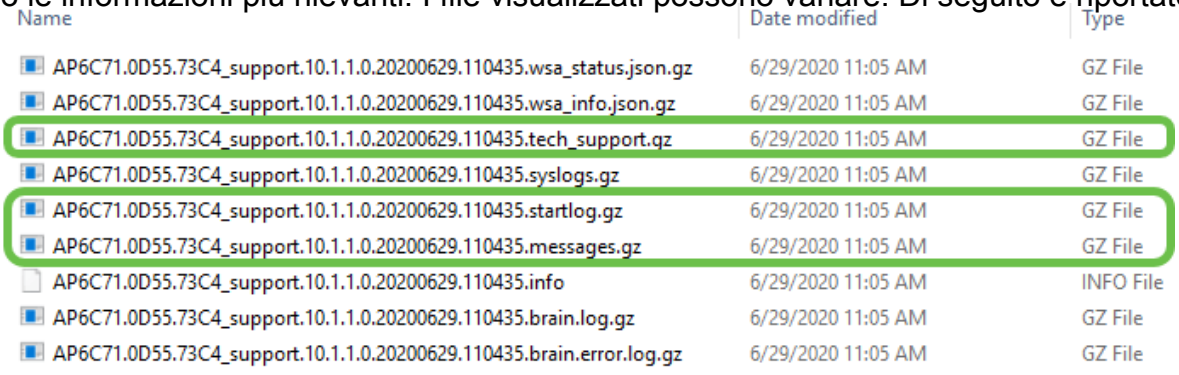
Passaggio 7

Verrà visualizzata la cartella *tech_support*. Fare doppio clic sulla cartella per aprire i file.



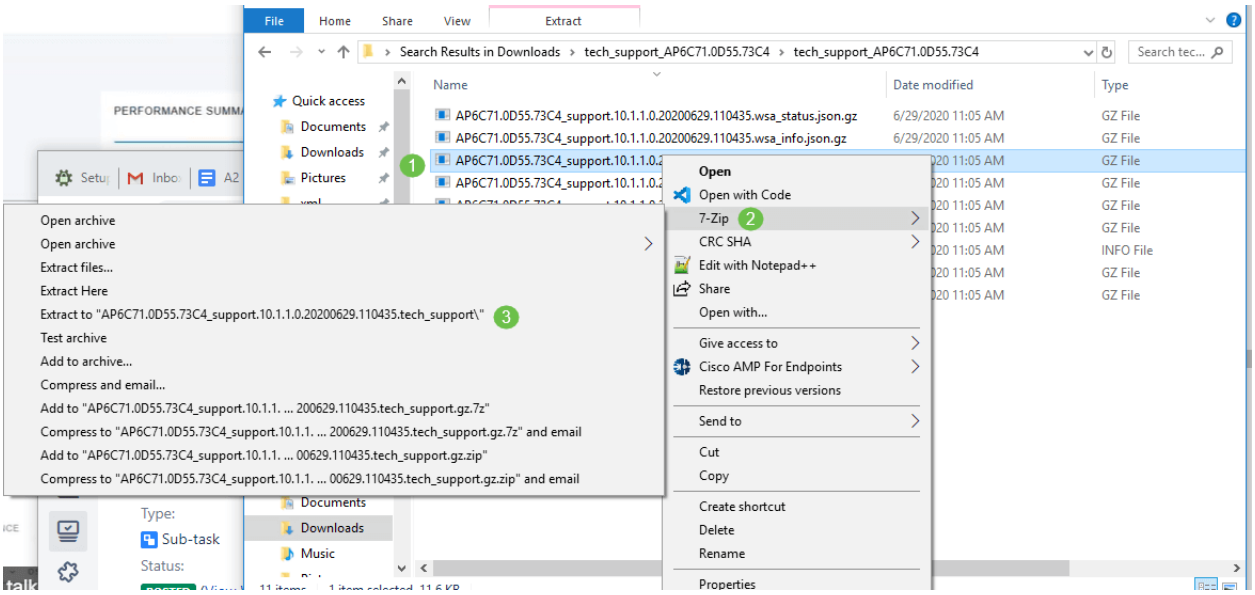
Passaggio 8

All'interno del bundle di supporto, *cli_file* (file di configurazione), *msg/syslogs* (log eventi) e *startlog* forniscono le informazioni più rilevanti. I file visualizzati possono variare. Di seguito è riportato un esempio.



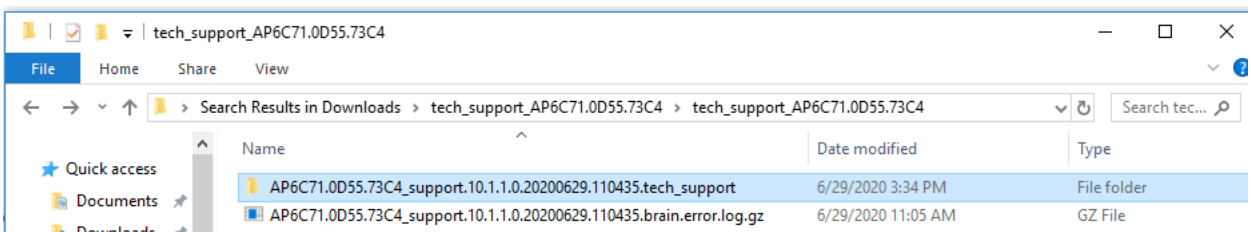
Passaggio 9

Fare clic con il pulsante destro del mouse sul file che si desidera decomprimere. In questo esempio, il file verrà decompresso in una cartella per *tech_support*.



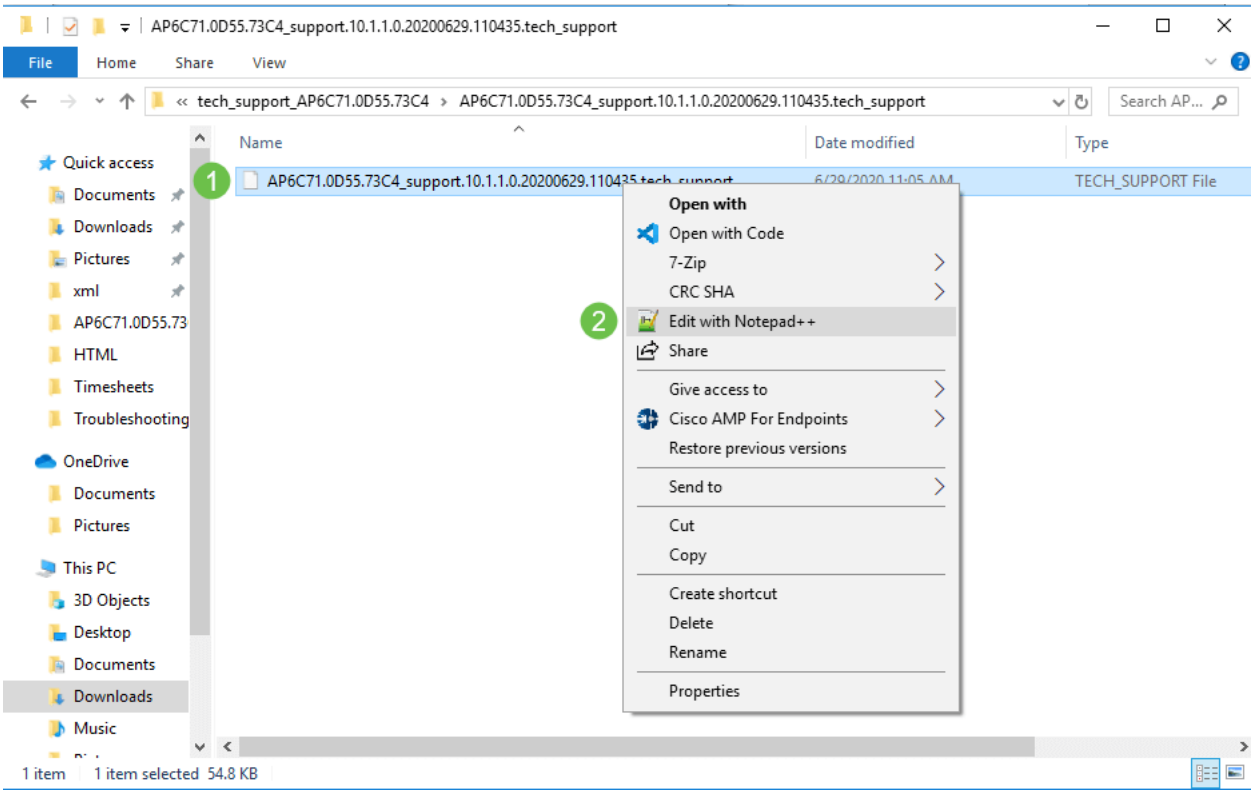
Passaggio 10

Verrà visualizzata la cartella *tech_support*. Fare doppio clic per aprire la cartella.



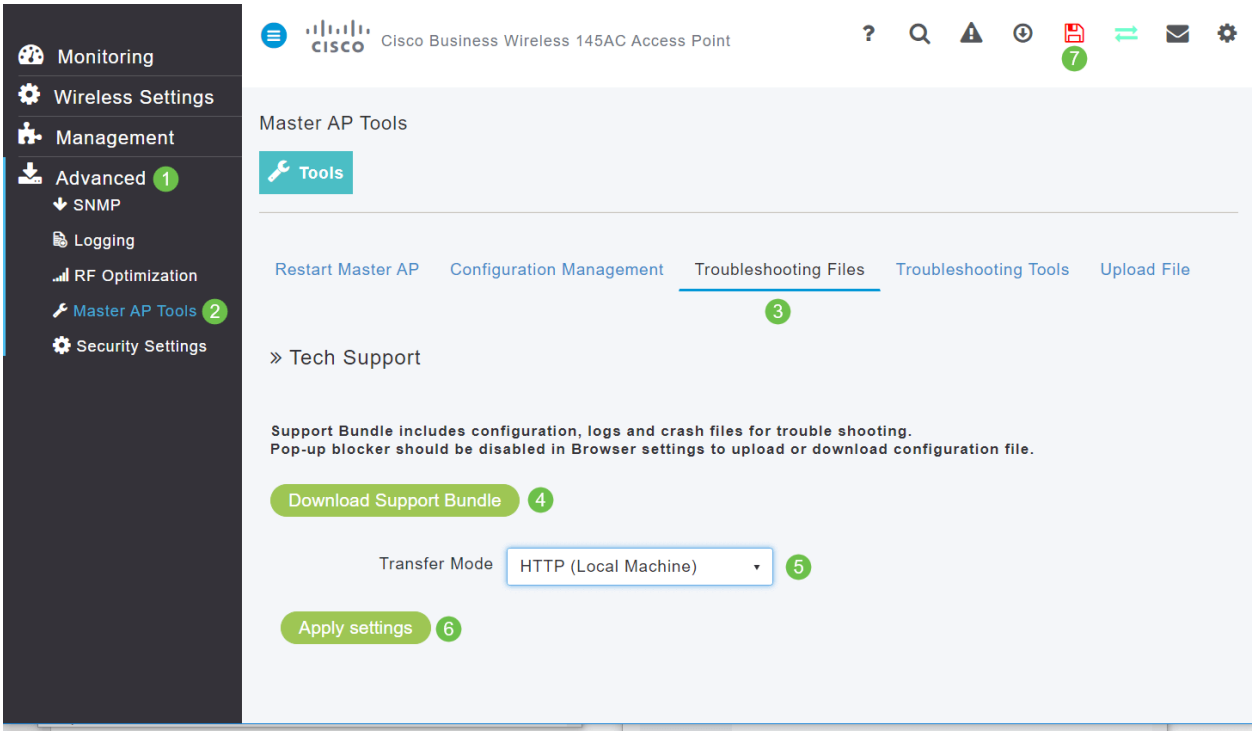
Passaggio 11

Fare clic con il pulsante destro del mouse sul file e selezionare un lettore di file di testo. Nell'esempio riportato di seguito è stato utilizzato **Modifica con Blocco note++**.



Accesso al pacchetto di supporto tecnico AP principale

Il pacchetto di supporto tecnico per il punto di accesso principale è la fonte principale di diagnostica. Per scaricare il pacchetto di supporto tecnico incorporato nell'access point primario o nel bundle del controller virtuale, selezionare **Avanzate > Strumenti principali access point**. Selezionare la scheda *Risoluzione dei problemi*. Selezionare **Download Support Bundle**. Per *Modalità trasferimento*, selezionare *HTTP* o *FTP*. Fare clic su **Applica impostazioni**. Fare clic sull'icona **Salva**.

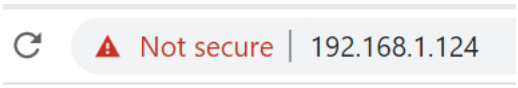


Regolare una delle impostazioni del cellulare CBW

Modificare le impostazioni 802.11r sulla rete CBW

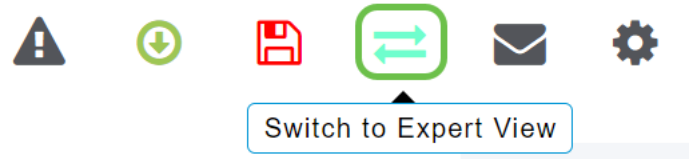
Passaggio 1

Accedere all'interfaccia utente Web immettendo l'indirizzo IP del punto di accesso primario in un browser Web. Verificare di non essere connessi a una rete VPN (Virtual Private Network). In caso contrario, l'operazione non funzionerà. Se vengono visualizzati avvisi di protezione, selezionare le richieste per procedere.



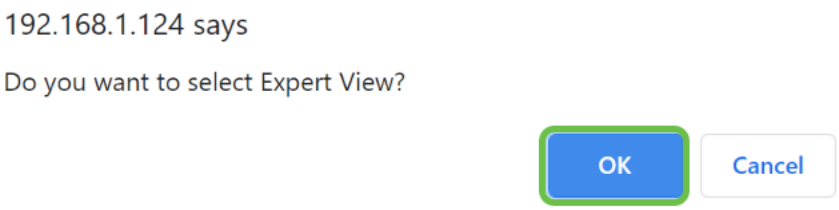
Passaggio 2

Nell'angolo superiore destro dell'interfaccia utente Web, fare clic sulle frecce opposte per passare alla visualizzazione avanzata.



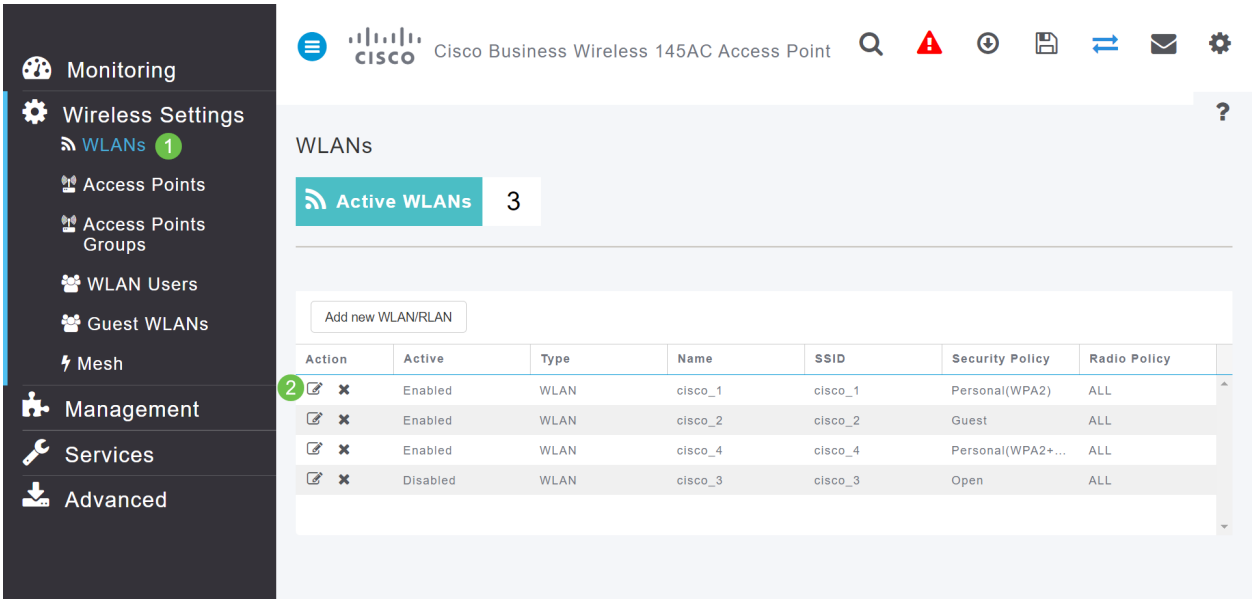
Passaggio 3

Viene visualizzata una finestra popup in cui viene chiesto se si desidera selezionare la visualizzazione per utenti esperti. Fare clic su **OK**.



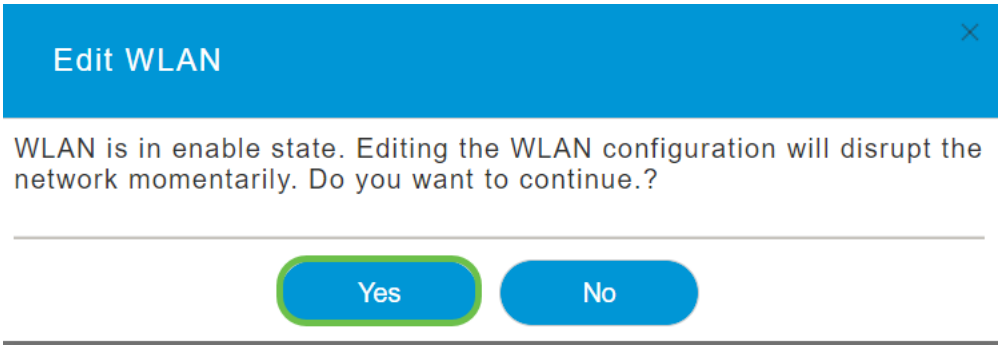
Passaggio 4

Selezionare **WLAN** e l'**icona di modifica** per la WLAN da modificare.



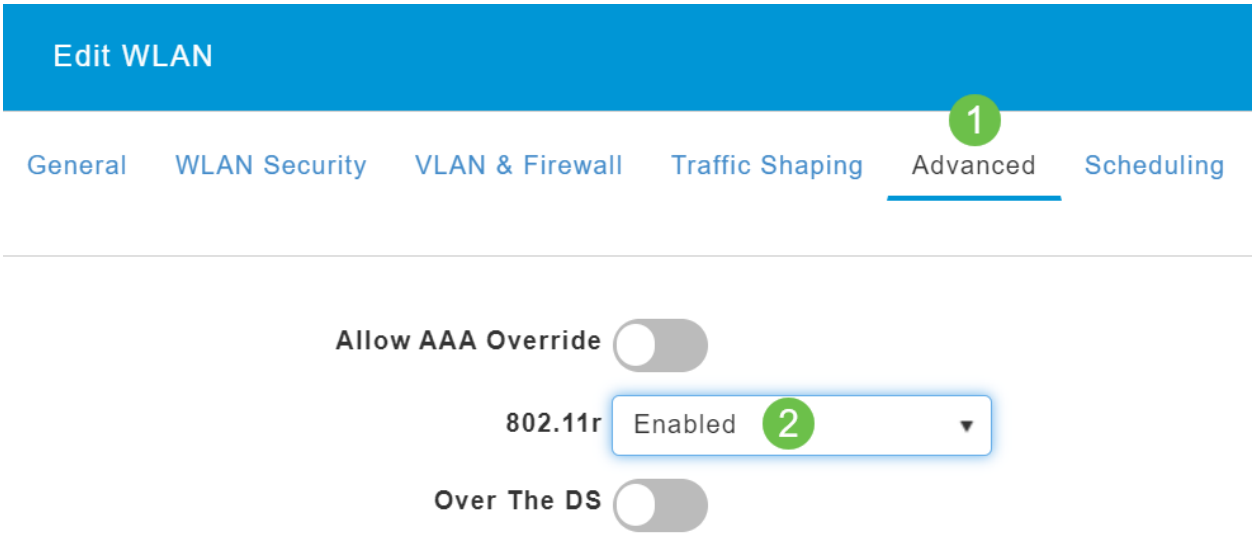
Passaggio 5

Viene visualizzata una finestra popup che chiede se si desidera continuare. Fare clic su **Sì**.



Passaggio 6

Fare clic sulla scheda **Avanzate**. Fare clic sul menu a discesa per 802.11r e selezionare **Abilitato**.



Passaggio 7

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

Passaggio 8

Per salvare definitivamente queste impostazioni, fare clic sull'**icona Salva** nella parte superiore destra dello schermo.

Se il problema persiste, ripristinare le impostazioni predefinite

Un'opzione di ultima istanza, che dovrebbe essere utilizzata solo per risolvere i problemi più gravi, ad esempio la perdita della capacità di accedere al portale di gestione, è quella di eseguire un reset dell'hardware sul router.

Quando si ripristinano le impostazioni predefinite di fabbrica, tutte le configurazioni vengono perse. Sarà necessario configurare nuovamente il router da zero in modo da avere i dettagli della connessione.

Il processo sui nuovi access point CBW è leggermente diverso da quello che si potrebbe verificare sugli altri access point. Per ulteriori informazioni sul ripristino, consultare l'articolo Ripristino delle impostazioni predefinite di fabbrica di un CBW AP.

Conclusioni

La nostra intenzione era di offrirti diverse opzioni per risolvere i problemi della tua rete mesh. Missione compiuta! A questo punto dovrebbe essere disponibile la connettività e si può continuare con la giornata.

Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco

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).