

Fehlerbehebung in einem Cisco Business Wireless Mesh-Netzwerk

Ziel

Dieses Dokument behandelt verschiedene Bereiche, die bei der Fehlerbehebung von Cisco Business Wireless (CBW) Mesh-Netzwerken analysiert werden müssen.

Wenn Sie über ein herkömmliches Wireless-Netzwerk verfügen, sollten Sie sich die [Fehlerbehebung bei einem herkömmlichen Cisco Business Wireless-Netzwerk](#) ansehen.

Unterstützte Geräte | Firmware-Version

- 140AC ([Datenblatt](#)) | 10.1.1.0 (Aktuelle Version herunterladen)
- 141ACM ([Datenblatt](#)) | 10.1.1.0 (Aktuelle Version herunterladen)
- 142ACM ([Datenblatt](#)) | 10.1.1.0 (Aktuelle Version herunterladen)
- 143ACM ([Datenblatt](#)) | 10.1.1.0 (Aktuelle Version herunterladen)
- 145AC ([Datenblatt](#)) | 10.1.1.0 (Aktuelle Version herunterladen)
- 240AC ([Datenblatt](#)) | 10.1.1.0 (Aktuelle Version herunterladen)

Inhalt

- [Beachten Sie diese Punkte, um optimale Leistung und Zuverlässigkeit zu erzielen.](#)
- [Beginnen Sie bei der Fehlerbehebung mit den Grundlagen.](#)
 - [Überprüfen Sie die physischen und Umgebungsbedingungen.](#)
 - [Weitere wichtige Überlegungen](#)
 - [Number of SSIDs](#)
- [Haben Sie Probleme bei der Anmeldung beim primären AP?](#)
- [Wird auf Ihren APs die neueste Version ausgeführt?](#)
 - [Bedeutung](#)
 - [Upgrade-Fehlerbehebung](#)
- [Trifft eine dieser Situationen auf Sie zu?](#)
- [Verbindungsprobleme überprüfen](#)
 - [Ausführen von Verbindungstests über die Webbenutzeroberfläche](#)
 - [Könnte das Problem bei DHCP-Problemen liegen?](#)
 - [Windows-Unterstützung](#)
- [Möglicherweise müssen die Einstellungen angepasst werden.](#)
 - [RF-Optimierung](#)
 - [Namen von Bridge-Gruppen](#)
 - [Zulassungslisten](#)
- [Überlegungen zu Interferenzen und Abständen](#)
 - [Schurken, Störsender und Funkkanäle - oh mein Gott!](#)
 - [Empfehlungen zu Platzbedarf und Bereitstellung](#)
 - [Signal-Rausch-Verhältnis zwischen "Hops"](#)
- [Werfen Sie einen Blick hinter den Vorhang](#)
 - [Syslogs](#)
 - [Support-Paket](#)

- [Zugriff auf das primäre AP Tech Support-Paket](#)
- [Eine der CBW-Mobiltelefoneinstellungen anpassen](#)
- [Wenn alles andere fehlschlägt, auf Werkseinstellungen zurücksetzen](#)

Einleitung

Mesh Wireless-Netzwerke sind großartig, aber seien wir ehrlich, die Dinge geschehen! Wie bei jedem Wireless-Netzwerk können auch hier eine Reihe von Problemen auftreten. Manchmal gibt es eine einfache Lösung, während andere komplizierter sein könnten.

Wenn Sie mit den Begriffen in diesem Dokument nicht vertraut sind, sehen Sie sich Folgendes an: [Cisco Business: Glossar neuer Begriffe](#).

Beachten Sie diese Punkte, um optimale Leistung und Zuverlässigkeit zu erzielen.

1. Stellen Sie sicher, dass der Bereich die erwartete Anzahl an Clients und deren Anwendungen vollständig abdeckt. Möglicherweise müssen weitere Wireless Access Points hinzugefügt werden, um die Leistung in der gesamten Wireless-Infrastruktur zu optimieren.
2. Achten Sie auf die Anwendungstypen, die sie verwenden (oder als Administrator auf die Anwendungstypen, die Sie zulassen).
3. Clients, auf denen Video-Streaming-Anwendungen ausgeführt werden, benötigen mehr Bandbreite als Clients, die nur Audio-Streaming-Programme nutzen. Für Videoanwendungen ist Pufferung die Grundlage für ein anständiges Erlebnis.
4. Clients, auf denen sprachbezogene Anwendungen ausgeführt werden, müssen sofort und ohne Verzögerungen bedient werden, ohne dabei die Bandbreite zu belasten. Da bei einem Sprachanruf keine Pufferung auftritt, ist es sehr wichtig, dass Pakete nicht verworfen werden.


Sind Sie bereit für eine Fehlerbehebung? Lasst uns reingehen!

Diese umschaltbare Sektion zeigt Tipps für Anfänger.

Anmeldung

Melden Sie sich bei der Webbenutzeroberfläche des primären Access Points an. Öffnen Sie dazu einen Webbrowser, und geben Sie <https://ciscobusiness.cisco.com> ein. Möglicherweise erhalten Sie eine Warnung, bevor Sie fortfahren. Geben Sie Ihre Anmeldeinformationen ein. Sie können auch auf den primären Access Point zugreifen, indem Sie [https://\[ipaddress\]](https://[ipaddress]) (des primären Access Points) in einen Webbrowser eingeben.

Quick-Info

Wenn Sie Fragen zu einem Feld in der Benutzeroberfläche haben, überprüfen Sie, ob der Tooltipp wie folgt aussieht: 

Probleme beim Auffinden des Symbols "Hauptmenü erweitern"?

Navigieren Sie zum Menü auf der linken Seite des Bildschirms. Wenn die Menüschaftfläche nicht



angezeigt wird, klicken Sie auf dieses Symbol, um das Menü in der Seitenleiste zu öffnen.

Cisco Business-Anwendung

Diese Geräte verfügen über Begleitanwendungen, die einige Verwaltungsfunktionen mit der Web-Benutzeroberfläche teilen. Nicht alle Funktionen der Web-Benutzeroberfläche sind in der App verfügbar.

[iOS-App herunterladen](#) [Android-App herunterladen](#)

Häufig gestellte Fragen

Wenn Sie noch Fragen haben, können Sie unser Dokument mit häufig gestellten Fragen lesen.

[Häufig gestellte Fragen](#)

Beginnen Sie bei der Fehlerbehebung mit den Grundlagen.

Überprüfen Sie die physischen und Umgebungsbedingungen.

Dies ist die einfachste Methode zur Fehlerbehebung, wird jedoch häufig übersehen. Auch wenn diese offensichtlich erscheinen, ist es gut, mit den Grundlagen zu beginnen.

1. Sind alle Geräte eingeschaltet?
2. Ist alles mit Macht ausgestattet?
3. Haben Sie eine durchgängig aktivierte Verbindungsanzeige? Grüne Lichter sind ein gutes Zeichen!
4. Sind die Kabel richtig angeschlossen?
5. Könnte es ein schlechtes Kabel sein?
6. Ist eines der Geräte überhitzt?
7. Könnte es Umweltfaktoren geben, wie z. B. den Standort?
8. Sind zwischen dem Access Point und dem Wireless-Gerät metallische oder dicke Wände vorhanden?
9. Wenn der Client nicht in der Lage ist, eine Verbindung herzustellen, könnte der Client außerhalb des zulässigen Bereichs liegen?

Weitere wichtige Überlegungen

1. AP neu starten
2. Prüfen Sie bei APs, die eine Verbindung zu einem Switch herstellen, die Switch-Konfiguration, und vergewissern Sie sich, dass der Switch einwandfrei läuft. Die CPU-Auslastung, die Temperatur und die Speichernutzung sollten unter den festgelegten Grenzwerten liegen.
3. Überprüfen Sie in der Webbenutzeroberfläche unter *Überwachung* das *Wireless Dashboard*, um Informationen zur Leistung und zu anderen Problemen zu sammeln.
4. Aktivieren Sie *Bonjour* und *Link Layer Discovery Protocol (LLDP)* auf dem Router, sofern verfügbar.
5. Aktivieren Sie die *Wireless-Multicast-Weiterleitung*, wenn diese für Spiele- und Streaming-Anwendungen verfügbar ist.
6. Vergewissern Sie sich, dass sich alle primären fähigen Access Points im selben VLAN

befinden.

7. Wenn Sie sich drahtlos beim primären Access Point angemeldet haben und bestimmte Einstellungen, z. B. das VLAN, bearbeiten, ist die Verbindung möglicherweise getrennt. Durch die kabelgebundene Verbindung mit dem primären Access Point bleibt diese Verbindung stabiler.

Number of SSIDs

Für jede SSID muss alle 100 Millisekunden (ms) ein Beacon-Frame gesendet werden, was eine hohe Kanalauslastung erfordern kann.

Es empfiehlt sich, die Gesamtzahl der SSIDs auf dem Access Point auf 1-2 SSIDs pro Funkeinheit oder pro Access Point zu begrenzen, obwohl das Mesh-Netzwerk bis zu 16 SSIDs pro Funkeinheit unterstützen kann.

Haben Sie Probleme bei der Anmeldung beim primären AP?

Möglicherweise haben Sie versucht, sich bei *ciscobusiness.cisco* anzumelden, und es treten Probleme auf. Hier einige einfache Vorschläge:

- Wenn Sie gerade die Day Zero-Konfigurationen abgeschlossen haben, schließen Sie die App, und starten Sie sie erneut.
- Vergewissern Sie sich, dass die richtige Service Set Identifier (SSID) ausgewählt ist. Dies ist der Name, den Sie für das Wireless-Netzwerk erstellt haben.
- Melden Sie sich beim primären Access Point mit *https://<IP-Adresse des primären Access Points> an*. Die primäre AP-Adresse ist die zugewiesene IP-Adresse, die Sie bei der Ersteinrichtung verwendet haben. Wenn Sie zu diesem Zeitpunkt die Zuweisung einer manuellen Adresse abgelehnt haben, überprüfen Sie den Router auf die DHCP-IP-Adresse, die Sie der Verwaltungsseite des primären Access Points gegeben haben. Die Management-Adresse wird der MAC-Adresse 00:00:5e:00:01:01 zugewiesen.
- Stellen Sie nach der Ersteinrichtung sicher, dass *https://* verwendet wird, unabhängig davon, ob Sie sich bei *ciscobusiness.cisco* anmelden oder die IP-Management-Adresse in Ihren Webbrowser eingeben. Abhängig von Ihren Einstellungen wurde Ihr Browser möglicherweise automatisch mit *http://* ausgefüllt, da Sie dies bei Ihrer ersten Anmeldung verwendet haben.
- Das Problem kann Ihr Webbrowser sein. Zum Beispiel würden Sie in Firefox auf das Menü oben rechts auf dem Bildschirm klicken. Wählen Sie **Hilfe > Fehlerbehebungsinformationen** und klicken Sie auf **Firefox aktualisieren**.
- Trennen Sie alle Virtual Private Networks (VPNs) für die mobile App oder den Laptop. Möglicherweise sind Sie sogar mit einem VPN verbunden, das Ihr Mobilfunkanbieter verwendet und das Sie möglicherweise noch nicht einmal kennen. Zum Beispiel, ein Android (Pixel 3) Telefon mit Google Fi als Service Provider gibt es ein integriertes VPN, das automatisch verbindet, ohne Benachrichtigung. Dies muss deaktiviert werden, um den primären Access Point zu finden.
- Wenn Sie ein Android-Telefon haben, verwenden Sie möglicherweise einen privaten DNS (Domain Name Server) und müssen diese Funktion möglicherweise deaktivieren, um die Verbindung herzustellen. Sie finden diese Option in der Regel unter **Einstellungen > Netzwerk und Internet > Erweitert > Privater DNS**.

Wird auf Ihren APs die neueste Version ausgeführt?

Bedeutung

Die Firmware, auch Software genannt, ist in den Access Point integriert. Ein Upgrade der Firmware verbessert die Leistung und Stabilität Ihres AP. Upgrades können neue Funktionen umfassen oder eine Schwachstelle beheben, die in der vorherigen Version der Software aufgetreten ist. Ist es wirklich so wichtig? Absolut! Es ist so wichtig, dass alle Links für Upgrades im Abschnitt [Firmware Version](#) dieses Artikels hinzugefügt wurden. Dies kann eine einfache Lösung sein, wenn Sie Netzwerkprobleme haben. Beim Hinzufügen des ersten Mesh Extender zu einem Netzwerk kann es zu Problemen kommen, wenn die Firmware-Version nicht übereinstimmt. Warum also nicht sofort alle aktualisieren?

Es ist äußerst wichtig, alle Mesh Extender zu aktualisieren, bevor Sie die primären fähigen APs aktualisieren.

Sie können die Firmware auf verschiedene Weise aktualisieren, es wird jedoch empfohlen, *Cisco.com* für das Upgrade zu verwenden. Wenn Sie Hilfe bei der Aktualisierung der Firmware benötigen, sehen Sie sich die [Update-Software eines Cisco Business Wireless Access Point an](#).

Upgrade-Fehlerbehebung

Manchmal läuft ein Upgrade nicht reibungslos. Es gibt einige einfache Dinge, die Sie ausprobieren können:

1. Aktualisieren oder schließen Sie den Webbrowser.
2. Löschen Sie den Browser-Cache, und melden Sie sich erneut beim primären Access Point an. Die Vorgehensweise hängt vom verwendeten Webbrowser ab.
3. Klicken Sie auf eine alternative Seite oder Registerkarte in der primären Webbenutzeroberfläche des Access Points, und kehren Sie dann zur Seite für die Softwareaktualisierung zurück, und versuchen Sie erneut, das Firmware-Image herunterzuladen.
4. Testen Sie einen neuen Webbrowser. Wenn Sie z. B. Chrome verwendet haben und es nicht funktioniert, versuchen Sie es mit Firefox.
5. In seltenen Fällen kann es erforderlich sein, alle Access Points und Mesh Extender im Netzwerk auszuschalten bzw. einzuschalten und das Firmware-Upgrade erneut durchzuführen, wenn die Management-Seite das Firmware-Upgrade nicht starten konnte oder nicht reagiert (keine Statusänderung nach dem Start des Upgrades).

Trifft eine dieser Situationen auf Sie zu?

- Wenn Sie den Downstream-Ethernet-Port des CBW240 verwenden, wechseln Sie zu einem anderen Port.
- Wenn Sie Captive Portal verwenden, vermeiden Sie die Verwendung von Chrome-basierten Browsern, einschließlich Microsoft Edge. Manchmal ist es nicht möglich, dem Netzwerk beizutreten. Es könnte so einfach sein, wie Firefox als Browser zu verwenden.
- Wenn ein Client eine VPN-Verbindung ohne Split-Tunneling/Split-DNS verwendet, ist der Zugriff auf die CBW-Verwaltungsseite möglicherweise nicht möglich, und die mobile App funktioniert möglicherweise nicht. Deaktivieren Sie vorübergehend das VPN auf dem Client, um auf die CBW-Verwaltungsfunktionen zuzugreifen.
- Wenn auf dem Client private DNS aktiviert ist, werden DNS-Abfragen verschlüsselt, und sie können von CBW nicht abgefangen werden. Dadurch kann die mobile Cisco Business-App

nicht mehr funktionieren, und die Datei ciscobusiness.cisco wird nicht aufgelöst. Es wird empfohlen, CBW entweder von einem Client aus zu verwalten, der dem Netzwerk ohne privaten DNS beigetreten ist, oder CBW über die Webbenutzeroberfläche über die Management-IP-Adresse zu verwalten.

- Stellen Sie sicher, dass CBW-Geräte nicht im selben VLAN wie ein Cisco Wireless LAN Controller eingerichtet sind.

Könnte es ein Verbindungsproblem sein?

Ausführen von Verbindungstests über die Webbenutzeroberfläche

Der WAP muss mit anderen Geräten kommunizieren können, um effektiv zu sein. Eine einfache Möglichkeit, dies zu überprüfen, besteht darin, einen Ping auszuführen.

Senden Sie einen Ping an den Access Point von mindestens zwei Clients, die mit dem jeweiligen Access Point verbunden sind.

Pingen Sie den Router an die IP-Adresse des Access Points, um festzustellen, ob eine End-to-End-Verbindung verfügbar ist. Senden Sie einen Ping vom Router an die mit dem Access Point verbundenen Wireless-Clients, um zu prüfen, ob diese vom Hauptnetzwerk aus erreichbar sind.

Potenzielle DHCP-Probleme

Auch wenn Sie Ihrem primären WAP wahrscheinlich eine statische IP-Adresse zugewiesen haben, muss dieser WAP dennoch auf einen DHCP-Server zugreifen können. Dieser DHCP-Server muss betriebsbereit und über den LAN-Ethernet-Port des WAP erreichbar sein. Dies ist erforderlich, damit der primäre WAP IP-Adressen für alle WAPs und Clients bereitstellen kann, die dem Netzwerk beitreten. Wenn Sie nach einem Neustart ein rotes Blinken am Primary sehen, könnte dies Ihr Problem sein.

Obwohl eine statische IP-Adresse für die CBW-Verwaltung ausgewählt werden kann, gilt sie nur für die Management-IP-Adresse. Jeder Access Point, einschließlich Mesh Extender, benötigt eine separate IP-Adresse für seine Access Point-Funktionalität. Die Management-MAC-Adresse lautet 00:00:5e:00:01:01.

Selbst wenn alle CBW-Adressen als statisch konfiguriert sind, ist beim Hinzufügen eines neuen AP oder Mesh Extenders für die Erstinstallation des neuen Geräts ein DHCP-Server erforderlich, selbst wenn Sie planen, das Gerät später in eine statische IP-Adresse zu ändern.

Möglicherweise benötigen mehr Clients eine IP-Adresse als im DHCP-Pool verfügbar sind. Weitere Informationen finden Sie im Abschnitt *Anzeigen oder Ändern des Pools mit IP-Adressen für DHCP* im Artikel [Best Practices für das Festlegen statischer IP-Adressen auf Cisco Business-Hardware](#).

In manchen Fällen werden zu viele DHCP-Adressen zwischengespeichert, sodass Clients möglicherweise keine IP-Adresse mehr erhalten. Weitere Informationen hierzu finden Sie in [Tipps, wie Sie die ARP-Tabelle für die DHCP-IP-Adressierung verfügbar halten](#). Sie können den Router auch neu starten, wenn dies praktischer ist.

Windows-Unterstützung

Wenn Sie Windows verwenden, wählen Sie Ihre Wireless-Verbindung im Bereich

Netzwerkverbindungen aus, und überprüfen Sie, ob ihr Status *Aktiviert* ist.

Detaillierte Anleitungen finden Sie im Microsoft Support Forum zur Fehlerbehebung von Wireless-Netzwerkverbindungen, das Sie über den folgenden Link aufrufen können: [Beheben von Wi-Fi-Verbindungsproblemen in Windows](#).

Möglicherweise müssen die CBW-Einstellungen angepasst werden.

Es gibt einige Standardeinstellungen, die bei einigen älteren Geräten zu Verbindungsproblemen führen können. Sie können versuchen, die folgenden Einstellungen zu ändern.

RF-Optimierung

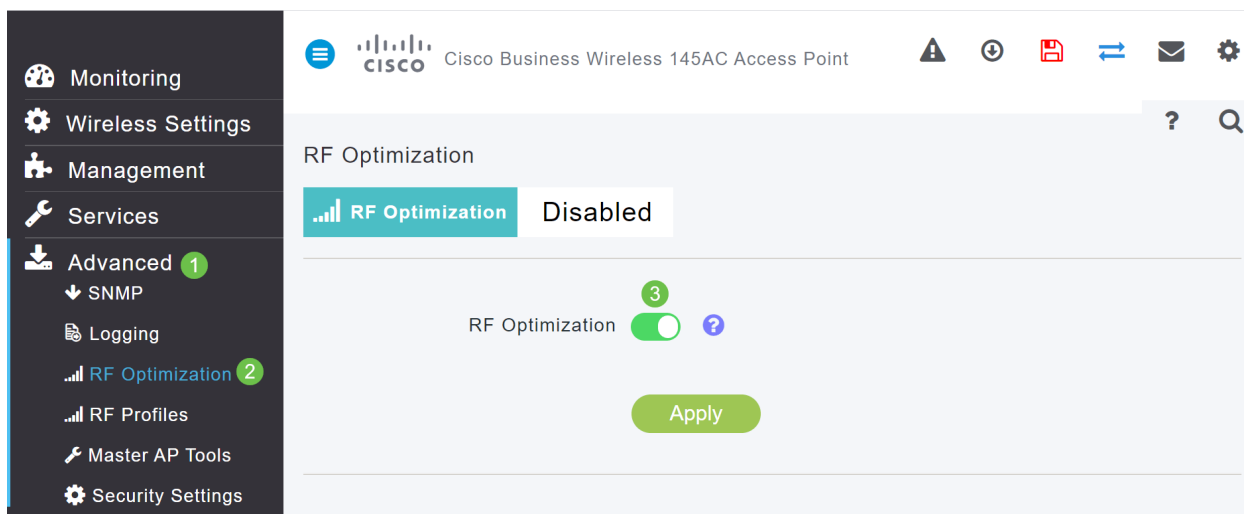
Schritt 1

Vergewissern Sie sich, dass Sie sich für diese Einstellungen in der *Expertenansicht* befinden.



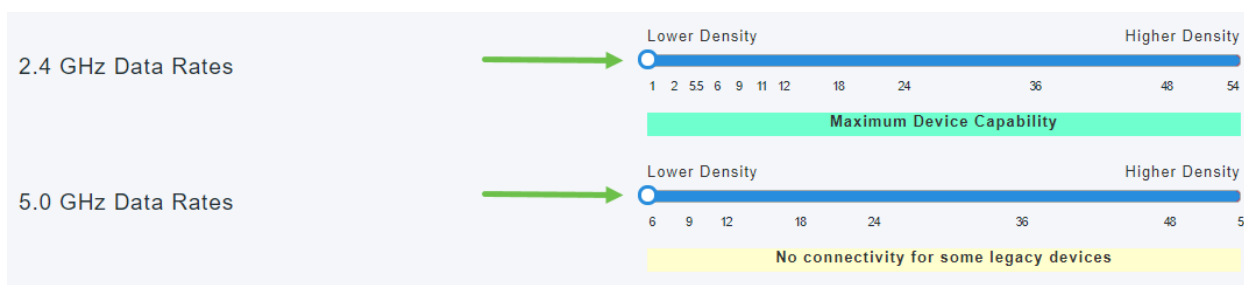
Schritt 2

Navigieren Sie zu **Erweitert > RF-Optimierung**. Schalten Sie auf *RF-Optimierung*.



Schritt 3

Blättern Sie auf diesem Bildschirm nach unten. Innerhalb jeder Funkfrequenz sollten Sie die Unterstützung für niedrigere Kontrollraten deaktivieren, um ältere Wireless-Modus-Clients wie 802.11b-Clients zu entfernen.



Schritt 4

Es wird eine Benachrichtigung angezeigt, dass ältere Geräte nicht unterstützt werden. Je weiter Sie nach rechts schieben, desto weniger können Sie verbinden.



Namen von Bridge-Gruppen

Wenn Sie Ihr Netzwerk mit allen APs werkseitig einrichten

Bei der Durchführung der Day-Zero-Konfigurationen für das Mesh-Netzwerk wurde automatisch ein BGN erstellt. Er entspricht dem ersten von Ihnen eingegebenen Service Set Identifier (SSID) (bis zu den ersten 10 Zeichen). Dieser BGN wird in APs verwendet, um Verbindungen herzustellen und sicherzustellen, dass die APs ordnungsgemäß verbunden bleiben. Wenn Sie Ihren primären Access Point einrichten und anschließend untergeordneten Access Points beitreten, sollte der BGN automatisch ohne weitere Konfigurationen übereinstimmen.

Wenn Sie einen primären Access Point zurücksetzen oder einen konfigurierten Access Point in ein neues Netzwerk verschieben

Wenn Sie den primären Access Point auf die Werkseinstellungen zurücksetzen oder die Access Points von einem konfigurierten Netzwerk in ein anderes verschieben, kann dies zu einer Inkongruenz der BGNs führen.

Wenn ein WAP in einem Szenario, in dem der BGN mit keinem verfügbaren Netzwerk übereinstimmt, versucht, einem Netzwerk beizutreten, versucht der untergeordnete WAP dennoch, vorübergehend mit dem stärksten Signal am Netzwerk teilzunehmen. Der Access Point kann dem Netzwerk beitreten, wenn er "[Allow Listed](#)" ([Liste zulassen](#)) lautet und genehmigt wurde.

Nachdem der WAP dem Netzwerk beigetreten ist und der BGN nicht übereinstimmt, sucht der untergeordnete WAP alle 10 bis 15 Minuten nach einem passenden BGN. Dies führt dazu, dass die Verbindung getrennt wird und erneut eine Verbindung hergestellt wird, wenn kein passender BGN gefunden wird. Dies kann zu zahlreichen Problemen mit der Verbindung im Wireless-Netzwerk führen, insbesondere dann, wenn ein stärkeres Wireless-Signal von einem anderen Wireless-Netzwerk ausgeht.

Damit alle APs zusammenarbeiten können, muss der BGN auf allen APs genau übereinstimmen. Um den BGN der anderen APs zu löschen, können Sie sie auf die Werkseinstellungen zurücksetzen oder manuell eine Übereinstimmung für jeden Access Point ändern.

Wenn Sie einen Bridge-Gruppennamen (BGN) auf einem AP anzeigen oder ändern möchten

Es wird empfohlen, dass BGNs den Mesh Extendern zugewiesen werden, wobei die meisten Hops zuerst konfiguriert werden und eine möglichst geringe Anzahl von Hops verwendet wird. Anschließend müssen die primären, funktionsfähigen APs mit BGNs versehen werden. Der primäre AP-BGN muss als letzter konfiguriert werden. Sie können diese nacheinander anzeigen

und ändern, indem Sie die folgenden Schritte ausführen.

Schritt 1

Melden Sie sich beim AP an, und geben Sie Ihre Anmeldeinformationen ein.



Cisco Business Wireless Access Point

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

Login

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

Schritt 2

Wechseln Sie zur *Expertenansicht*, indem Sie auf das Pfeilsymbol klicken.



Schritt 3

Navigieren Sie zu **Wireless Settings > Access Points**. Klicken Sie auf das **Bearbeitungssymbol** des AP, den Sie bearbeiten oder anzeigen möchten.

Action	Manage	Type	Location	Name	IP Address	AP Mac	Up Time	AP Model
		Master Capable	default locat...	APA453.0E1...	192.168.1.127	a4:53:0e:1f:...	44 days, 21 ...	CBW140AC-B
		Mesh Extender	default locat...	AP68CA.E46...	192.168.1.112	68:ca:e4:6e:...	23 days, 16 ...	CBW142AC...

Schritt 4

In einem Popup-Fenster wird bestätigt, dass Sie die AP-Konfiguration bearbeiten möchten. Wählen Sie **Ja aus**.



Access Point Radio(s) is in enable state. Editing the AP configuration will disrupt the network momentarily. Do you want to continue.?

Schritt 5

Klicken Sie auf die Registerkarte *Mesh*. Hier können Sie den *Bridge-Gruppennamen* anzeigen und ändern. Wenn Sie Änderungen vornehmen, klicken Sie auf **Übernehmen**.

APA453.0E1F.E488(Active Master AP) ×

General Master AP Radio 1 (2.4 GHz) Radio 2 (5GHz) **Mesh**

1

AP Role

Bridge Type

Bridge Group Name 2 ?

Strict Matching BGN

Backhaul Interface

Install Mapping on Radio Backhaul

Ethernet Link Status

Mesh Backhaul Slot ?

5 GHz 2.4 GHz

Ethernet Bridging

Enable

Acti...	Interface Name	Oper Status	Mode	VLAN Id
---------	----------------	-------------	------	---------

0 0

No items to display

3

Schritt 6

Wiederholen Sie die Schritte für jeden Access Point im Netzwerk, den Sie überprüfen möchten. Klicken Sie auf das **Speichersymbol**, um die Änderungen dauerhaft zu speichern. Beachten Sie, dass das Gerät einen Neustart ausführt, wenn ein Bridge-Gruppen-Name zugewiesen wird. Da die Wi-Fi-Verbindung durch einen Neustart unterbrochen wird, wird dies während der Geschäftszeiten nicht empfohlen.



Zulassungslisten

Um andere primärfähige Access Points und Mesh Extender anzuschließen, müssen Sie eine Zulassungsliste für einen primären Access Point erstellen, die die MAC-Adresse (Media Access Control) aller Access Points enthält.

Darüber hinaus müssen untergeordnete WAPs mit einer Zulassungsliste versehen sein, damit der primäre WAP auf die anderen WAPs zugreifen und diese aktualisieren kann. Dies ist für die

Aufrechterhaltung des Netzwerkbetriebs unerlässlich.

Diese Zulassungsliste unterstützt zusammen mit allen APs mit demselben Bridge-Gruppen-Namen (BGN) eine effiziente und konsistente Verbindung. Führen Sie die folgenden Schritte aus, um eine MAC-Adresse (Media Access Control) hinzuzufügen und sie als Zulassungsliste zu kennzeichnen.

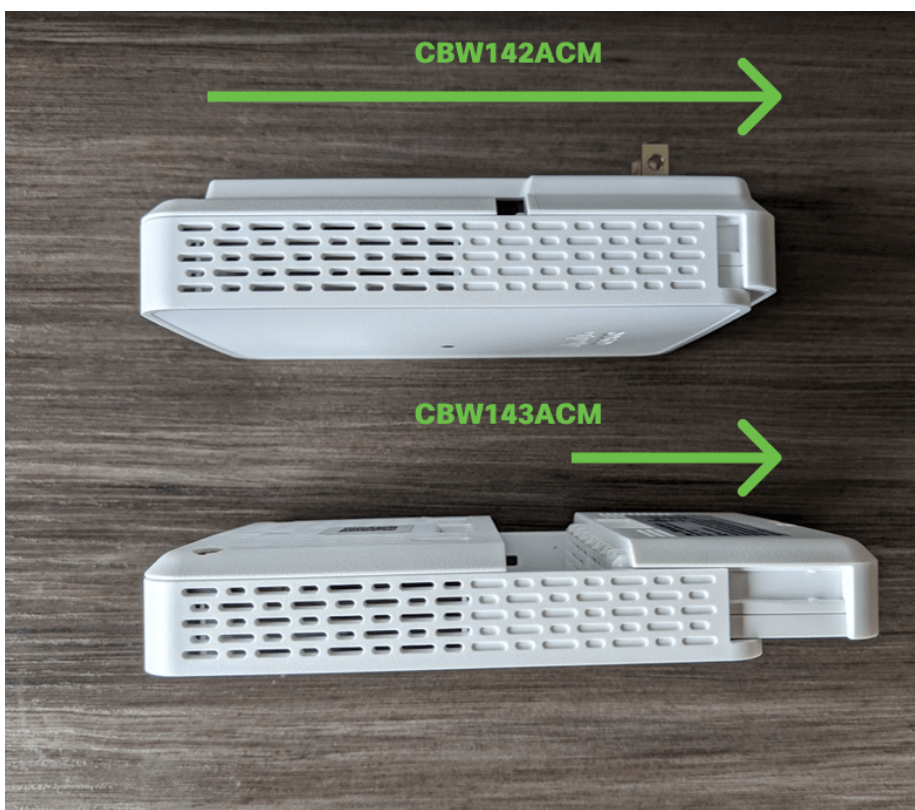
Schritt 1

Sie müssen die MAC-Adresse des Access Points kennen. Wenn Sie die MAC-Adresse Ihres AP kennen, können Sie mit [Schritt 4](#) fortfahren.

Eine MAC-Adresse besteht aus Zahlen und Buchstaben in Paaren, die durch Doppelpunkte voneinander getrennt sind.

Schritt 2

Bei den meisten APs befindet sich die MAC-Adresse außerhalb des eigentlichen AP. Auf dem 142ACM und 143ACM müssen Sie das Stromversorgungsgerät herauschieben, um die MAC-Adresse anzuzeigen. Üben Sie dazu leichten Druck auf den Access Point aus, wenn die Pfeile darauf hinweisen. Schieben Sie das Netzteil, und heben Sie es ab.



Schritt 3

Auf dem 142ACM und 143ACM wird die MAC-Adresse an den unten angegebenen Standorten angezeigt.



Schritt 4

1. **Wireless-Einstellungen** auswählen
2. **WLAN-Benutzer** auswählen
3. **Lokale MAC-Adressen** auswählen
4. **MAC-Adresse hinzufügen** auswählen

The screenshot shows the Cisco Business Wireless 140AC Access Point configuration page. The left sidebar is dark with 'Monitoring' and 'Wireless Settings' sections. 'Wireless Settings' is expanded, showing 'WLAN Users' selected. The main content area is titled 'WLAN Users' and shows a 'Users' count of 0. Below this, there are two tabs: 'WLAN Users' and 'Local MAC Addresses', with the latter selected. A search bar is present above a table. The table has columns for 'Action', 'MAC Address', 'Type', 'Profile Name', and 'Description'. Two entries are listed: one with MAC '68:ca:...' and another with 'a4:53:...', both of type 'WhiteList'. Below the table, there are navigation controls and a '10 items per page' indicator.

Schritt 5

Geben Sie die folgenden Informationen ein:

1. *MAC-Adresse*
2. *Beschreibung* (bis zu 32 Zeichen)
3. Aktivieren Sie das Optionsfeld *Zulassungsliste*
4. Klicken Sie auf **Anwenden**

The 'Add MAC Address' dialog box is shown. It has a blue header with a close button. Below the header are four main sections: 1. 'MAC Address' field with the value 'a4:52:0f:1e:16:5a'. 2. 'Description' field with the value 'ACM141'. 3. 'Type' section with radio buttons for 'BlackList' and 'WhiteList', where 'WhiteList' is selected. 4. 'Profile Name' dropdown menu with 'Any WLAN/RLAN' selected. At the bottom, there are two buttons: 'Apply' and 'Cancel'.

Überlegungen zu Interferenzen und Abständen

Schurken, Störsender und Funkkanäle - oh mein Gott!

Interferenzen können Probleme in Wireless-Netzwerken verursachen und von mehr Quellen als je zuvor verursacht werden. Mikrowellen, Sicherheitskameras, Smartwatches, Bewegungsmelder oder sogar Leuchtstoffröhren können Interferenzen verursachen.

Wie stark sich diese auf das Netzwerk auswirken, kann von vielen Faktoren abhängen, z. B. davon, wie viel Energie ausgegeben wird, wenn das Objekt permanent aktiv ist oder unregelmäßig ist. Je stärker das Signal bzw. desto häufiger tritt es auf, desto mehr Probleme können auftreten.

Nicht autorisierte APs und nicht autorisierte Clients können Probleme verursachen, wenn sich zu viele Access Points im selben Kanal befinden.

Interferenzen können die Leistung des Wireless-Netzwerks erheblich beeinträchtigen und zu Sicherheitslücken und instabilen Wireless-Netzwerken führen.

Es stehen Tools zur Verfügung, mit denen Sie die aktuell verwendeten Kanäle überwachen können. Sie können auch die Kanäle wechseln. Weitere Informationen finden Sie in den folgenden Artikeln.

- [Identifizieren von nicht autorisierten Clients](#)
- [Identifizieren von Störquellen](#)
- [Wechseln von Funkkanälen](#)

Empfehlungen zu Platzbedarf und Bereitstellung

1. Platzieren Sie Mesh Extender in der Reihe der primärfähigen APs.
2. Downstream-Mesh-Extender im Line-of-Site des übergeordneten Mesh Extender
3. Downstream-Mesh-Extender benötigen eine gute/ausgezeichnete Backhaul-SSID-Signalstärke von Upstream-APs mit primärfähigen Funktionen.
4. Mesh Extender müssen ein Signal-Rausch-Verhältnis (SNR) von mindestens 30 aufweisen.
5. Vermeiden Sie es, Mesh Extender zu nahe an anderen Mesh Extendern oder anderen primärfähigen APs anzuordnen.

Im folgenden Diagramm sind die erwarteten Abdeckungsbereiche in einem offenen Bereich aufgeführt. Wenn Sie Ihr Netzwerk in einem nicht offenen Bereich bereitstellen, reduzieren Sie diese Werte um 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

Signal-Rausch-Verhältnis zwischen "Hops"

In allen Netzwerken müssen Sie an einem starken Signal zwischen Clients und den APs arbeiten. In einem Mesh-Netzwerk müssen Sie auch sicherstellen, dass ein starkes Signal zwischen den verschiedenen APs besteht. Wenn einer der "Hops" kein gutes Signal, kein höheres Signal-Rausch-Verhältnis hat, müssen Sie eine Fehlerbehebung durchführen. Möglicherweise müssen Sie den Standort anpassen oder überprüfen, um festzustellen, was die Interferenz verursacht.

Schritt 1

Navigieren Sie zu **Monitoring > Network Summary > Access Points**, und klicken Sie auf einen beliebigen Access Point in der Tabelle, um die zugehörige Client-Signalstärke zu überprüfen.

Access Points

AP Name	Role	Type	Cli...	Usage	Uptime	Adm... Stat...	Ope... Stat...	Channels
AP6C71.0D55.5DA4		Mesh Exten...	0	178.4 KB	3 days, 02 h 14 m ...	Enabled	UP	1
AP6C71.0D55.73C4		Master AP	0	8.2 MB	3 days, 04 h 54 m ...	Enabled	UP	11

Schritt 2

Wenn die *Access Point-Ansicht* geöffnet wird, sehen Sie sich die Informationen unter *Leistungsübersicht* an.

Access Point View

GENERAL

AP Name: **AP6C71.0D55.73C4**
 Location: **default location**

MAC Address: 6c:71:0d:55:73:c4
 Base Radio MAC: a4:b2:39:df:f1:20
 IP Address: 192.168.1.29
 CDP / LLDP: c47d4feca352, gl1
 Ethernet Speed: 1000 Mbps
 Model / Domain: CBW145AC-B / 802.11bg--A 802.11a--B
 Power status: PoE/Full Power
 Serial Number: FGL2418L84T
 Max Capabilities: 802.11n 2.4GHz, 802.11ac 5GHz
 Spatial Streams: 2 (2.4GHz), 2 (5.0GHz)
 Max. Data Rate: 144 Mbps(2.4GHz), 867 Mbps(5.0GHz)

Tech Support: **Start** **Download**
 Tech Support Status: Not Started

PERFORMANCE SUMMARY

	2.4GHz	5GHz
Number of clients	0	2
Channels	11	(36, 40, 44, 48)
Configured Rate	Min: 1 Mbps, Max: 144 Mbps	Min: 6 Mbps, Max: 867 Mbps
Usage Traffic	9.8 MB	3.9 GB
Throughput	0	14.5 KB
Transmit Power	20 dBm	18 dBm
Noise	Not Available	Not Available
Channel Utilization	65%	12%
Interference	59%	0%
Traffic	6%	12%
Admin Status	Enabled	Enabled
Interferer Detection	Up	Up

Schritt 3

Sie können auch Informationen zu allen Mesh-Extender-Hop-Zählungen und *Signal-Rausch-Verhältnis* sammeln. Navigieren Sie zu **Monitoring > Network Summary > Mesh Extender**.

Mesh Extender 1

AP Name	AP Model	Ethernet M...	Parent AP ...	Hop	Link SNR (...)	Channel Ut...	Channel	Clients
AP6C71.0D...	CBW141AC...	6c:71:0d:55...	AP6C71.0D...	1	25	5	(36,40,44,48)	0

Werfen Sie einen Blick hinter den Vorhang

Syslogs

Die Erkennung von Ereignissen kann für einen reibungslosen Netzbetrieb und die Vermeidung von Ausfällen sorgen. Syslogs sind nützlich bei der Fehlerbehebung im Netzwerk, beim Debuggen des Paketflusses und bei der Überwachung von Ereignissen.

Diese Protokolle können auf der Webbenutzeroberfläche (UI) des primären Access Points und, falls konfiguriert, auf Remote-Protokollservern angezeigt werden. Ereignisse werden beim Neustart in der Regel aus dem System gelöscht, wenn sie nicht auf einem Remote-Server gespeichert werden.

Weitere Informationen finden Sie unter [Einrichten von Systemnachrichtenprotokollen \(Syslogs\) in einem CBW-Netzwerk](#).

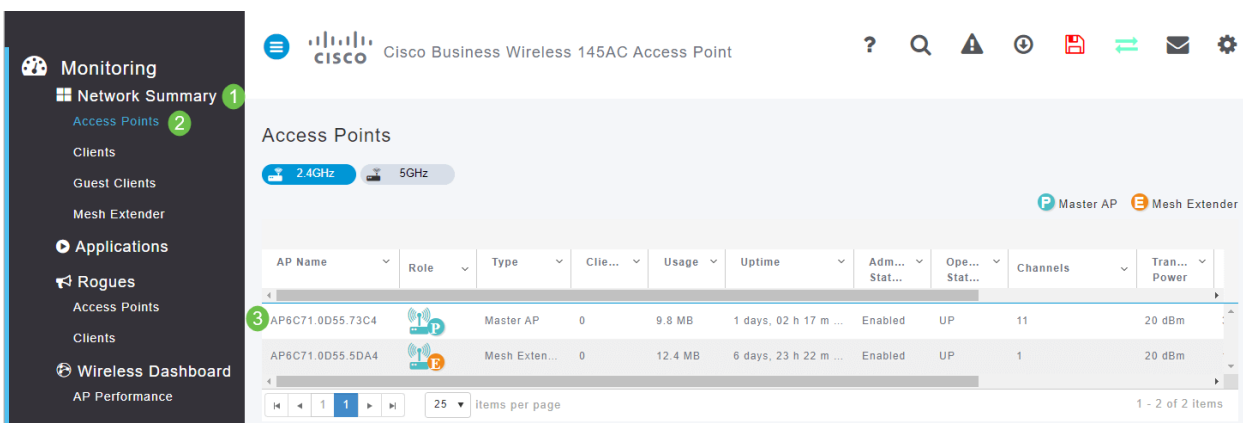
Support-Paket

Eine Funktion dieser CBW-Geräte ist das Herunterladen eines Support-Pakets. Ein Support-Paket ist ein Tool, das bei der Fehlerbehebung hilfreich sein kann. Es stellt die AP-Startprotokolle bereit und gibt die angewendeten Konfigurationen an. Um ein vollständiges Bild zu erhalten, muss dies möglicherweise auf jedem AP durchgeführt werden.

Bevor Sie das Support-Paket auf den primären Access Point herunterladen, stellen Sie sicher, dass Sie die aktuellste Firmware-Version verwenden. Um die Firmware zu aktualisieren, wählen Sie den richtigen Link unter [Anwendbare Geräte aus. | Firmware-Version](#). Wenn Sie Hilfe bei der Aktualisierung der Firmware benötigen, sehen Sie sich die [Update-Software eines Cisco Business Wireless Access Point an](#).

Schritt 1

Wählen Sie **Monitoring > Access Points** aus, um das speziell für die Access Point-Funktionalität konzipierte Paket für den technischen Support herunterzuladen. Wählen Sie den AP aus, auf den Sie zugreifen möchten.



Schritt 2

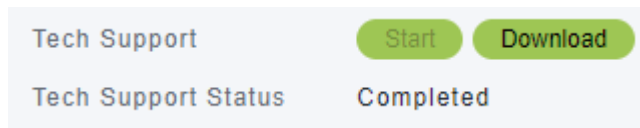
Wählen Sie im Abschnitt *Technischer Support* die Option **Starten aus**.



Access Point View

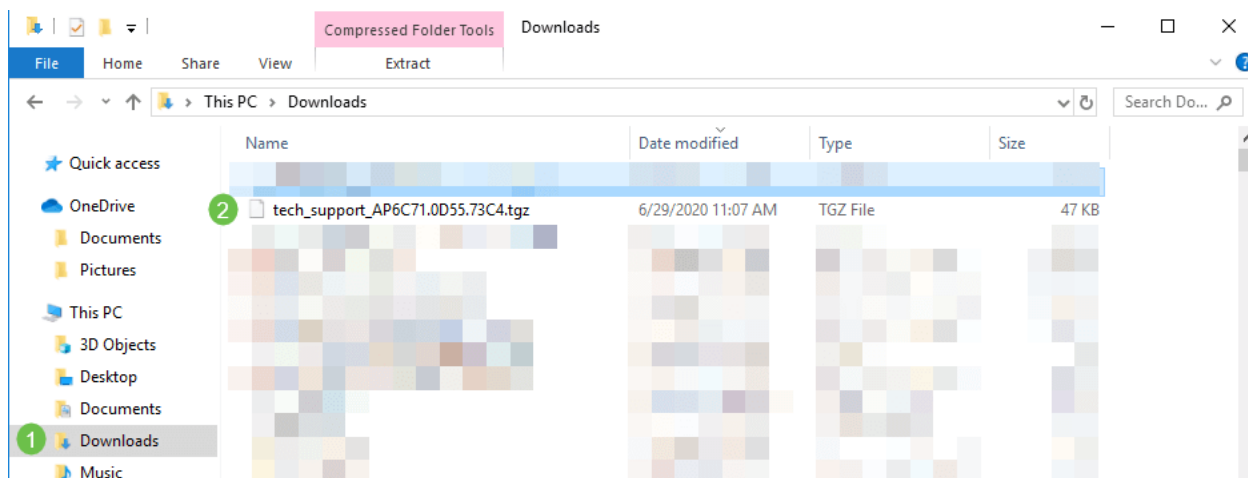
Schritt 3

Wenn der Download abgeschlossen ist, wird der *Status* des *technischen Supports* als *abgeschlossen angezeigt*. Wählen Sie die Schaltfläche **Download**, um die Dateien herunterzuladen. Selbst wenn der Download fehlschlägt, wird er zu diesem Zeitpunkt aus dem Speicher des Access Points gelöscht. Dies geschieht, wenn Sie Popups nicht zulassen.



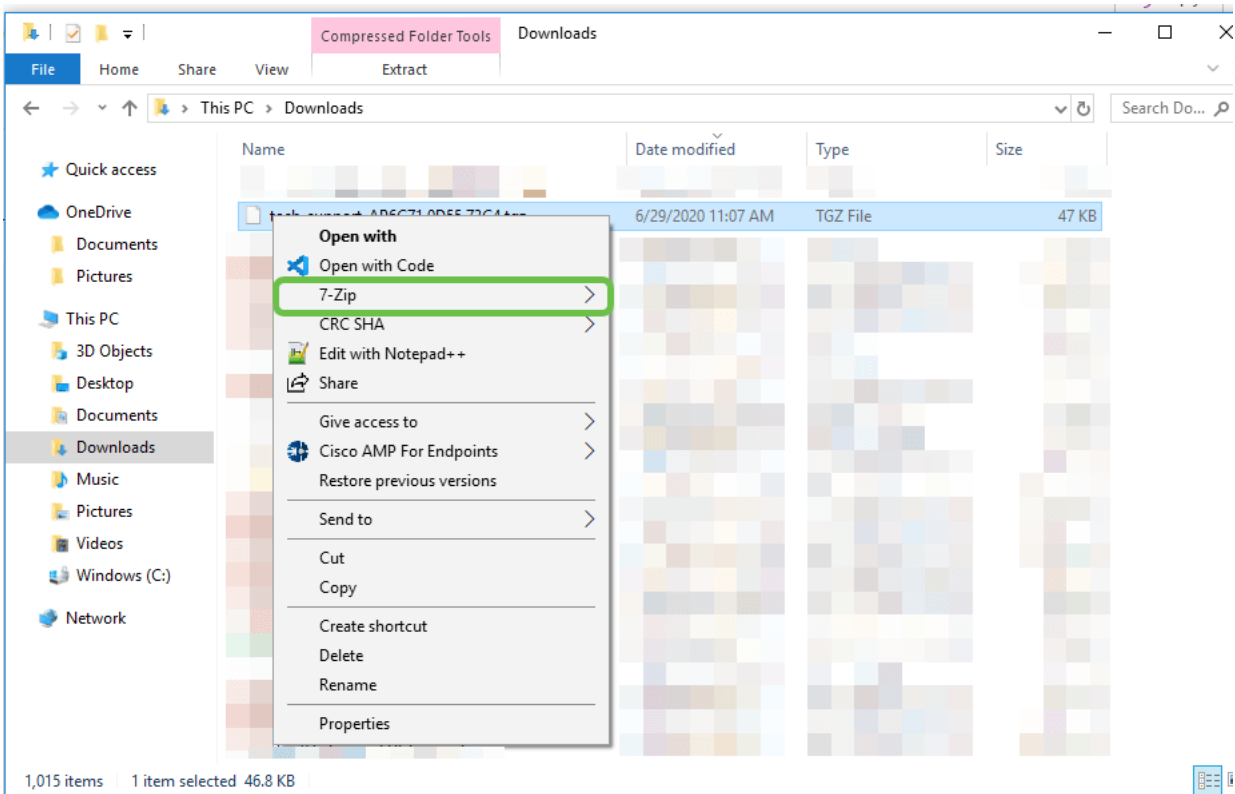
Schritt 4

Im Ordner *Download* Ihrer Computerdateien sehen Sie eine *.tgz*-Datei für den technischen Support. Die Dateien in diesem Ordner müssen extrahiert werden.



Schritt 5

Klicken Sie mit der rechten Maustaste, und wählen Sie die zu verwendende Unzip-Anwendung aus. In diesem Beispiel wurde *7-Zip* verwendet. Wählen Sie diese Option aus, um die Dateien an den von Ihnen ausgewählten Speicherort zu extrahieren. Standardmäßig werden die Dateien in den Ordner *Downloads* gesendet.

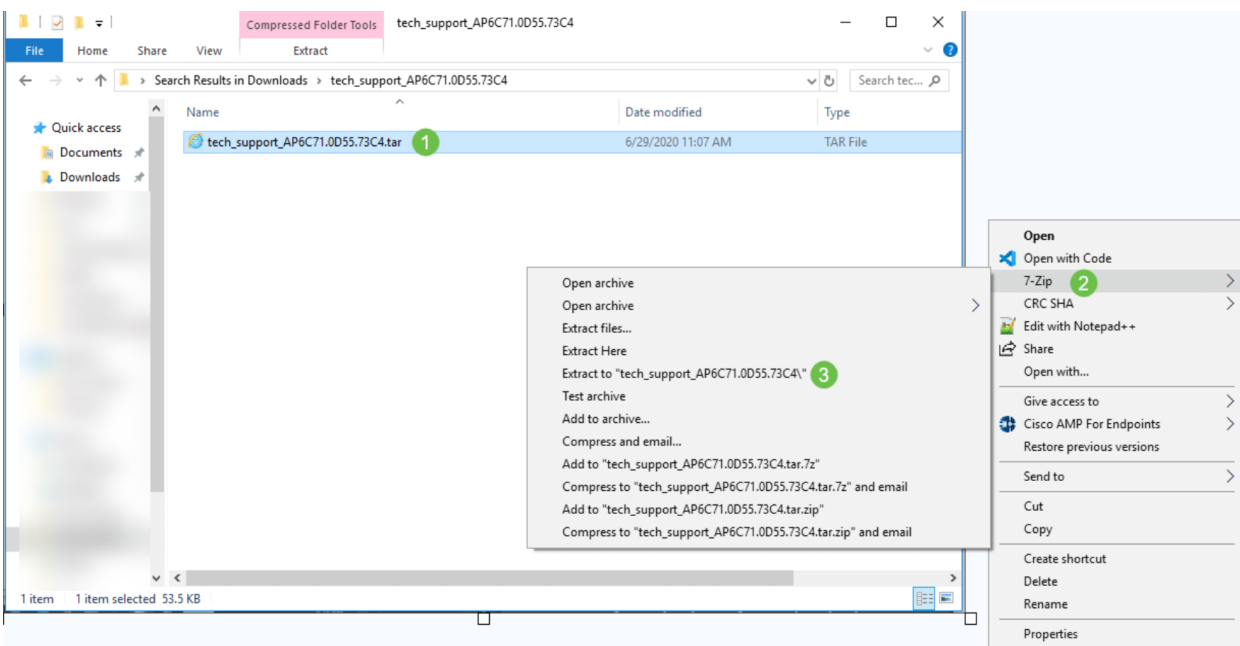


(Alternative Ansicht) Wenn Sie einen Core-Absturz haben, sehen Sie möglicherweise stattdessen diese Ordner.

Name	Date modified	Type	Size
ap-core-crash	6/25/2020 7:51 AM	File folder	
ctrl	6/25/2020 7:51 AM	File folder	
internal-ap	6/25/2020 7:51 AM	File folder	
tech_support.tar	6/25/2020 7:51 AM	TAR File	927 KB

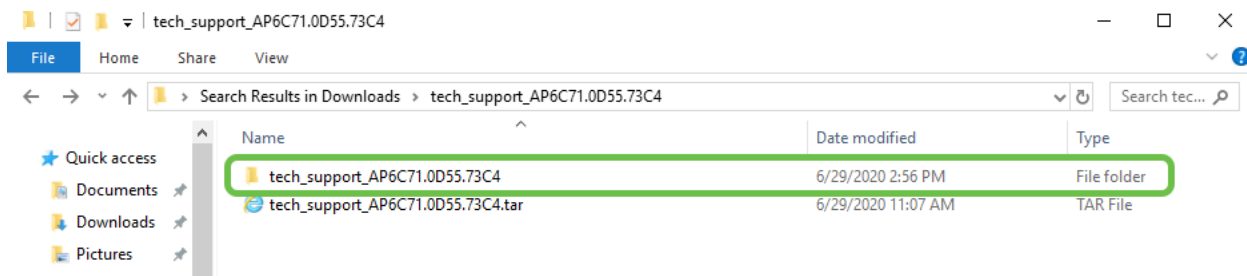
Schritt 6

Sobald die Dateien aus der .tgz-Datei extrahiert wurden, befinden sie sich in einer .tar-Datei. Diese Datei muss erneut extrahiert werden.



Schritt 7

Sie sehen den Ordner *tech_support*. Doppelklicken Sie auf den Ordner, um die Dateien zu öffnen.



Schritt 8

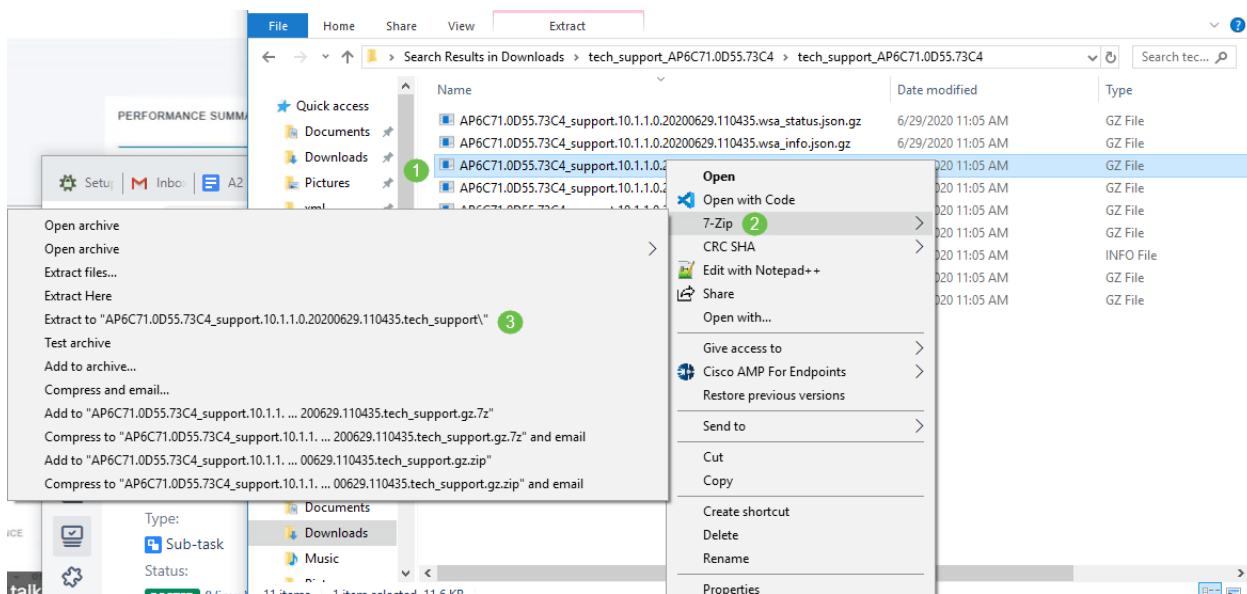
Die relevantesten Informationen im Supportpaket sind *cli_file* (Konfigurationsdatei), *msg/syslogs* (Ereignisprotokolle) und *startlog*. Die angezeigten Dateien können variieren. Ein Beispiel ist hier

Name	Date modified	Type
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.wsa_status.json.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.wsa_info.json.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.tech_support.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.syslogs.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.startlog.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.messages.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.info	6/29/2020 11:05 AM	INFO File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.brain.log.gz	6/29/2020 11:05 AM	GZ File
AP6C71.0D55.73C4_support.10.1.1.0.20200629.110435.brain.error.log.gz	6/29/2020 11:05 AM	GZ File

dargestellt.

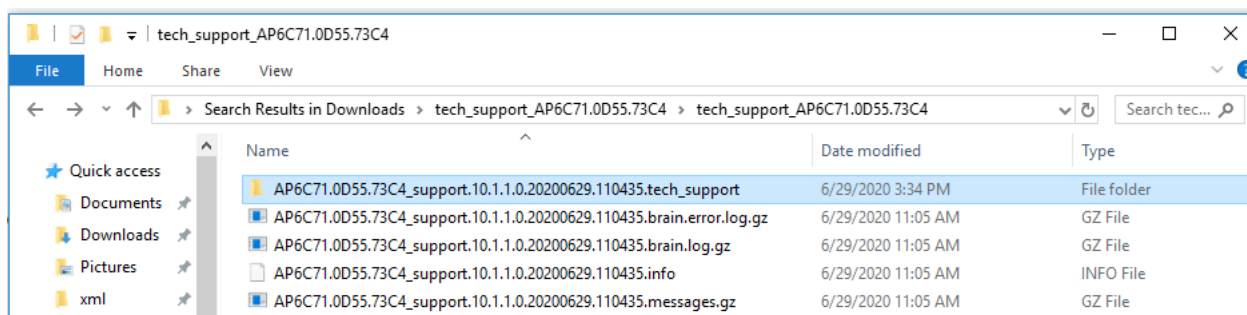
Schritt 9

Klicken Sie mit der rechten Maustaste auf die Datei, die Sie entpacken möchten. In diesem Beispiel wird die Datei in einen Ordner für *tech_support* entpackt.



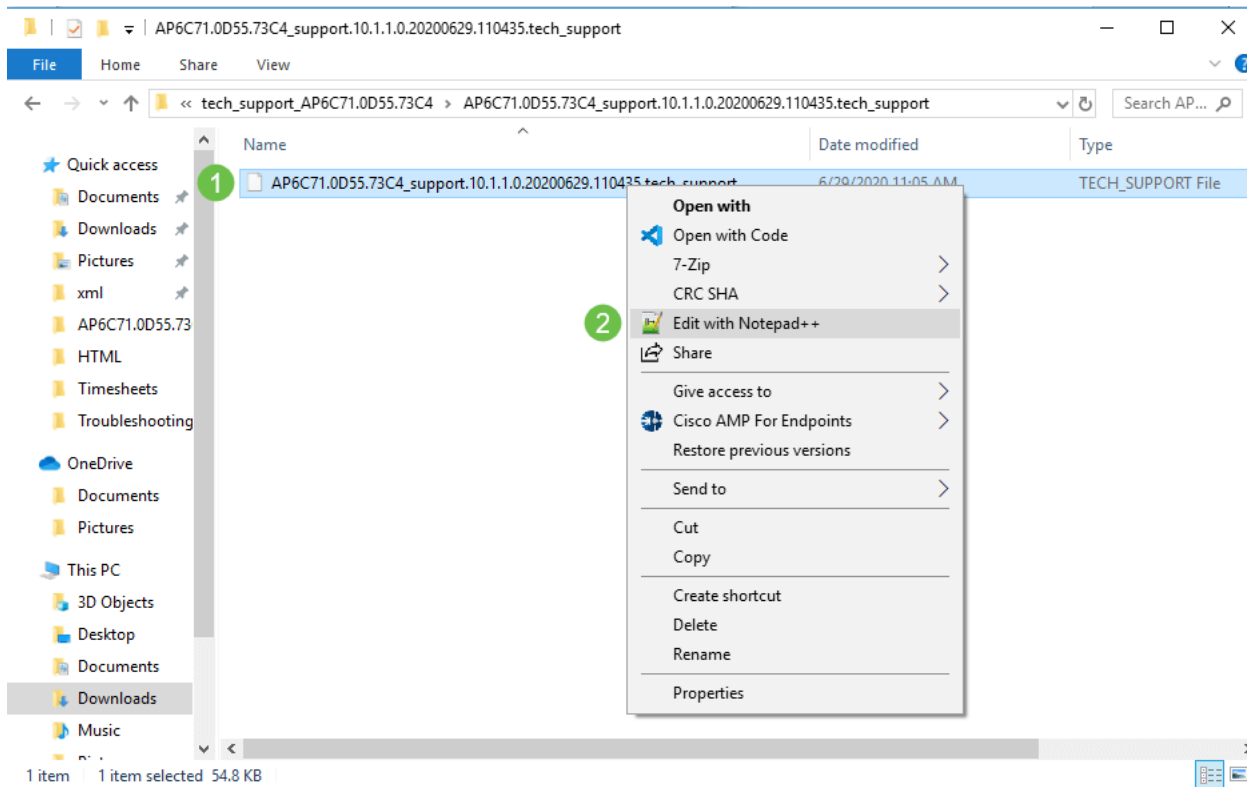
Schritt 10

Der Ordner *tech_support* wird angezeigt. Doppelklicken Sie, um den Ordner zu öffnen.



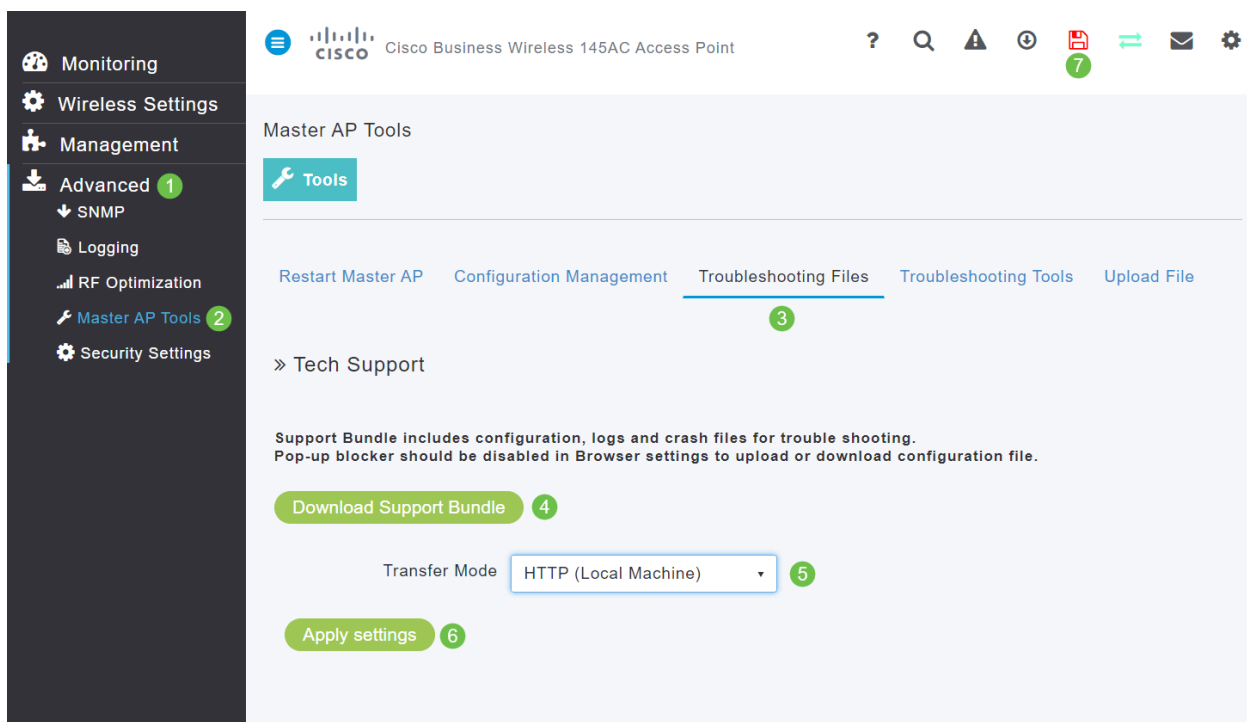
Schritt 11

Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie einen Textdateileser aus. In diesem Beispiel wurde **Bearbeiten mit Notepad++** verwendet.



Zugriff auf das primäre AP Tech Support-Paket

Das primäre technische Supportpaket des AP ist die wichtigste Diagnosequelle. Um das im primären Access Point oder im virtuellen Controller-Paket integrierte technische Support-Paket herunterzuladen, navigieren Sie zu **Advanced > Primary AP Tools**. Wählen Sie die Registerkarte **Fehlerbehebungsdateien**. Wählen Sie **Support-Paket herunterladen aus**. Wählen Sie als **Übertragungsmodus HTTP** oder **FTP** aus. Klicken Sie auf **Einstellungen übernehmen**. Klicken Sie auf das Symbol **Speichern**.

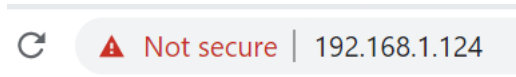


Eine der CBW-Mobiltelefoneinstellungen anpassen

802.11r-Einstellungen im CBW-Netzwerk ändern

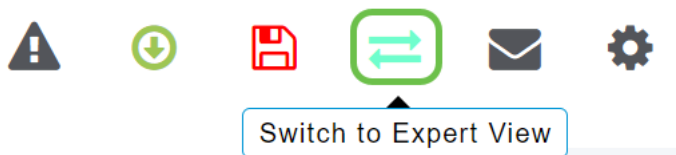
Schritt 1

Greifen Sie auf die Web-Benutzeroberfläche zu, indem Sie die IP-Adresse des primären Access Points in einen Webbrowser eingeben. Vergewissern Sie sich, dass Sie sich nicht in einem Virtual Private Network (VPN) befinden, da dies sonst nicht funktioniert. Wenn Sicherheitswarnungen auftreten, wählen Sie die Aufforderungen aus, um fortzufahren.



Schritt 2

Klicken Sie rechts oben auf der Web-Benutzeroberfläche auf die gegenüberliegenden Pfeile, um zur Expertenansicht zu wechseln.



Schritt 3

In einem Popup-Fenster werden Sie gefragt, ob Sie die Expertenansicht auswählen möchten. Klicken Sie auf **OK**.

192.168.1.124 says

Do you want to select Expert View?



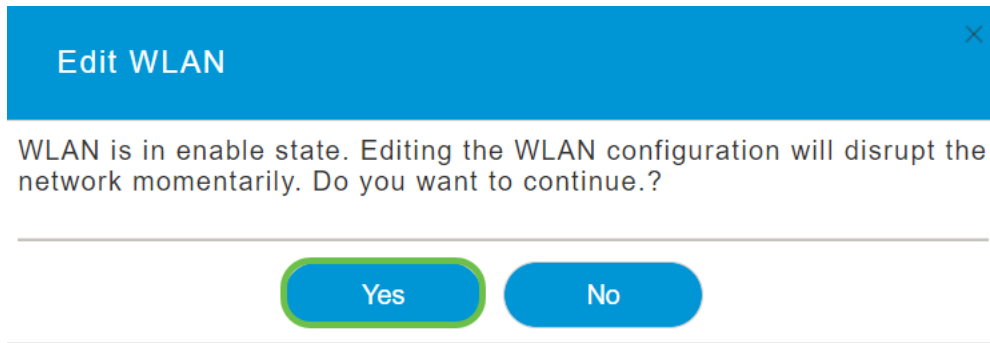
Schritt 4

Wählen Sie **WLANS** und das **Bearbeitungssymbol** für das WLAN aus, das Sie bearbeiten möchten.

Action	Active	Type	Name	SSID	Security Policy	Radio Policy
	Enabled	WLAN	cisco_1	cisco_1	Personal(WPA2)	ALL
	Enabled	WLAN	cisco_2	cisco_2	Guest	ALL
	Enabled	WLAN	cisco_4	cisco_4	Personal(WPA2+...	ALL
	Disabled	WLAN	cisco_3	cisco_3	Open	ALL

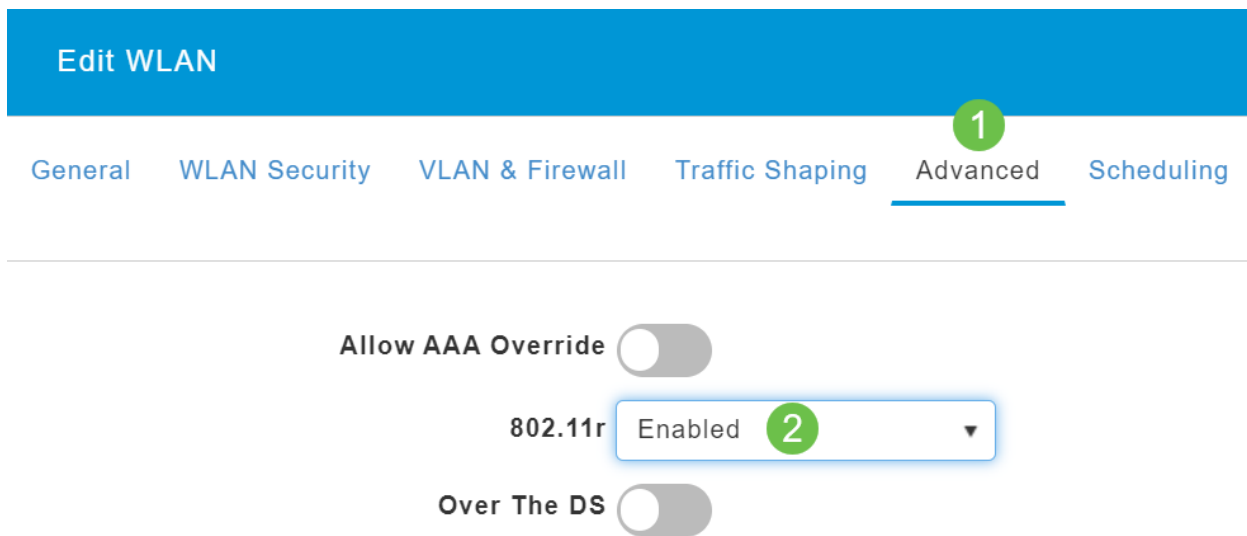
Schritt 5

Ein Popup-Fenster wird angezeigt, in dem Sie gefragt werden, ob Sie fortfahren möchten. Klicken Sie auf **Ja**.



Schritt 6

Klicken Sie auf die Registerkarte **"Erweitert"**. Klicken Sie auf das Dropdown-Menü für 802.11r, und wählen Sie **Enabled (Aktiviert)**.



Schritt 7

Klicken Sie auf **Apply** (Anwenden).



Schritt 8

Um diese Einstellungen dauerhaft zu speichern, klicken Sie oben rechts auf Ihrem Bildschirm auf das **Symbol zum Speichern**.



Wenn alles andere fehlschlägt, auf Werkseinstellungen zurücksetzen

Eine Option der letzten Instanz, die nur durchgeführt werden sollte, um die schwerwiegendsten

Probleme zu beheben, wie den Verlust der Fähigkeit, Zugriff auf das Management-Portal zu erhalten, ist ein Hardware-Reset auf dem Router.

Wenn Sie die Werkseinstellungen wiederherstellen, gehen alle Konfigurationen verloren. Sie müssen den Router von Grund auf neu einrichten, damit Sie über die Verbindungsdetails verfügen.

Der Prozess für die neuen CBW-APs unterscheidet sich geringfügig von dem für andere APs. Weitere Informationen zum Zurücksetzen finden Sie im Artikel [Zurücksetzen eines CBW-AP auf die Werkseinstellungen](#).

Schlussfolgerung

Es war unsere Absicht, Ihnen verschiedene Optionen zur Fehlerbehebung Ihres Mesh-Netzwerks anzubieten. Mission erfüllt! Sie sollten jetzt über Konnektivität verfügen und können mit Ihrem Tag fortfahren.

[Video zu diesem Artikel anzeigen ...](#)

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.