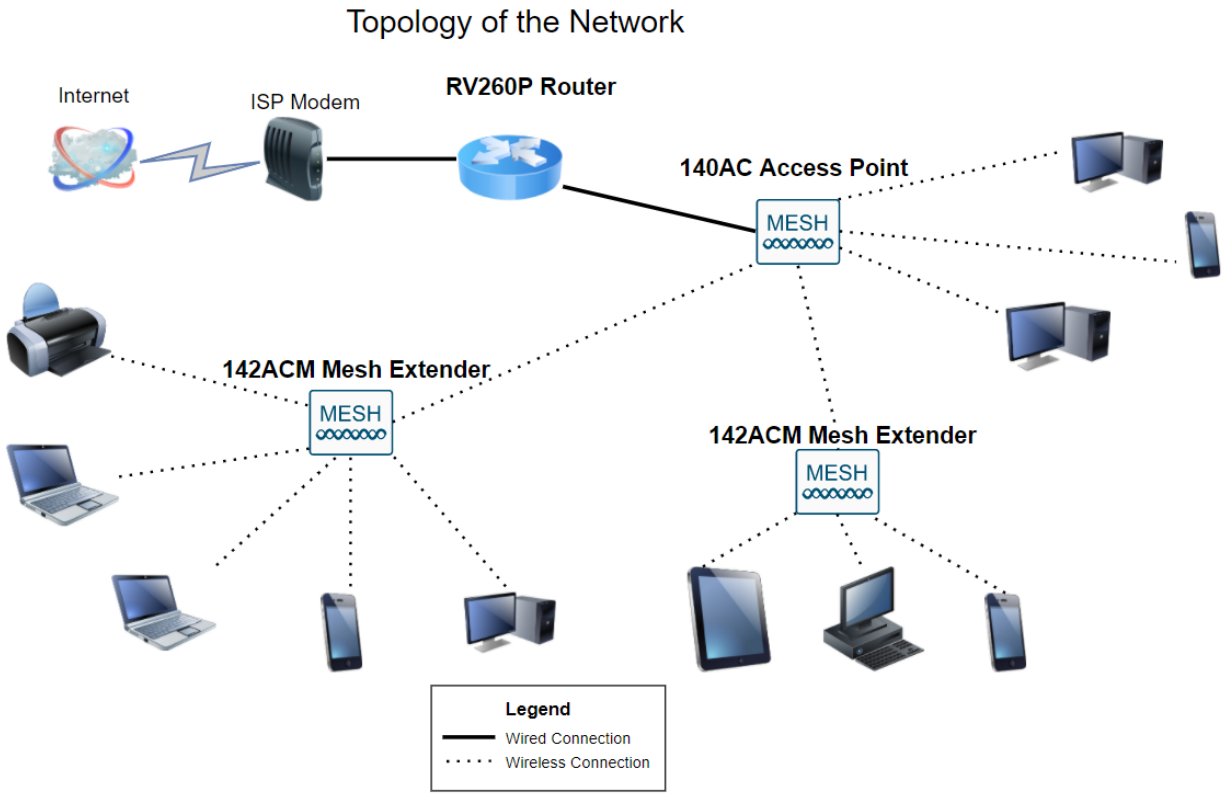
# Netzwerkkonfiguration gesamt: RV260P mit Cisco Business Wireless und Weboberfläche

## Ziel:

In diesem Leitfaden wird die Konfiguration eines Wireless Mesh-Netzwerks mithilfe eines RV260P-Routers, eines CBW140AC-Access Points und zweier CBW142ACM-Mesh-Extender erläutert.

In diesem Artikel wird die Webbenutzeroberfläche (UI) zum Einrichten des Wireless-Mesh-Netzwerks verwendet. Wenn Sie die mobile Anwendung verwenden möchten, die für die einfache Wireless-Einrichtung empfohlen wird, klicken Sie auf den Artikel, der die mobile Anwendung verwendet. Wenn Sie die Webbenutzeroberfläche verwenden möchten, lesen Sie weiter!

## Topologie:




## Einleitung

Sie können Ihr neues Netzwerk einrichten. Es ist ein aufregender Tag! In diesem Szenario wird ein RV260P-Router verwendet. Dieser Router bietet Power over Ethernet (PoE), mit dem der CBW140AC an den Router und nicht an einen Switch angeschlossen werden kann. Die Mesh-Extender CBW140AC und CBW142ACM werden zum Erstellen eines Wireless Mesh-Netzwerks verwendet.

Wenn Sie mit einigen der in diesem Dokument verwendeten Begriffe nicht vertraut sind

oder weitere Informationen zu Mesh Networking benötigen, lesen Sie die folgenden Artikel:

- Cisco Business: Glossar neuer Begriffe
- Willkommen bei der Cisco Business Wireless Mesh Networking
- Häufig gestellte Fragen (FAQs) zu einem Cisco Business Wireless Network

Sind Sie bereit? Kommen wir dazu!

### Unterstützte Geräte | Softwareversion

- RV260P | 1.0.0.17
- CBW140AC | 10.3.1.0
- CBW142ACM | 10.3.1.0 (Mindestens ein Mesh-Extender ist für das Mesh-Netzwerk erforderlich)

### Inhalt



## Bevor Sie beginnen

1. Stellen Sie sicher, dass Sie über eine aktuelle Internetverbindung verfügen.
2. Wenden Sie sich an Ihren ISP, um spezielle Anweisungen für die Verwendung Ihres RV260-Routers zu erhalten. Einige ISPs bieten Gateways mit integrierten Routern an. Wenn Sie über ein Gateway mit integriertem Router verfügen, müssen Sie den Router möglicherweise deaktivieren und die IP-Adresse des Wide Area Network (WAN) (die

eindeutige Internetprotokolladresse, die der Internetanbieter Ihrem Konto zuweist) sowie den gesamten Netzwerkverkehr an Ihren neuen Router weiterleiten.

3. Legen Sie fest, wo Sie den Router platzieren sollen. Wenn möglich sollten Sie einen offenen Bereich suchen. Dies ist möglicherweise nicht einfach, da Sie den Router vom Internetdienstanbieter (ISP) an das Breitband-Gateway (Modem) anschließen müssen.

# Konfigurieren des RV260P-Routers

Ein Router ist in einem Netzwerk unerlässlich, da er Pakete weiterleitet. Sie ermöglicht es einem Computer, mit anderen Computern zu kommunizieren, die sich nicht im gleichen Netzwerk oder Subnetz befinden. Ein Router greift auf eine Routing-Tabelle zu, um zu bestimmen, wohin Pakete gesendet werden sollen. In der Routing-Tabelle werden Zieladressen aufgelistet. Statische und dynamische Konfigurationen können in der Routing-Tabelle aufgelistet werden, um Pakete an ihr spezifisches Ziel zu senden.

Der RV260P verfügt über Standardeinstellungen, die für viele kleine und mittlere Unternehmen optimiert sind. Allerdings können Sie bei Ihren Netzwerkanforderungen oder Ihrem Internetdienstanbieter (ISP) einige dieser Einstellungen ändern. Nachdem Sie sich bezüglich der Anforderungen an Ihren ISP gewandt haben, können Sie Änderungen über die Webbenutzeroberfläche (UI) vornehmen.

## RV260P einsatzbereit

### Schritt 1

Verbinden Sie das Ethernetkabel von einem der RV260P-LAN-Ports (Ethernet) mit dem Ethernet-Port des Computers. Sie benötigen einen Adapter, wenn Ihr Computer keinen Ethernet-Port hat. Das Terminal muss sich im selben kabelgebundenen Subnetz wie der RV260P befinden, um die Erstkonfiguration durchzuführen.

### Schritt 2

Stellen Sie sicher, dass Sie das mit dem RV260P gelieferte Netzteil verwenden. Die Verwendung eines anderen Netzadapters kann den RV260P beschädigen oder einen Ausfall der USB-Dongles verursachen. Der Netzschalter ist standardmäßig eingeschaltet.

Schließen Sie das Netzteil an den 12-V-Gleichstrom-Port des RV260P an, stecken Sie es jedoch noch nicht ein.

### Schritt 3

Stellen Sie sicher, dass das Modem ausgeschaltet ist.

### Schritt 4

Verwenden Sie ein Ethernetkabel, um Ihr Kabel- oder DSL-Modem an den WAN-Port

des RV260P anzuschließen.

### Schritt 5

Schließen Sie das andere Ende des RV260P-Adapters an eine Steckdose an. Dadurch wird der RV260 eingeschaltet. Schließen Sie das Modem wieder an, damit es auch hochgefahren werden kann. Die Betriebsanzeige an der Frontblende leuchtet stetig grün, wenn der Netzadapter korrekt angeschlossen ist, und der RV260P ist mit dem Booten fertig.

## Router einrichten

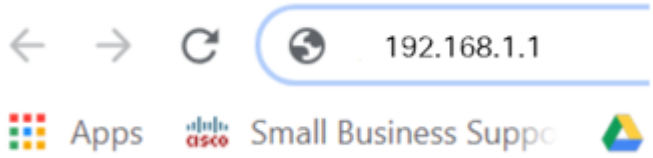
Jetzt ist es an der Zeit einige Konfigurationen vorzunehmen! So starten Sie die Webbenutzeroberfläche:

### Schritt 1

Wenn Ihr Computer so konfiguriert ist, dass er ein Dynamic Host Configuration Protocol (DHCP)-Client wird, wird dem PC eine IP-Adresse im Bereich 192.168.1.x zugewiesen. DHCP automatisiert den Prozess der Zuweisung von IP-Adressen, Subnetzmasken, Standard-Gateways und anderen Einstellungen zu Computern. Computer müssen so eingestellt werden, dass sie am DHCP-Prozess teilnehmen, um eine Adresse zu erhalten. Dazu wählen Sie in den Eigenschaften von TCP/IP auf dem Computer automatisch eine IP-Adresse aus.

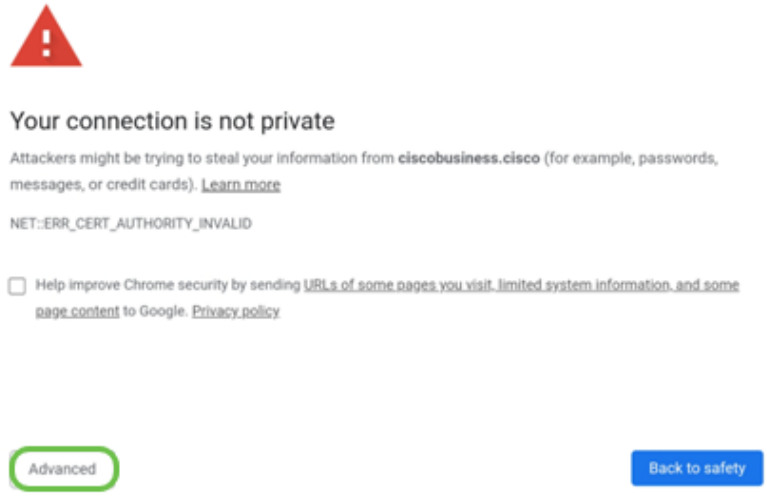
### Schritt 2

Öffnen Sie einen Webbrowser wie Safari, Internet Explorer oder Firefox. Geben Sie in die Adressleiste die Standard-IP-Adresse des RV260P ein, d. h. 192.168.1.1.



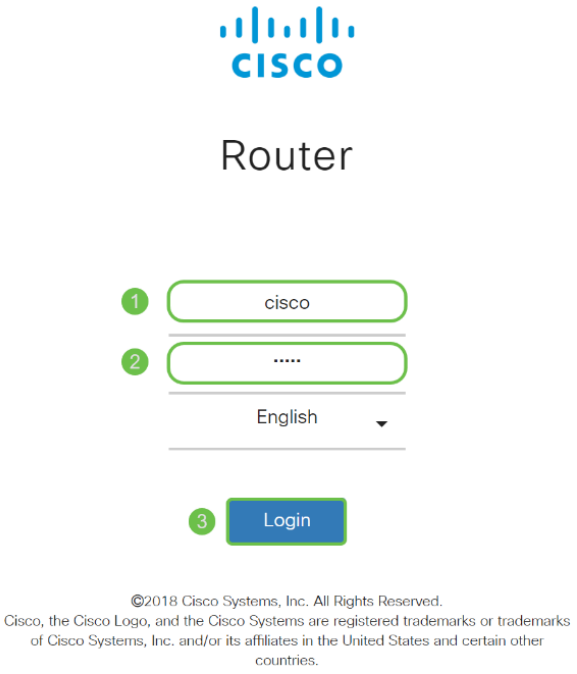

### Schritt 3

Der Browser gibt möglicherweise eine Warnung aus, dass die Website nicht vertrauenswürdig ist. Weiter zur Website. Wenn Sie nicht verbunden sind, fahren Sie mit der Fehlerbehebung für die Internetverbindung fort.




**Schritt 4**

Wenn die Anmeldeseite angezeigt wird, geben Sie den Standardbenutzernamen cisco und das Standardkennwort *cisco ein*. Bei Benutzername und Kennwort wird zwischen Groß- und Kleinschreibung unterschieden.




**Schritt 5**

Klicken Sie auf **Anmelden**. Die Seite *"Getting Started"* wird angezeigt. Nachdem Sie die Verbindung bestätigt und sich beim Router angemeldet haben, springen Sie zum Abschnitt "Erstkonfiguration" in diesem Artikel.

## Fehlerbehebung bei der Internetverbindung

Dang es, wenn Sie diese lesen, haben Sie wahrscheinlich Probleme, die Verbindung mit dem Internet oder der Web-Benutzeroberfläche. Eine dieser Lösungen sollte helfen.

Unter dem angeschlossenen Windows-Betriebssystem können Sie die Netzwerkverbindung testen, indem Sie die Eingabeaufforderung öffnen. Geben Sie

ping 192.168.1.1 ein (die Standard-IP-Adresse des Routers). Wenn die Anfrage das Zeitlimit überschreitet, können Sie nicht mit dem Router kommunizieren.

Wenn die Verbindung nicht hergestellt wird, können Sie die Fehlerbehebung auf den Routern RV160 und RV260 überprüfen.

Einige weitere Punkte sollten Sie ausprobieren:

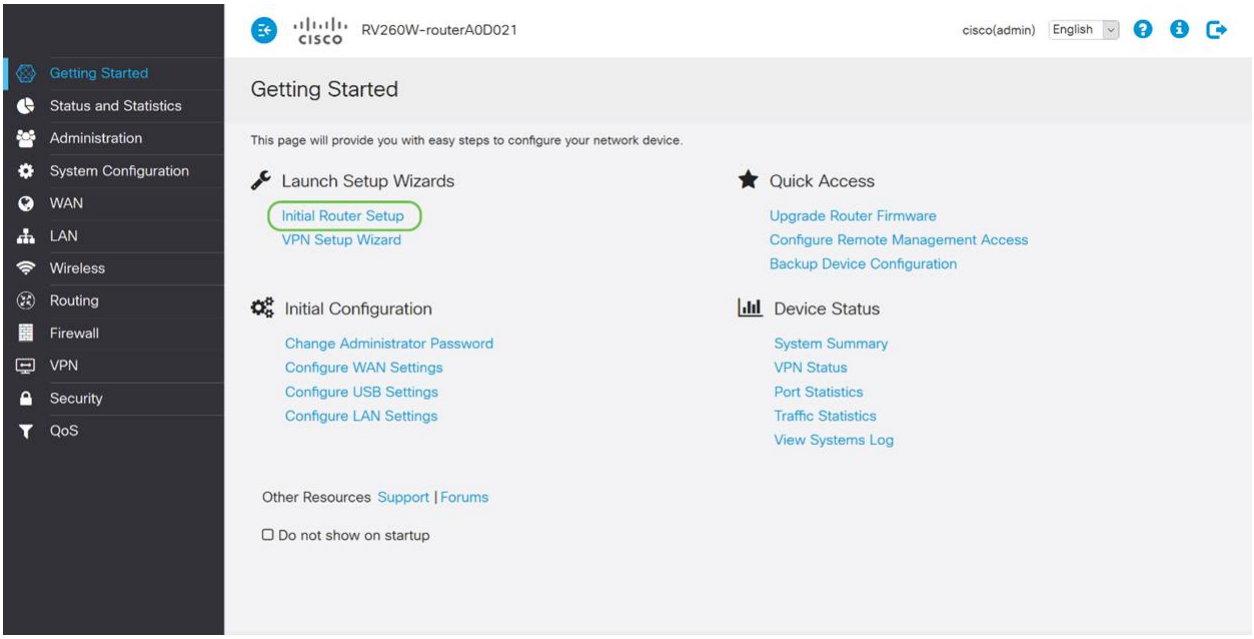
1. Stellen Sie sicher, dass Ihr Webbrowser nicht auf Offline arbeiten eingestellt ist.
2. Überprüfen Sie die Einstellungen für die lokale Netzwerkverbindung des Ethernet-Adapters. Der PC sollte über DHCP eine IP-Adresse erhalten. Alternativ kann der PC eine statische IP-Adresse im Bereich 192.168.1.x haben, wobei das Standard-Gateway auf 192.168.1.1 (die Standard-IP-Adresse des RV260P) festgelegt ist. Um eine Verbindung herzustellen, müssen Sie möglicherweise die Netzwerkeinstellungen des RV260P ändern. Wenn Sie Windows 10 verwenden, überprüfen Sie die Anweisungen in Windows 10, um die Netzwerkeinstellungen zu ändern.
3. Wenn Sie bereits Geräte mit der IP-Adresse 192.168.1.1 besitzen, müssen Sie diesen Konflikt beheben, damit das Netzwerk funktioniert. Mehr dazu am Ende dieses Abschnitts, oder klicken Sie hier direkt dorthin.
4. Setzen Sie das Modem und den RV260P zurück, indem Sie beide Geräte ausschalten. Schalten Sie anschließend das Modem ein, und lassen Sie es etwa 2 Minuten untätig. Schalten Sie dann den RV260P ein. Sie sollten jetzt eine WAN-IP-Adresse erhalten.
5. Wenn Sie ein DSL-Modem haben, bitten Sie Ihren ISP, das DSL-Modem in den Bridge-Modus zu schalten.

## Erstkonfiguration

Es wird empfohlen, die Schritte des Assistenten für die Ersteinrichtung zu durchlaufen, die in diesem Abschnitt aufgeführt sind. Sie können diese Einstellungen jederzeit ändern.

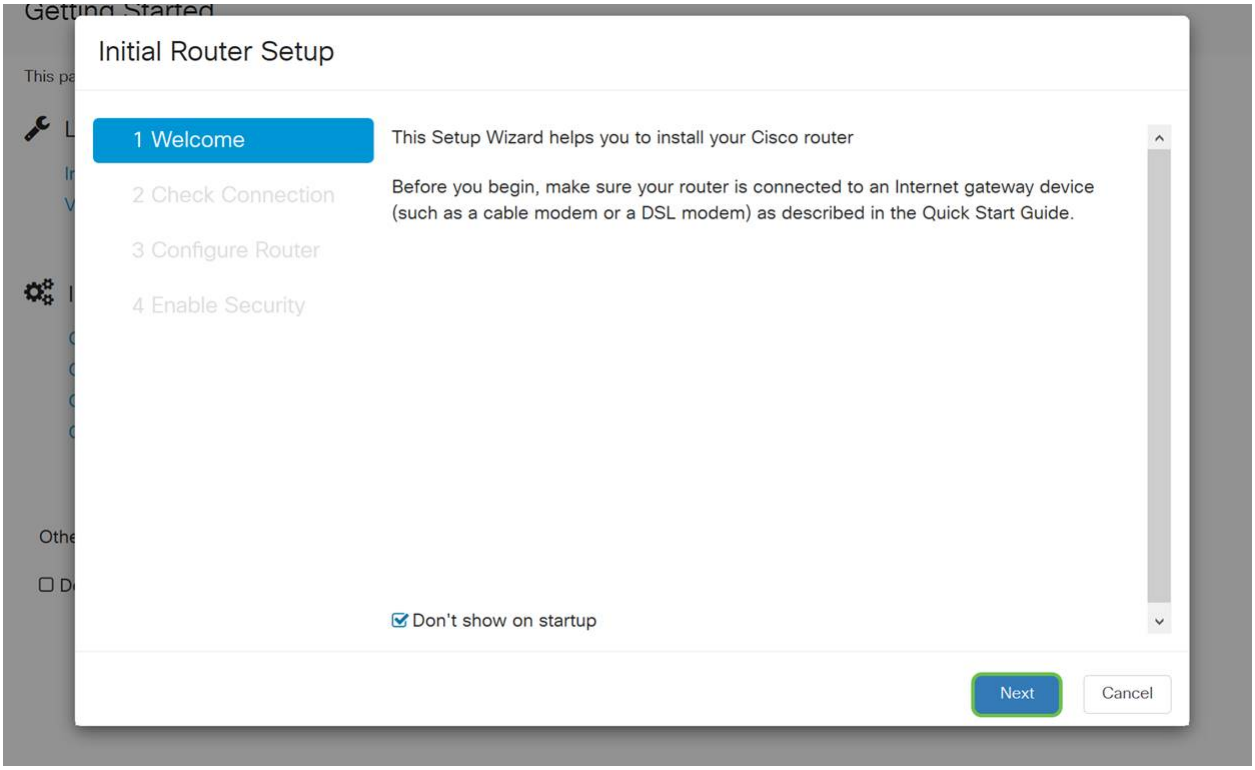
### Schritt 1

Klicken Sie auf der Seite "*Getting Started*" auf **Assistent für die Ersteinrichtung**.



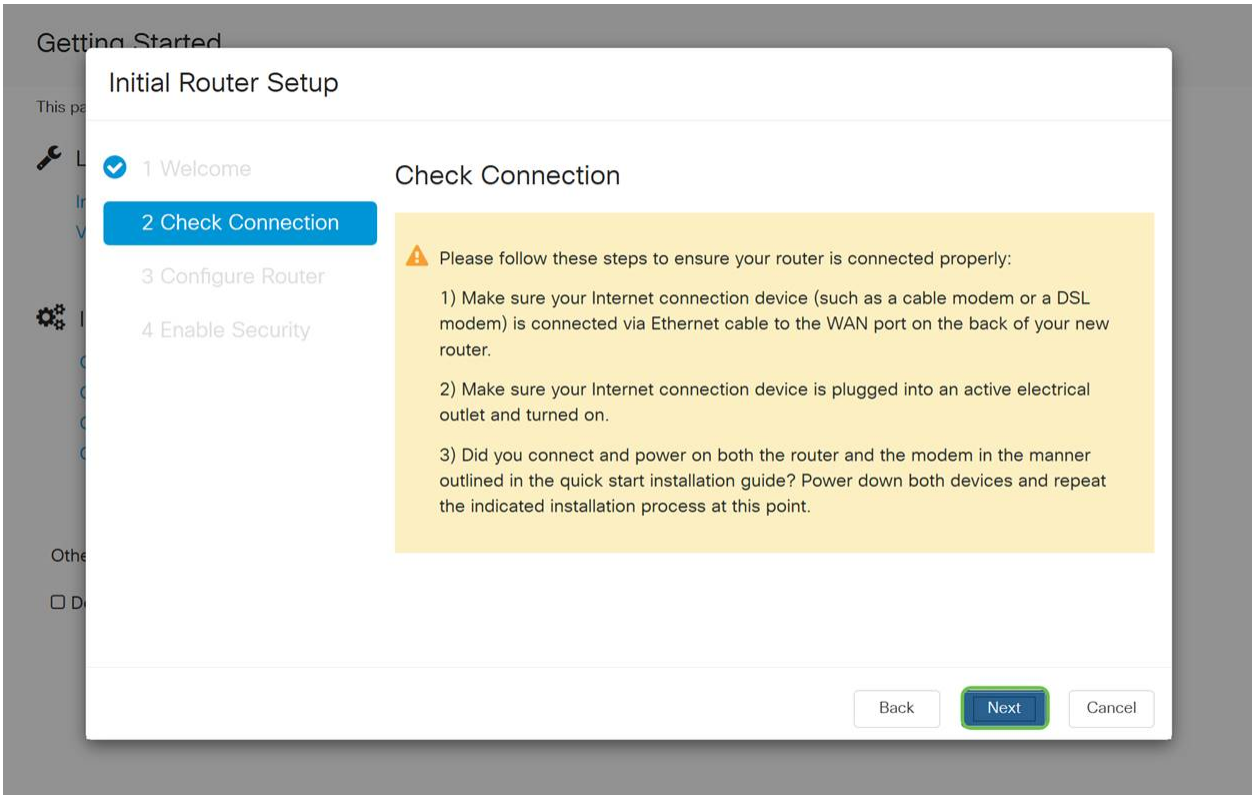

**Schritt 2**

Dieser Schritt bestätigt, dass die Kabel angeschlossen sind. Da Sie dies bereits bestätigt haben, klicken Sie auf **Weiter**.



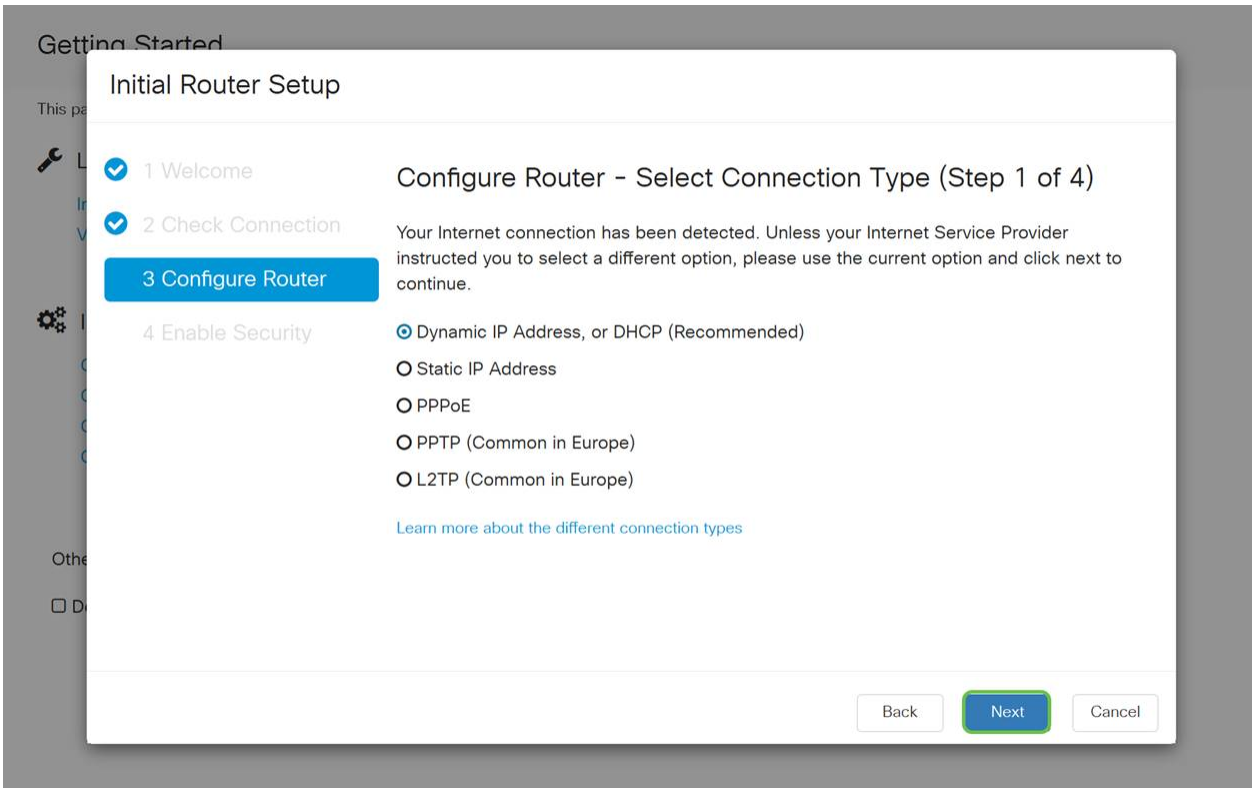

**Schritt 3**

In diesem Schritt werden grundlegende Schritte beschrieben, um sicherzustellen, dass Ihr Router angeschlossen ist. Da Sie dies bereits bestätigt haben, klicken Sie auf **Weiter**.



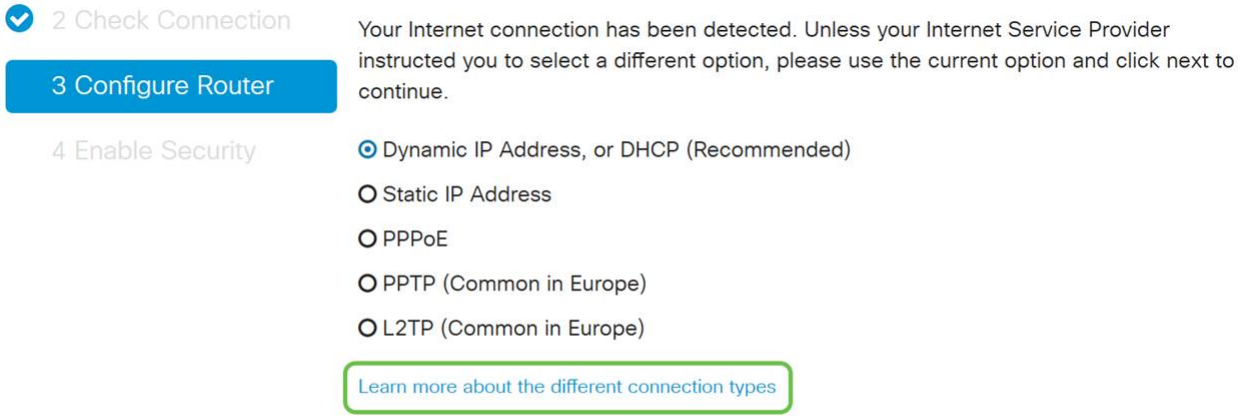

**Schritt 4**

Im nächsten Bildschirm werden Ihre Optionen für die Zuweisung von IP-Adressen zu Ihrem Router angezeigt. In diesem Szenario müssen Sie DHCP auswählen. Klicken Sie auf **Weiter**.



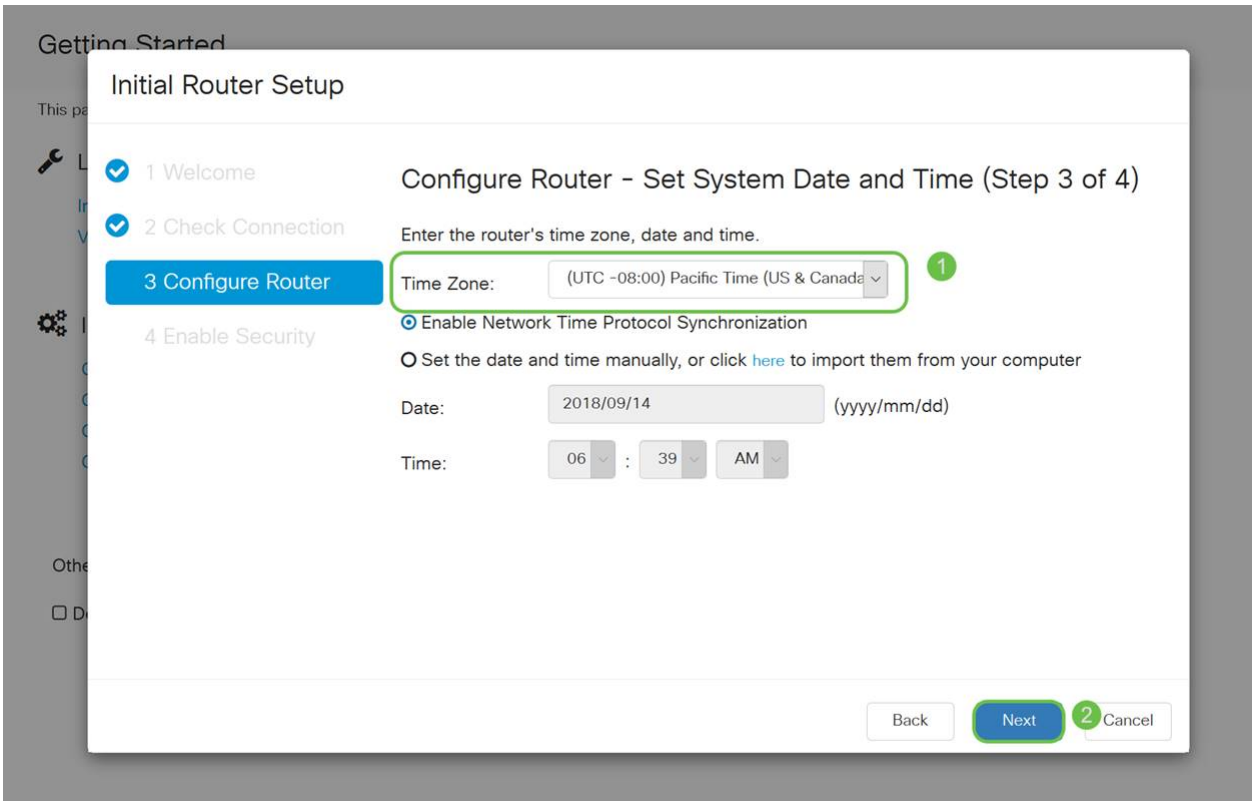

Obwohl Sie DHCP für diese Ersteinrichtung verwenden müssen, können Sie auswählen, *um weitere Informationen über die verschiedenen Verbindungstypen* am unteren Bildschirmrand als zukünftige Referenz *zu erhalten*. Weitere Einzelheiten hierzu finden Sie in den folgenden Artikeln:

- [WAN-Konfiguration auf RV160x- und RV260x-Geräten]
- [Konfigurieren von statischem Routing auf dem RV160 und dem RV260]



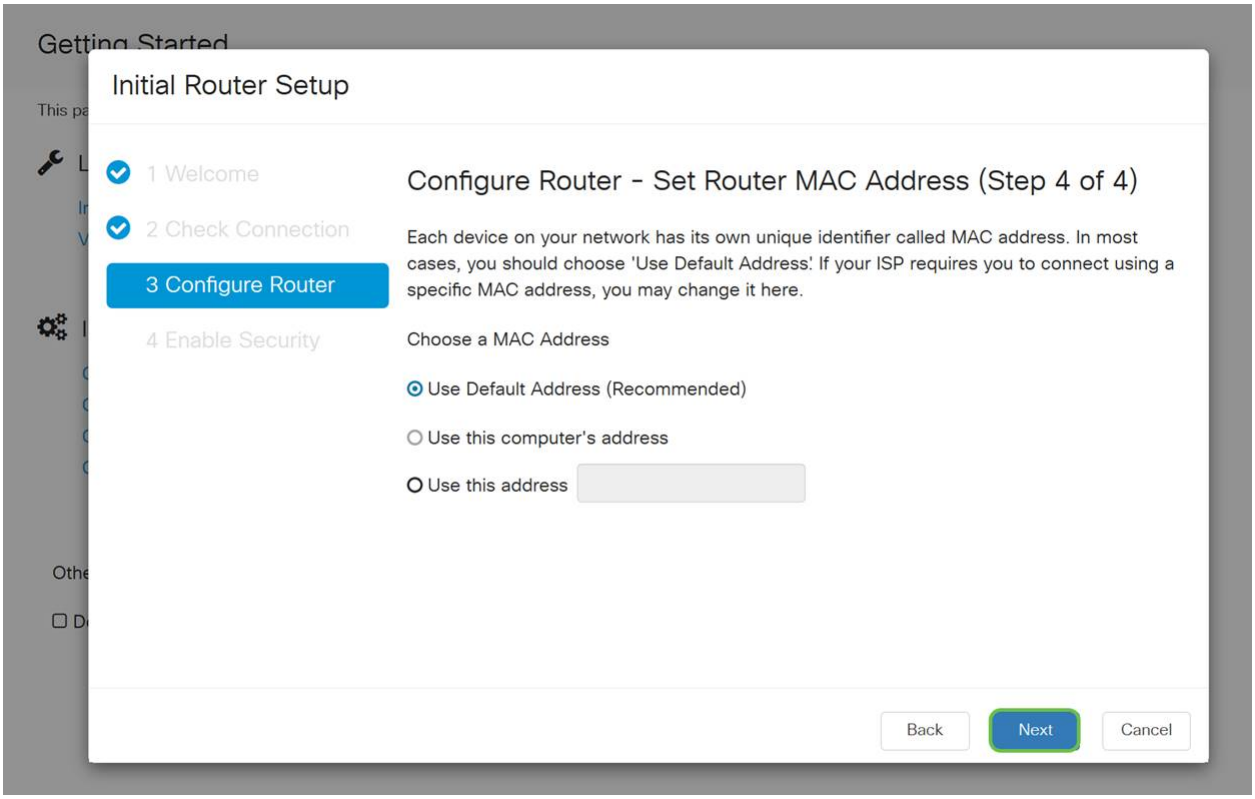

## Schritt 5

Hier werden Sie aufgefordert, die Zeiteinstellungen für den Router festzulegen. Dies ist wichtig, da es beim Überprüfen von Protokollen oder bei der Fehlerbehebung Präzision ermöglicht. Wählen Sie Ihre **Zeitzone aus** und klicken Sie dann auf **Weiter**.



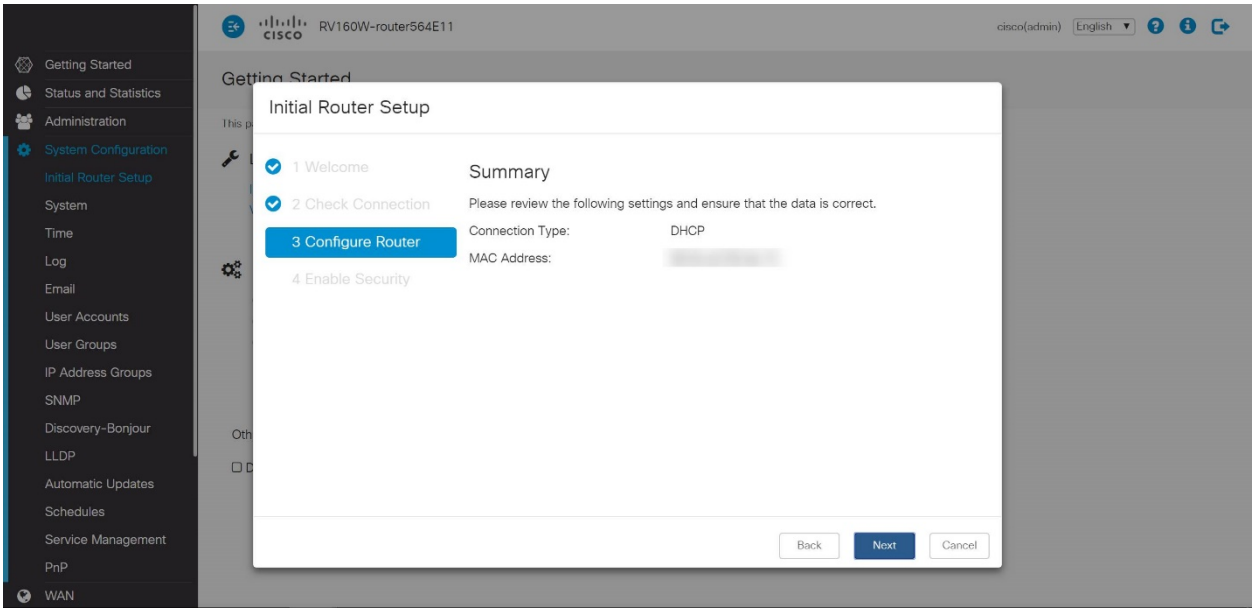

## Schritt 6

In diesem Bildschirm wählen Sie die MAC-Adressen aus, die Geräten zugewiesen werden sollen. In den meisten Fällen verwenden Sie die Standardadresse. Klicken Sie auf **Weiter**.



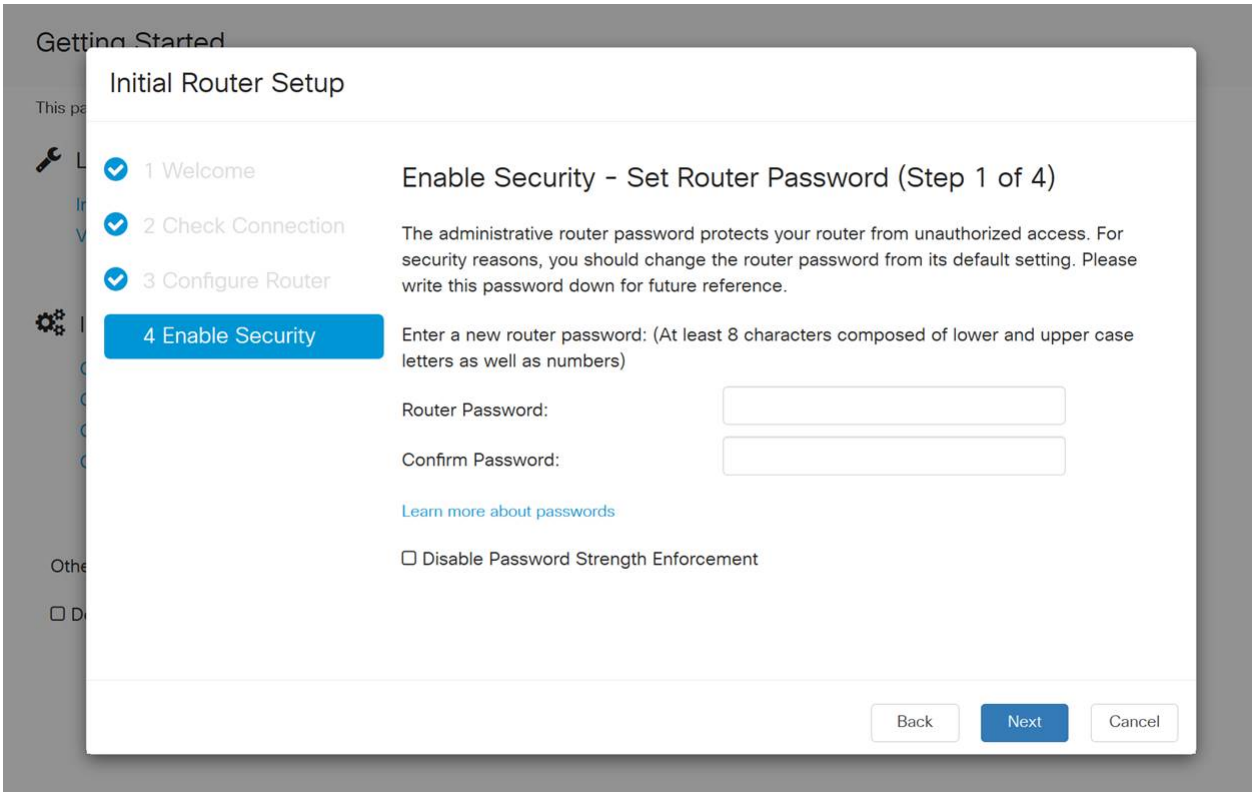

**Schritt 7**

Auf der folgenden Seite finden Sie eine Zusammenfassung der ausgewählten Optionen. Prüfen und auf **Weiter** klicken, wenn sie zufrieden sind.




**Schritt 8**

Im nächsten Schritt wählen Sie ein Kennwort aus, das bei der Anmeldung beim Router verwendet werden soll. Kennwörter müssen standardmäßig mindestens 8 Zeichen (Groß- und Kleinbuchstaben) enthalten und enthalten Zahlen. **Geben Sie ein Kennwort ein**, das den Festigkeitsanforderungen entspricht. Klicken Sie auf **Weiter**. Notieren Sie sich Ihr Kennwort für zukünftige Anmeldungen.




Es wird *nicht* empfohlen, die *Durchsetzung der Kennwortstärke* deaktivieren auszuwählen. Mit dieser Option können Sie ein Kennwort so einfach wie 123 auswählen, das für Angreifer so einfach wie 1-2-3 ist.

**Schritt 9**

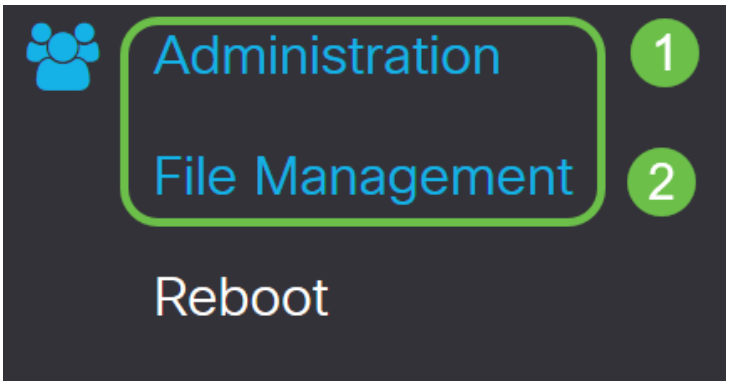
Klicken Sie auf das **Speichersymbol**.

## Firmware aktualisieren, falls erforderlich

Dies ist ein wichtiger Abschnitt. Überspringen Sie ihn nicht!

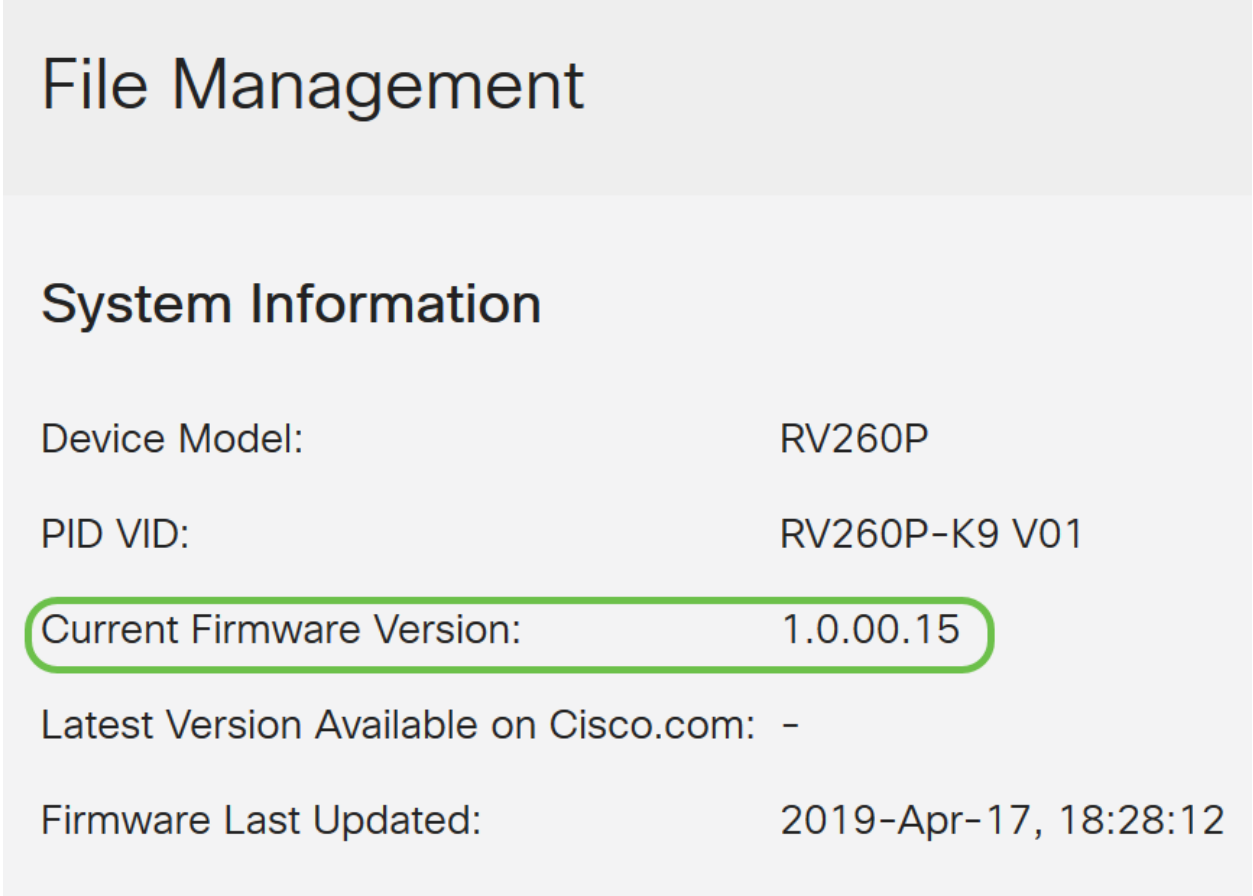
**Schritt 1**

Wählen Sie **Administration > File Management aus**.



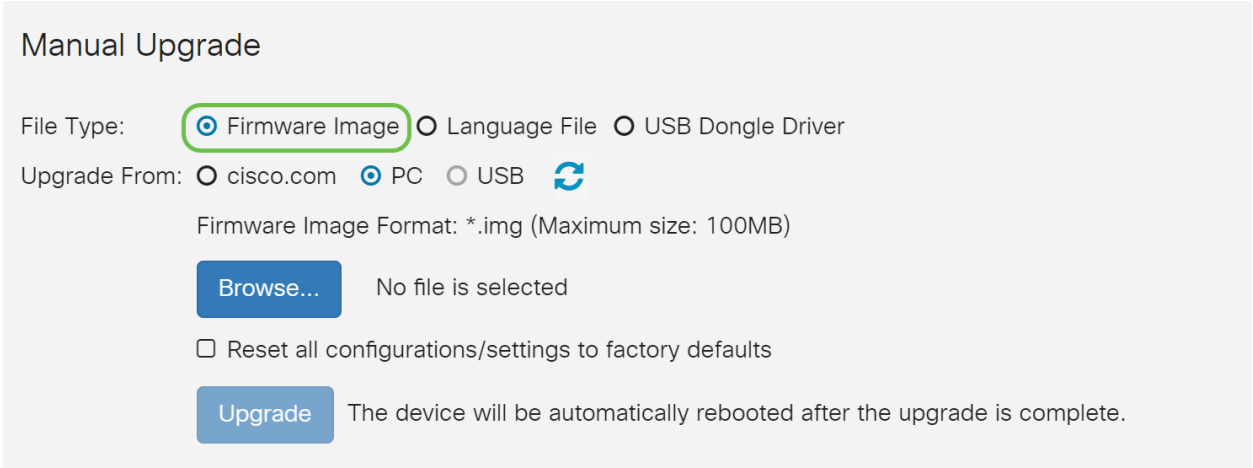
Im Bereich *Systeminformationen* beschreiben die folgenden Unterbereiche Folgendes:

- Gerätemodell: Zeigt das Gerätemodell an.
- PID VID - Produkt-ID und Anbieter-ID des Routers.
- Aktuelle Firmware-Version - Die Firmware, die derzeit auf dem Gerät ausgeführt wird.
- Neueste auf Cisco.com verfügbare Version - Die neueste Version der Software, die auf der Cisco Website verfügbar ist.
- Firmware zuletzt aktualisiert - Datum und Uhrzeit des letzten Firmware-Updates auf dem Router.



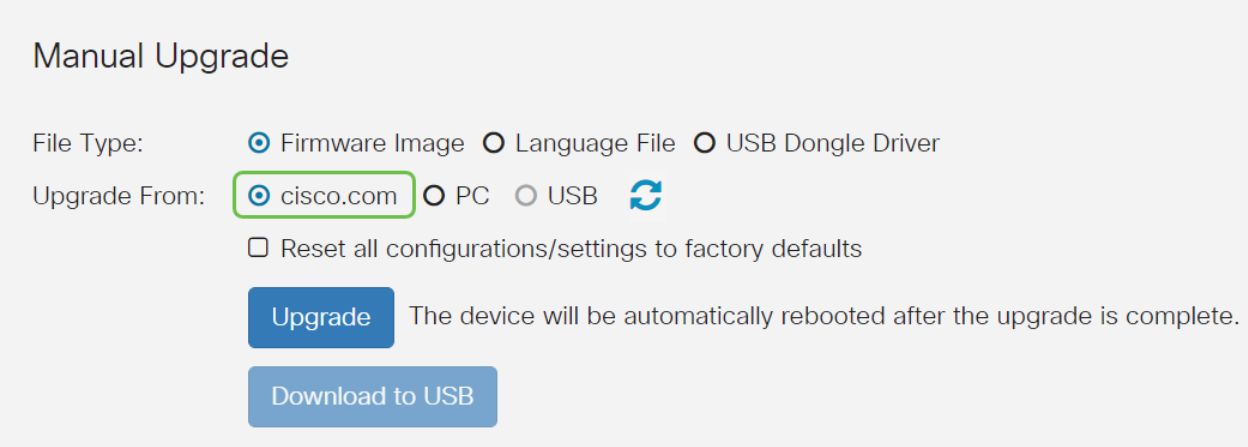

**Schritt 2**

Klicken Sie im Abschnitt *Manuelle Aktualisierung* auf das Optionsfeld **Firmware-Image** für *Dateityp*.



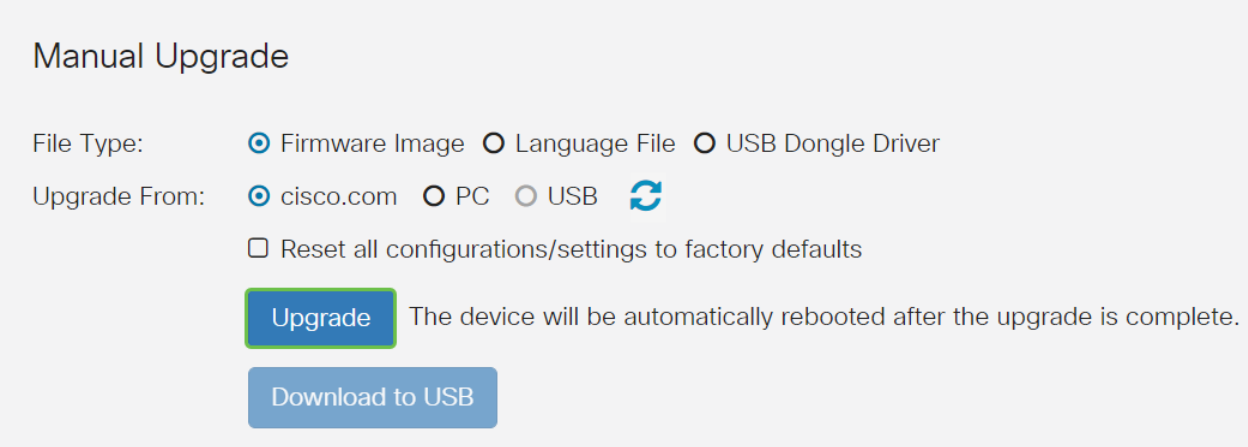

**Schritt 3**

Klicken Sie auf der Seite *Manuelle Aktualisierung* auf ein Optionsfeld, um cisco.com auszuwählen. Es gibt noch einige weitere Optionen, aber dies ist die einfachste Möglichkeit, ein Upgrade durchzuführen. Bei diesem Vorgang wird die neueste Upgrade-Datei direkt von der Cisco Software Downloads-Webseite installiert.



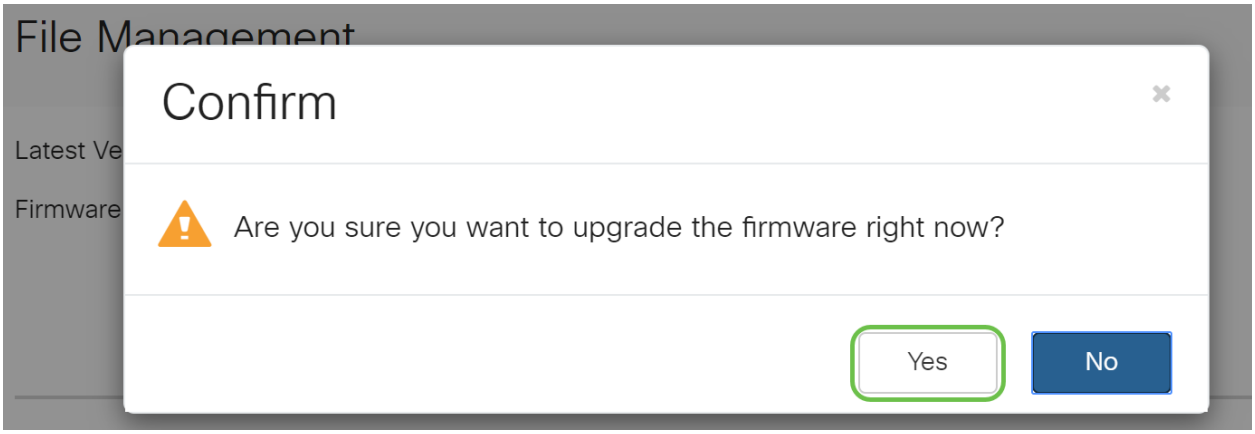

**Schritt 4**

Klicken Sie auf **Upgrade**.



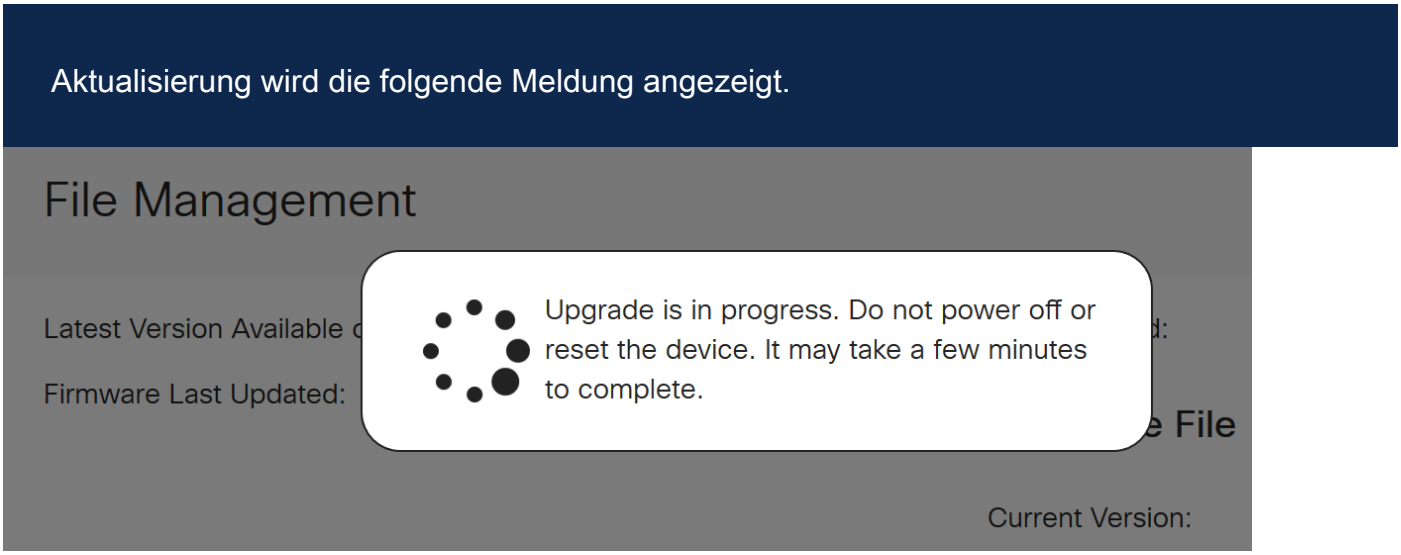

**Schritt 5**

Klicken Sie im Bestätigungsfenster auf **Ja**, um fortzufahren.

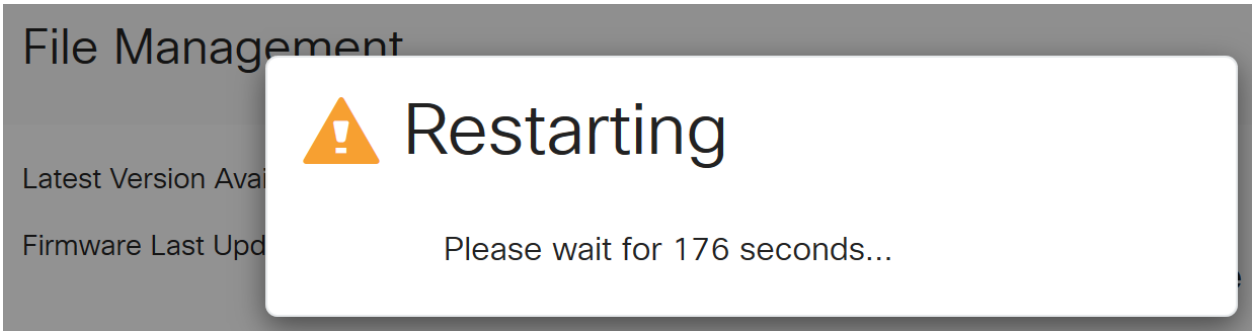



Der Aktualisierungsvorgang muss unterbrechungsfrei ausgeführt werden. Während der

Aktualisierung wird die folgende Meldung angezeigt.

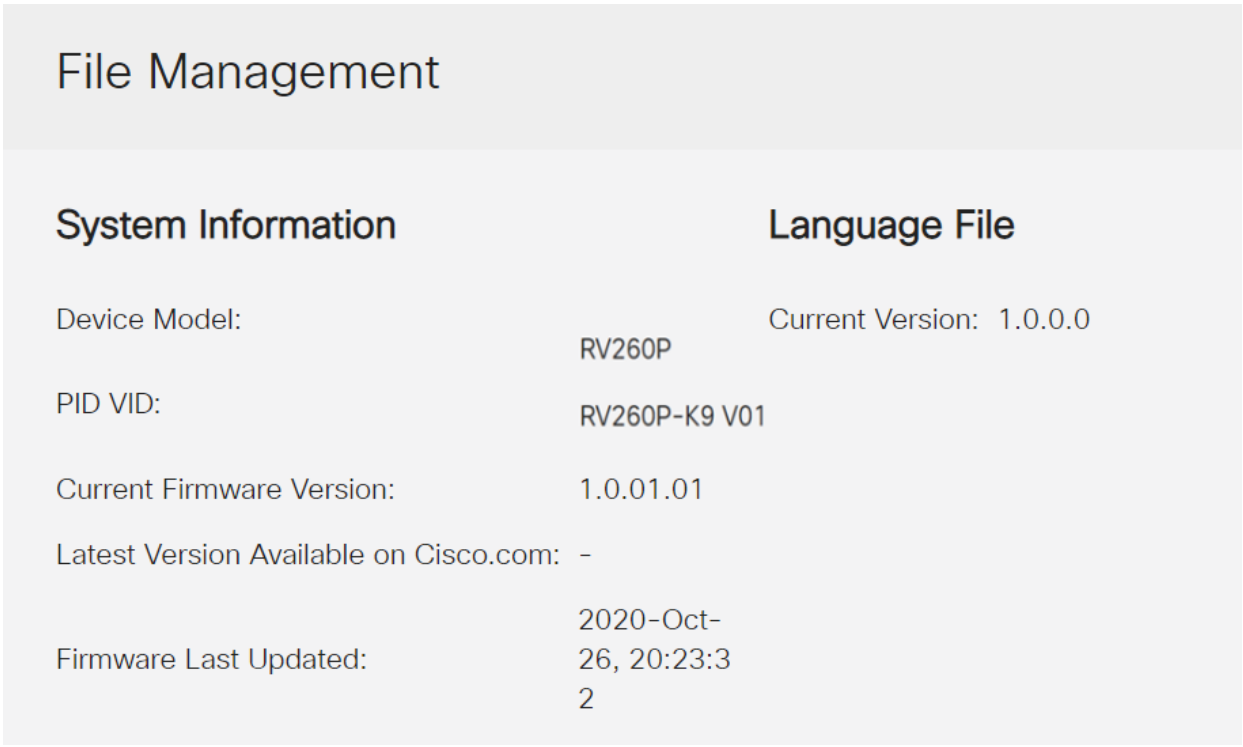



Nach Abschluss der Aktualisierung wird ein Benachrichtigungsfenster angezeigt, in dem Sie darüber informiert werden, dass der Router *neu gestartet* wird und eine Countdown für die geschätzte Zeit bis zum Abschluss des Vorgangs angezeigt wird. Danach werden Sie abgemeldet.




**Schritt 6**

Melden Sie sich wieder beim webbasierten Dienstprogramm an, um zu überprüfen, ob die Router-Firmware aktualisiert wurde, und navigieren Sie zu den *Systeminformationen*. Im Bereich *Aktuelle Firmware-Version* sollte jetzt die aktualisierte Firmware-Version angezeigt werden.




Herzlichen Glückwunsch! Ihre Grundeinstellungen auf Ihrem Router sind abgeschlossen! Sie haben einige Konfigurationsoptionen vorgezogen.

Ich empfehle Ihnen, weiter durch den Artikel zu blättern, um mehr über diese Optionen und, wenn sie auf Sie zutreffen zu erfahren. Wenn Sie möchten, können Sie auf einen der Hyperlinks klicken, um zu einem Abschnitt zu springen.

- VLANs konfigurieren (optional)
- IP-Adresse bearbeiten (optional)
- Hinzufügen statischer IP-Adressen (optional)
- Ich bin bereit, den Mesh Wireless-Teil meines Netzwerks zu konfigurieren!

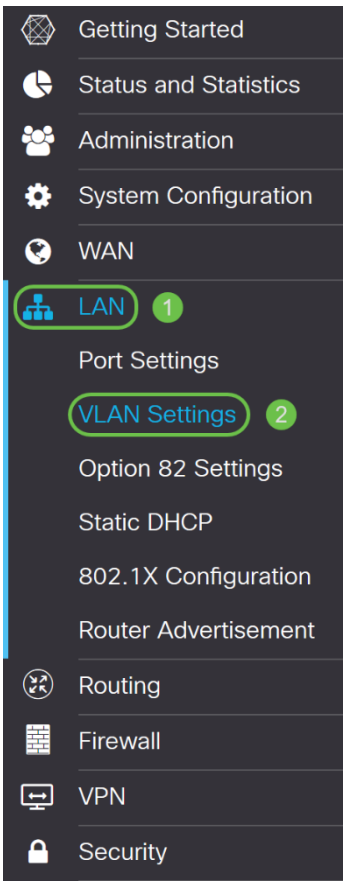
## VLANs konfigurieren (optional)

Mit einem Virtual Local Area Network (VLAN) können Sie ein Local Area Network (LAN) logisch in verschiedene Broadcast-Domänen segmentieren. In Umgebungen, in denen über das Netzwerk möglicherweise vertrauliche Daten übertragen werden, kann durch die Erstellung von VLANs die Sicherheit verbessert werden. Eine Übertragung kann dann auf ein spezifisches VLAN beschränkt werden. Mithilfe von VLANs kann auch die Leistung verbessert werden, da Broadcasts und Multicasts seltener an unnötige Ziele gesendet werden müssen. Sie können ein VLAN erstellen, dies hat jedoch keine Auswirkungen, bis das VLAN mindestens einem Port entweder manuell oder dynamisch angeschlossen ist. Ports müssen immer einem oder mehreren VLANs angehören.

Wenn Sie keine VLANs erstellen möchten, können Sie zum nächsten Abschnitt übergehen.

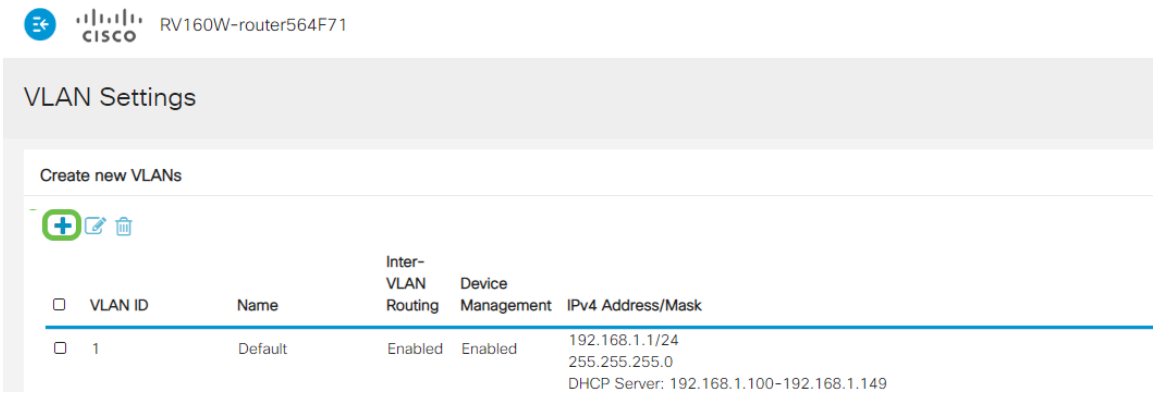
### Schritt 1

Navigieren Sie zu **LAN > VLAN Settings**.




## Schritt 2

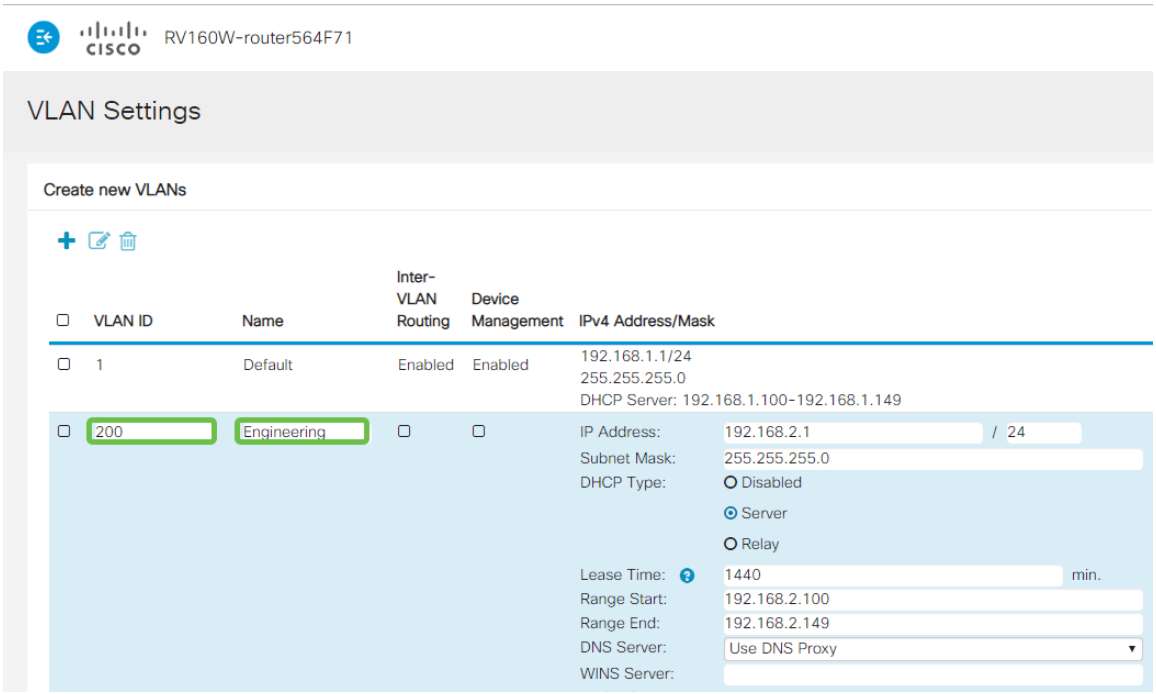
Klicken Sie auf **Hinzufügen**, um ein neues VLAN zu erstellen.




## Schritt 3

Geben Sie die *VLAN-ID*, die Sie erstellen möchten, und einen *Namen* dafür ein. Der *VLAN-ID*-Bereich liegt zwischen 1 und 4093.

Wir haben **200** als *VLAN-ID* und **Engineering** als *Namen* für das VLAN eingegeben.



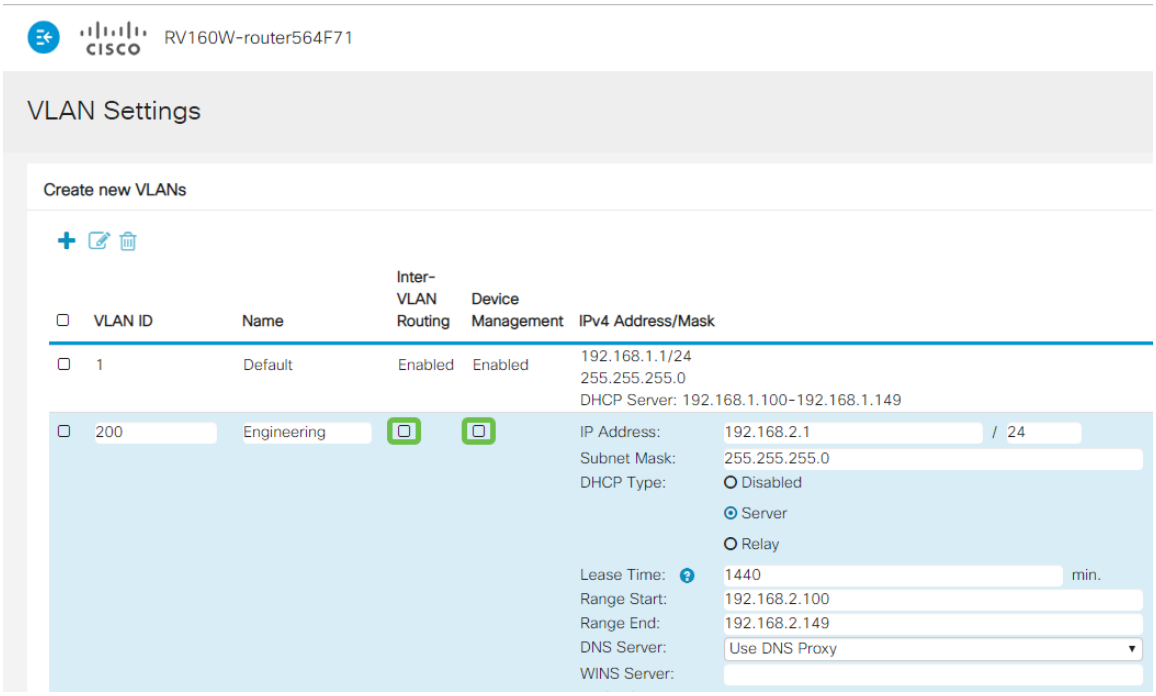

## Schritt 4

Deaktivieren Sie das *Kontrollkästchen Enabled (Aktiviert)* für *Inter-VLAN-Routing* und *Gerätemanagement*, wenn gewünscht.

Inter-VLAN-Routing wird verwendet, um Pakete von einem VLAN zu einem anderen VLAN zu routen. Im Allgemeinen wird dies für Gastnetzwerke nicht empfohlen, da Sie Gastbenutzer isolieren möchten. Die Sicherheit der VLANs wird dadurch beeinträchtigt. Es kann vorkommen, dass VLANs untereinander routen müssen. In diesem Fall können Sie das VLAN-übergreifende Routing auf einem RV34x-Router mit Zugriffskontrolllisten (Targeted ACL Restrictions) ausprobieren, um den zwischen VLANs zulässigen Datenverkehr zu konfigurieren.

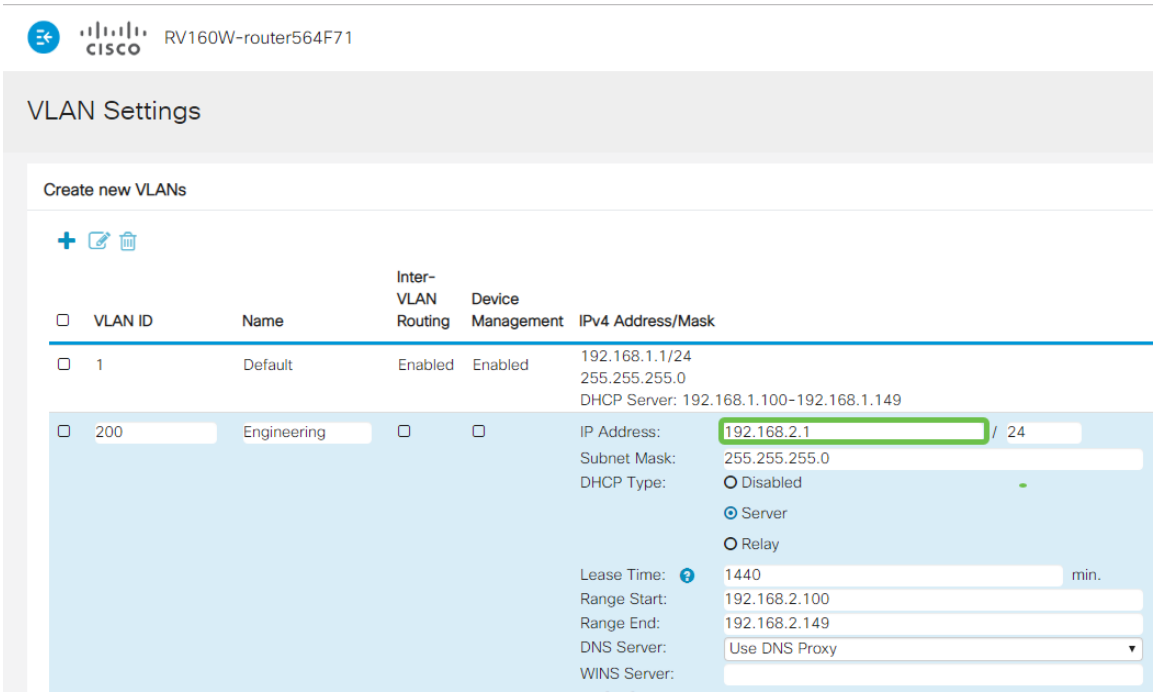
Die Geräteverwaltung ist die Software, mit der Sie sich über Ihren Browser über die Webbenutzeroberfläche des RV260P vom VLAN aus anmelden und den RV260P verwalten können. Dies sollte auch in Gastnetzwerken deaktiviert werden.

In diesem Beispiel haben wir weder das *VLAN-übergreifende Routing* noch das *Gerätemanagement* aktiviert, um die Sicherheit des VLAN zu erhöhen.




## Schritt 5

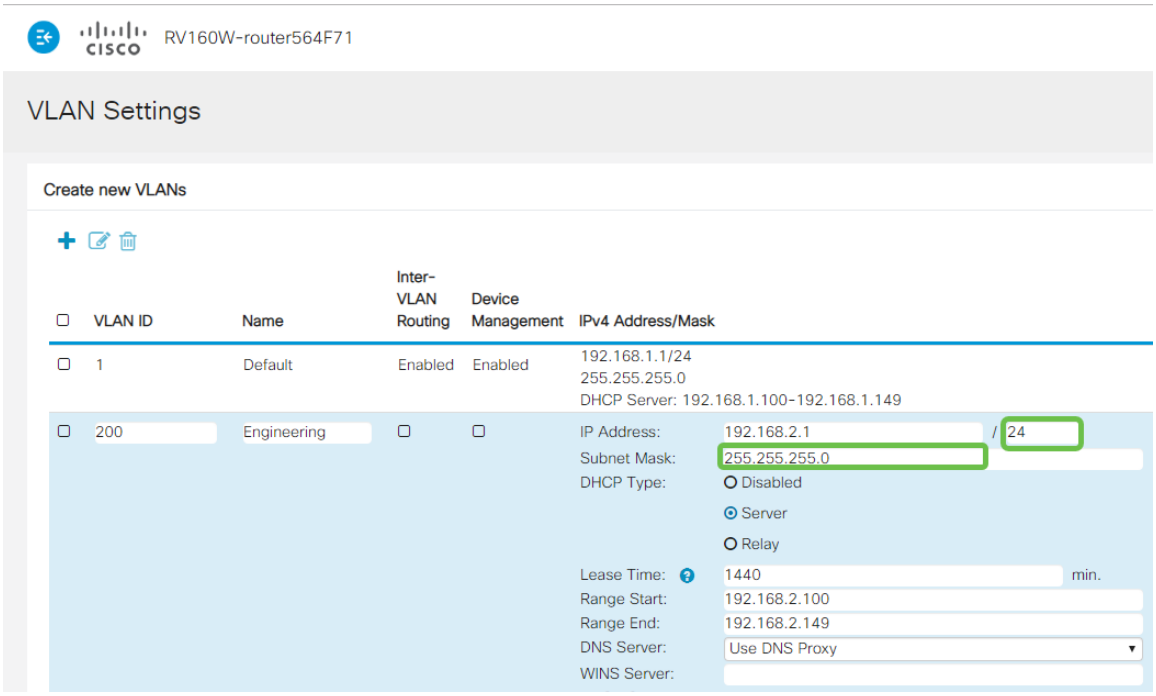
Die private IPv4-Adresse wird automatisch im Feld *IP-Adresse* eingetragen. Sie können dies auf Wunsch anpassen. In diesem Beispiel ist für das Subnetz 192.168.2.100-192.168.2.149 IP-Adressen für DHCP verfügbar. Für statische IP-Adressen sind die Werte 192.168.2.168.2.99 und 192.168.2.150-192.168.2.254 verfügbar.




## Schritt 6

Die Subnetzmaske unter der *Subnetzmaske* wird automatisch eingetragen. Wenn Sie Änderungen vornehmen, wird das Feld automatisch angepasst.

Für diese Demonstration verlassen wir die *Subnetzmaske* als **255.255.255.0** oder **/24**.



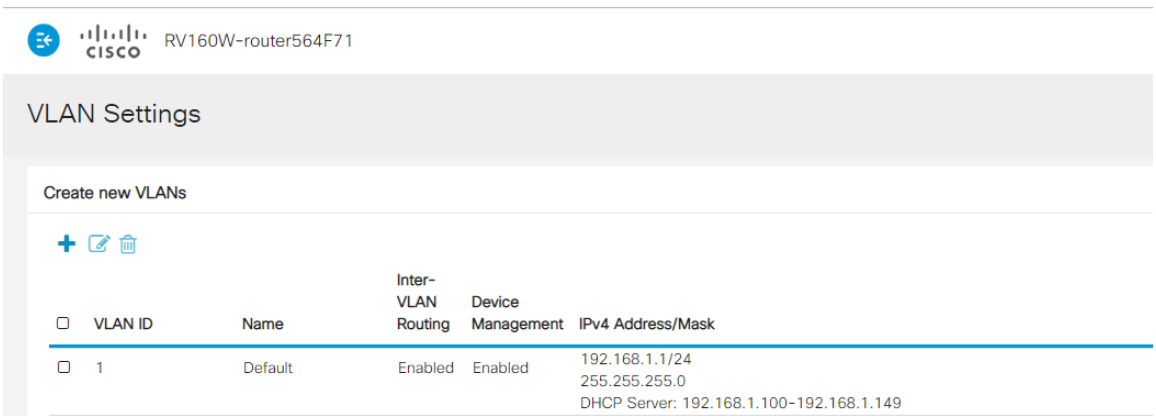

## Schritt 7

Wählen Sie einen *Dynamic Host Configuration Protocol (DHCP)-Typ aus*. Folgende Optionen sind verfügbar:

*Disabled (Deaktiviert)*: Deaktiviert den DHCP-IPv4-Server im VLAN. Dies wird in einer Testumgebung empfohlen. In diesem Szenario müssen alle IP-Adressen manuell konfiguriert werden, und die gesamte Kommunikation ist intern.

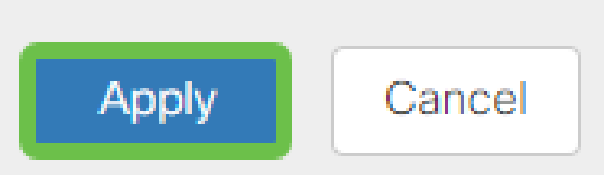
*Server*: Dies ist die am häufigsten verwendete Option.

- Leasingzeit: Geben Sie einen Zeitwert von 5 bis 43.200 Minuten ein. Der Standardwert ist 1440 Minuten (entsprechend 24 Stunden).
- Range Start and Range End (Anfang und Ende des Bereichs): Geben Sie den Anfang und das Ende der IP-Adressen ein, die dynamisch zugewiesen werden können.
- DNS Server (DNS-Server): Wählen Sie diese Option aus, um den DNS-Server als Proxy oder von ISP aus der Dropdown-Liste zu verwenden.
- WINS-Server - Geben Sie den WINS-Servernamen ein.
- DHCP-Optionen:
    - Option 66 - Geben Sie die IP-Adresse des TFTP-Servers ein.
    - Option 150 - Geben Sie die IP-Adresse einer Liste von TFTP-Servern ein.
    - Option 67 - Geben Sie den Konfigurationsdateinamen ein.
- Relay (Relay) - Geben Sie die IPv4-Adresse des Remote-DHCP-Servers ein, um den DHCP Relay Agent zu konfigurieren. Dies ist eine erweiterte Konfiguration.



### Schritt 8

Klicken Sie auf **Apply**, um das neue VLAN zu erstellen.




## VLANs Ports zuweisen

Auf dem RV260 können 16 VLANs mit einem VLAN für das Wide Area Network (WAN) konfiguriert werden. VLANs, die sich nicht auf einem Port befinden, sollten *ausgeschlossen* werden. Auf diese Weise wird der Datenverkehr an diesem Port ausschließlich für die VLANs/VLANs aufrechterhalten, die dem Benutzer eigens zugewiesen wurden. Sie gilt als Best Practice.

Ports können als Access-Port oder Trunk-Port festgelegt werden:

- Access Port - Ein VLAN zugewiesen. Ungetaggte Frames werden übergeben.
- Trunk-Port - Kann mehr als ein VLAN übertragen. 802.1q. Beim Trunking kann ein natives VLAN nicht markiert werden. VLANs, die Sie nicht auf dem Trunk verwenden möchten, sollten ausgeschlossen werden.

Ein VLAN hat einen eigenen Port zugewiesen:

- Als Access-Port eingestuft.
- Das VLAN, dem dieser Port zugewiesen ist, sollte als Untagged gekennzeichnet sein.
- Alle anderen VLANs sollten für diesen Port mit Excluded (Ausgeschlossen) gekennzeichnet sein.

Zwei oder mehr VLANs, die einen Port gemeinsam nutzen:

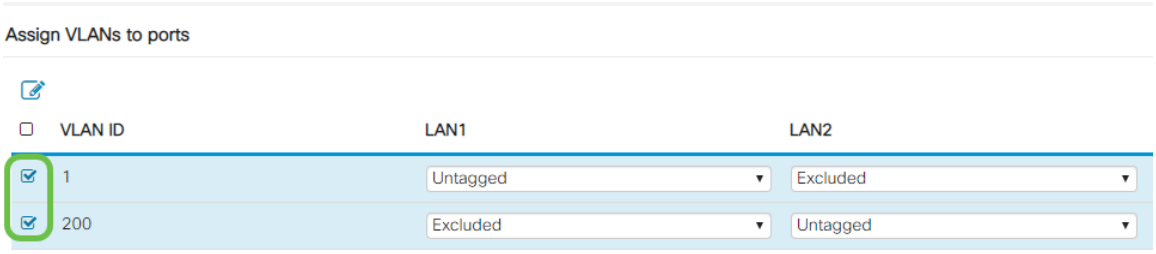
- Als Trunk-Port angesehen.
- Eines der VLANs kann als Untagged bezeichnet werden.
- Die übrigen VLANs, die Teil des Trunk-Ports sind, müssen mit Tagged gekennzeichnet werden.
- Die VLANs, die nicht Teil des Trunk-Ports sind, sollten für diesen Port mit Excluded (Ausgeschlossen) gekennzeichnet werden.

**Hinweis:** In diesem Beispiel gibt es keine Trunks.

### Schritt 9

Wählen Sie die zu bearbeitenden *VLAN-IDs* aus. Klicken Sie auf **Bearbeiten**.

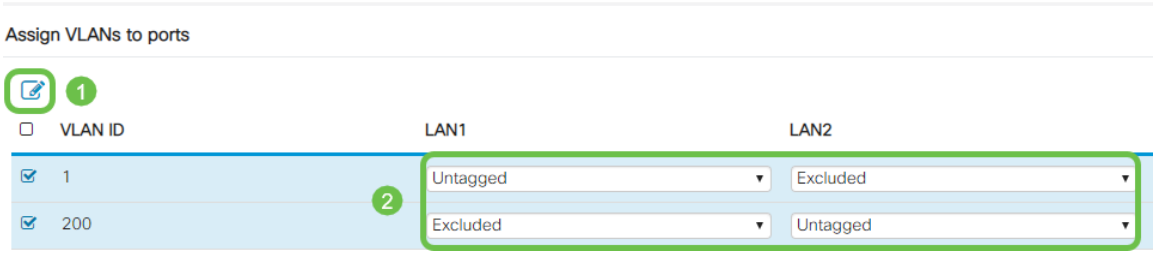
In diesem Beispiel haben wir *VLAN 1* und *VLAN 200* ausgewählt.




**Schritt 10**

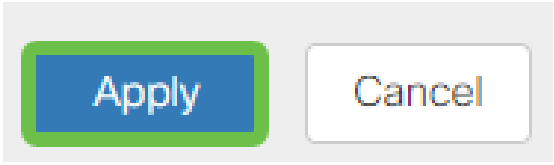
Klicken Sie auf **Bearbeiten**, um einem LAN-Port ein VLAN zuzuweisen, und geben Sie jede Einstellung als *Tagged*, *Untagged* oder *Excluded* an.

In diesem Beispiel haben wir VLAN 1 für LAN1 als **Untagged** und VLAN 200 als **Excluded** zugewiesen. Für LAN2 wurde VLAN 1 als **Excluded** und VLAN 200 als **Untagged** zugewiesen.




**Schritt 11**

Klicken Sie auf **Apply**, um die Konfiguration zu speichern.




Sie sollten jetzt erfolgreich ein neues VLAN erstellt und VLANs für die Ports des RV260 konfiguriert haben. Wiederholen Sie den Vorgang, um die anderen VLANs zu erstellen. So wird beispielsweise VLAN300 für Marketing mit dem Subnetz 192.168.3.x erstellt, und VLAN400 für die Buchhaltung mit dem Subnetz 192.168.4.x.

Das sind die Grundlagen von VLANs. Klicken Sie auf den Hyperlink, um mehr über VLAN Best Practices und Security Tips für Cisco Business Router zu erfahren.

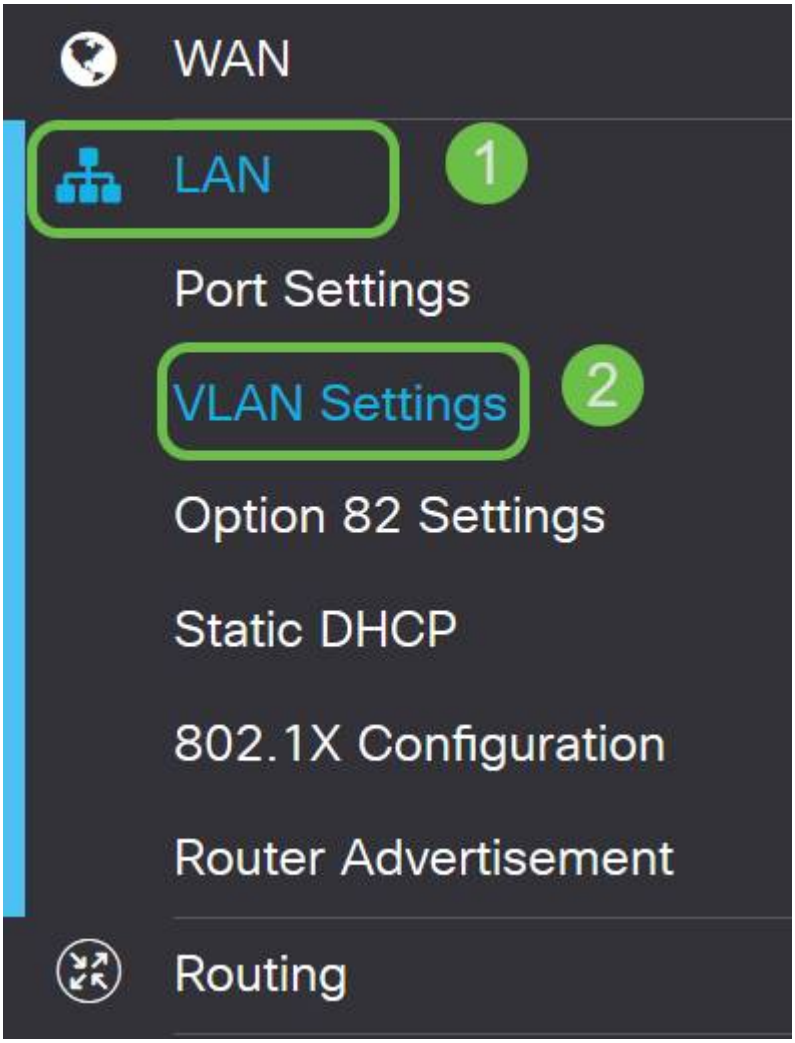
## IP-Adresse bearbeiten (optional)

Nach Abschluss des *Assistenten für die Ersteinrichtung* können Sie eine statische IP-Adresse auf dem Router festlegen, indem Sie die VLAN-Einstellungen bearbeiten. Führen Sie die folgenden Schritte aus, um den Assistenten zur Ersteinrichtung erneut auszuführen.

Wenn Sie keine IP-Adresse bearbeiten müssen, können Sie zum nächsten Abschnitt dieses Artikels wechseln.

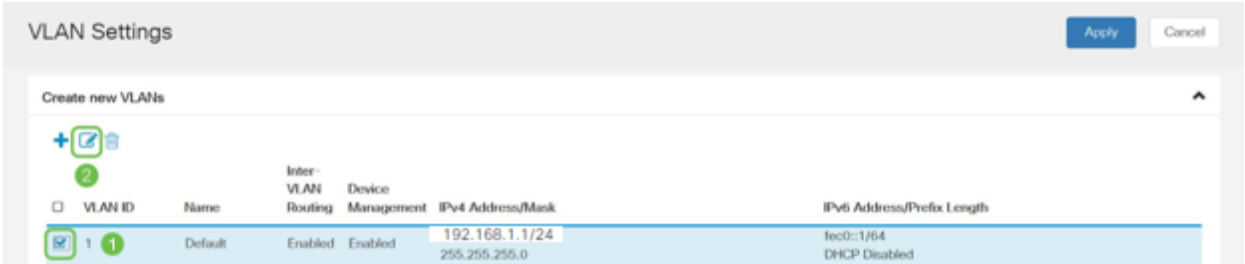
**Schritt 1**

Klicken Sie in der linken Menüleiste auf **LAN > VLAN Settings**.



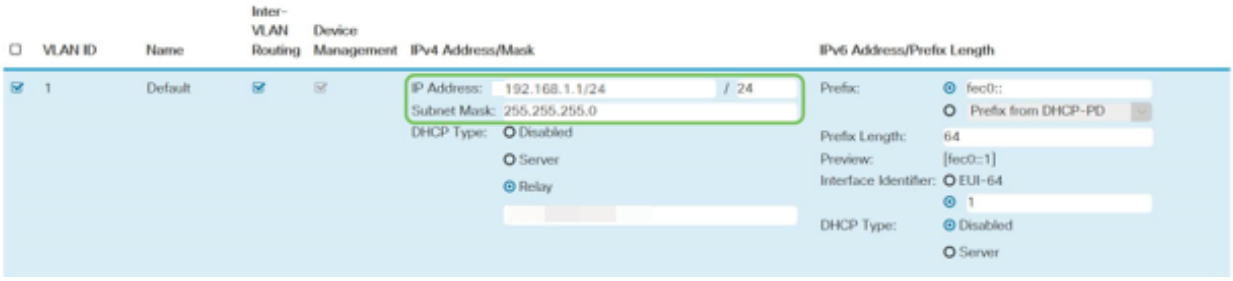

**Schritt 2**

Wählen Sie dann das **VLAN** aus, das Ihr Routing-Gerät enthält, und klicken Sie dann auf das **Bearbeitungssymbol**.



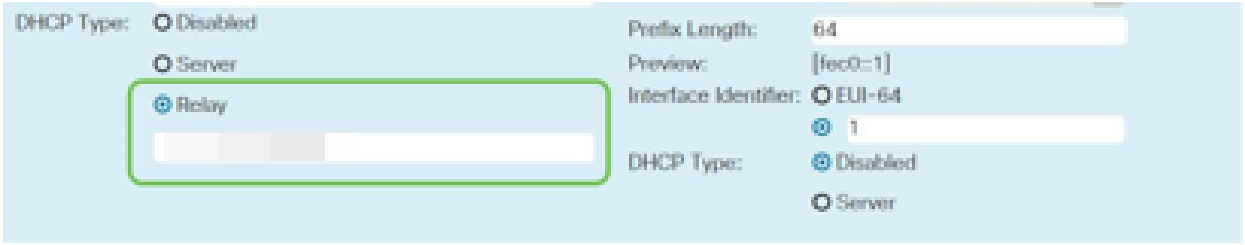

**Schritt 3**

Geben Sie die gewünschte **statische IP-Adresse ein** und klicken Sie in der rechten oberen Ecke auf **Apply**.




**Schritt 4 (optional)**

Wenn Ihr Router nicht der DHCP-Server bzw. das DHCP-Gerät ist, dem IP-Adressen zugewiesen werden, können Sie die DHCP-Relay-Funktion verwenden, um DHCP-Anfragen an eine bestimmte IP-Adresse zu leiten. Die IP-Adresse ist wahrscheinlich der Router, der mit dem WAN/Internet verbunden ist.



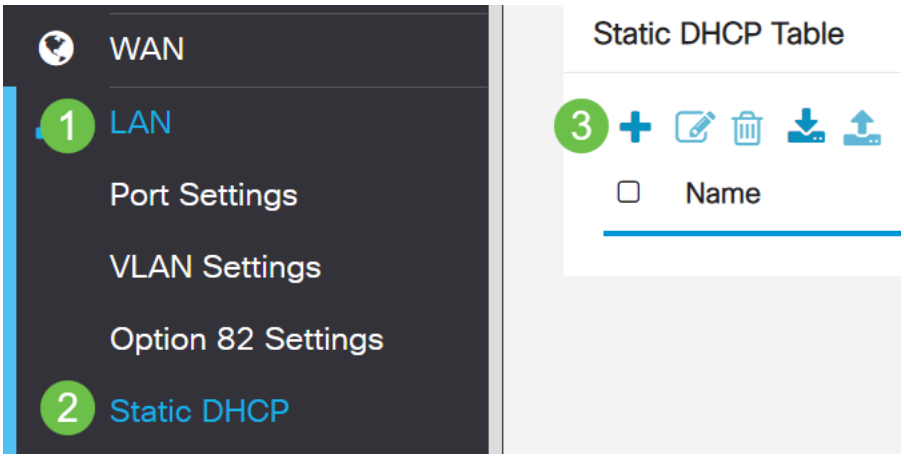

## Hinzufügen einer statischen IP

Wenn Sie möchten, dass ein bestimmtes Gerät für andere VLANs erreichbar ist, können Sie diesem Gerät eine statische lokale IP-Adresse zuweisen und eine Zugriffsregel erstellen, um darauf zuzugreifen. Dies funktioniert nur, wenn Inter-VLAN-Routing aktiviert ist. Es gibt andere Situationen, in denen eine statische IP von Nutzen sein kann. Weitere Informationen zum Einstellen statischer IP-Adressen finden Sie in den Best Practices zum Einstellen statischer IP-Adressen auf der Cisco Business-Hardware.

Wenn Sie keine statische IP-Adresse hinzufügen müssen, können Sie mit dem nächsten Abschnitt dieses Artikels zur Konfiguration der Access Points fortfahren.

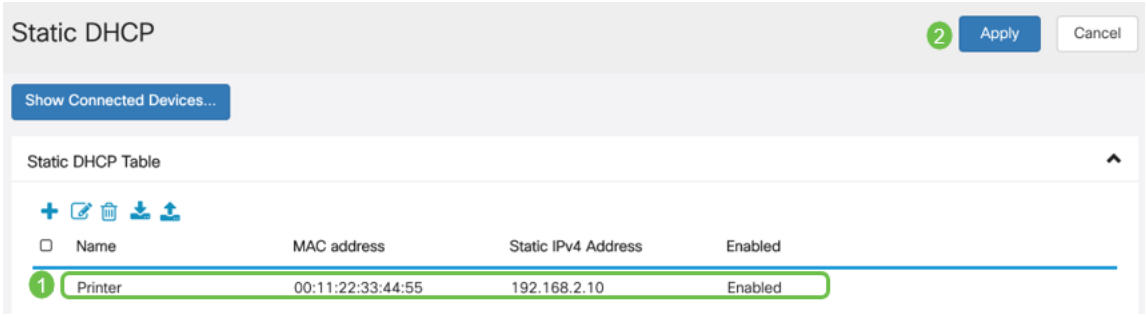
**Schritt 1**

Navigieren Sie zu **LAN > Static DHCP (LAN > Static DHCP).** Klicken Sie auf das **Pluszeichen**.



**Schritt 2**

Fügen Sie die **statischen DHCP-**Informationen für das Gerät hinzu. In diesem Beispiel ist das Gerät ein Drucker.




Herzlichen Glückwunsch! Sie haben die Konfiguration Ihres RV260P-Routers abgeschlossen. Wir werden jetzt Ihre Cisco Business Wireless-Geräte konfigurieren.

# Konfigurieren des CBW140AC

## Sofort einsatzbereiter CBW140AC

Schließen Sie zunächst ein Ethernetkabel vom PoE-Port Ihres CBW140AC an einen PoE-Port des RV260P an. Die ersten vier Ports des RV260P können PoE bereitstellen, sodass alle Ports verwendet werden können.

Überprüfen Sie den Status der Leuchtanzeigen. Der Startvorgang des Access Points dauert ca. 10 Minuten. Die LED blinkt in mehreren Mustern grün, wechselt schnell durch grün, rot und orange, bevor sie wieder grün wird. Die LED-Farbintensität und der Farbton können von Gerät zu Einheit geringfügig variieren. Wenn die LED-Anzeige grün blinkt, fahren Sie mit dem nächsten Schritt fort.

Der PoE-Ethernet-Uplink-Port am primären Access Point kann NUR für die Bereitstellung eines Uplink zum LAN und NICHT für die Verbindung mit anderen primären und Mesh-Extender-Geräten verwendet werden.

Wenn Ihr Access Point nicht neu ist, stellen Sie sicher, dass er sofort auf die Werkseinstellungen zurückgesetzt ist, damit der *CiscoBusiness-Setup* SSID in Ihren Wi-Fi-Optionen angezeigt wird. Weitere Informationen hierzu finden Sie unter Neustarten und Zurücksetzen auf die werkseitigen Standardeinstellungen auf RV260-Routern.

## Richten Sie den primären 140AC Wireless Access Point auf der Webbenutzeroberfläche ein.

Sie können den Access Point mithilfe der mobilen Anwendung oder der Webbenutzeroberfläche einrichten. Dieser Artikel verwendet die Webbenutzeroberfläche für die Einrichtung, die mehr Konfigurationsoptionen bietet, aber etwas komplizierter ist. Wenn Sie die mobile Anwendung für die nächsten Abschnitte verwenden möchten, klicken Sie auf die Anweisungen für mobile

Anwendungen.

Wenn Sie Probleme beim Herstellen einer Verbindung haben, lesen Sie den Abschnitt Tipps zur Fehlerbehebung bei Wireless-Netzwerken in diesem Artikel.

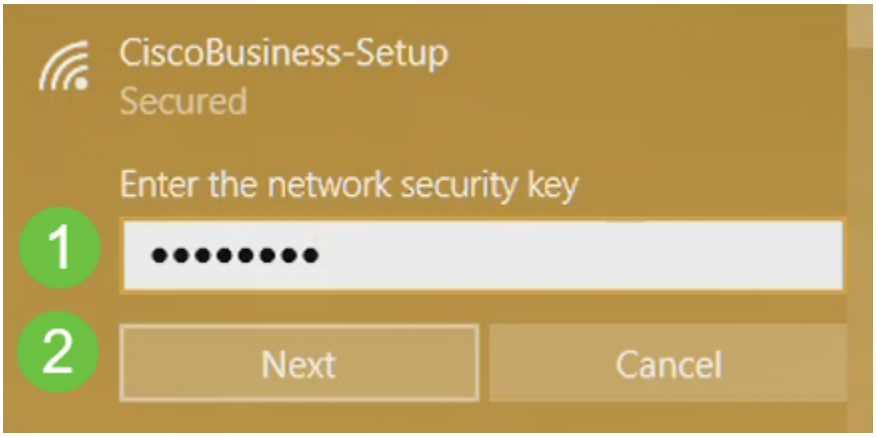
### Schritt 1

Klicken Sie auf Ihrem PC auf das **Wi-Fi-Symbol** und wählen Sie *CiscoBusiness-Setup* Wireless Network. Klicken Sie auf Verbinden.


Wenn Ihr Access Point nicht neu ist, stellen Sie sicher, dass er sofort auf die Werkseinstellungen zurückgesetzt ist, damit der *CiscoBusiness-Setup* SSID in Ihren Wi-Fi-Optionen angezeigt wird.

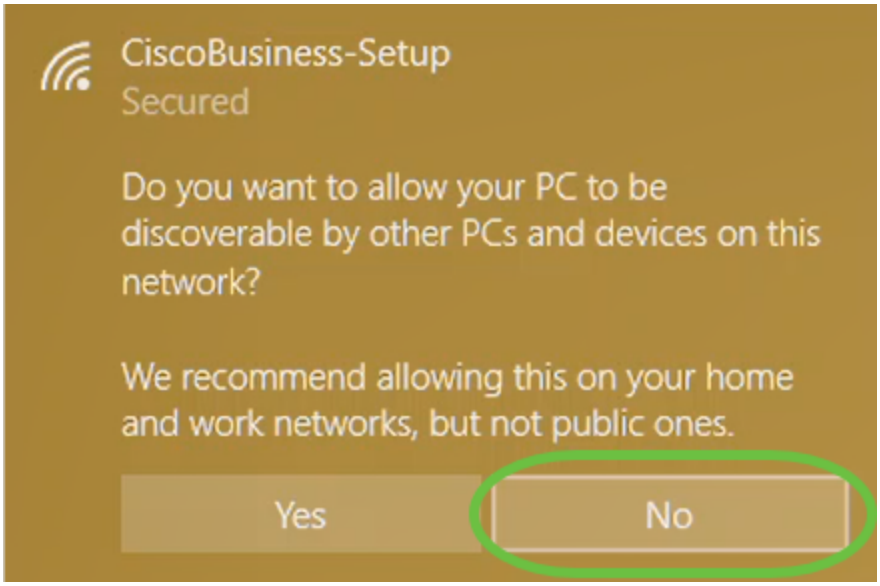
### Schritt 2

Geben Sie die Passphrase **cisco123 ein** und klicken Sie auf **Weiter**.




**Schritt 3**

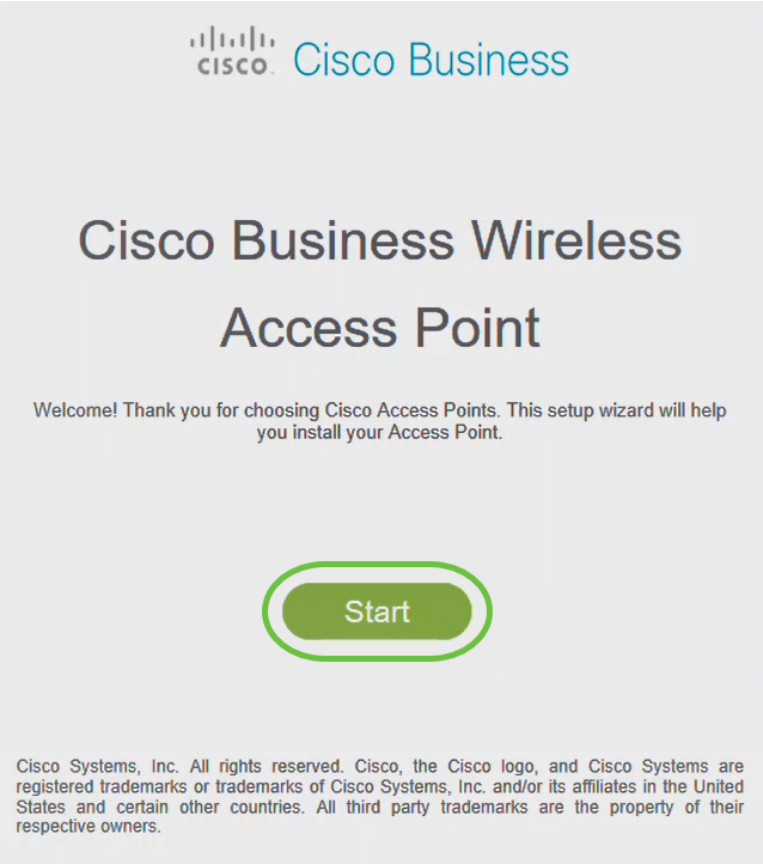
Sie erhalten den folgenden Bildschirm. Da immer nur ein Gerät konfiguriert werden kann, klicken Sie auf **Nein**.




Es kann nur ein Gerät an die *CiscoBusiness-Setup*-SSID angeschlossen werden. Wenn ein zweites Gerät versucht, eine Verbindung herzustellen, ist dies nicht möglich. Wenn Sie keine Verbindung zum SSID herstellen können und das Kennwort validiert haben, hat möglicherweise ein anderes Gerät die Verbindung hergestellt. Starten Sie den Access Point neu, und versuchen Sie es erneut.

**Schritt 4**

Sobald die Verbindung hergestellt ist, sollte der Webbrowser automatisch zum CBW AP-Einrichtungsassistenten umleiten. Falls nicht, öffnen Sie einen Webbrowser wie Internet Explorer, Firefox, Chrome oder Safari. Geben Sie in die Adressleiste **http://ciscobusiness.cisco ein** und drücken **Sie die Eingabetaste**. Klicken Sie auf der Webseite auf **Start**.




Wenn die Webseite nicht angezeigt wird, warten Sie einige Minuten, oder laden Sie die Seite erneut. Nach der Ersteinrichtung können Sie sich unter https://ciscobusiness.cisco anmelden. Wenn Ihr Webbrowser automatisch mit *http://* ausgefüllt wird, müssen Sie das *https://* manuell eingeben , um Zugriff zu erhalten.

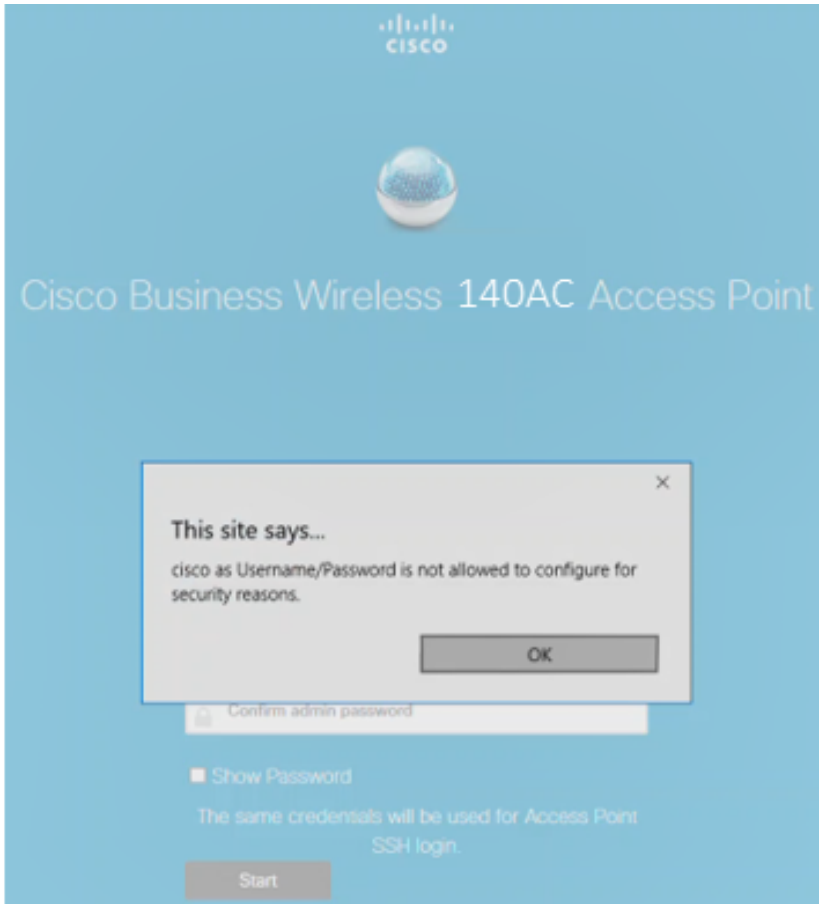
**Schritt 5**

Erstellen Sie ein *Administratorkonto*, indem Sie Folgendes eingeben:

- Benutzername des Administrators (maximal 24 Zeichen)
- Administratorkennwort
- Administratorkennwort bestätigen

Sie können das Kennwort anzeigen, indem Sie das Kontrollkästchen neben *Kennwort anzeigen* aktivieren. Klicken Sie auf **Start**.


Verwenden Sie nicht *cisco* oder deren Varianten in den Feldern für den Benutzernamen oder das Kennwort. Wenn dies der Fall ist, erhalten Sie eine Fehlermeldung wie unten gezeigt.

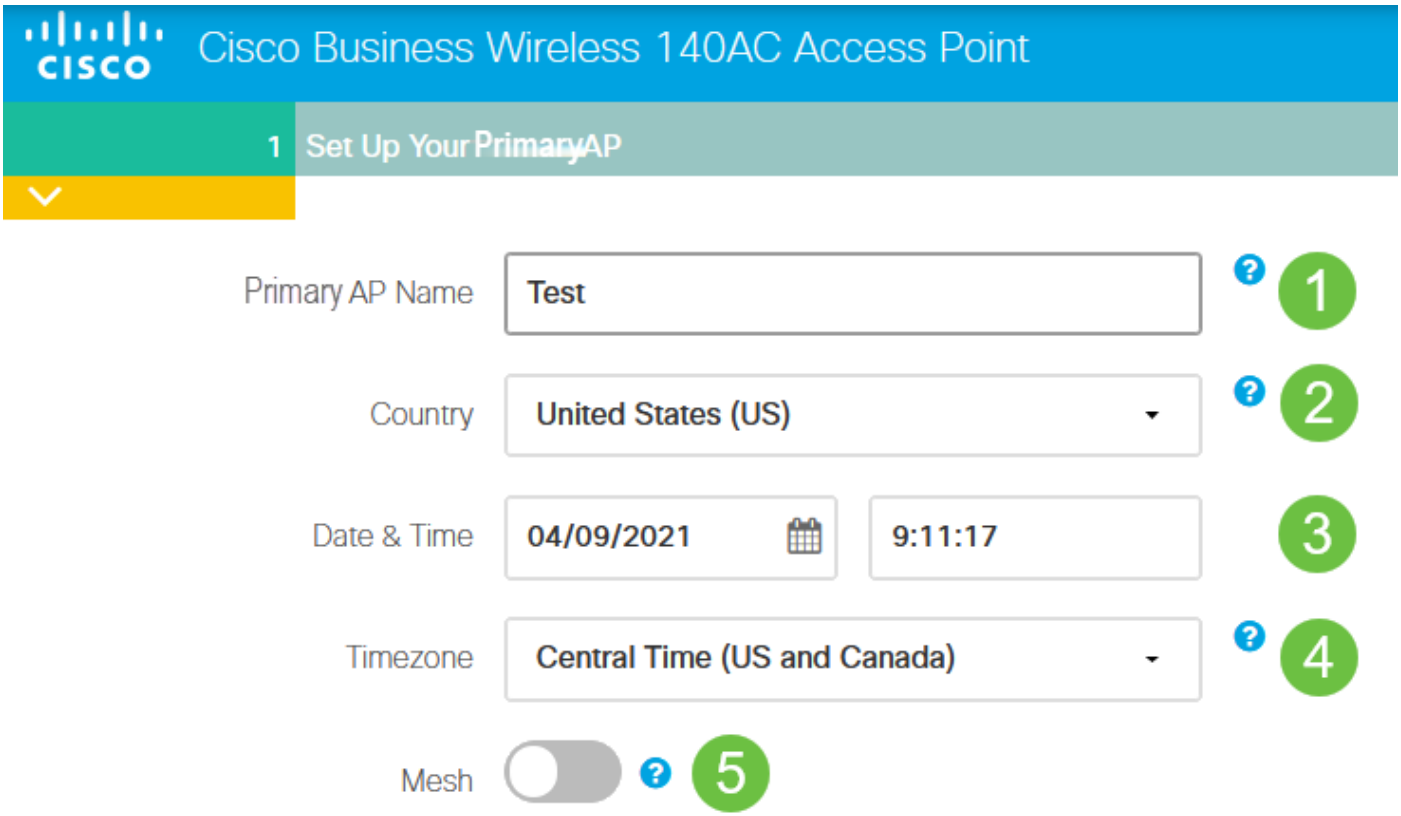



**Schritt 6**

*Richten Sie den primären Access Point ein*, indem Sie Folgendes eingeben:

- Primärer AP-Name

- Land
- Datum und Uhrzeit
- Zeitzone
- Mesh



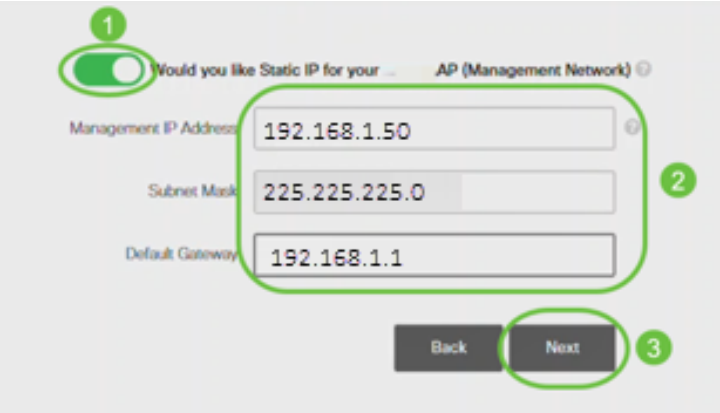

*Mesh* sollte nur aktiviert werden, wenn Sie ein Mesh-Netzwerk erstellen möchten. Standardmäßig ist sie deaktiviert.

**Schritt 7**

(Optional) Sie können die *statische IP für Ihren* CBW140AC aktivieren, um Verwaltungszwecke zu übernehmen. Andernfalls erhält die Schnittstelle eine IP-Adresse von Ihrem DHCP-Server. Um statische IP zu konfigurieren, geben Sie Folgendes ein:

- Management-IP-Adresse
- Subnetzmaske
- Standard-Gateway

Klicken Sie auf **Weiter**.



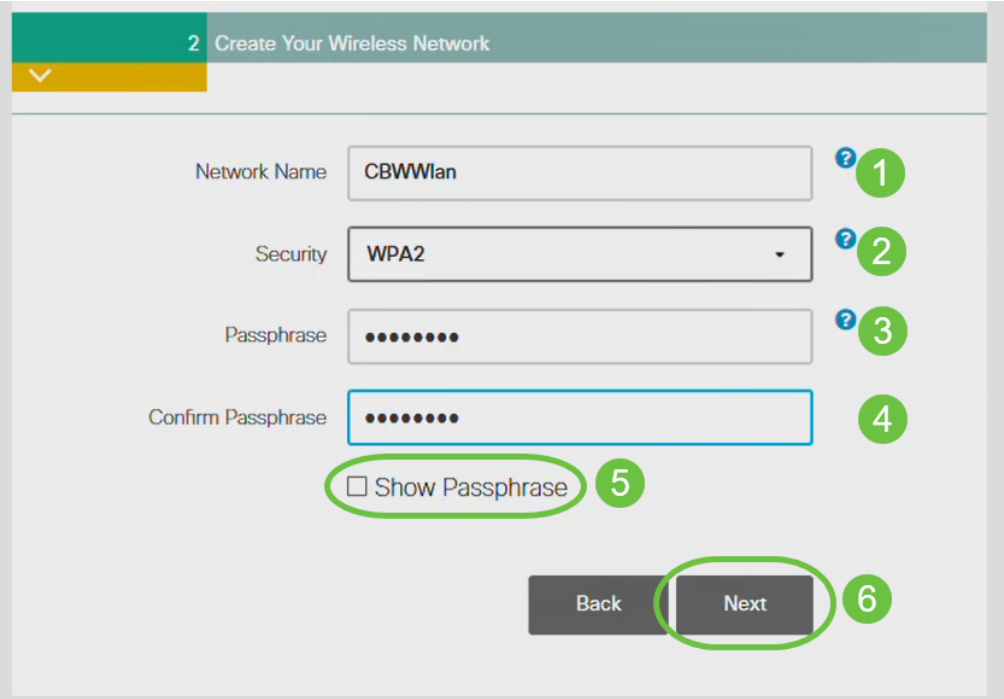

Diese Option ist standardmäßig deaktiviert.

### Schritt 8

*Erstellen Sie Ihre Wireless-Netzwerke*, indem Sie Folgendes eingeben:

- Netzwerkname
- Sicherheit auswählen
- Passphrase
- Passphrase bestätigen
- (Optional) Aktivieren Sie das Kontrollkästchen Passphrase anzeigen.

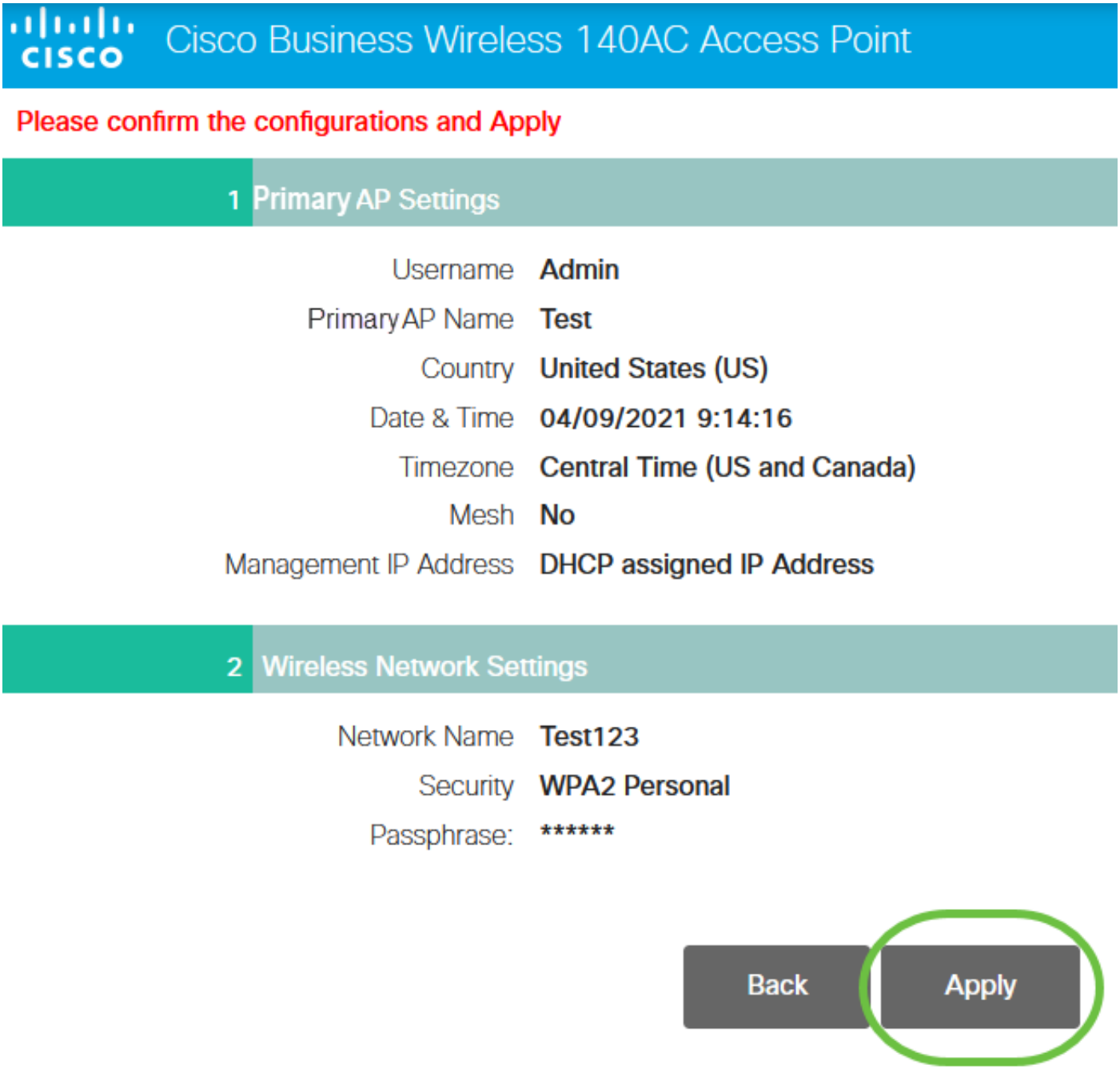
Klicken Sie auf **Weiter**.




Wi-Fi Protected Access (WPA) Version 2 (WPA2) ist der aktuelle Standard für die Wi-Fi-Sicherheit.

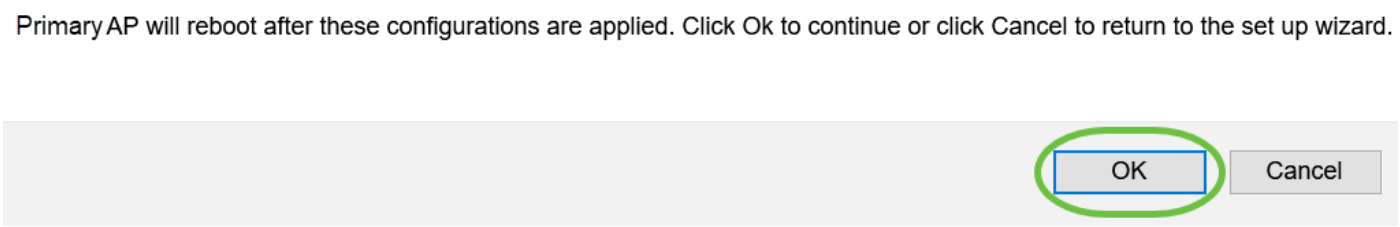
### Schritt 9

Bestätigen Sie die Einstellungen, und klicken Sie auf **Übernehmen**.

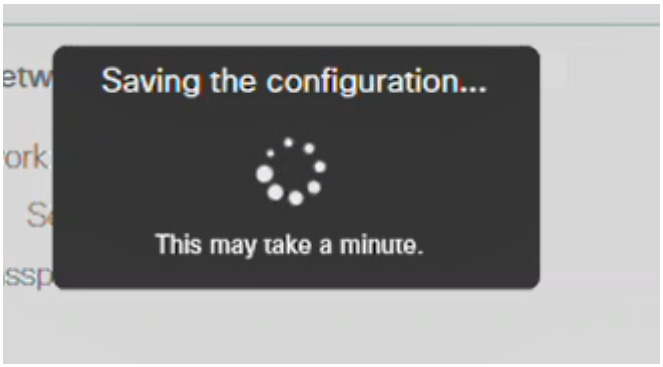



**Schritt 10**

Klicken Sie auf **OK**, um die Einstellungen zu übernehmen.




Während der Speicherung der Konfigurationen und dem Neustart des Systems wird der folgende Bildschirm angezeigt. Dies kann 10 Minuten dauern.

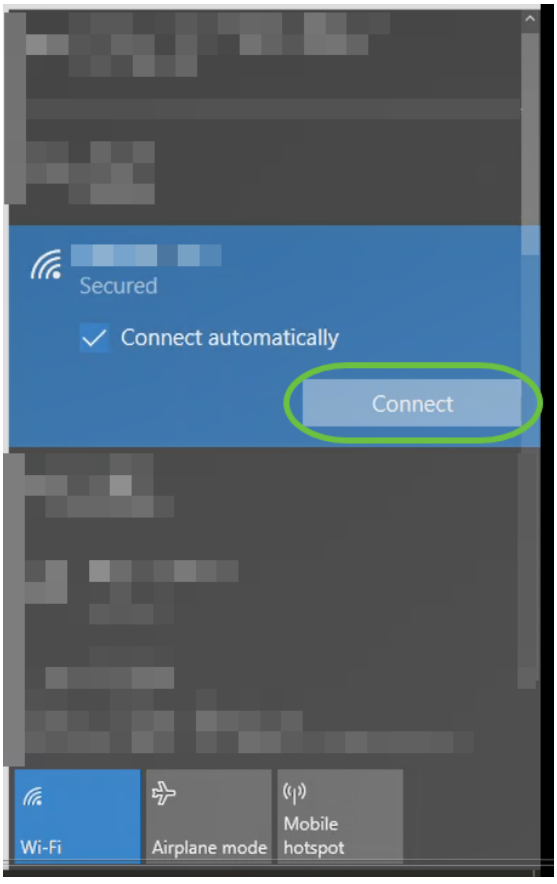



Während des Neustarts durchläuft die LED im Access Point mehrere Farbmuster. Wenn die LED grün blinkt, fahren Sie mit dem nächsten Schritt fort. Wenn die LED das rote Blinkmuster nicht überschreitet, weist dies darauf hin, dass kein DHCP-Server in Ihrem Netzwerk vorhanden ist. Stellen Sie sicher, dass der AP mit einem Switch oder Router mit einem DHCP-Server verbunden ist.

### Schritt 11

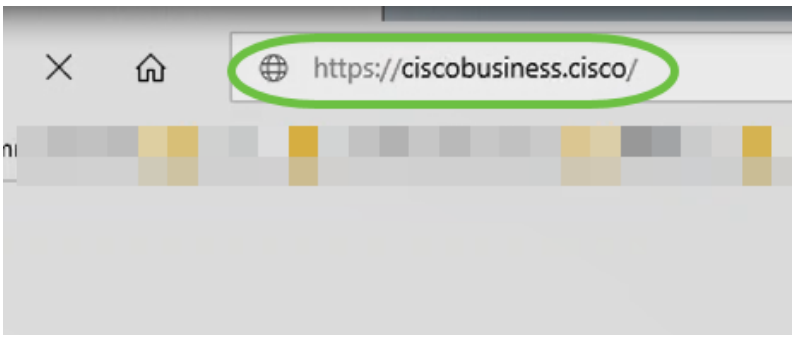
Gehen Sie zu den Wireless-Optionen auf Ihrem PC, und wählen Sie das Netzwerk aus, das Sie konfiguriert haben. Klicken Sie auf **Verbinden**.

Die *CiscoBusiness-Setup*-SSID wird nach dem Neustart ausgeblendet.




### Schritt 12

Öffnen Sie einen Webbrowser, und geben Sie *https:///[IP-Adresse des CBW AP]* ein. Alternativ können Sie *https://ciscobusiness.cisco* in die Adressleiste eingeben und die Eingabetaste betätigen.



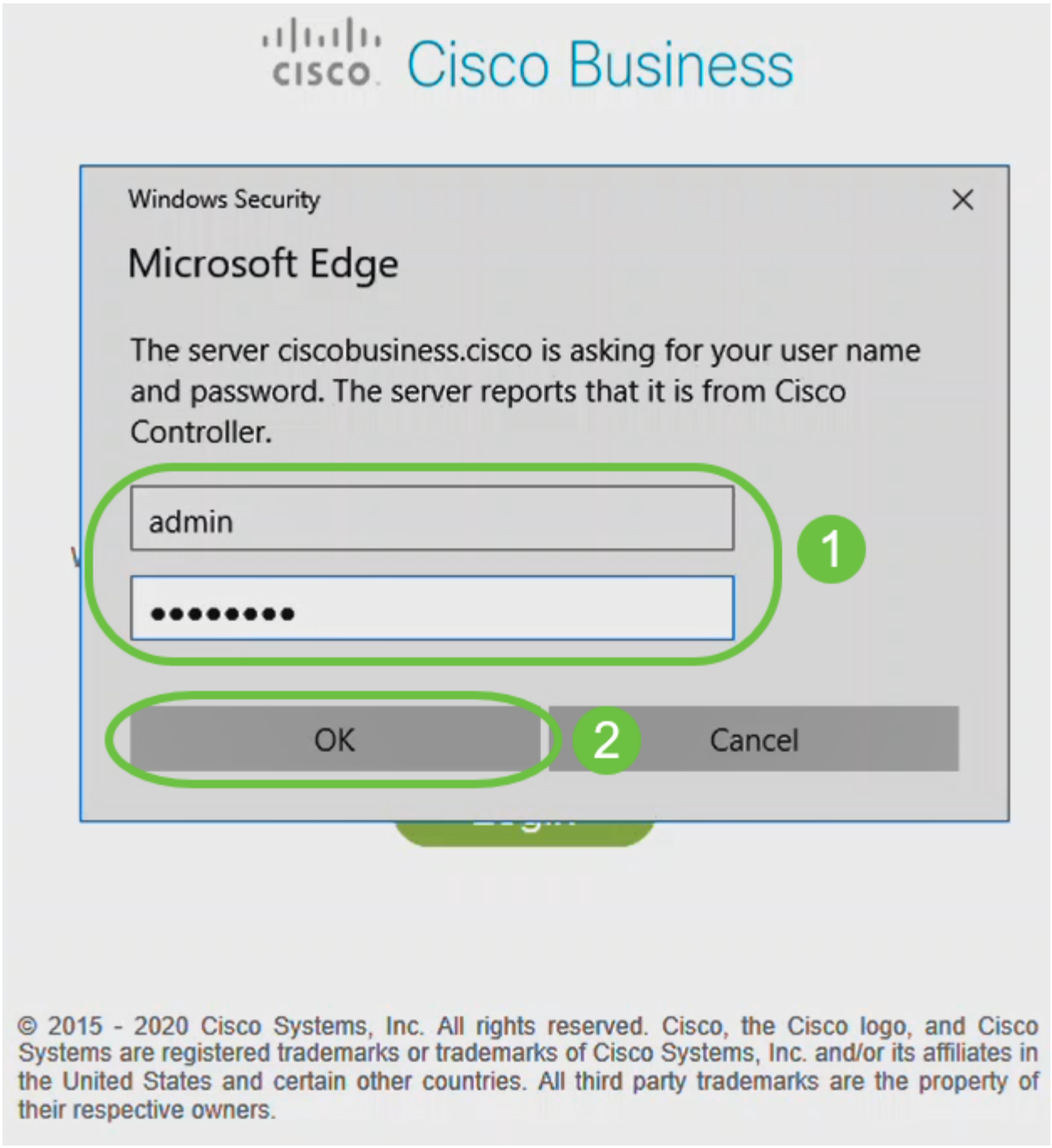

Stellen Sie sicher, dass Sie in diesem Schritt *https* und nicht *http* eingeben.

**Schritt 13**

Klicken Sie auf **Anmelden**.


**Schritt 14**

Melden Sie sich mit den konfigurierten Anmeldeinformationen an. Klicken Sie auf **OK**.




**Schritt 15**

Sie können auf die Webbenutzeroberflächenseite des Access Points zugreifen.

# Tipps zur Wireless-Fehlerbehebung

Wenn Sie Probleme haben, lesen Sie die folgenden Tipps:

- Stellen Sie sicher, dass der richtige Service Set Identifier (SSID) ausgewählt ist. Dies ist der Name, den Sie für das Wireless-Netzwerk erstellt haben.
- Trennen Sie alle VPNs für die mobile App oder einen Laptop. Möglicherweise sind Sie sogar mit einem VPN verbunden, das Ihr Mobilnetzanbieter verwendet, das Sie vielleicht noch nicht einmal kennen. Ein Android-Telefon (Pixel 3) mit Google Fi als Service Provider verfügt beispielsweise über ein integriertes VPN, das eine automatische, Benachrichtigungsverbindung herstellt. Diese muss deaktiviert werden, um den primären Access Point zu finden.
- Melden Sie sich mit https://<IP-Adresse des primären Access Points> beim primären Access Point an.
- Stellen Sie nach der Ersteinrichtung sicher, dass https:// is unabhängig davon, ob Sie sich bei *ciscobusiness.cisco* anmelden oder die IP-Adresse in Ihren Webbrowser eingeben. Abhängig von Ihren Einstellungen wird Ihr Computer möglicherweise automatisch mit http:// since ausgefüllt. Dies ist das, was Sie bei der ersten Anmeldung verwendet haben.
- Um bei Problemen mit dem Zugriff auf die Webbenutzeroberfläche oder bei Browserproblemen während der Verwendung des Access Points zu helfen, klicken Sie im Webbrowser (in diesem Fall Firefox) auf das Menü Öffnen, gehen Sie zu Hilfe > Informationen zur Fehlerbehebung, und klicken Sie auf Firefox aktualisieren.

# Konfigurieren der CBW142ACM-Mesh-Extender mithilfe der Webbenutzeroberfläche

Sie befinden sich im Hauptbereich der Einrichtung dieses Netzwerks, Sie müssen nur Ihre Mesh-Extender hinzufügen!

### Schritt 1

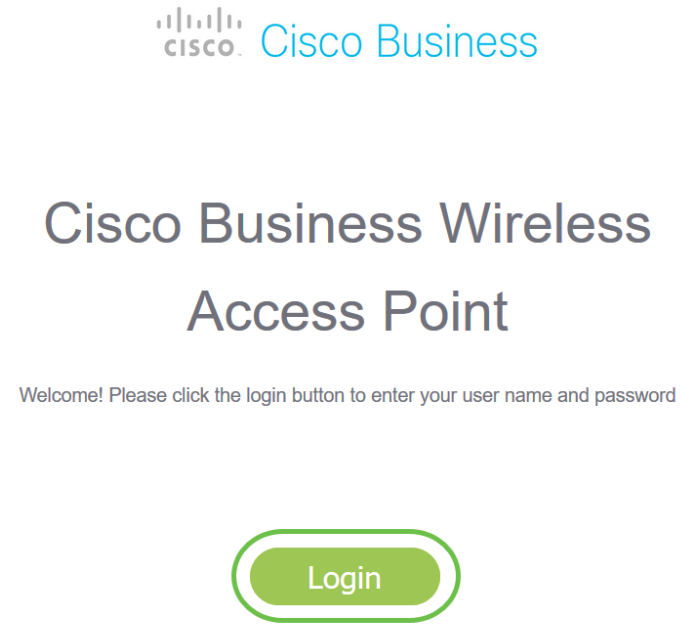
Schließen Sie die beiden Mesh-Extender an die Wand an den ausgewählten Standorten an. Notieren Sie die MAC-Adresse jedes Mesh-Extenders.

### Schritt 2

Warten Sie etwa 10 Minuten, bis der Mesh Extender hochgefahren ist.

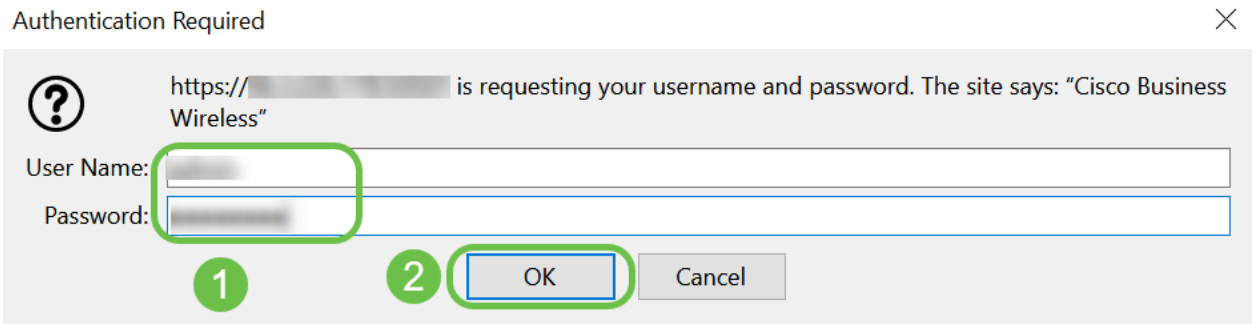
### Schritt 3

Geben Sie die IP-Adresse der primären Access Points (APs) im Webbrowser ein. Klicken Sie auf **Anmelden**, um auf den primären Access Point zuzugreifen.



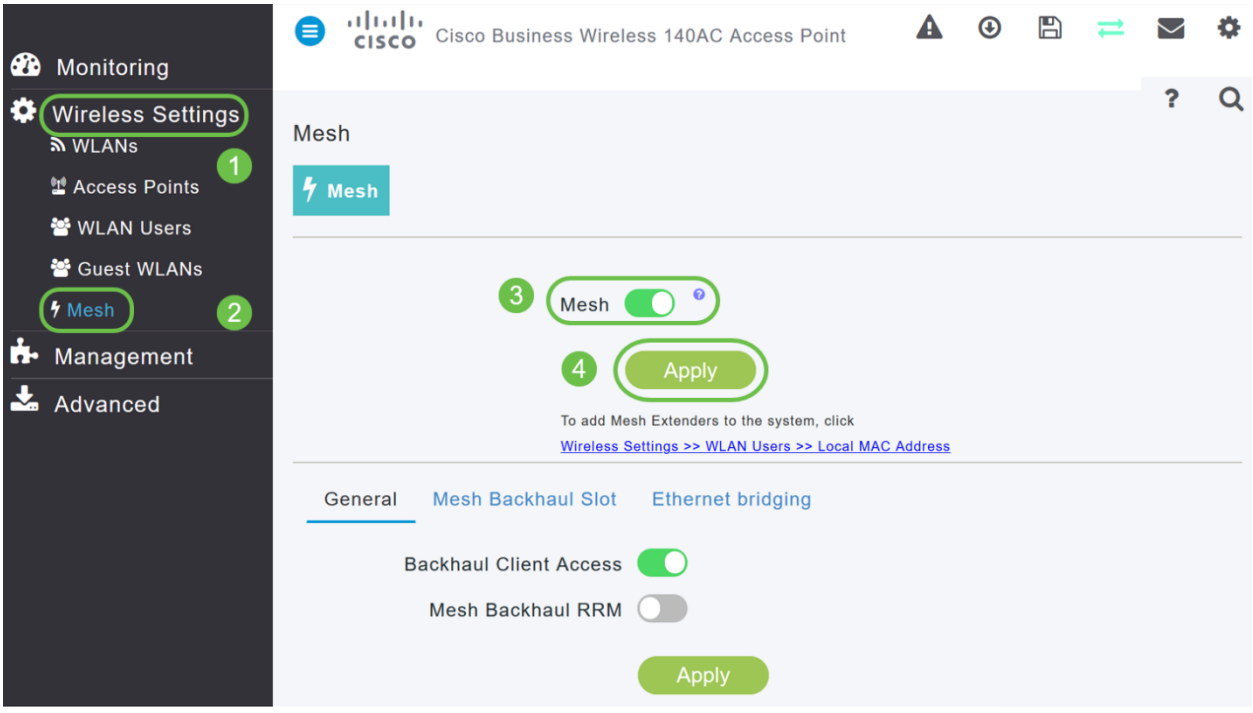

### Schritt 4

Geben Sie Ihren *Benutzernamen* und Ihre *Kennwort*-Anmeldeinformationen ein, um auf den primären Access Point zuzugreifen. Klicken Sie auf **OK**.




### Schritt 5

Navigieren Sie zu **Wireless Settings > Mesh (Wireless-Einstellungen > Mesh)**. Stellen Sie sicher, dass die *Mesh* aktiviert ist. Klicken Sie auf Apply (Anwenden).

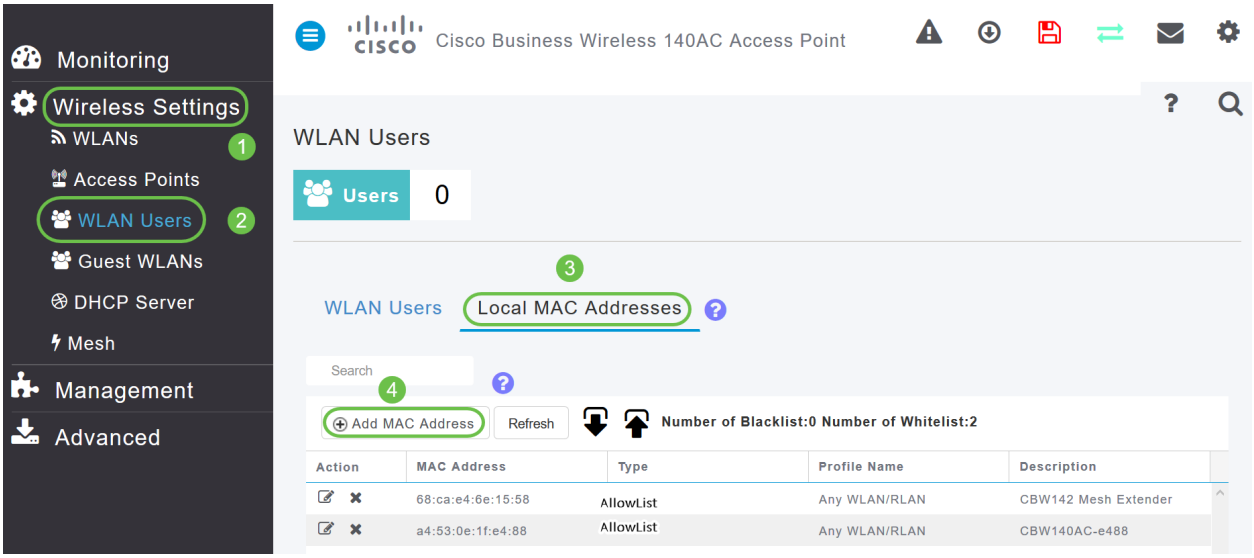


## Schritt 6

Wenn Mesh nicht bereits aktiviert war, muss der WAP möglicherweise einen Neustart durchführen. Ein Popup-Fenster erscheint, um einen Neustart durchzuführen. Bestätigen. Dies wird etwa 10 Minuten dauern. Während eines Neustarts blinkt die LED in mehreren Mustern grün, wechselt schnell durch grün, rot und orange, bevor sie wieder grün wird. Die LED-Farbintensität und der Farbton können von Gerät zu Einheit geringfügig variieren.

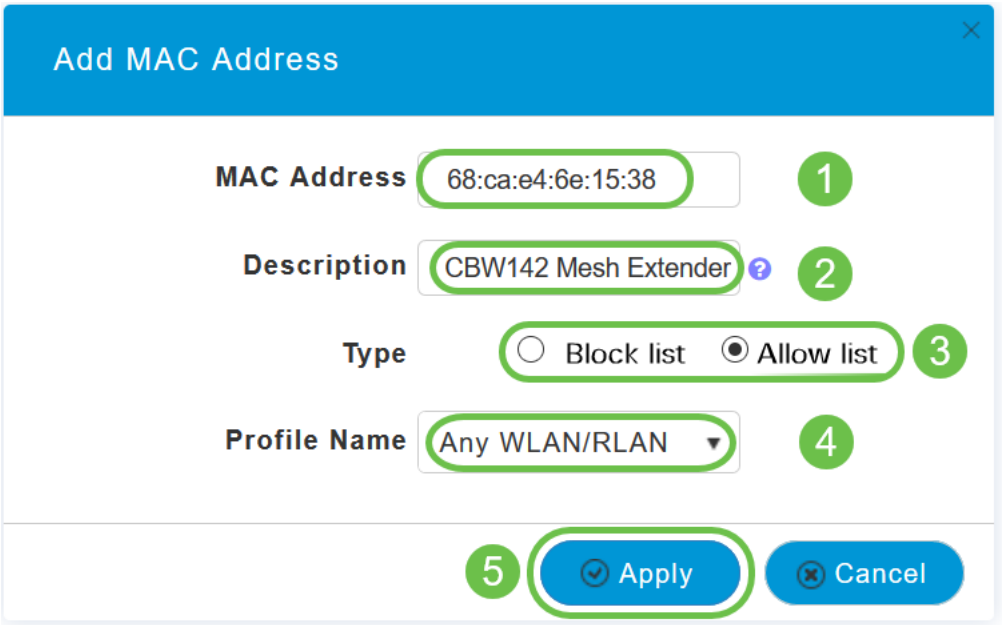
## Schritt 7

Navigieren Sie zu **Wireless Settings > WLAN Users > Local MAC Addresses**. Klicken Sie auf **MAC-Adresse hinzufügen**.




## Schritt 8

Geben Sie die MAC-Adresse und die Beschreibung des Mesh Extender ein. Wählen Sie den *Typ* als Zulassungsliste aus. Wählen Sie den *Profilnamen* aus dem Dropdown-Menü aus. Klicken Sie auf Apply (Anwenden).




**Schritt 9**

Speichern Sie alle Konfigurationen, indem Sie das **Speichersymbol** oben rechts im Bildschirm drücken.

Wiederholen Sie diese Schritte für jeden Mesh-Extender.

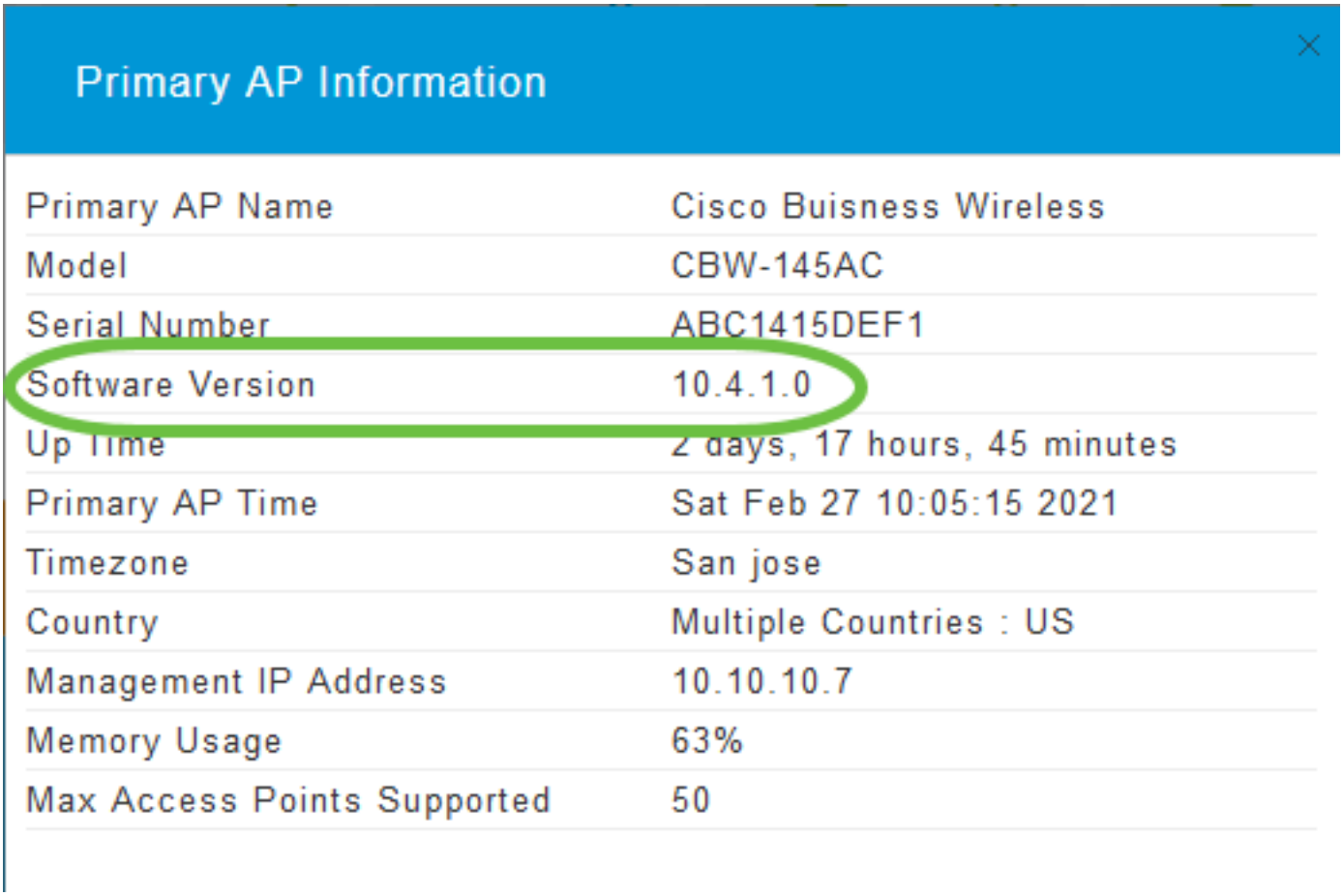
## Überprüfen und Aktualisieren der Software mithilfe der Webbenutzeroberfläche

Überspringen Sie diesen wichtigen Schritt nicht! Es gibt einige Möglichkeiten, Software zu aktualisieren, aber die unten aufgeführten Schritte werden als die einfachste Ausführung empfohlen, wenn Sie die Webbenutzeroberfläche verwenden.

So zeigen Sie die aktuelle Softwareversion des primären Access Points an und aktualisieren sie.

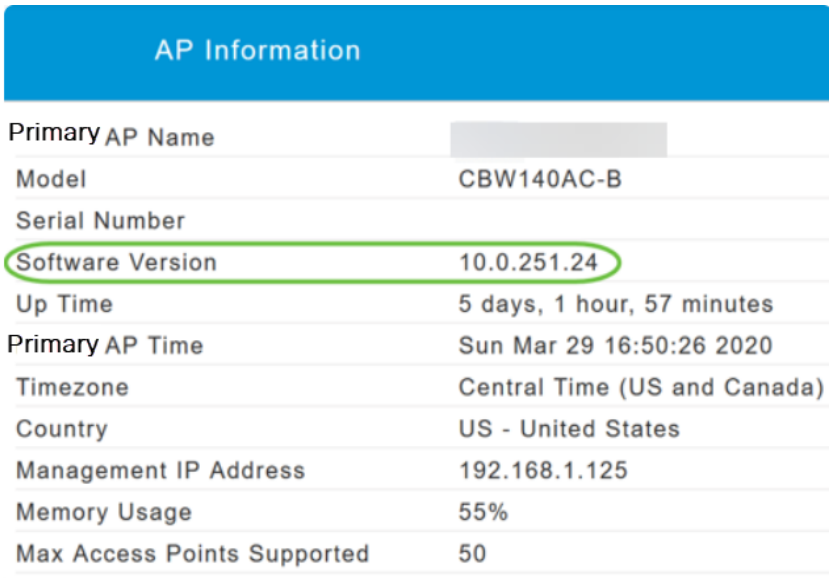
**Schritt 1**

Klicken Sie auf das **Zahnrad-Symbol** oben rechts in der Webschnittstelle, und klicken Sie dann auf **Primäre AP-Informationen**.




**Schritt 2**

Vergleichen Sie die aktuelle Version mit der neuesten Softwareversion. Schließen Sie das Fenster, sobald Sie wissen, ob Sie die Software aktualisieren müssen.



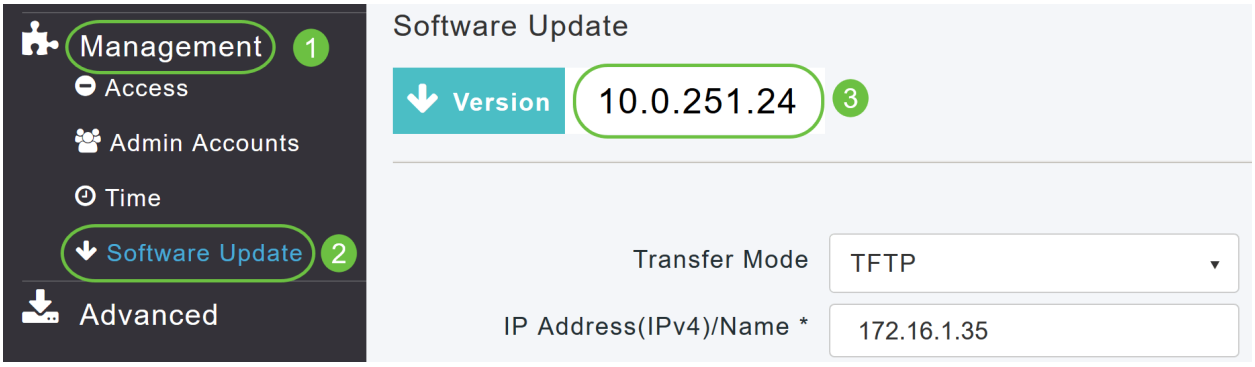

Wenn Sie die neueste Version der Software ausführen, können Sie zum Abschnitt Create WLANs (WLANs erstellen) springen.

**Schritt 3**

Wählen Sie **Management > Software Update** aus dem Menü aus.

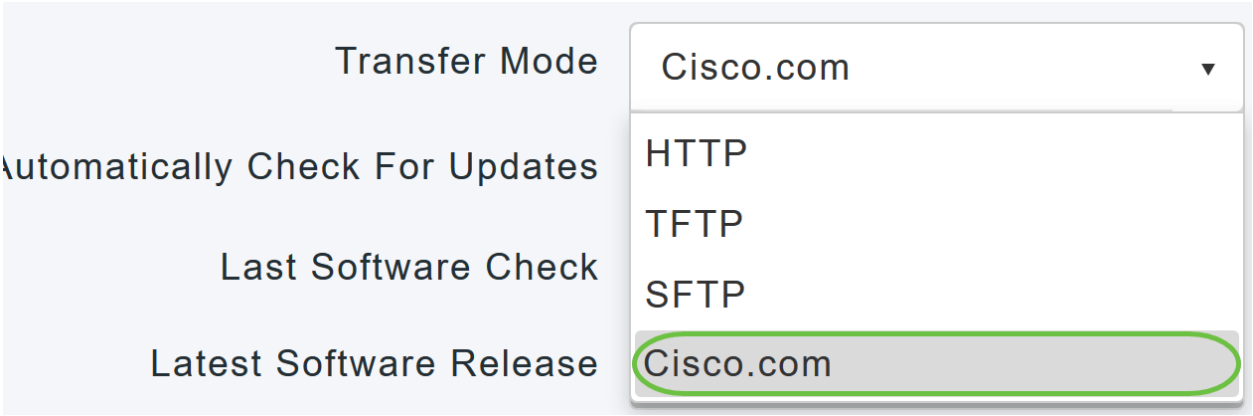
Das Fenster *Software Update* wird mit der aktuellen Softwareversionsnummer oben

angezeigt.



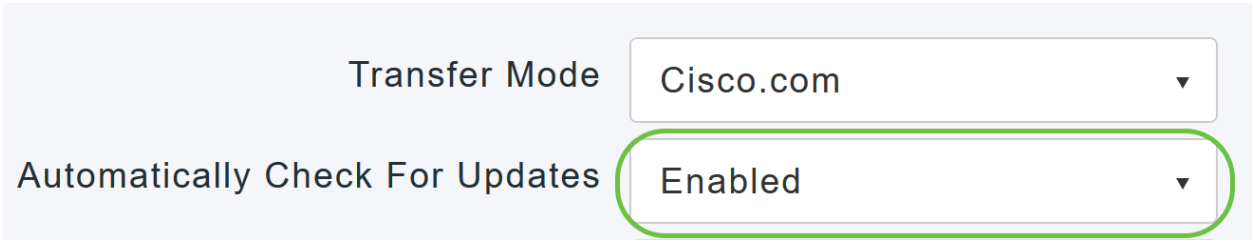

Sie können die CBW AP-Software aktualisieren, und die aktuellen Konfigurationen auf dem primären Access Point werden nicht gelöscht.

Wählen Sie in der Dropdown-Liste *Transfer Mode* (Übertragungsmodus) die Option **Cisco.com aus**.



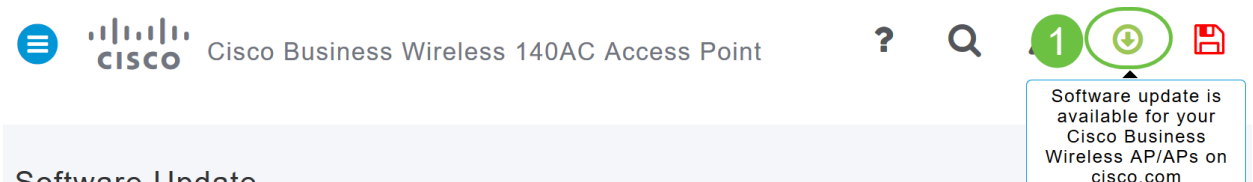

**Schritt 4**

Um den primären Access Point so einzustellen, dass er automatisch nach Software-Updates sucht, wählen Sie **Enabled (Aktiviert)** in der Dropdown-Liste *Automatisch nach Updates suchen aus*. Dies ist standardmäßig aktiviert.



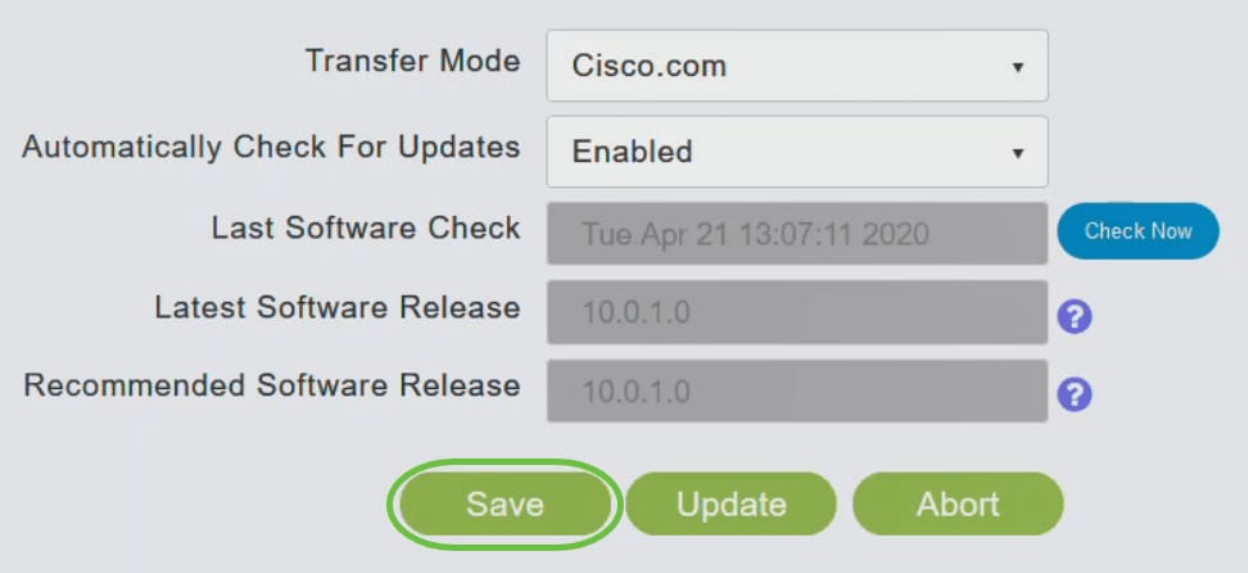

Wenn eine Softwareprüfung durchgeführt wird und eine neuere Aktualisierung der neuesten oder empfohlenen Software auf Cisco.com verfügbar ist, dann:

- Das **Warnsymbol für Software-Updates** oben rechts auf der Webbenutzeroberfläche ist grün (oder grau). Durch Klicken auf das Symbol gelangen Sie zur Seite Software Update (Software-Aktualisierung).
- Die Schaltfläche Aktualisieren am unteren Rand der Seite *Software Update* ist aktiviert.

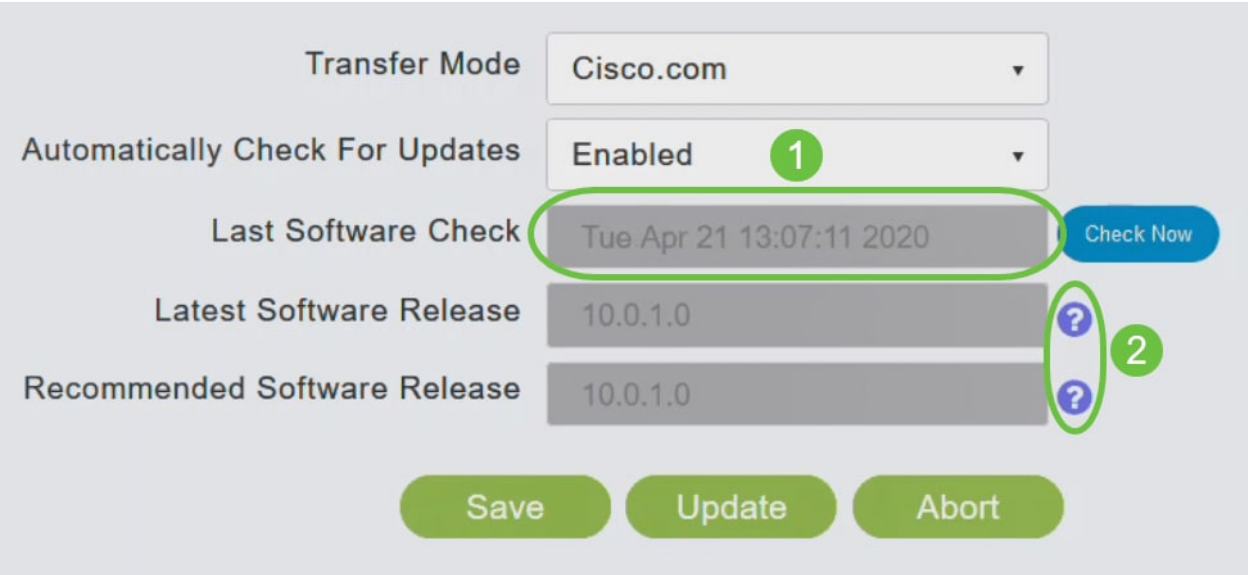


## Schritt 5

Klicken Sie auf **Speichern**. Dadurch werden die Einträge oder Änderungen gespeichert, die Sie sowohl im *Transfermodus* als auch *automatisch nach Updates suchen*.

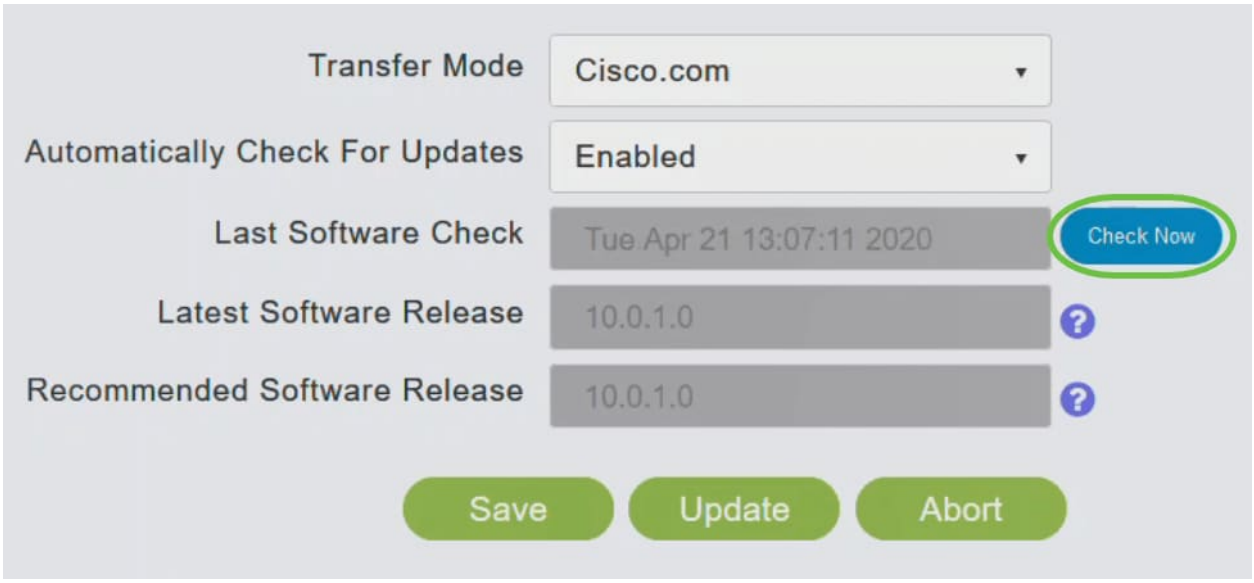



Im Feld *Letzte Softwareprüfung* wird der Zeitstempel der letzten automatischen oder manuellen Softwareprüfung angezeigt. Sie können die Notizen der angezeigten Versionen anzeigen, indem Sie auf das **Fragezeichen-Symbol** neben dem Symbol klicken.



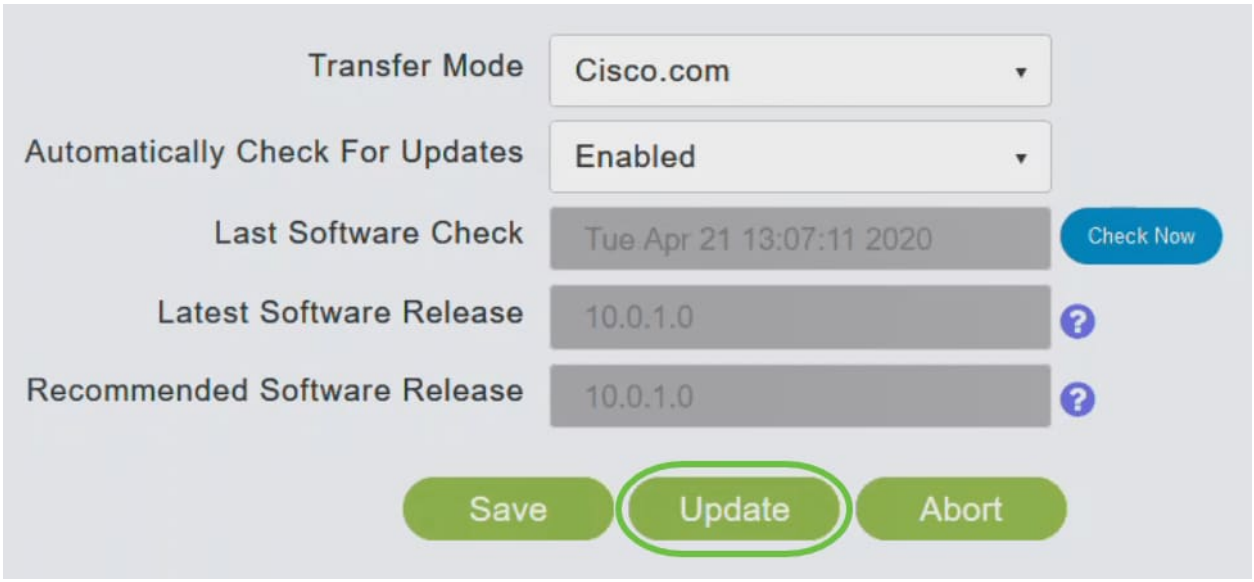

## Schritt 6

Sie können eine Softwareüberprüfung jederzeit manuell ausführen, indem Sie auf *Jetzt prüfen* klicken.




**Schritt 7**

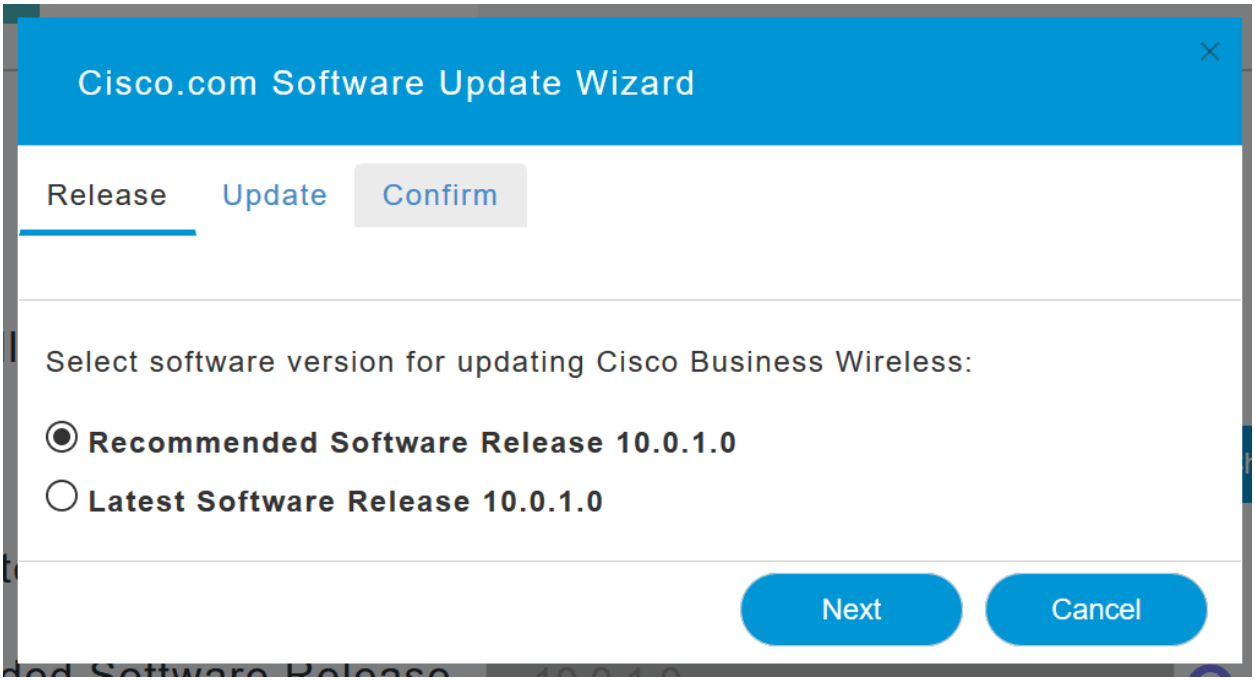
Um mit der Softwareaktualisierung fortzufahren, klicken Sie auf **Aktualisieren**.




Der *Software Update Wizard* wird angezeigt. Der Assistent führt Sie durch die folgenden drei Registerkarten in der Abfolge:

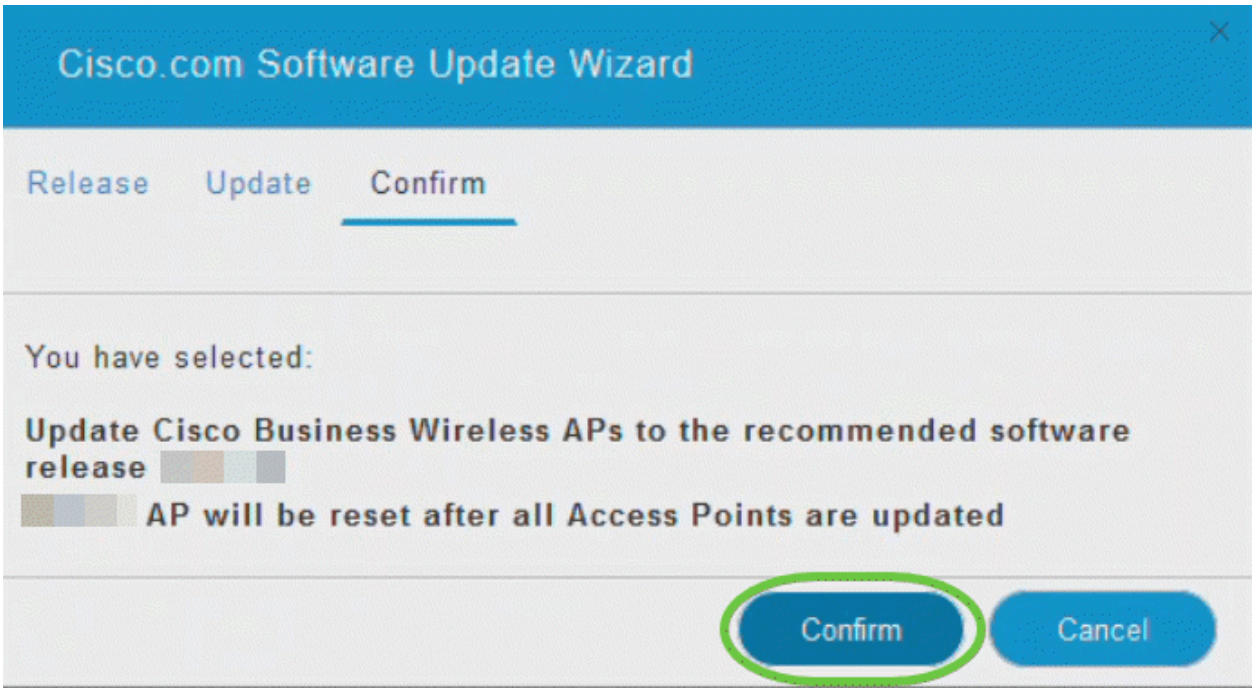
- Registerkarte "Version": Geben Sie an, ob Sie auf die empfohlene Softwareversion oder die neueste Softwareversion aktualisieren möchten.
- Registerkarte "Aktualisieren": Geben Sie an, wann die Access Points zurückgesetzt werden sollen. Sie können entweder sofort entscheiden, ob Sie den Vorgang abschließen möchten oder ihn für einen späteren Zeitpunkt planen. Aktivieren Sie das Kontrollkästchen Auto Restart (Autom. Neustart), um den primären Access Point so einzustellen, dass er automatisch neu gestartet wird, nachdem das Image-Vordownload abgeschlossen ist.
- Registerkarte bestätigen: Bestätigen Sie Ihre Auswahl.

Befolgen Sie die Anweisungen im Assistenten. Sie können jederzeit zu einer beliebigen Registerkarte zurückkehren, bevor Sie auf *Bestätigen* klicken.




**Schritt 8**

Klicken Sie auf **Bestätigen**.

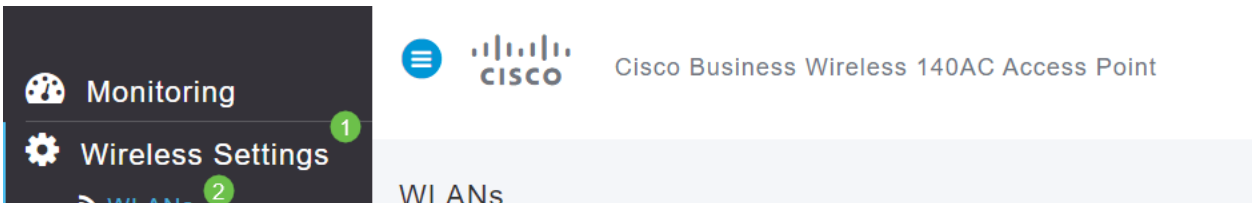



## Erstellen von WLANs auf der Webbenutzeroberfläche

In diesem Abschnitt können Sie Wireless Local Area Networks (WLANs) erstellen.

**Schritt 1**

Um ein WLAN zu erstellen, navigieren Sie zu **Wireless Settings > WLANs**. Wählen Sie anschließend **Neues WLAN/RLAN hinzufügen aus**.



## Schritt 2

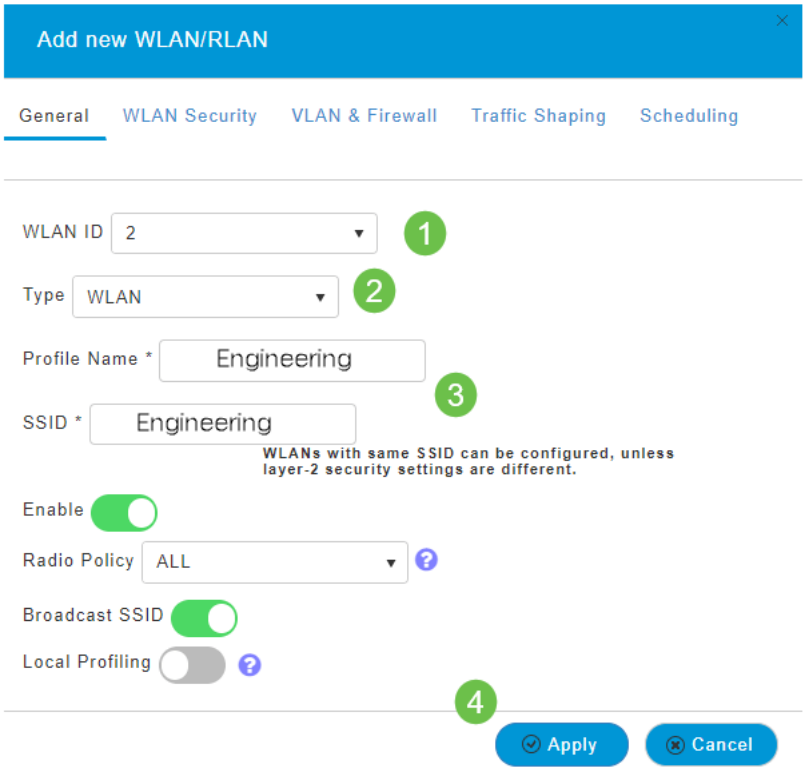
Geben Sie auf der Registerkarte *Allgemein* die folgenden Informationen ein:

- WLAN-ID - Wählen Sie eine Nummer für das WLAN aus.
- Typ - **WLAN** auswählen
- Profilname: Wenn Sie einen Namen eingeben, wird die SSID automatisch mit demselben Namen angezeigt. Der Name muss eindeutig sein und darf 31 Zeichen nicht überschreiten.

Die folgenden Felder wurden in diesem Beispiel als Standardfelder beibehalten. Für den Fall, dass Sie sie anders konfigurieren möchten, werden jedoch Erklärungen aufgelistet.

- SSID - Der Profilname fungiert auch als SSID. Sie können das ändern, wenn Sie möchten. Der Name muss eindeutig sein und darf 31 Zeichen nicht überschreiten.
- Aktivieren: Diese Option sollte aktiviert bleiben, damit das WLAN funktioniert.
- Funkrichtlinie - In der Regel sollte dies als **All** (**Alle**) beibehalten werden, damit 2,4-GHz- und 5-GHz-Clients auf das Netzwerk zugreifen können.
- Broadcast SSID (SSID senden): In der Regel sollte die SSID erkannt werden, damit Sie diese Option als aktiviert lassen möchten.
- Lokale Profilerstellung: Sie möchten diese Option nur aktivieren, um das Betriebssystem anzuzeigen, das auf dem Client ausgeführt wird, oder um den Benutzernamen anzuzeigen.

Klicken Sie auf Apply (Anwenden).




## Schritt 3

Sie gelangen zur Registerkarte *WLAN-Sicherheit*.

In diesem Beispiel wurden die folgenden Optionen als Standard beibehalten:

- Gastnetzwerk, Captive Network Assistant und MAC Filtering wurden deaktiviert. Details zum Einrichten eines Gastnetzwerks finden Sie im nächsten Abschnitt.
- WPA2 Personal - Wi-Fi Protected Access 2 mit Pre-Shared Key (PSK) Passphrase-Format - ASCII. Diese Option steht für Wi-Fi Protected Access 2 mit Pre-Shared Key (PSK).

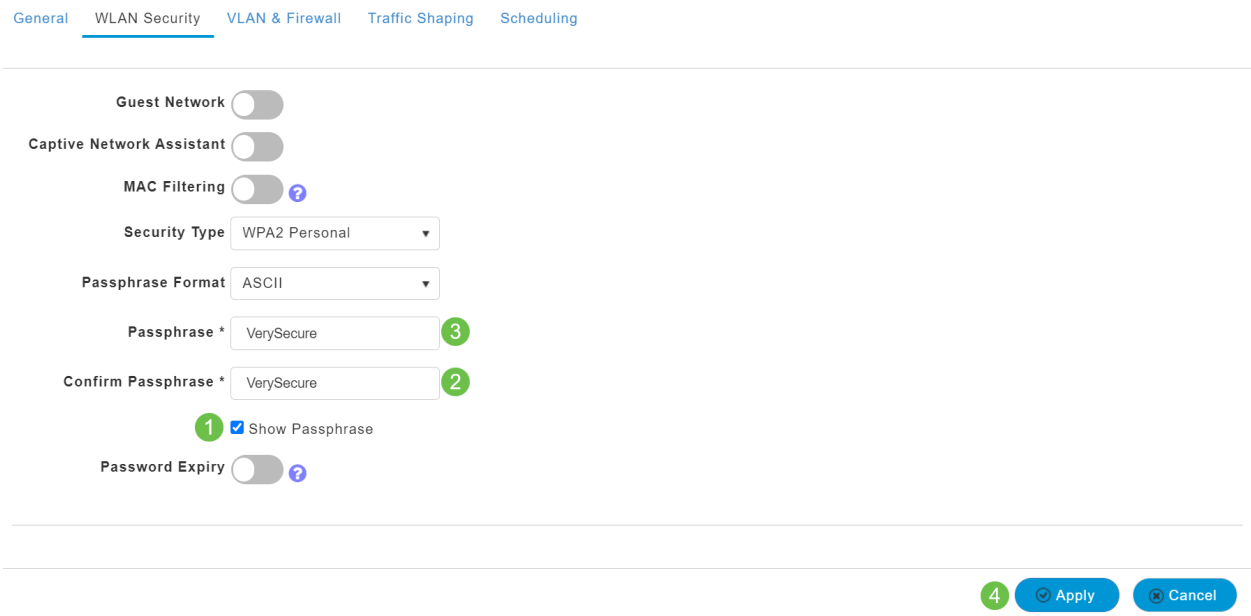
WPA2 Personal ist eine Methode zur Sicherung Ihres Netzwerks mithilfe einer PSK-Authentifizierung. Der PSK wird sowohl auf dem primären Access Point, unter der WLAN-Sicherheitsrichtlinie als auch auf dem Client separat konfiguriert. WPA2 Personal verlässt sich nicht auf einen Authentifizierungsserver in Ihrem Netzwerk.

- Passphrasenformat: **ASCII wird als Standard beibehalten.**

In diesem Szenario wurden die folgenden Felder eingegeben:

- Passphrase anzeigen: Aktivieren Sie das Kontrollkästchen, um die von Ihnen eingegebene Passphrase anzuzeigen.
- Passphrase: Geben Sie einen Namen für die Passphrase (Kennwort) ein.
- Passphrase bestätigen: Geben Sie das Kennwort erneut zur Bestätigung ein.

Klicken Sie auf Apply (Anwenden). Dadurch wird das neue WLAN automatisch aktiviert.

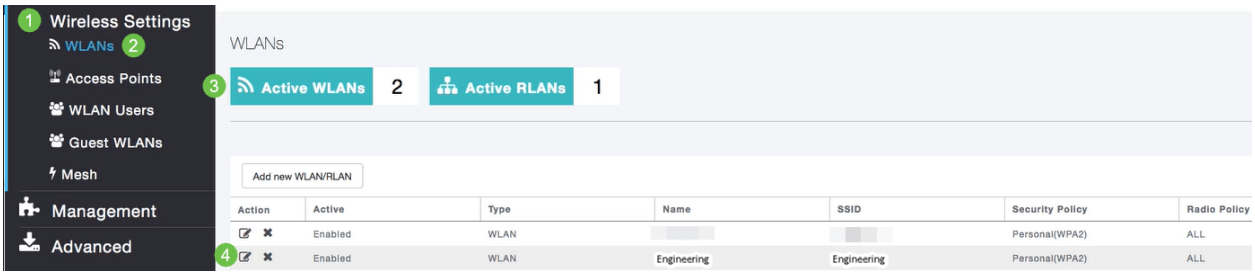



## Schritt 4

Speichern Sie Ihre Konfigurationen, indem Sie im rechten oberen Bereich des Bildschirms der Webbenutzeroberfläche auf das **Speichersymbol** klicken.

Schritt 5

Um das von Ihnen erstellte WLAN anzuzeigen, wählen Sie **Wireless Settings > WLANs (Wireless-Einstellungen > WLANs)**. Die Anzahl der aktiven WLANs wird auf 2 erhöht, und das neue WLAN wird angezeigt.




Wiederholen Sie diese Schritte für andere WLANs, die Sie erstellen möchten.

# Optionale Wireless-Konfigurationen

Sie haben nun alle Standardkonfigurationen eingestellt und können nun rollen. Sie haben einige Optionen. Sie können also zu einem der folgenden Abschnitte springen:

- Erstellen eines Gast-WLAN mithilfe der Webbenutzeroberfläche (optional)
- Erstellung von Anwendungsprofilen (optional)
- Client Profiling (optional)
- Ich kann das alles zusammenfassen und mein Netzwerk verwenden.

## Erstellen eines Gast-WLAN mithilfe der Webbenutzeroberfläche (optional)

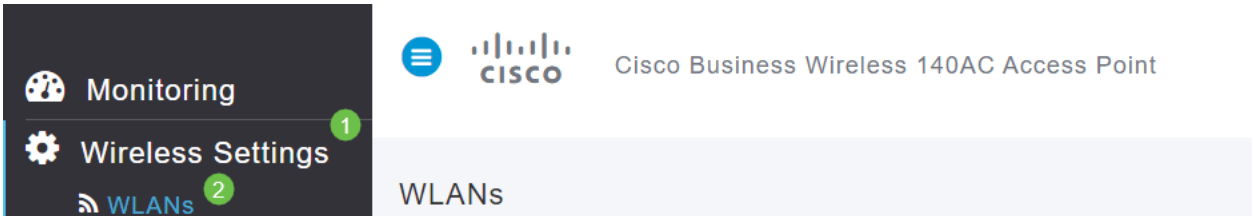
Ein Gast-WLAN bietet Gastzugriff auf Ihr Cisco Business Wireless-Netzwerk.

### Schritt 1

Melden Sie sich bei der Webbenutzeroberfläche des primären Access Points an. Öffnen Sie einen Webbrowser, und geben Sie www.https://ciscobusiness.cisco ein. Möglicherweise erhalten Sie eine Warnung, bevor Sie fortfahren. Geben Sie Ihre Anmeldeinformationen ein. Sie können auch darauf zugreifen, indem Sie die IP-Adresse des primären Access Points eingeben.

### Schritt 2

Um ein Wireless Local Area Network (WLAN) zu erstellen, navigieren Sie zu **Wireless Settings > WLANs**. Wählen Sie anschließend **Neues WLAN/RLAN hinzufügen aus**.



## Schritt 3

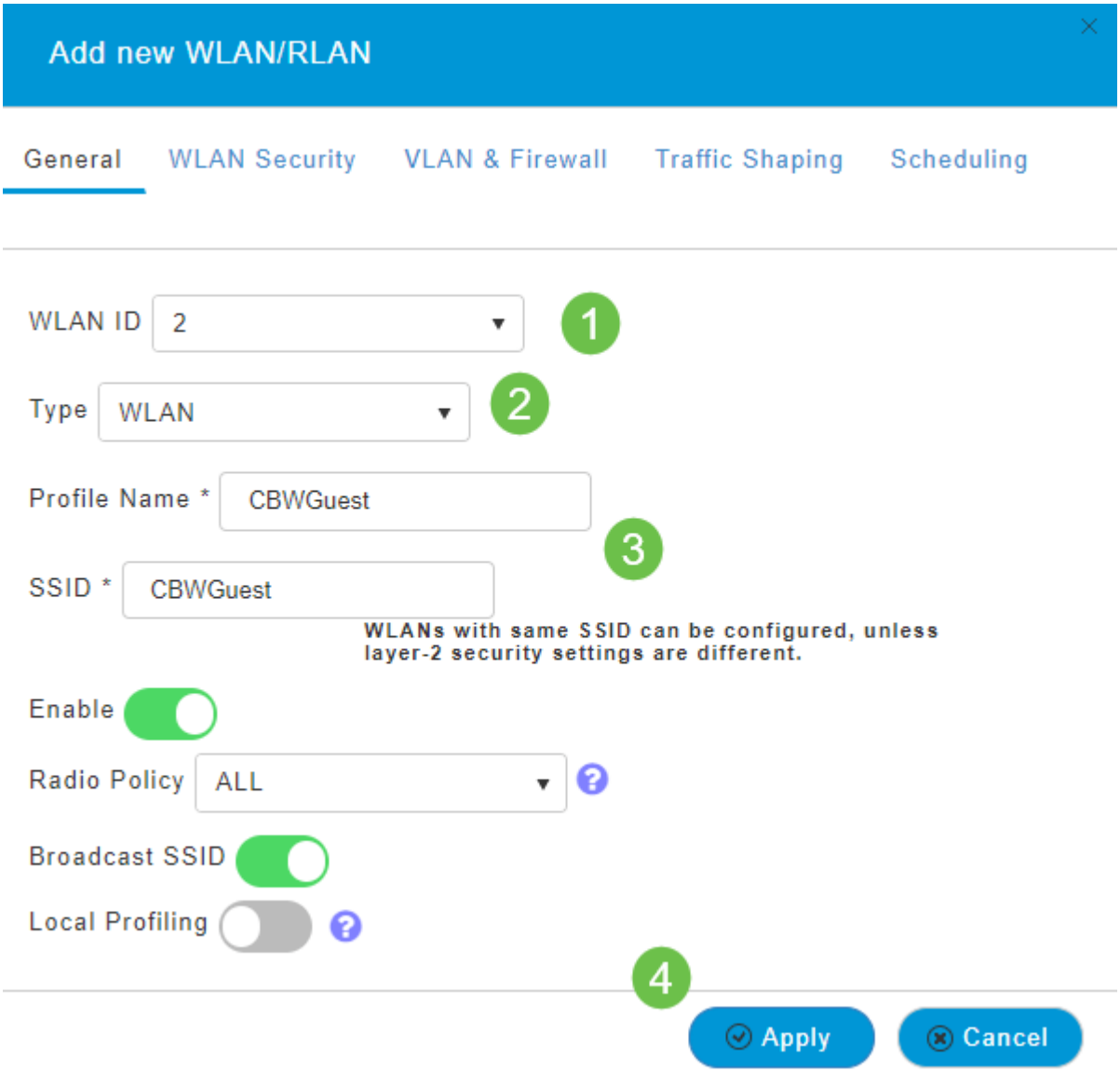
Geben Sie auf der Registerkarte *Allgemein* die folgenden Informationen ein:

*WLAN-ID* - Wählen Sie eine Nummer für das WLAN aus.
*Typ* - **WLAN** auswählen
*Profilname*: Wenn Sie einen Namen eingeben, wird die SSID automatisch mit demselben Namen angezeigt. Der Name muss eindeutig sein und darf 31 Zeichen nicht überschreiten.

Die folgenden Felder wurden in diesem Beispiel als Standardfelder beibehalten. Für den Fall, dass Sie sie anders konfigurieren möchten, werden jedoch Erklärungen aufgelistet.

*SSID*: Der Profilname fungiert auch als SSID. Sie können das ändern, wenn Sie möchten. Der Name muss eindeutig sein und darf 31 Zeichen nicht überschreiten.
*Aktivieren*: Diese Option sollte aktiviert bleiben, damit das WLAN funktioniert.
*Funkrichtlinie* - In der Regel sollte dies als **All** (**Alle**) angezeigt werden, damit 2,4-GHz- und 5-GHz-Clients auf das Netzwerk zugreifen können.
*Broadcast SSID*: In der Regel sollte die SSID erkannt werden, sodass Sie diese Option als aktiviert lassen möchten.
*Lokale Profilerstellung*: Sie möchten diese Option nur aktivieren, um das Betriebssystem anzuzeigen, das auf dem Client ausgeführt wird, oder um den Benutzernamen anzuzeigen.

Klicken Sie auf Apply (Anwenden).

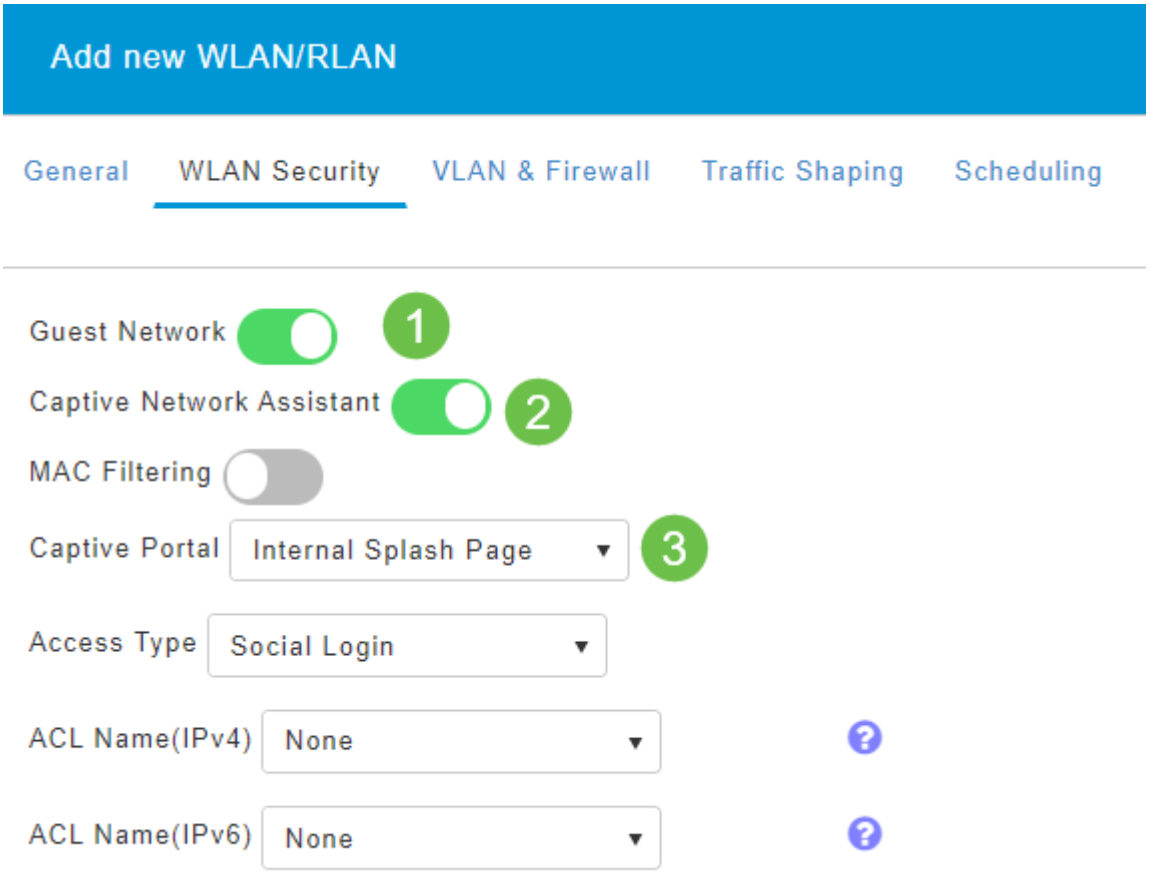



**Schritt 4**

Sie gelangen zur Registerkarte *WLAN-Sicherheit*. In diesem Beispiel wurden die folgenden Optionen ausgewählt.

- Gastnetzwerk - Aktivieren
- Captive Network Assistant: Wenn Sie Mac oder IOS verwenden, möchten Sie dies wahrscheinlich aktivieren. Diese Funktion erkennt das Vorhandensein eines Captive Portals, indem eine Webanfrage für die Verbindung mit einem Wireless-Netzwerk gesendet wird. Diese Anfrage wird an einen Uniform Resource Locator (URL) für iPhone-Modelle weitergeleitet. Wenn eine Antwort eingeht, wird davon ausgegangen, dass der Internetzugang verfügbar ist und keine weitere Interaktion erforderlich ist. Wenn keine Antwort eingeht, wird davon ausgegangen, dass der Internetzugriff vom Captive Portal blockiert wird, und der Captive Network Assistant (CNA) von Apple startet den Pseudo-Browser automatisch, um die Anmeldung des Portals in einem kontrollierten Fenster anzufordern. Beim Umleiten zu einem Captive Portal der Identity Services Engine (ISE) kann die CNA Pause machen. Der primäre Access Point verhindert, dass dieser Pseudo-Browser aufspringt.
- Captive Portal - Dieses Feld ist nur sichtbar, wenn die Option Guest Network (Gastnetzwerk) aktiviert ist. Mit diesem Parameter wird der Typ des Webportals festgelegt, der für Authentifizierungszwecke verwendet werden kann. Wählen Sie

Internal Splash Page (Interne Splash-Seite) aus, um die standardmäßige, auf dem Cisco Webportal basierende Authentifizierung zu verwenden. Wählen Sie External Splash Page (Externe Splash-Seite) aus, wenn Sie über eine Captive Portal-Authentifizierung mit einem Webserver außerhalb Ihres Netzwerks verfügen. Geben Sie außerdem die URL des Servers im Feld Site URL (URL-Adresse der Site) an.




In diesem Beispiel wird das Gast-WLAN mit einem aktivierten Zugriffstyp für Social Login erstellt. Sobald der Benutzer eine Verbindung zu diesem Gast-WLAN hergestellt hat, wird er auf die Cisco Standard-Anmeldeseite weitergeleitet, auf der er die Anmeldeschaltflächen für Google und Facebook finden kann. Der Benutzer kann sich über sein Google- oder Facebook-Konto anmelden, um Internetzugang zu erhalten.

## Schritt 5

Wählen Sie auf derselben Registerkarte im Dropdown-Menü einen *Zugriffstyp* aus. In diesem Beispiel wurde *Social Login* ausgewählt. Mit dieser Option können Gäste ihre Google- oder Facebook-Anmeldeinformationen für die Authentifizierung und den Zugriff auf das Netzwerk verwenden.

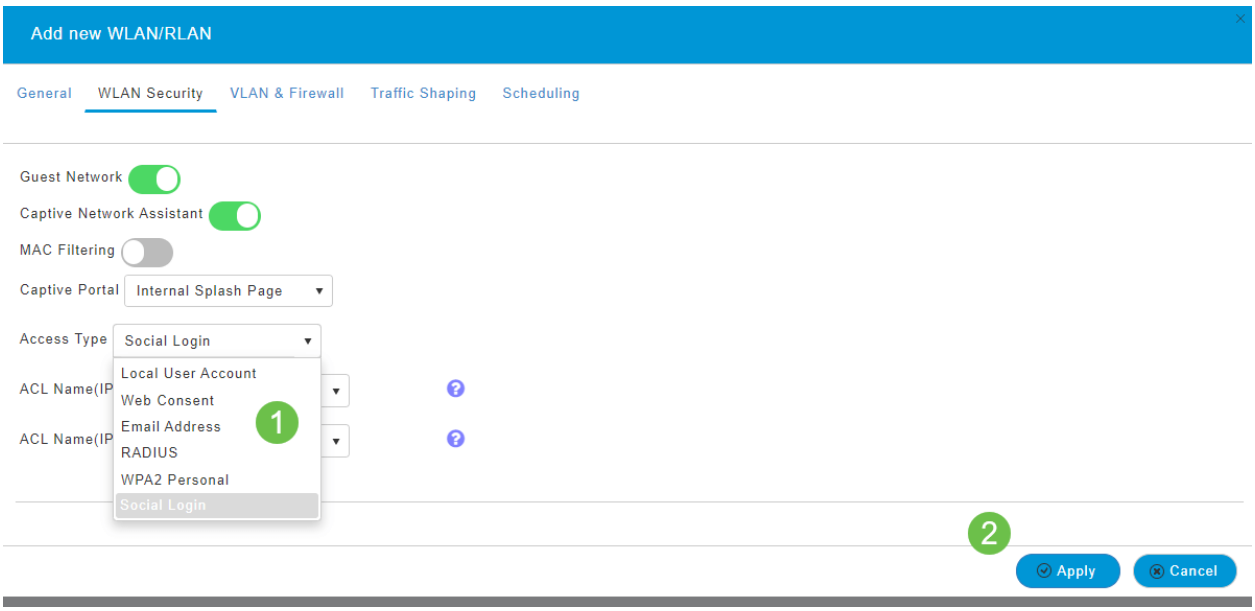
Weitere Optionen für den *Zugriffstyp* sind:

*Lokales Benutzerkonto* - Die Standardoption. Wählen Sie diese Option aus, um Gäste mit dem Benutzernamen und dem Kennwort zu authentifizieren, die Sie für Gastbenutzer dieses WLAN unter **Wireless Settings > WLAN Users** angeben können. Dies ist ein Beispiel für die interne Splash-Standardseite.

Sie können dies anpassen, indem Sie zu **Wireless Settings > Guest WLANs** navigieren. Von hier aus können Sie eine *Page Überschrift* und *Page Message* eingeben. Klicken Sie auf Apply (Anwenden). Klicken Sie auf **Vorschau**.

*Web Consent* - Ermöglicht Gästen den Zugriff auf das WLAN, sobald sie die angezeigten Geschäftsbedingungen akzeptieren. Gastbenutzer können auf das WLAN zugreifen, ohne einen Benutzernamen und ein Kennwort einzugeben.
*E-Mail-Adresse* - Gastbenutzer müssen ihre E-Mail-Adresse eingeben, um auf das Netzwerk zugreifen zu können.
*RADIUS* - Verwenden Sie diesen Parameter zusammen mit einem externen Authentifizierungsserver.
*WPA2 Personal* - Wi-Fi Protected Access 2 mit Pre-Shared Key (PSK)

Klicken Sie auf Apply (Anwenden).




**Schritt 6**

Speichern Sie Ihre Konfigurationen, indem Sie im rechten oberen Bereich des Bildschirms der Webbenutzeroberfläche auf das **Speichersymbol** klicken.

Sie haben jetzt ein Gastnetzwerk erstellt, das im CBW-Netzwerk verfügbar ist. Ihre Gäste werden den Komfort schätzen.

## Erstellen von Anwendungsprofilen mithilfe der Webbenutzeroberfläche (optional)

Die Profilerstellung ist eine Teilmenge von Funktionen, die die Umsetzung von Unternehmensrichtlinien ermöglichen. Sie ermöglicht die Anpassung und Priorisierung von Datenverkehrstypen. Wie Regeln entscheiden, wie der Datenverkehr klassifiziert oder verworfen wird. Das Cisco Business Mesh Wireless-System bietet Funktionen zur Erstellung von Client- und Anwendungsprofilen. Der Zugriff auf ein Netzwerk als Benutzer beginnt mit vielen Datenaustauschvorgängen, darunter auch der Art des Datenverkehrs. Die Richtlinie unterbricht den Datenverkehrsfluss, um den Pfad zu

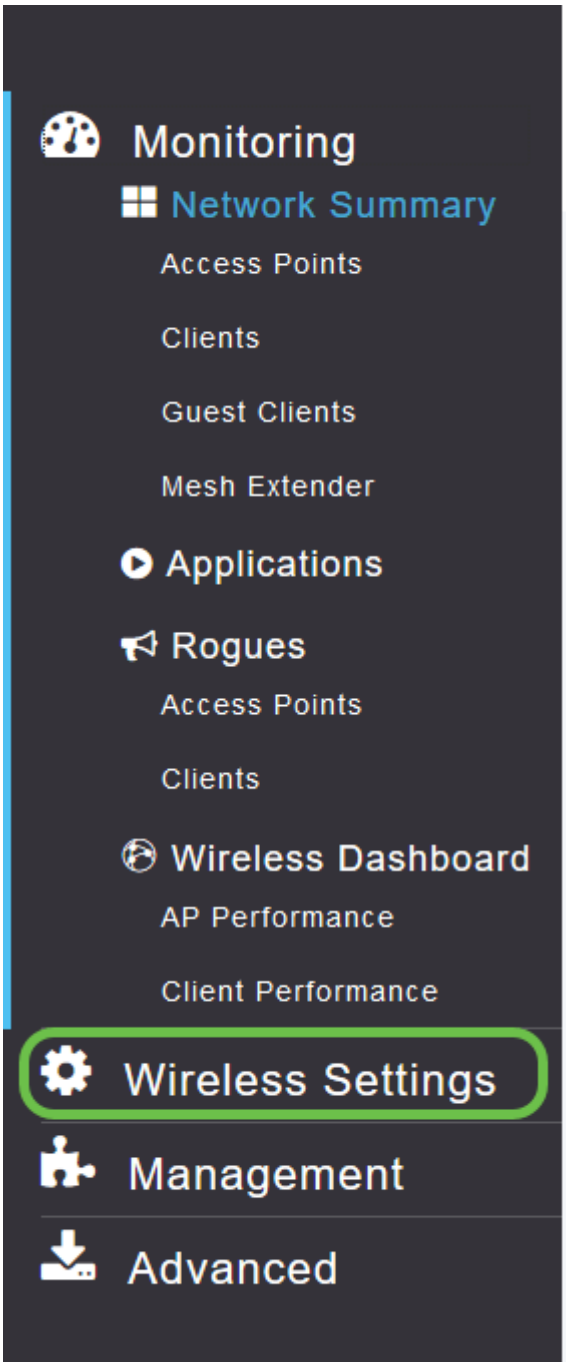
leiten, ähnlich wie ein Flussdiagramm. Weitere Richtlinienfunktionen sind Gastzugriff, Zugriffskontrolllisten und QoS.

### Schritt 1

Navigieren Sie zum Menü auf der linken Bildschirmseite, wenn Sie die linke Menüleiste nicht sehen.

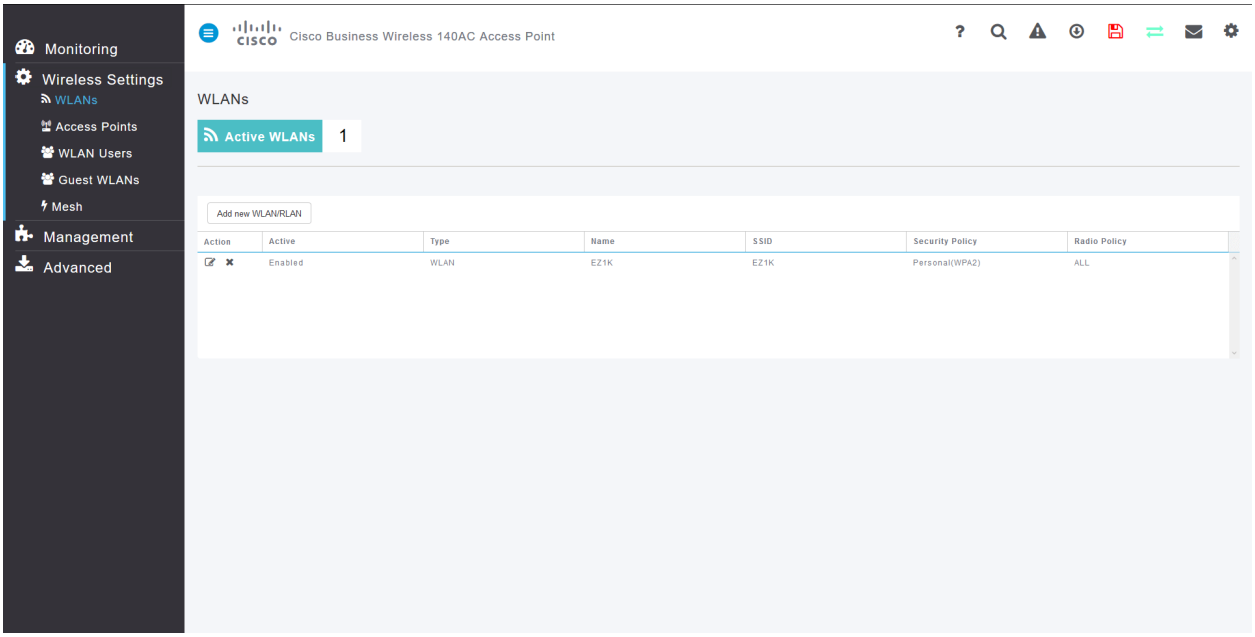
### Schritt 2

Das Menü Überwachung wird standardmäßig geladen, wenn Sie sich beim Gerät anmelden. Sie müssen auf **Wireless Settings (Wireless-Einstellungen)** klicken.



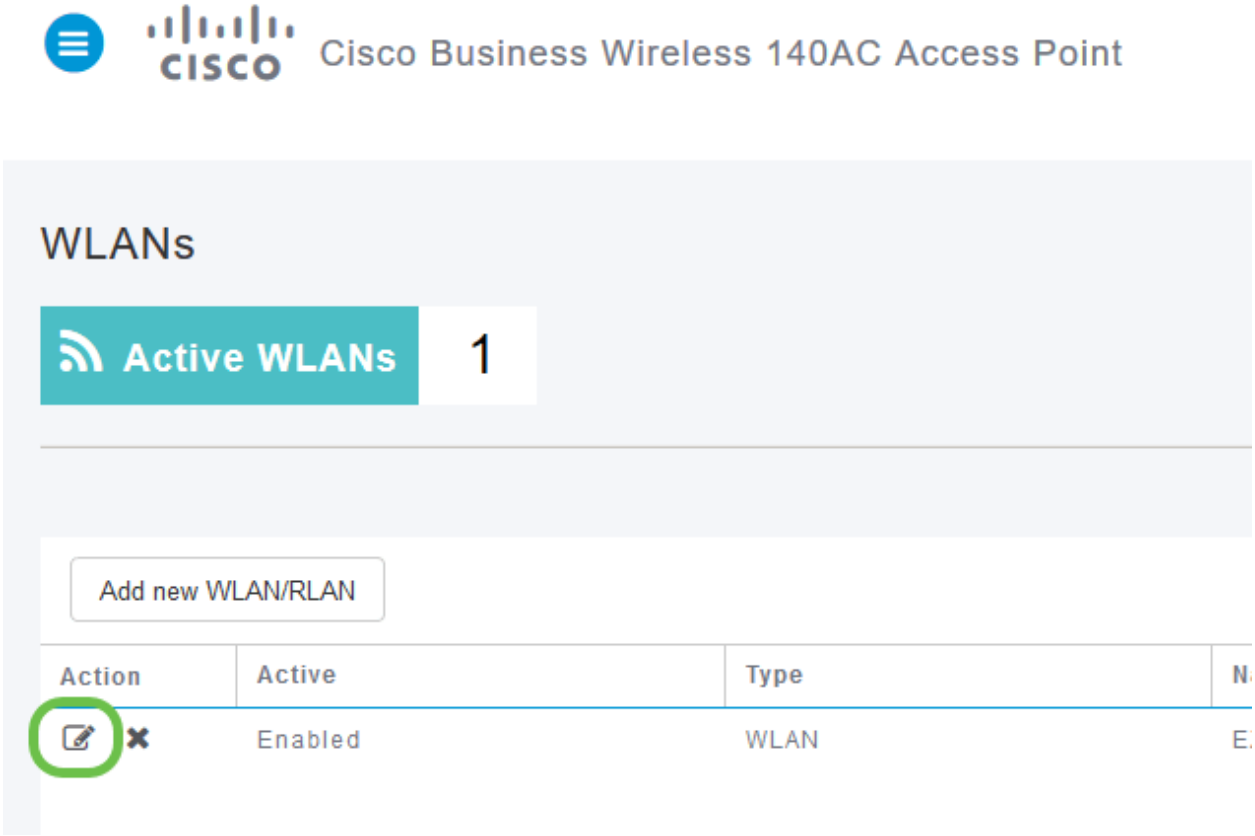

Das Bild unten ähnelt dem Bild, das Sie sehen, wenn Sie auf den Link Wireless

Settings (Wireless-Einstellungen) klicken.

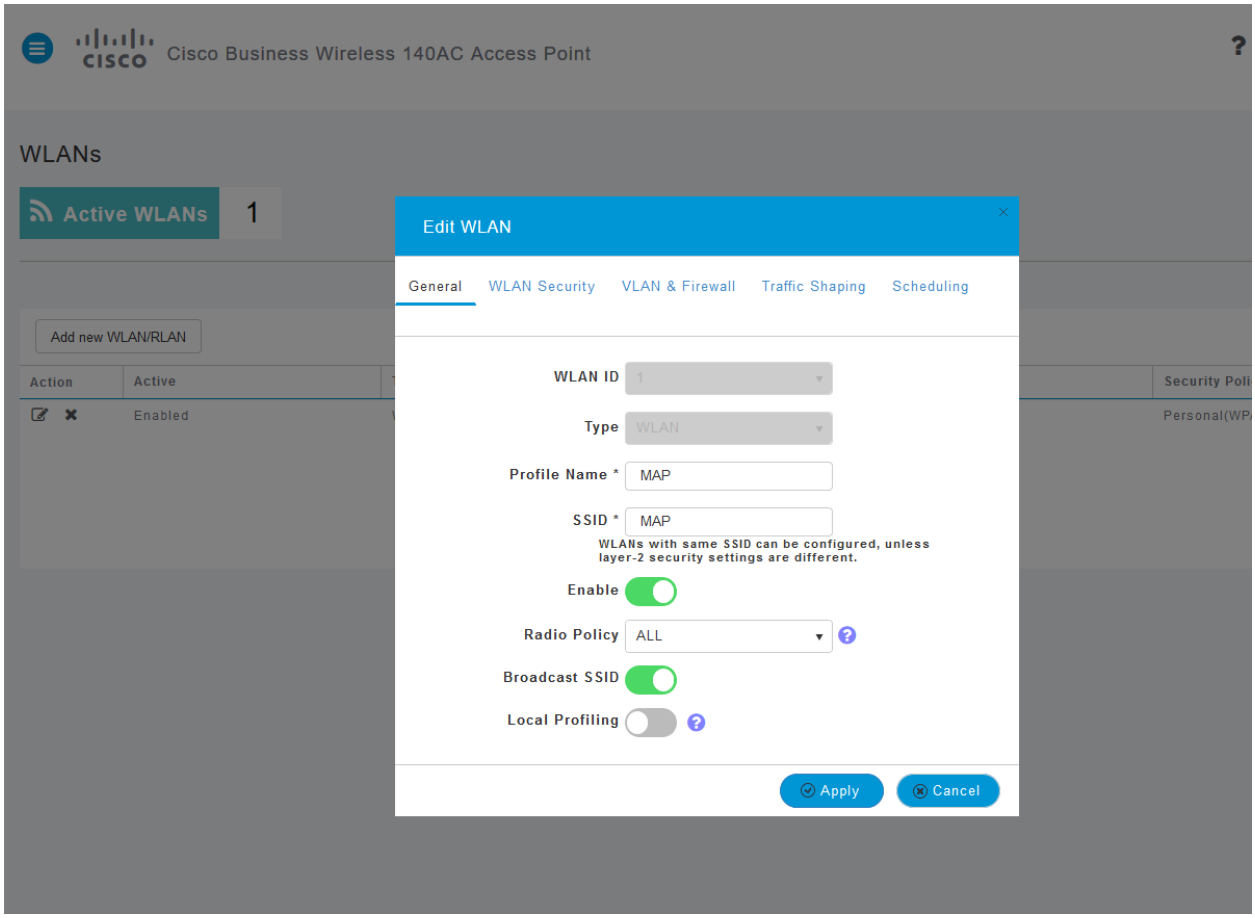



## Schritt 3

Klicken Sie auf das **Bearbeitungssymbol** links neben dem Wireless Local Area Network (Wireless-LAN), auf dem die Anwendung aktiviert werden soll.

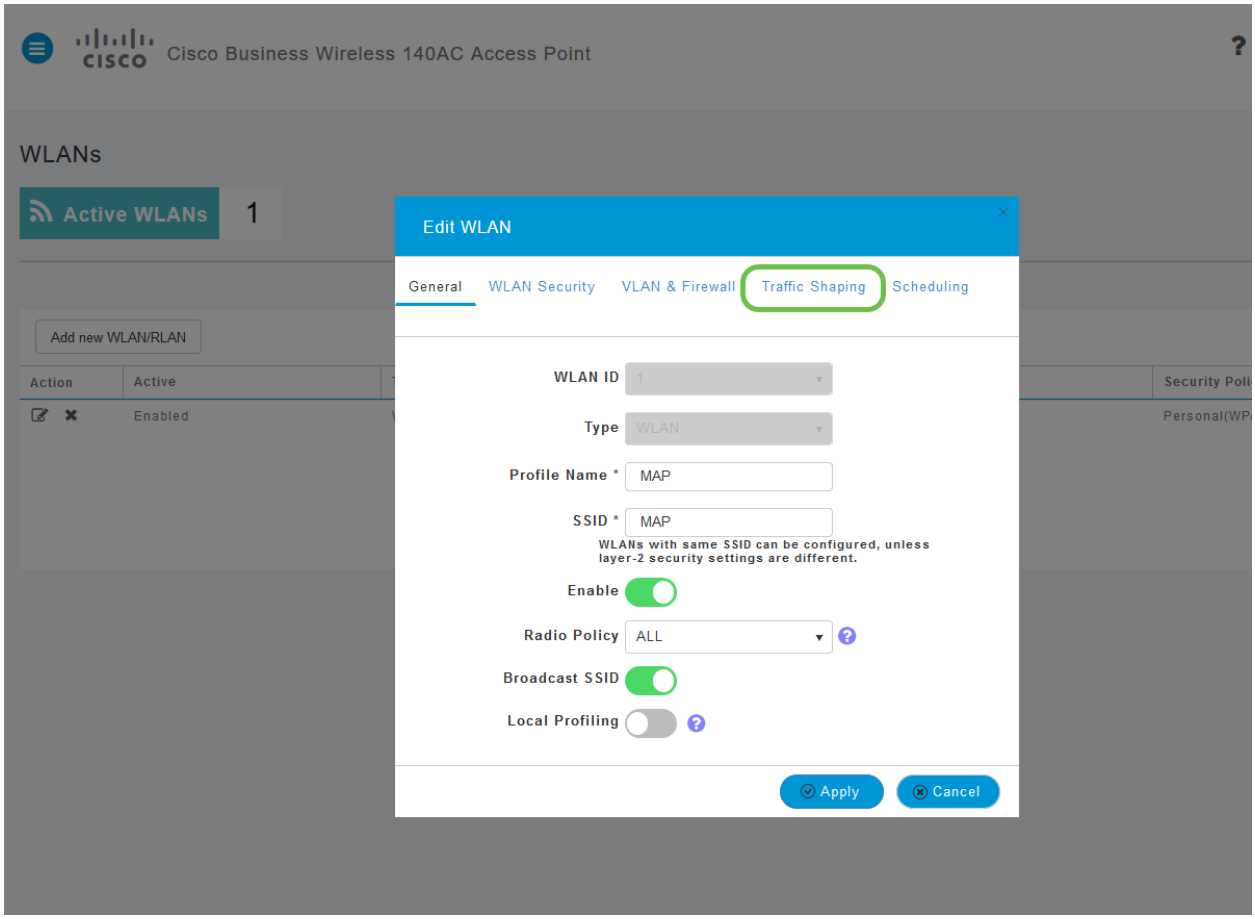



Da Sie vor kurzem das WLAN hinzugefügt haben, wird Ihre Seite *Edit WLAN* wie folgt angezeigt:

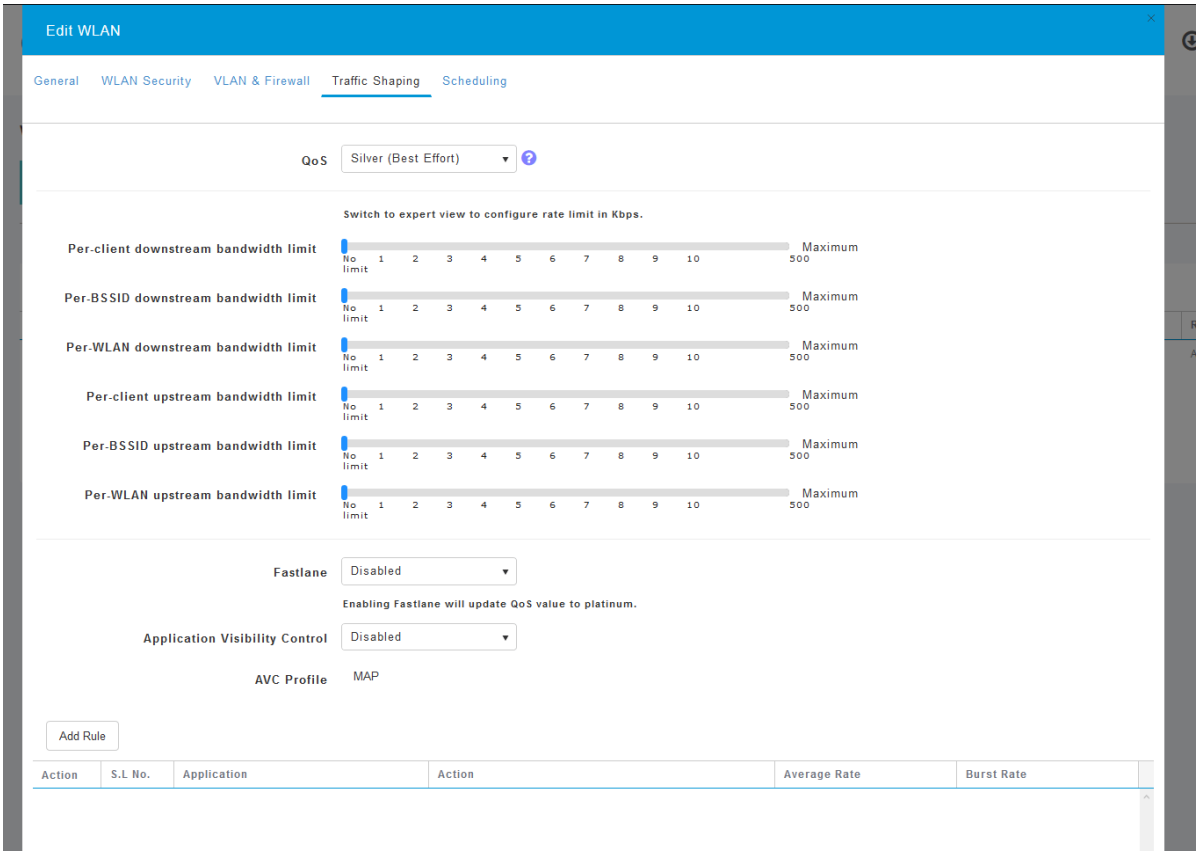



## Schritt 4

Navigieren Sie zur Registerkarte **Traffic Shaping**, indem Sie darauf klicken.

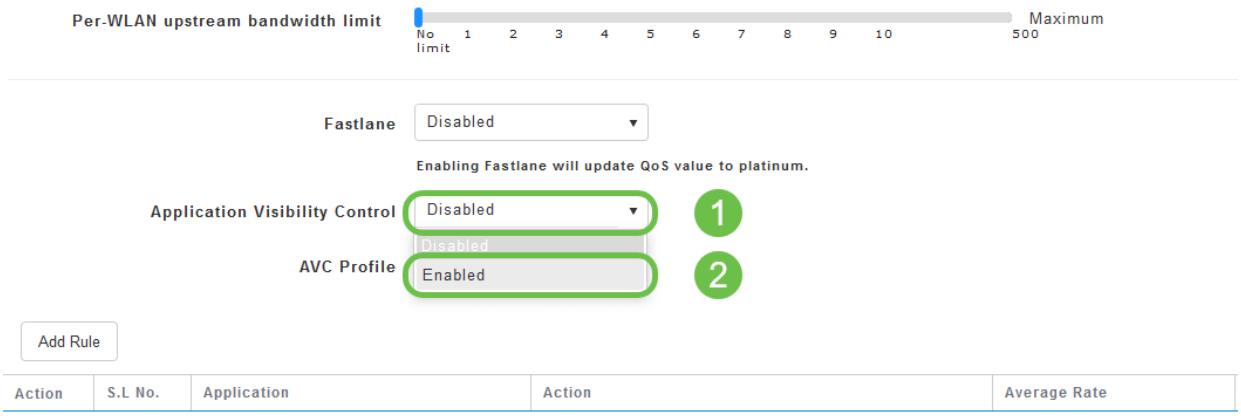



Ihr Bildschirm wird möglicherweise wie folgt angezeigt:



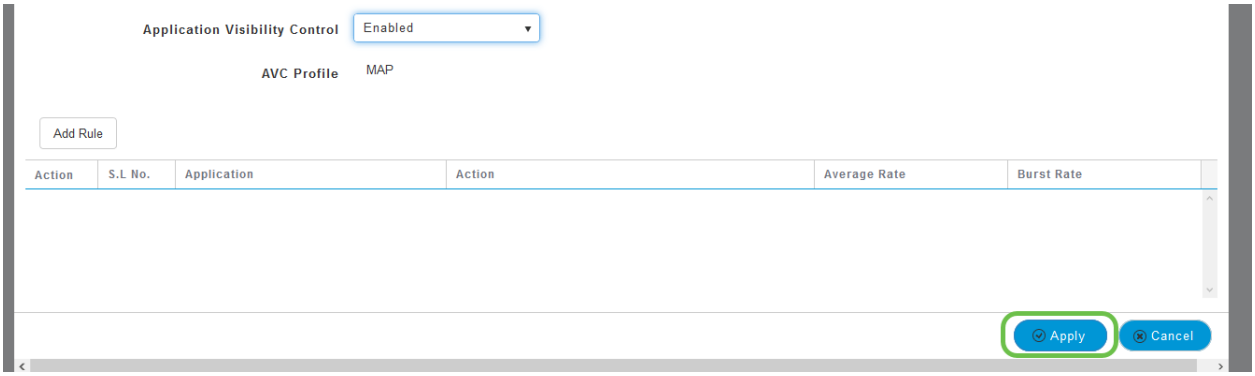

## Schritt 5

Unten auf der Seite befindet sich das *Application Visibility Control*-Feature. Dies ist standardmäßig deaktiviert. Klicken Sie auf das Dropdown-Menü, und wählen Sie **Enabled (Aktiviert)** aus.




## Schritt 6

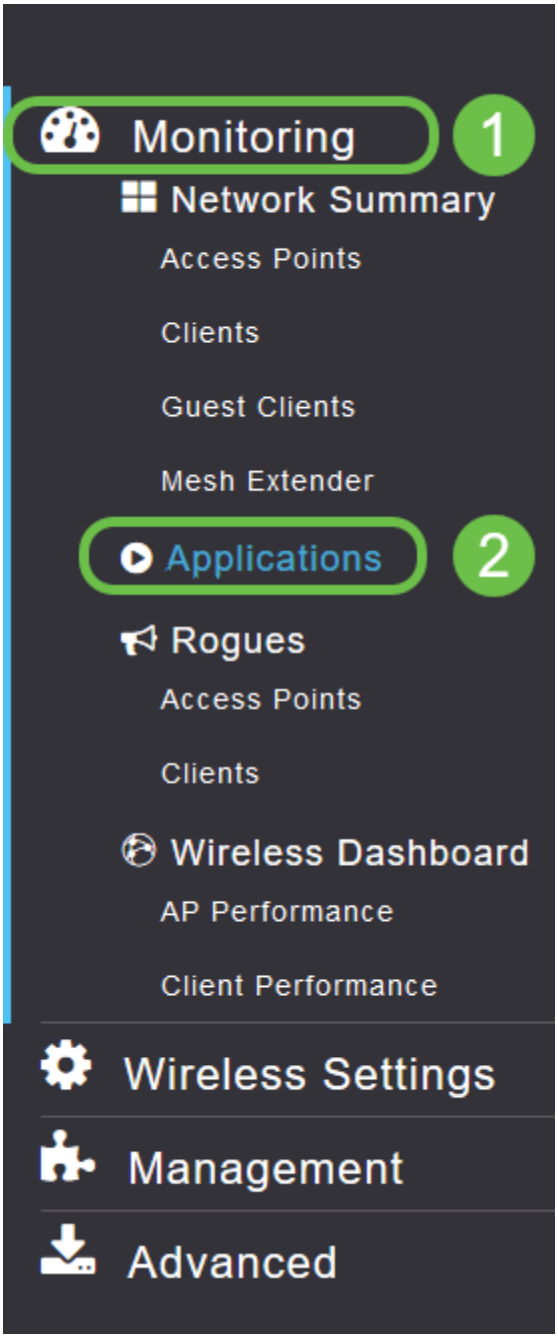
Klicken Sie auf die Schaltfläche **Übernehmen**.



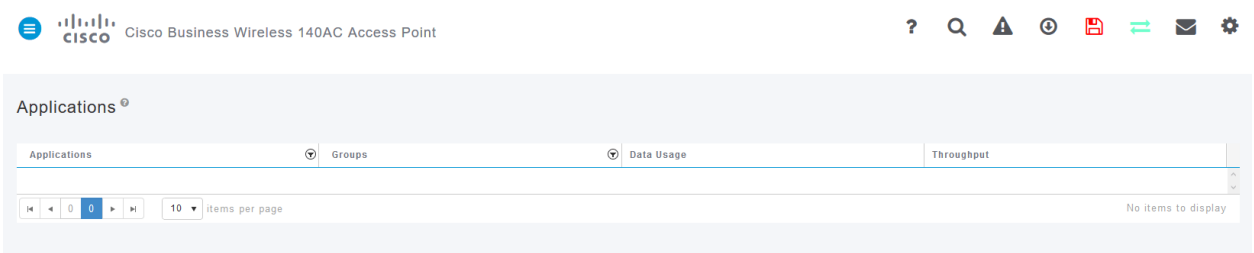

Diese Einstellung muss aktiviert werden, da die Funktion sonst nicht funktioniert.

## Schritt 7

Klicken Sie auf die Schaltfläche Abbrechen, um das WLAN-Untermenü zu schließen. Klicken Sie dann in der linken Menüleiste auf das **Überwachungsmenü**. Klicken Sie auf die Menüoption **Anwendungen**.




Wenn Sie keinen Datenverkehr zu einer Quelle hatten, wird Ihre Seite wie unten gezeigt leer sein.




Auf dieser Seite werden folgende Informationen angezeigt:

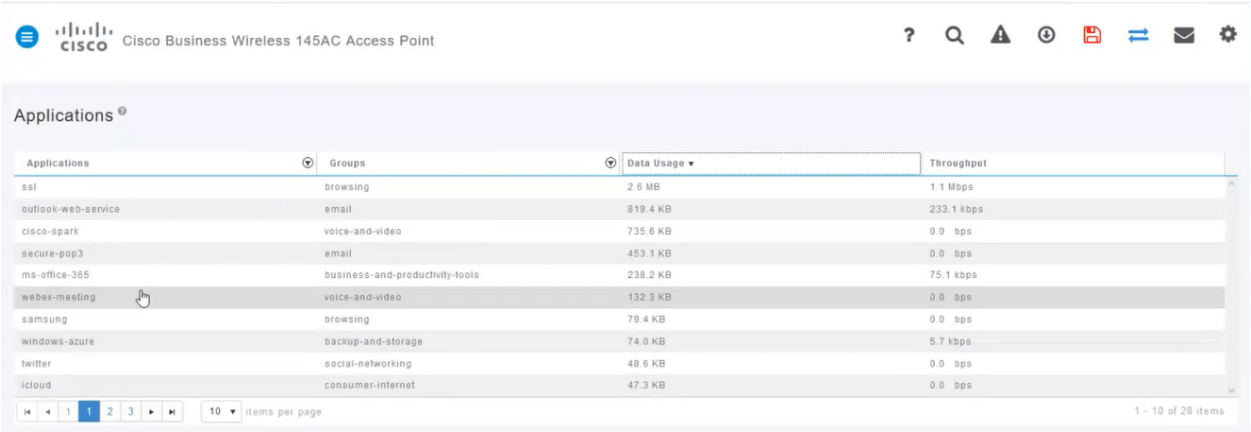
- Anwendung - umfasst viele verschiedene Typen
- Gruppen: Gibt den Typ der Anwendungsgruppe an, um das Sortieren zu vereinfachen.
- Datennutzung - Die von diesem Service insgesamt verwendete Datenmenge
- Durchsatz - Die von der Anwendung genutzte Bandbreite

Sie können auf die Registerkarten klicken, um sie von der größten bis zur kleinsten sortieren zu lassen. Dadurch können Sie die größten Nutzer von Netzwerkressourcen identifizieren.

Diese Funktion ist sehr leistungsstark für die präzise Verwaltung Ihrer WLAN-Ressourcen. Im Folgenden finden Sie einige der gebräuchlichsten Gruppen und Anwendungstypen. Ihre Liste enthält wahrscheinlich noch viele weitere, darunter die folgenden Gruppen und Beispiele:

- Durchsuchen
  - EX: Client-spezifisch, SSL
- E-Mail
  - EX: Outlook, SecurePop3
- Sprach- und Videofunktionen
  - EX: WebEx, Cisco Spark,
- Business-and-Productivity-Tools
  - EX: Microsoft Office 365
- Backup und Speicherung
  - EX: Windows Azure
- Privatnutzer-Internet
  - iCloud, Google Drive
- Soziale Netzwerke
  - EX: Twitter, Facebook
- Software-Updates
  - EX: Google Play, IOS
- Instant Messaging
  - EX: Nachrichten

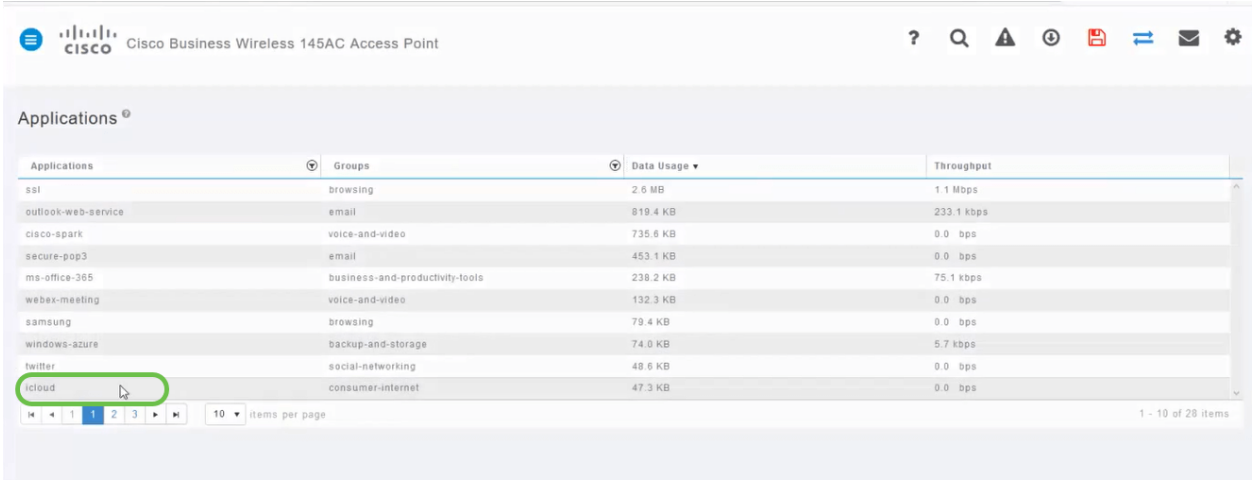
Hier sehen Sie ein Beispiel dafür, wie die Seite aussieht, wenn sie ausgefüllt wird.




Jede Tabellenüberschrift kann zum Sortieren angeklickt werden, was besonders für *Datenverwendung* und *Durchsatz* nützlich ist.

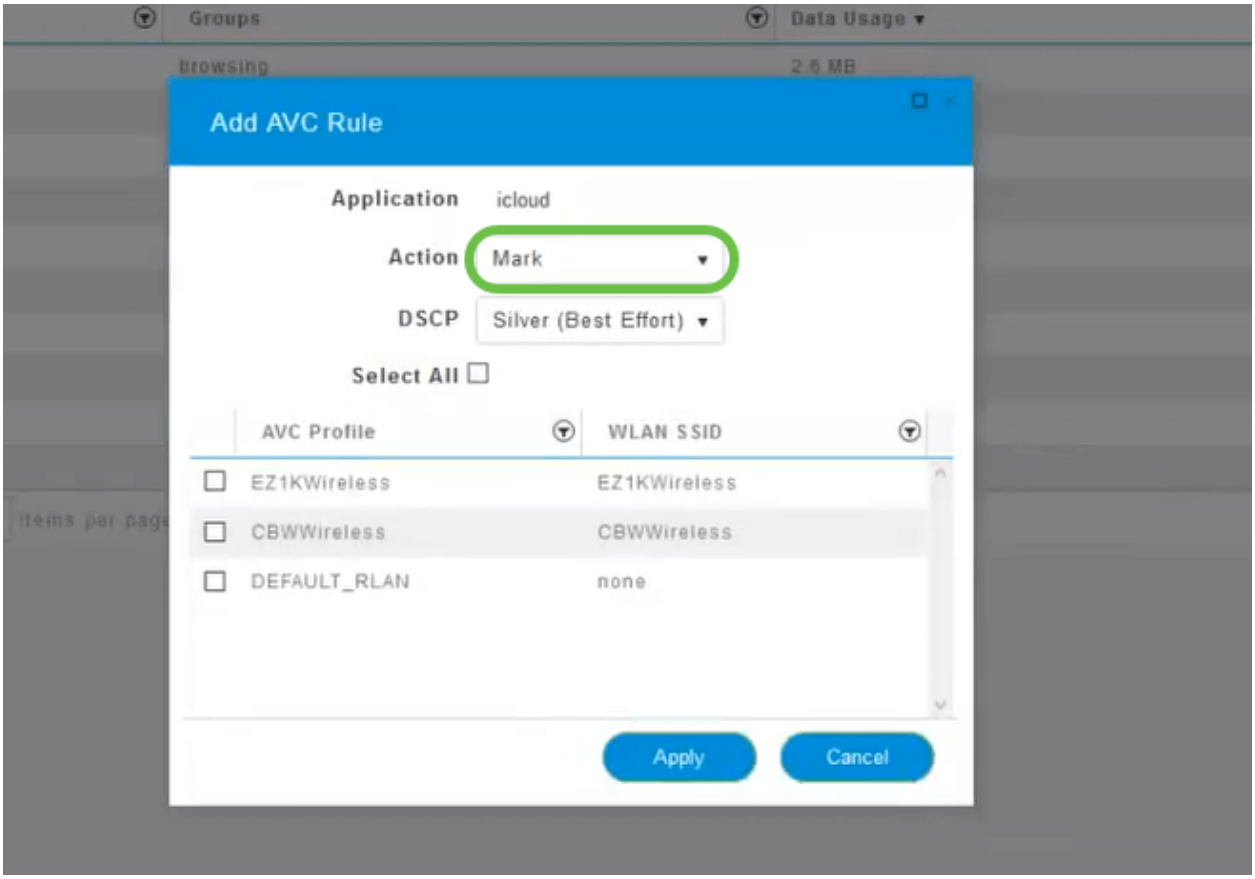
## Schritt 8

Klicken Sie auf die Zeile für den Datenverkehrstyp, den Sie verwalten möchten.




## Schritt 9

Klicken Sie auf das Dropdown-Feld **Aktion**, um festzulegen, wie Sie diesen Datenverkehrstyp behandeln möchten.



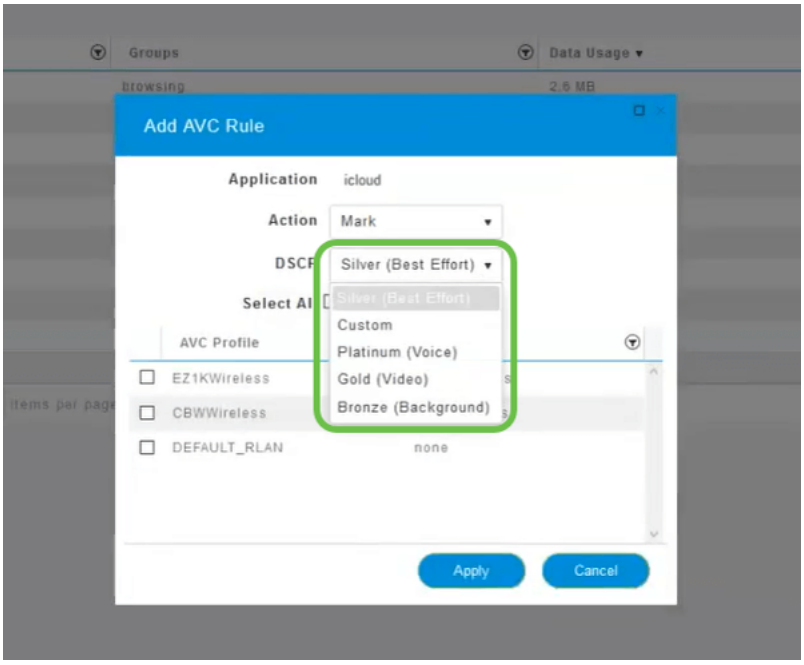

Bei diesem Beispiel überlassen wir diese Option *Mark*.

Maßnahmen zur Aufnahme des Datenverkehrs

- Markierung: Unterteilt den Datenverkehrstyp in eine der drei Ebenen des Differentiated Services Code Point (DSCP), wobei festgelegt wird, wie viele Ressourcen für den Anwendungstyp verfügbar sind.
- Verwerfen: Tun Sie nichts, außer den Datenverkehr zu verwerfen.
- Übertragungsratenlimit - Ermöglicht Ihnen, die Durchschnittssätze und die Burst Rate in Kbit/s festzulegen.

## Schritt 10

Klicken Sie auf das Dropdown-Feld im Feld **DSCP**, um eine der folgenden Optionen auszuwählen.



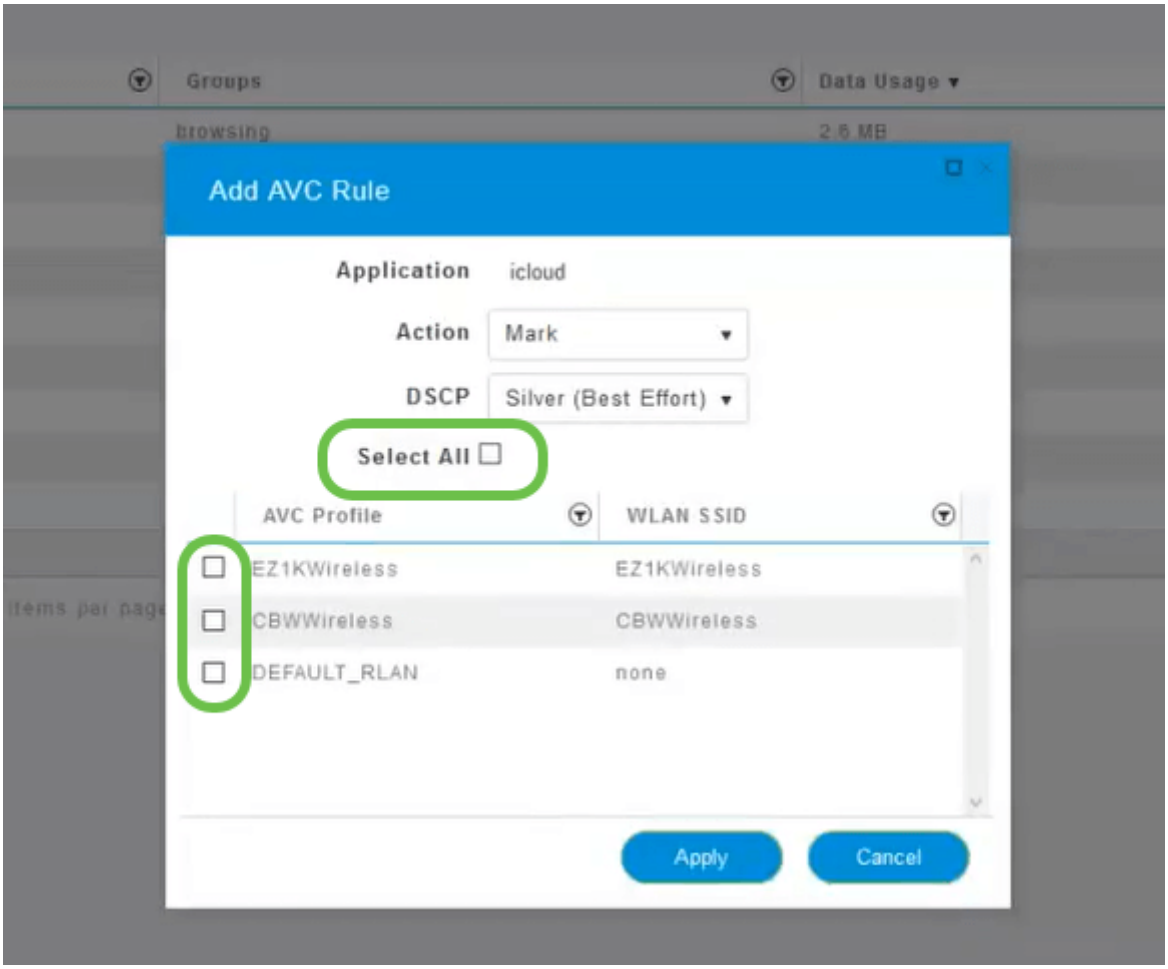

Nachfolgend sind die DSCP-Optionen für den zu markierenden Datenverkehr aufgeführt. Diese Optionen gehen von weniger Ressourcen zu mehr Ressourcen über, die für den zu bearbeitenden Datenverkehrstyp verfügbar sind.

- Bronze (Hintergrund) - weniger
- Silver (Best Effort)
- Gold (Video)
- Platinum (Sprache) Mehr
- Benutzerdefiniert - Benutzerset

Als Webkonvention wurde der Datenverkehr in Richtung SSL-Browsing migriert, wodurch Sie nicht sehen können, was sich in den Paketen befindet, während diese von Ihrem Netzwerk in das WAN verschoben werden. Daher wird ein großer Teil des Web-Datenverkehrs SSL verwenden. Wenn Sie SSL-Datenverkehr mit einer niedrigeren Priorität einstellen, kann dies sich negativ auf das Surfen auswirken.

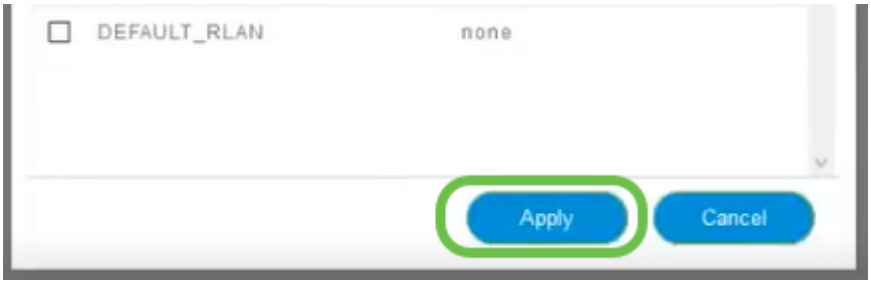
## Schritt 11

Wählen Sie nun die individuelle SSID aus, die diese Richtlinie ausführen soll, oder klicken Sie auf **Alles auswählen**.




**Schritt 12**

Klicken Sie nun auf **Apply**, um diese Richtlinie zu starten.




In zwei Fällen könnte dies gelten:

- Gäste/Benutzer streamen eine große Menge an Datenverkehr ab, um geschäftskritischen Datenverkehr zu verhindern. Sie können entweder die Priorität für Sprache erhöhen, die Priorität des Netflix-Datenverkehrs verringern, um die Dinge zu verbessern.
- Das Herunterladen großer Software-Updates während der Geschäftszeiten kann eingeschränkt oder mit einer eingeschränkten Rate werden.

Du hast es getan! Die Erstellung von Anwendungsprofilen ist ein sehr leistungsstarkes Tool, das durch die Aktivierung der Client Profiling-Funktion weiter unterstützt werden kann. Dies wird im nächsten Abschnitt beschrieben.

## Client-Profiling mithilfe der Webbenutzeroberfläche (optional)

Bei der Verbindung mit einem Netzwerk tauschen Geräte Informationen zur Erstellung von Client-Profilen aus. Standardmäßig ist die *Client-Profilerstellung* deaktiviert. Diese Informationen können Folgendes umfassen:

- Hostname - oder der Name des Geräts
- Betriebssystem - die Kernsoftware des Geräts
- Betriebssystemversion - Die Iteration der entsprechenden Software

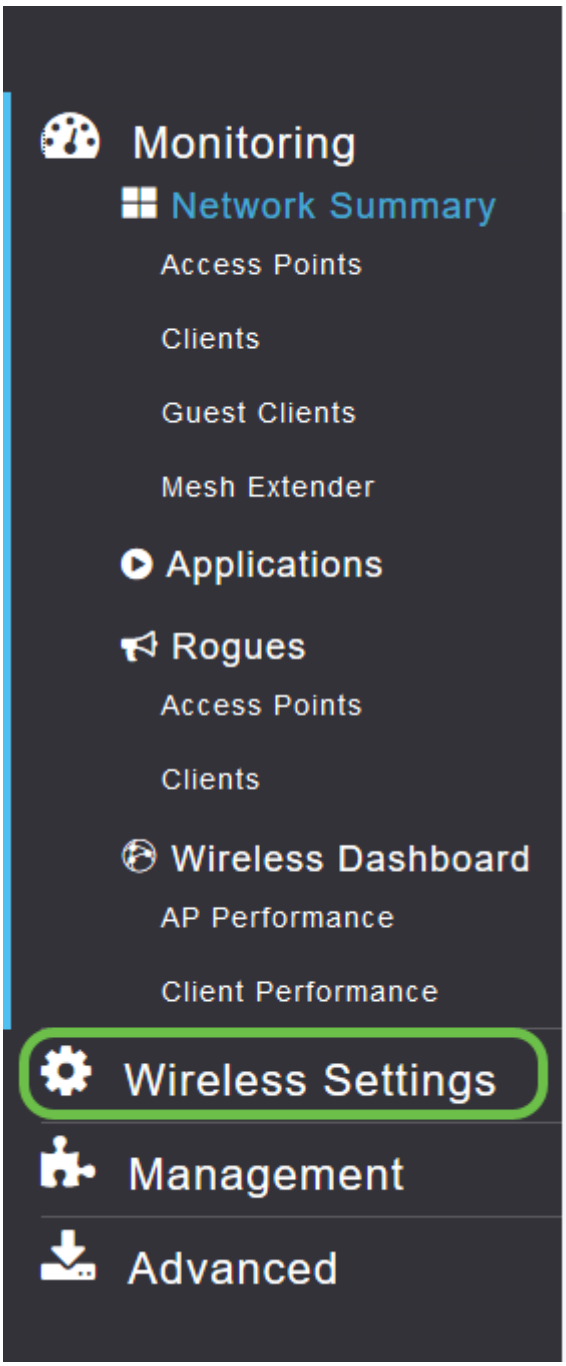
Statistiken über diese Clients enthalten die Menge der verwendeten Daten und den Durchsatz.

Die Verfolgung von Client-Profilen ermöglicht eine bessere Kontrolle über das Wireless Local Area Network. Oder Sie können es als Funktion einer anderen Funktion verwenden. Beispielsweise können Sie Gerätetypen zur Drosselung von Anwendungen verwenden, die keine geschäftskritischen Daten übertragen.

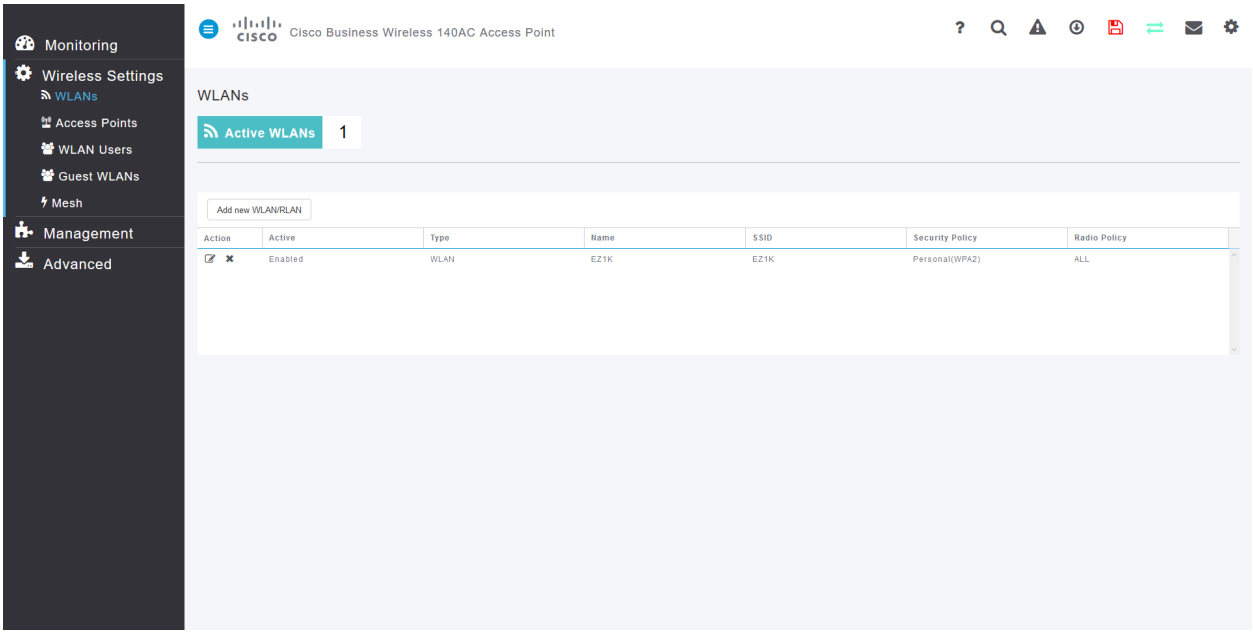
Nach der Aktivierung finden Sie die Clientdetails für Ihr Netzwerk im Abschnitt Überwachung der Webbenutzeroberfläche.

**Schritt 1**

Klicken Sie auf **Wireless Settings**.

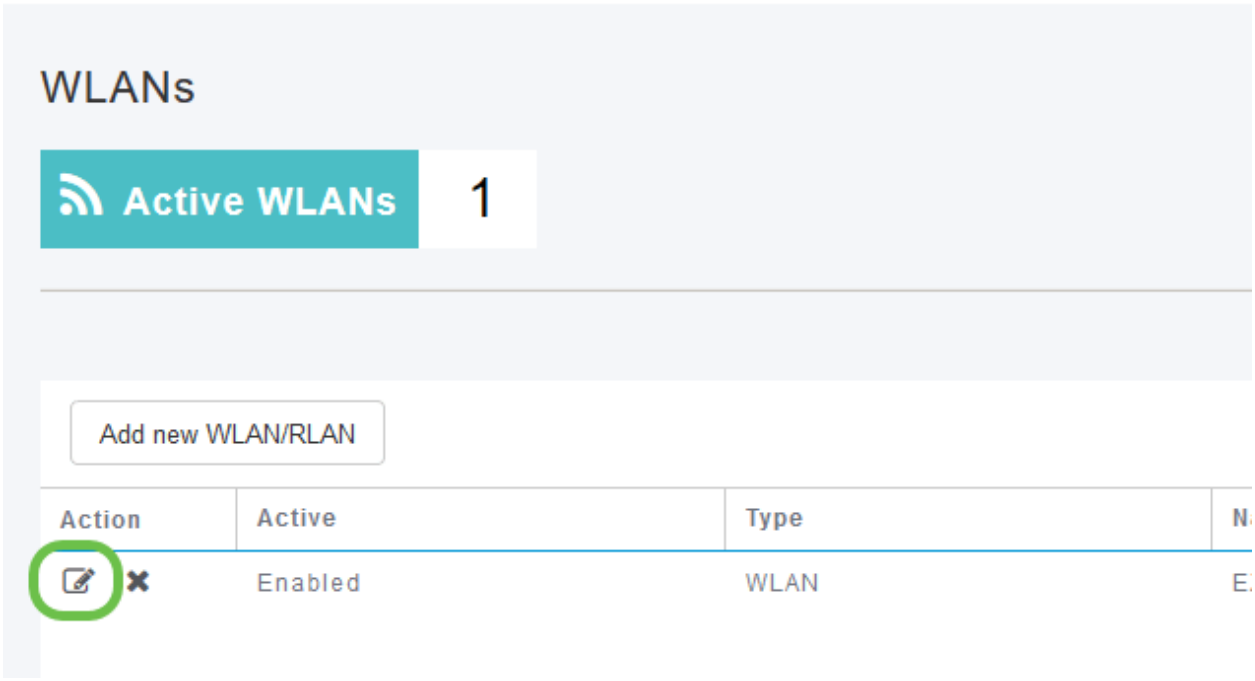



Die folgende Abbildung ähnelt der Anzeige, wenn Sie auf den Link Wireless Settings (Wireless-Einstellungen) klicken:



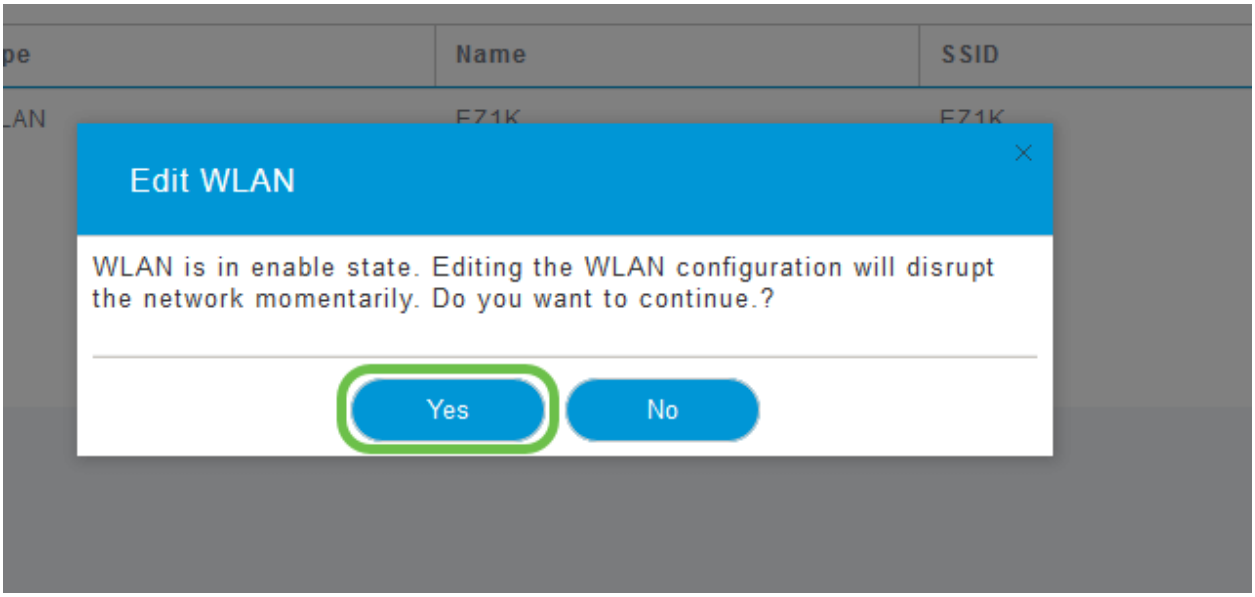

## Schritt 2

Wählen Sie das WLAN aus, das Sie für die Anwendung verwenden möchten, und klicken Sie links auf das **Bearbeitungssymbol**.




## Schritt 3

Ein Popup-Menü wird möglicherweise ähnlich wie unten angezeigt. Diese wichtige Nachricht kann sich vorübergehend auf den Service in Ihrem Netzwerk auswirken. Klicken Sie auf **Ja**, um fortzufahren.

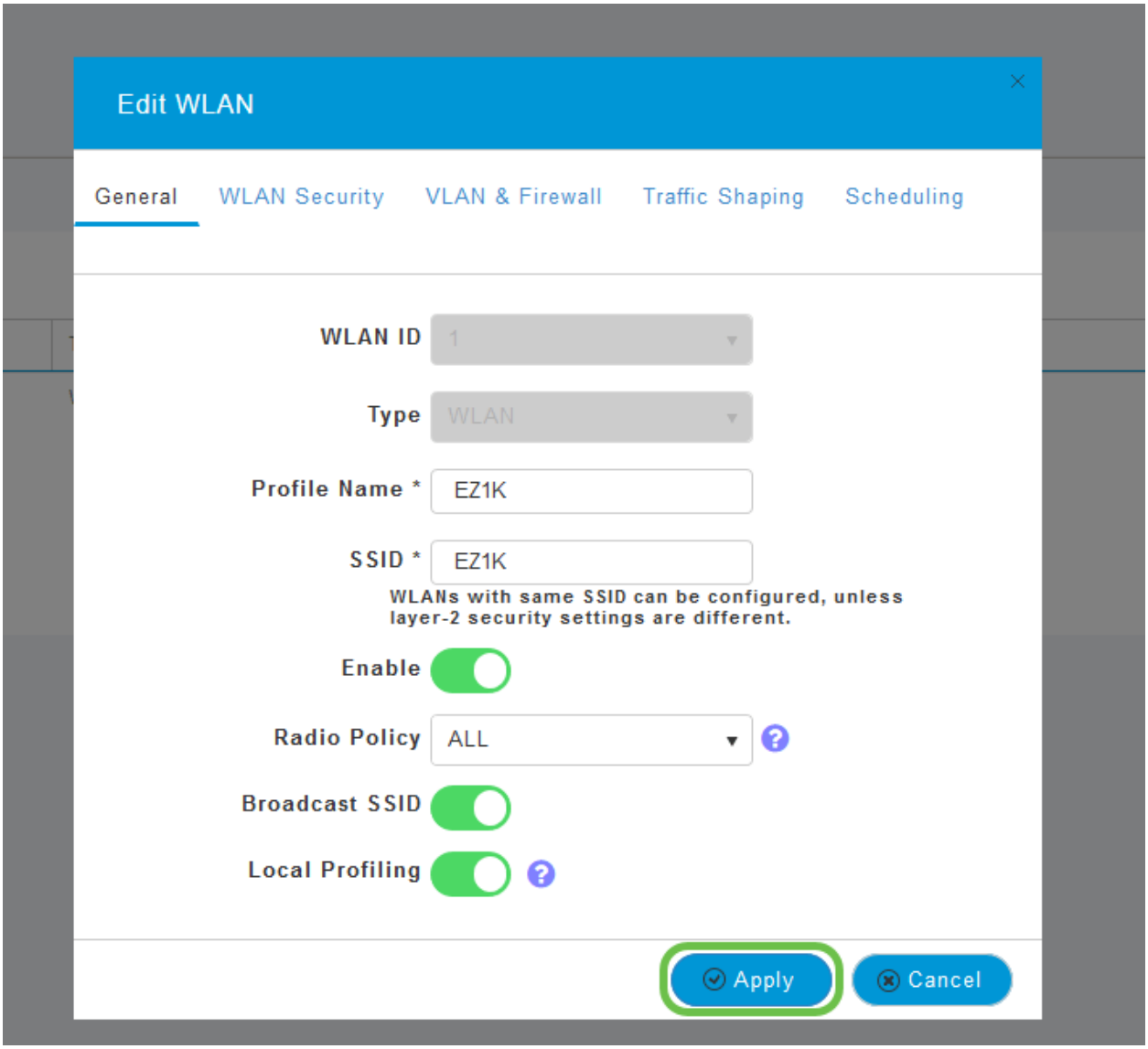



**Schritt 4**

Schalten Sie die Client-Profilerstellung um, indem Sie auf die Schaltfläche **Lokale Profilerstellung** klicken.

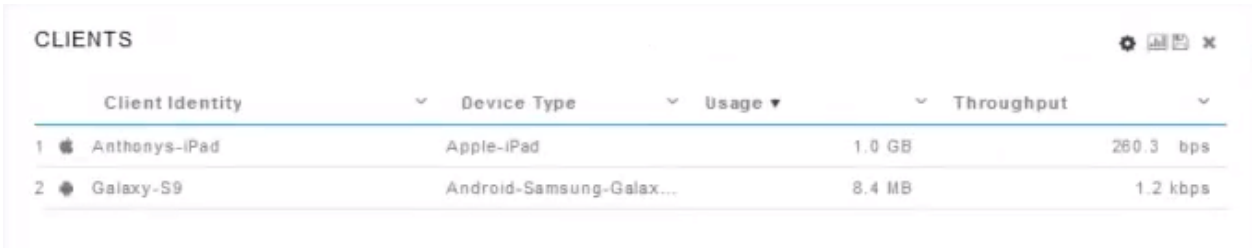

**Schritt 5**

Klicken Sie auf Apply (Anwenden).




**Schritt 6**

Klicken Sie links auf die Menüoption **Monitoring** (Überwachung). Sie sehen, dass die Client-Daten auf der Registerkarte *Überwachung* im Dashboard angezeigt werden.




## Schlussfolgerung

Sie haben nun die Einrichtung Ihres sicheren Netzwerks abgeschlossen. Was für ein großes Gefühl, jetzt eine Minute zu feiern und dann zur Arbeit!

Wir wünschen unseren Kunden das Beste. Sie haben also Kommentare oder Vorschläge zu diesem Thema, senden Sie uns bitte eine E-Mail an das Cisco Content Team.

Weitere Artikel und Dokumentationen finden Sie auf den Support-Seiten für Ihre

Hardware:

- Cisco RV260P VPN-Router mit PoE
- Cisco Business Access Point der Serie 140AC
- Cisco Business 142ACM Mesh Extender