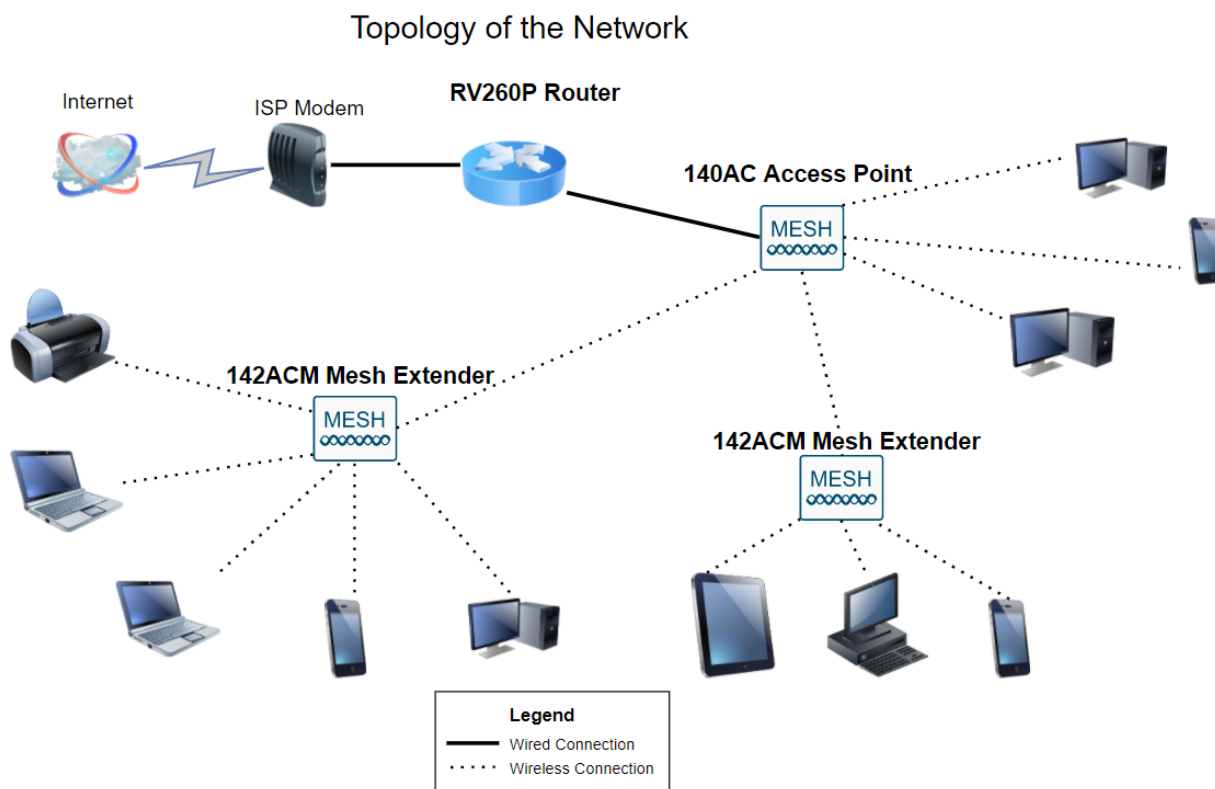


Netzwerkkonfiguration gesamt: RV260P mit CBW und der Cisco Business Mobile App

Ziel:

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

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 ein Cisco Business Wireless (CBW) 140AC an den Router und nicht an einen Switch angeschlossen werden kann. Mit dem CBW140AC Access Point und den CBW142ACM Mesh Extendern wird ein Wireless Mesh-Netzwerk erstellt.

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:

- [Willkommen bei der Cisco Business Wireless Mesh Networking](#)

- [Häufig gestellte Fragen \(FAQs\) zu einem Cisco Business Wireless Network](#)

Die mobile Anwendung wird als einfachste Methode zum Festlegen von Basiskonfigurationen für CBW empfohlen. Es können jedoch nicht alle Funktionen in der Anwendung konfiguriert werden. Wenn Sie die Cisco Business Wireless-App noch nicht besitzen, lesen Sie die folgenden Artikel:

- [Machen Sie sich mit der Cisco Business CB-Wireless-Mesh-App vertraut](#)
- [Cisco Business Wireless: CBW-App und Web-Benutzeroberfläche](#)

Wenn Sie die Webbenutzeroberfläche verwenden möchten, wenn Sie das Wireless-Mesh-Netzwerk konfigurieren, klicken Sie auf, um die Version anzuzeigen, die [nur die Webbenutzeroberfläche verwendet](#).

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

- [Konfigurieren des RV260P-Routers](#)
- [Konfigurieren des CBW140AC](#)
- [Konfigurieren der CBW142ACM-Mesh-Extender](#)

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 auch 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 und der RV260P mit dem Booten fertig ist.

Router einrichten

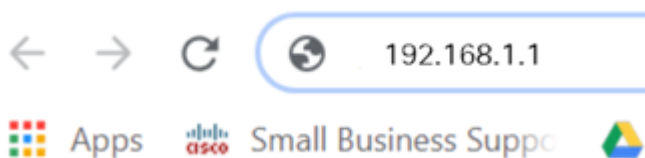
Jetzt ist es an der Zeit einige Konfigurationen vorzunehmen! So starten Sie die Webbenutzeroberfläche:

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. Wählen Sie dazu aus, *um automatisch eine IP-Adresse* in den Eigenschaften von TCP/IP auf dem Computer *abzurufen*.

Schritt 2

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



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](#).



Your connection is not private

Attackers might be trying to steal your information from [ciscobusiness.cisco](#) (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Advanced

Back to safety

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.



Router

1

2

English ▾

3

©2018 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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 Sie eine Antwort erhalten, haben Sie Konnektivität und können zum Abschnitt "[Erstkonfiguration](#)" dieses Artikels übergehen.

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, sehen Sie sich die [Anweisungen in Windows 10 an, um die Netzwerkeinstellungen des RV260P zu ändern](#).

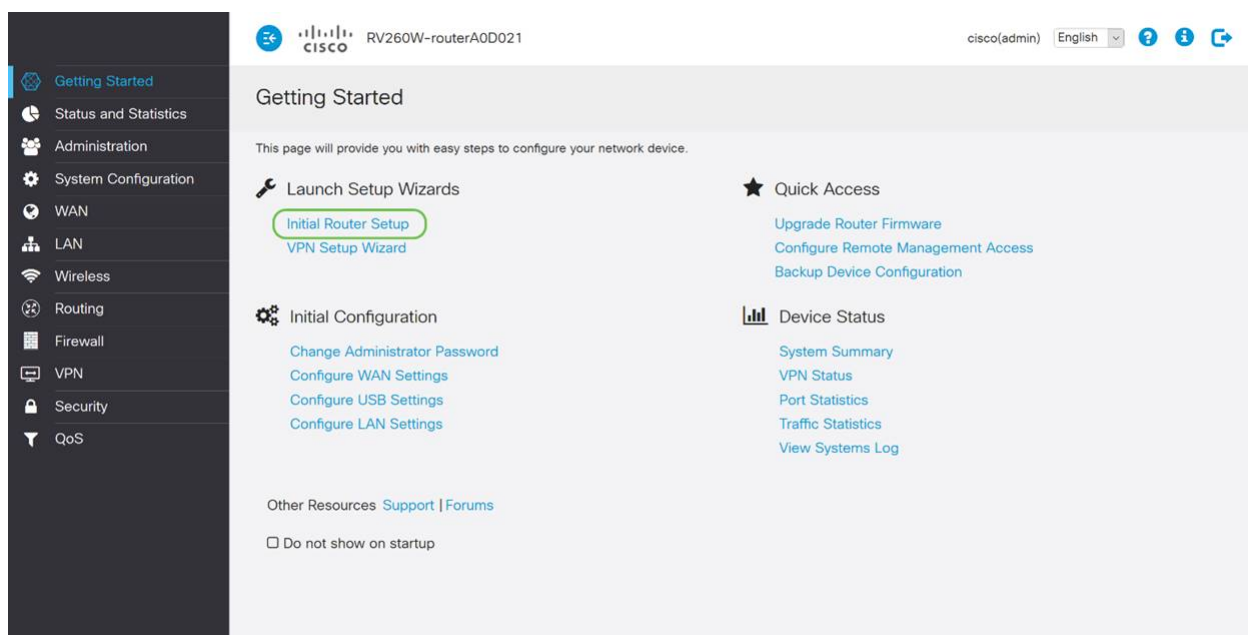
3. Wenn Sie bereits Geräte mit der IP-Adresse 192.168.1.1 besitzen, müssen Sie diesen Konflikt beheben, damit das Netzwerk funktioniert. Mehr dazu am Ende dieses Abschnitts, oder [klicken Sie hier direkt dorthin](#).
4. Setzen Sie das Modem und den RV260P zurück, indem Sie beide Geräte ausschalten. Schalten 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. Wenn Artikel für eine bestimmte Einstellung vorhanden sind, werden diese am Ende des Schritts aufgelistet.

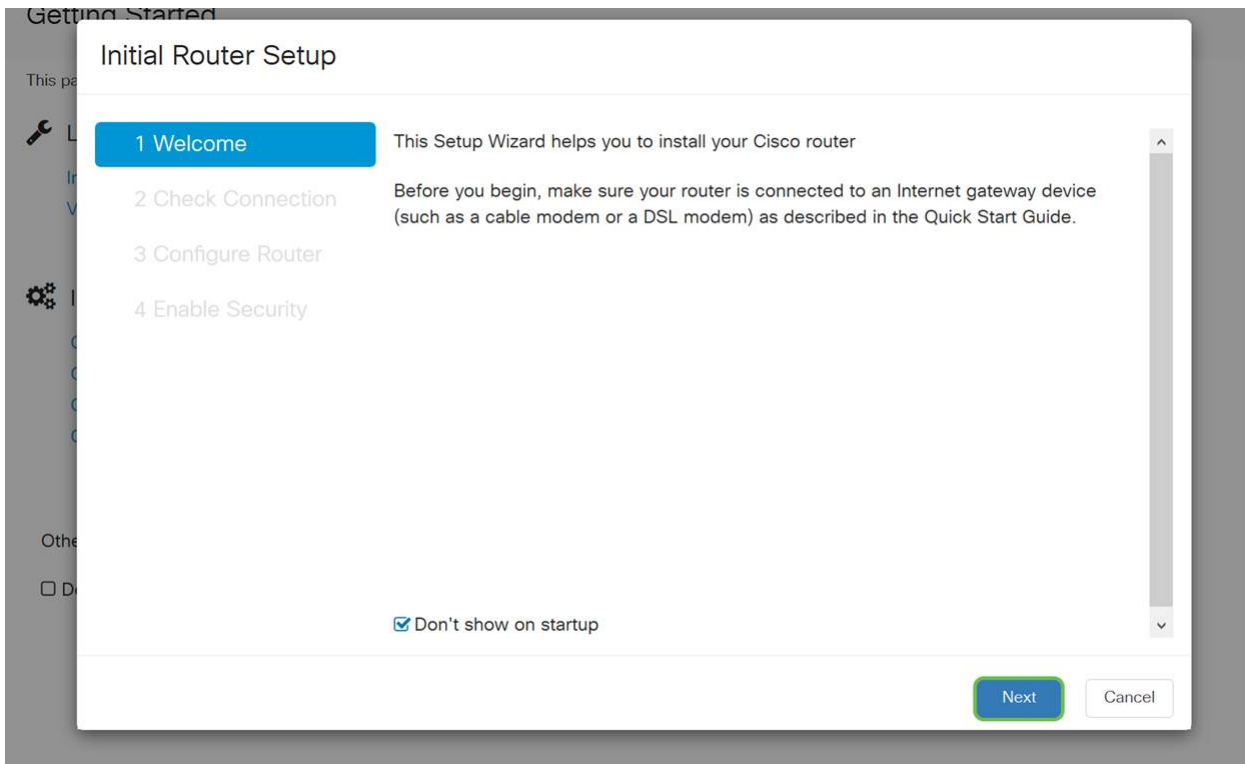
Schritt 1

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



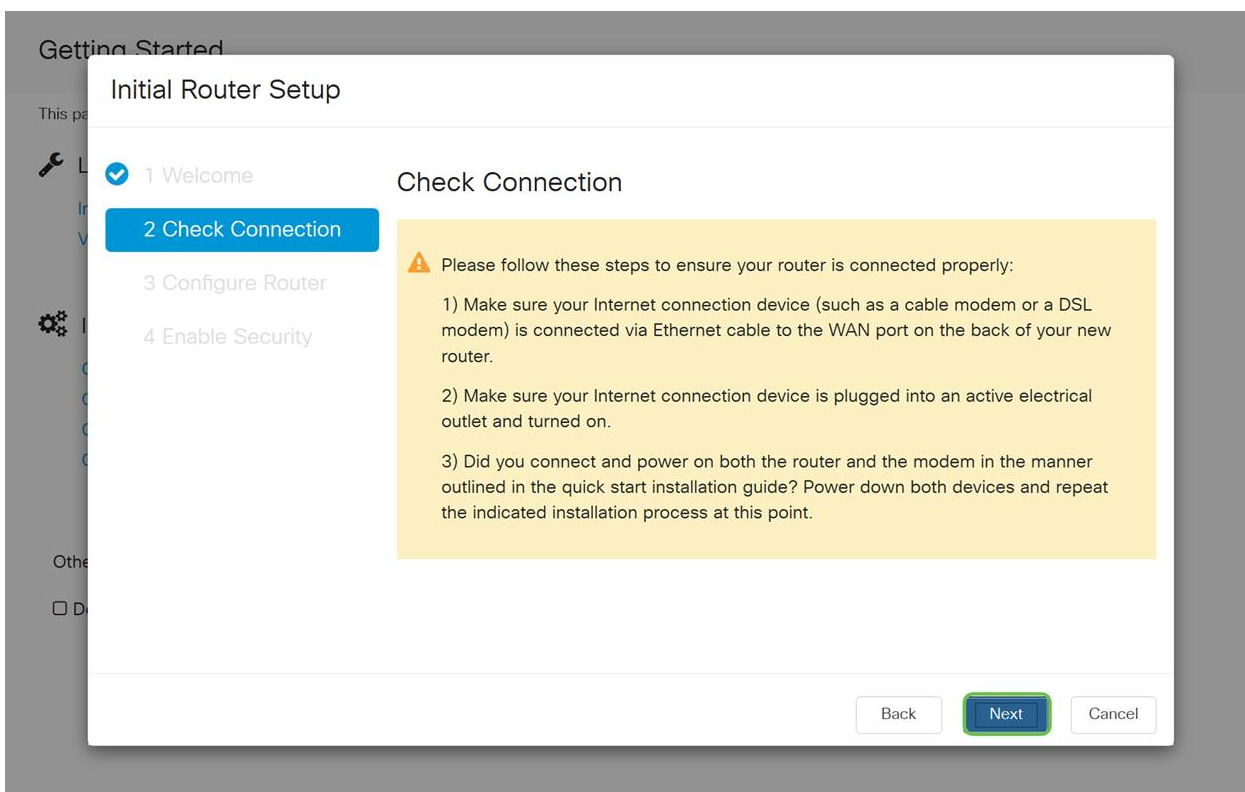
Schritt 2

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



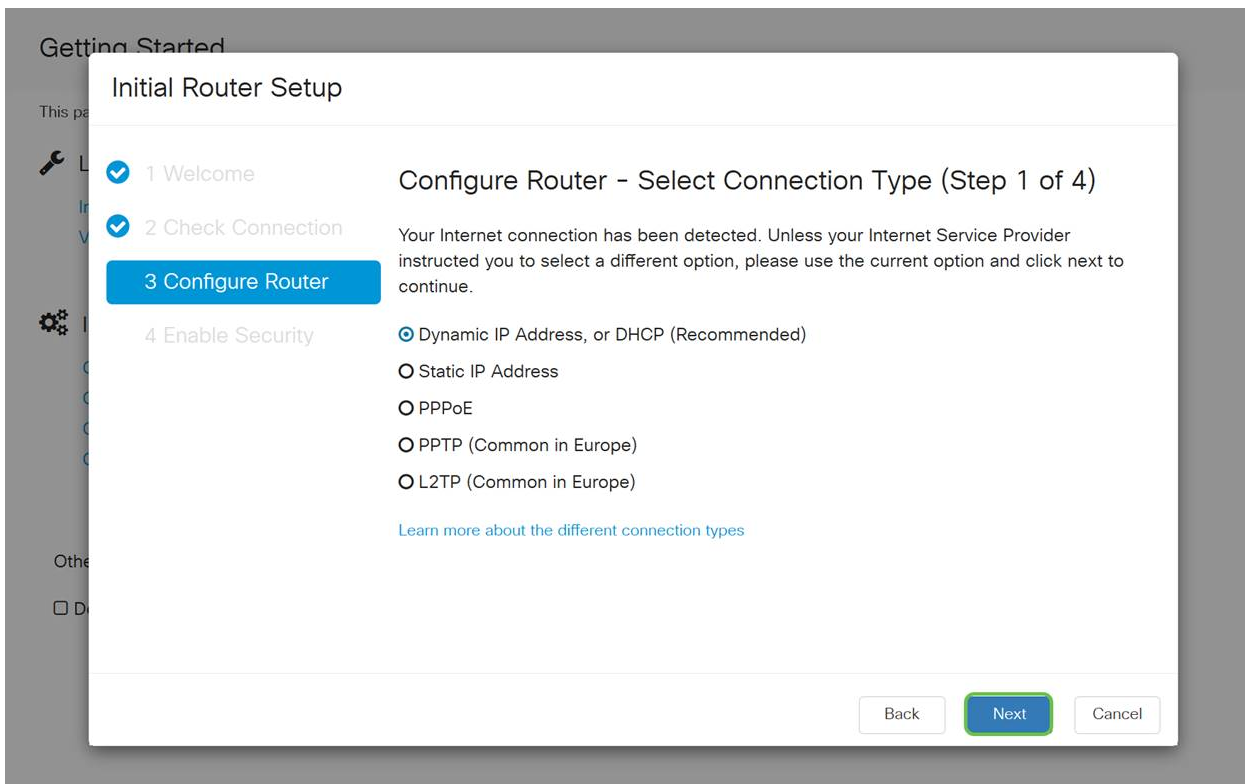
Schritt 3

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



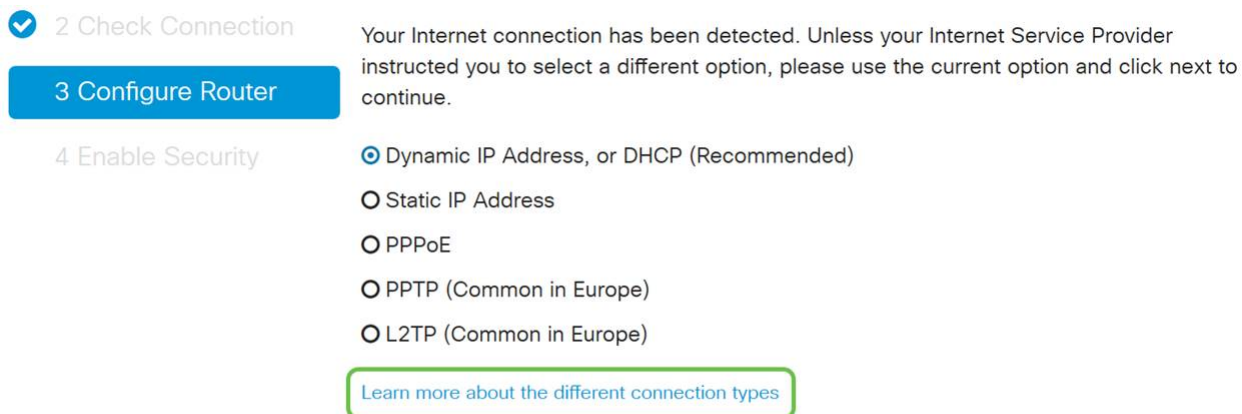
Schritt 4

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**.



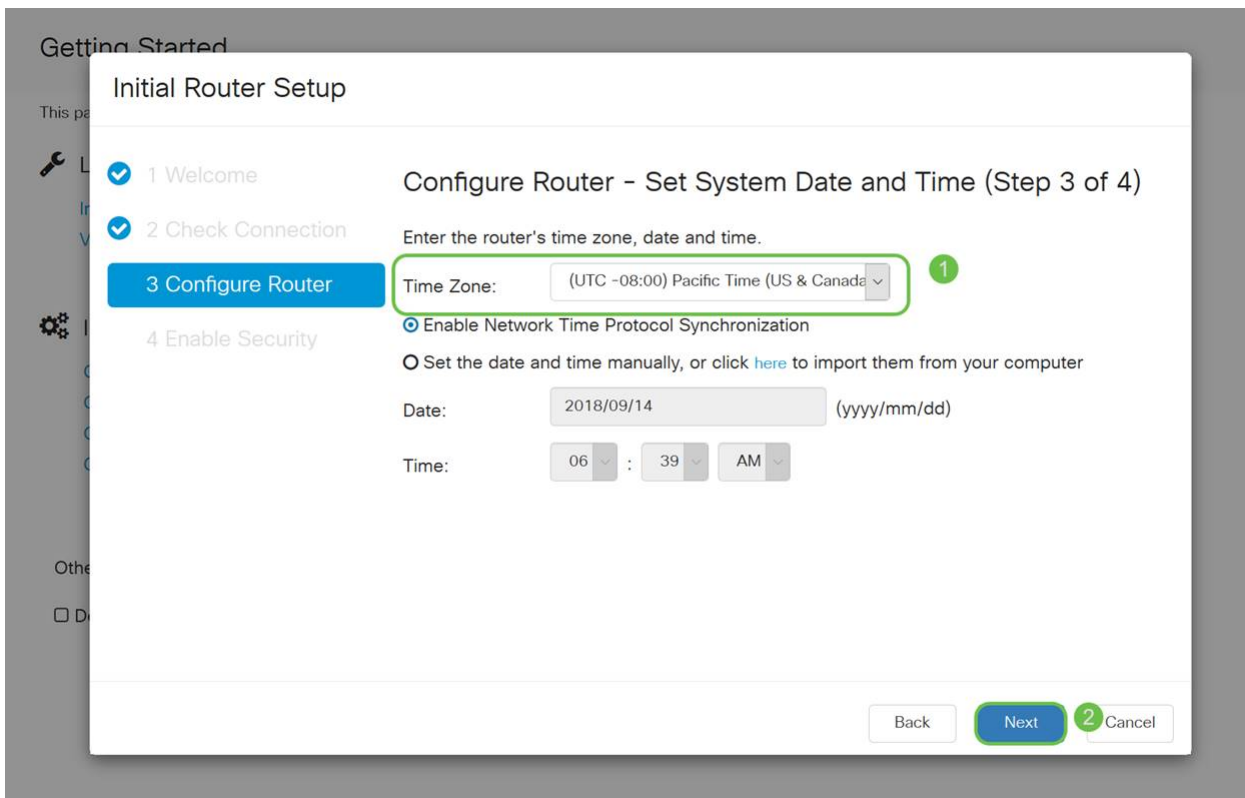
Obwohl Sie DHCP für diese Ersteinrichtung verwenden müssen, können Sie auswählen, **um weitere Informationen über die verschiedenen Verbindungstypen** am unteren Bildschirmrand als zukünftige Referenz zu erhalten. Weitere Einzelheiten hierzu finden Sie unter:

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



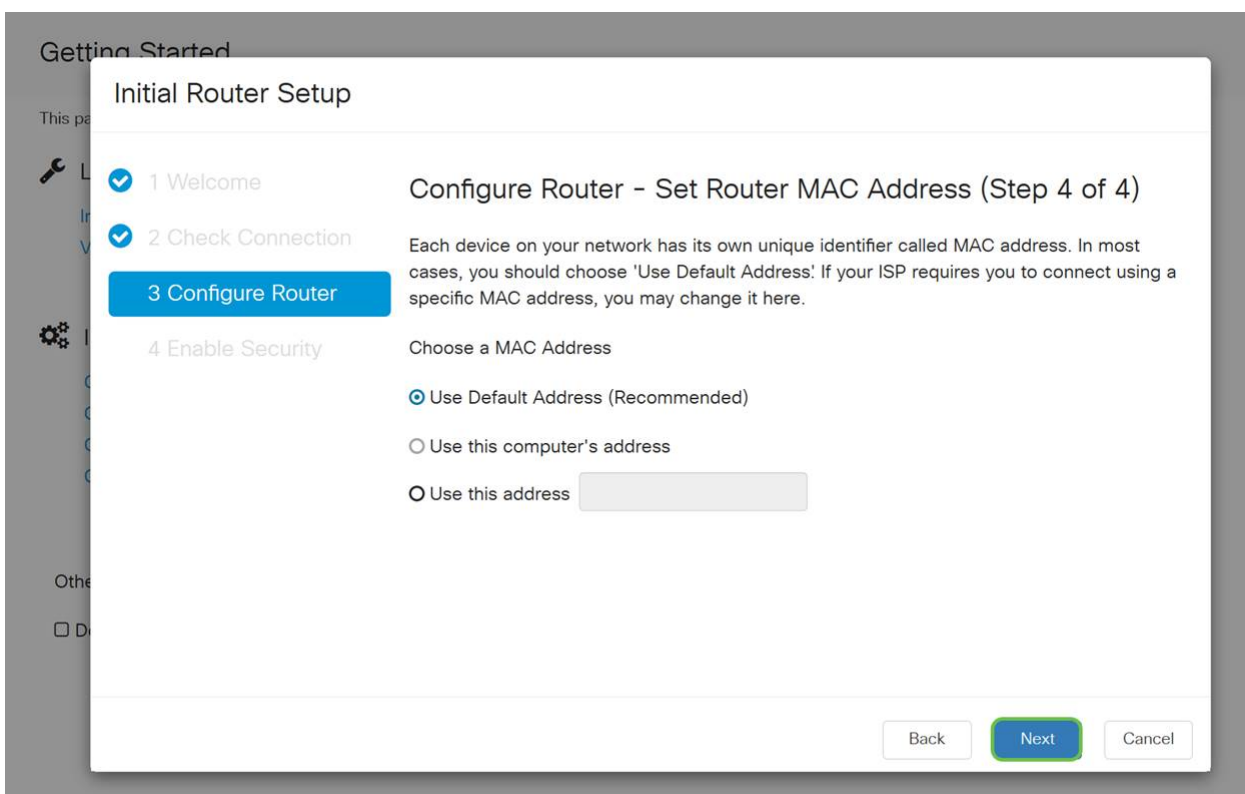
Schritt 5

Als Nächstes 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**.



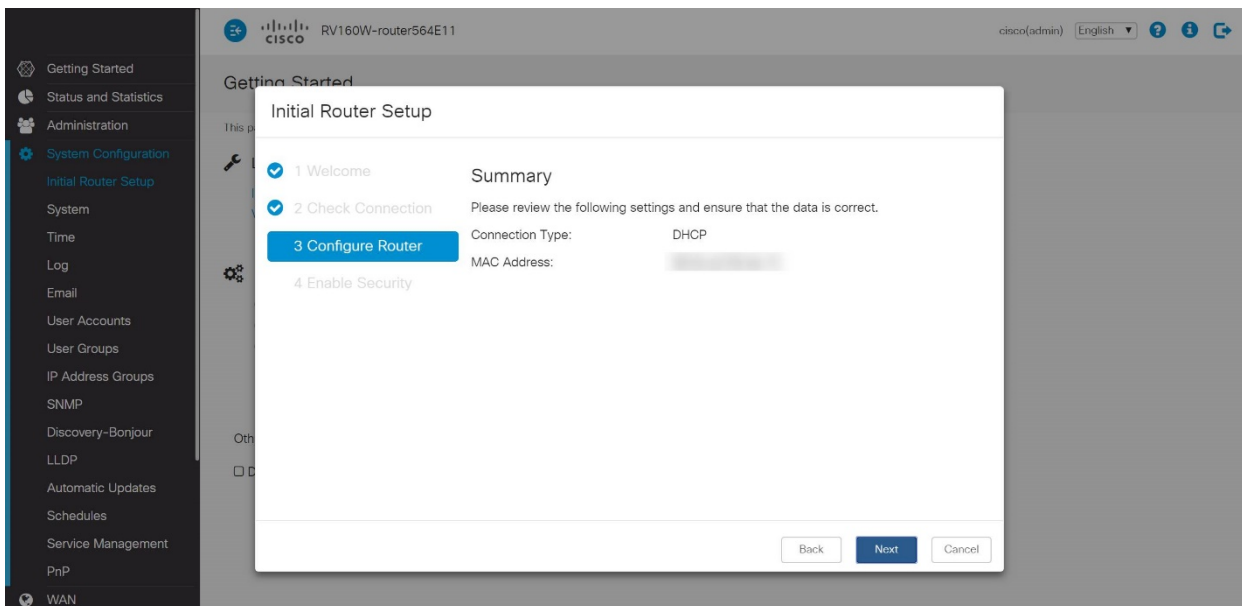
Schritt 6

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



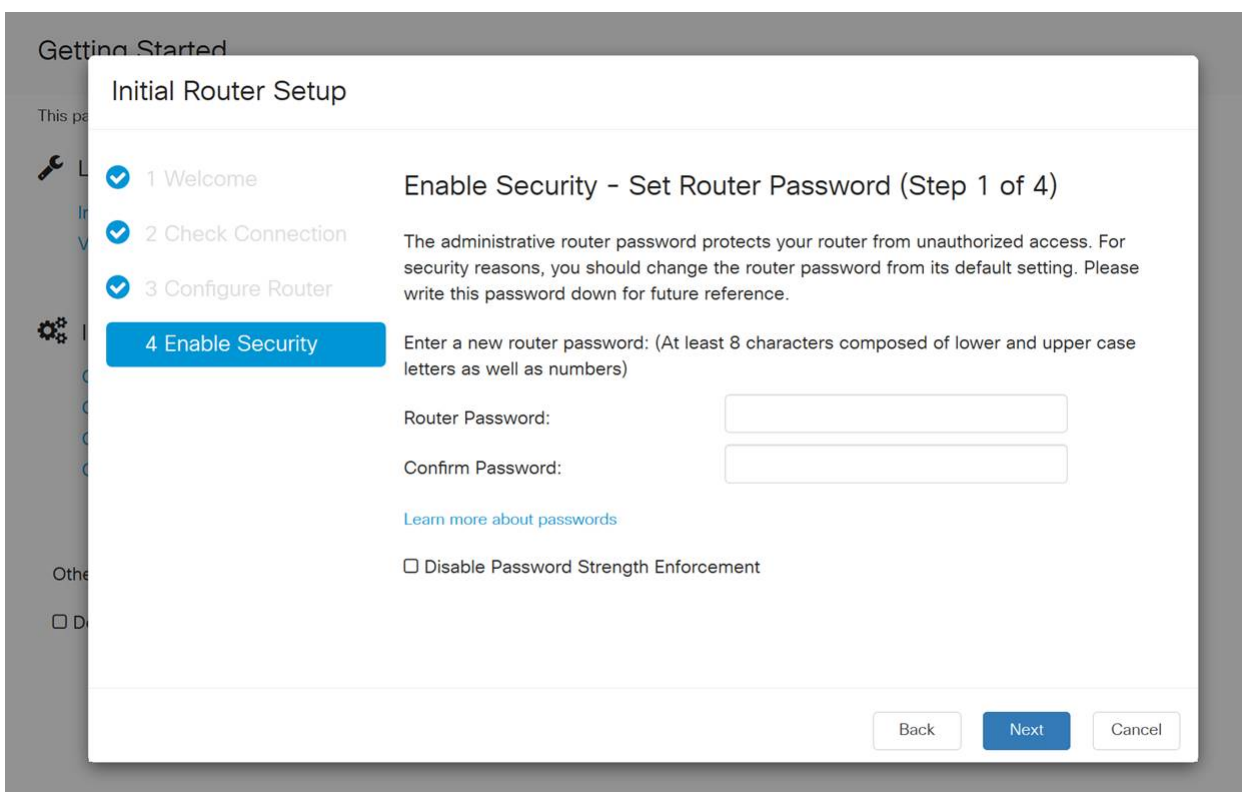
Schritt 7

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) und Zahlen enthalten. **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 **Symbol Speichern**.

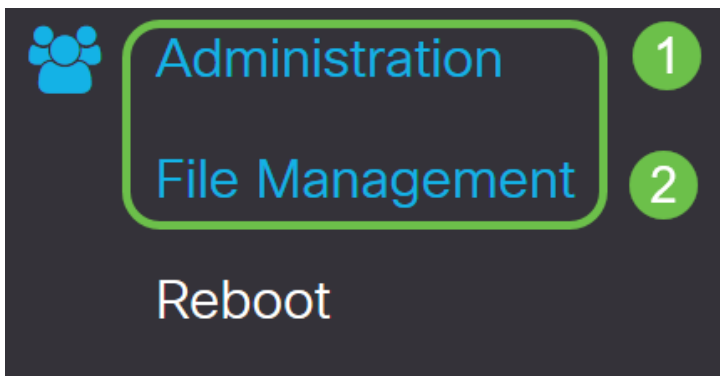


Firmware aktualisieren, falls erforderlich

Das ist wichtig, überspringen Sie es nicht!

Schritt 1

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



Im Bereich *Systeminformationen* beschreiben die folgenden Unterbereiche Folgendes:

- **Gerätmodell:** Zeigt das Gerätmodell 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.

File Management

System Information


Device Model:	RV260P
PID VID:	RV260P-K9 V01
Current Firmware Version:	1.0.00.15
Latest Version Available on Cisco.com:	-
Firmware Last Updated:	2019-Apr-17, 18:28:12

Schritt 2

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

Manual Upgrade

File Type: Firmware Image Language File USB Dongle Driver

Upgrade From: cisco.com PC USB 

Firmware Image Format: *.img (Maximum size: 100MB)

No file is selected

Reset all configurations/settings to factory defaults


The device will be automatically rebooted after the upgrade is complete.

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.

Manual Upgrade

File Type: Firmware Image Language File USB Dongle Driver

Upgrade From: cisco.com PC USB 

Reset all configurations/settings to factory defaults


The device will be automatically rebooted after the upgrade is complete.

Schritt 4

Klicken Sie auf **Upgrade**.

Manual Upgrade

File Type: Firmware Image Language File USB Dongle Driver

Upgrade From: cisco.com PC USB 

Reset all configurations/settings to factory defaults

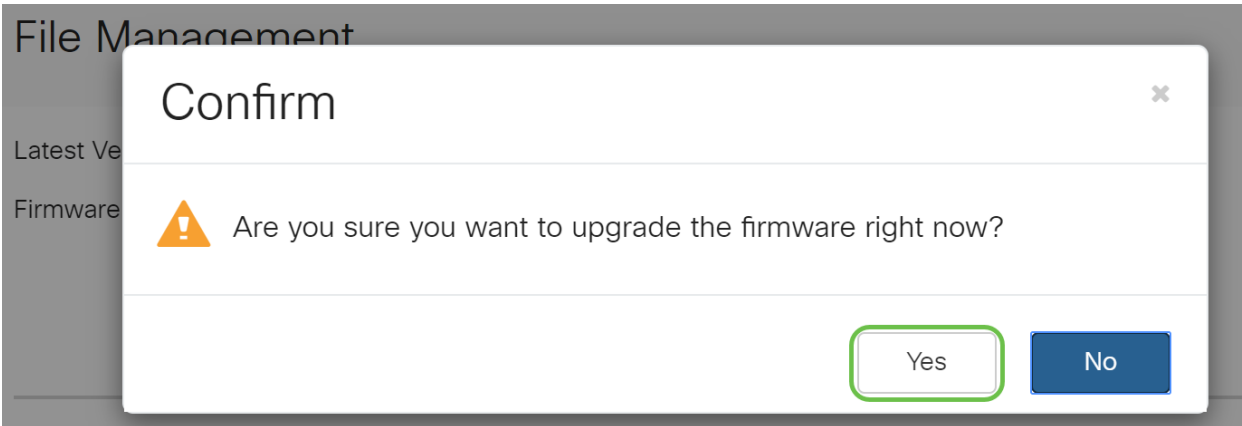
Upgrade

The device will be automatically rebooted after the upgrade is complete.

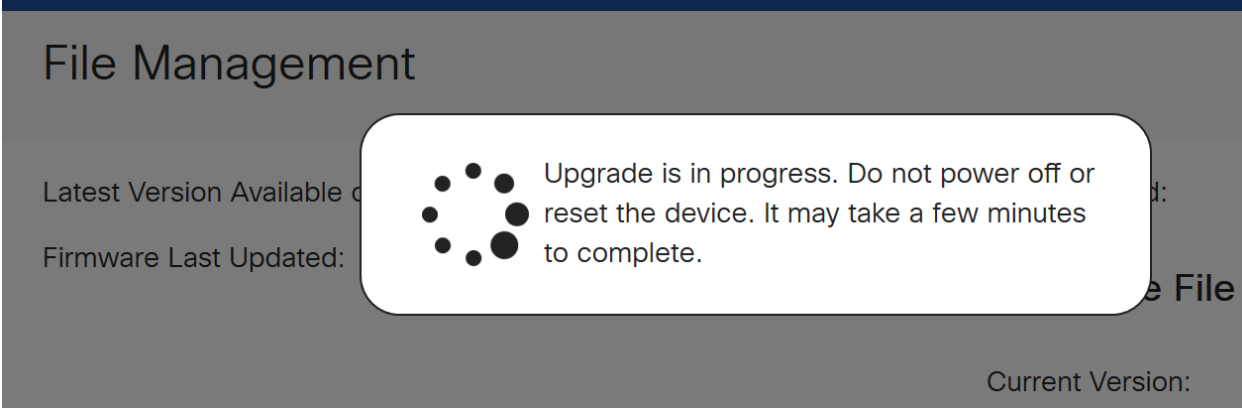
Download to USB

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.

File Management

Latest Version Available

Firmware Last Updated



Restarting

Please wait for 176 seconds...

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.

File Management

System Information

Device Model:	RV260P
PID VID:	RV260P-K9 V01
Current Firmware Version:	1.0.00.15
Latest Version Available on Cisco.com:	-
Firmware Last Updated:	2019-Apr-17, 18:28:12

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

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

- [Virtual Local Area Networks \(VLANs\)](#)
- [IP-Adresse bearbeiten](#)
- [statische IP-Adressen hinzufügen](#)
- [Ich kann den Mesh Wireless-Teil meines Netzwerks konfigurieren.](#)

VLANs konfigurieren (optional)

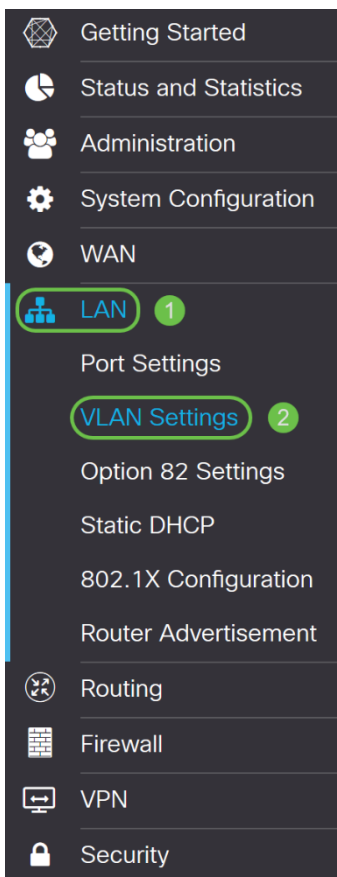
Mit einem Virtual Local Area Network (VLAN) können Sie ein Local Area Network (LAN) logisch in verschiedene Broadcast-Domänen segmentieren. In Umgebungen, in

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.

VLAN Settings

Create new VLANs



<input type="checkbox"/>	VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149

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.

VLAN Settings

Create new VLANs



<input type="checkbox"/>	VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input type="checkbox"/>	200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

Schritt 4

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

RV160W-router564F71

VLAN Settings

Create new VLANs

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
200	Engineering	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

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.

RV160W-router564F71

VLAN Settings

Create new VLANs

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

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**.

The screenshot shows the 'VLAN Settings' page for a Cisco RV160W router. It features a table of existing VLANs and a configuration form for a new VLAN. The new VLAN is named 'Engineering' with ID 200. The IP Address is 192.168.2.1 and the Subnet Mask is 255.255.255.0. The DHCP Type is set to 'Server'.

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
1	Default	Enabled	Enabled	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
200	Engineering	<input type="checkbox"/>	<input type="checkbox"/>	IP Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input checked="" type="radio"/> Server Lease Time: 1440 min. Range Start: 192.168.2.100 Range End: 192.168.2.149 DNS Server: Use DNS Proxy WINS Server:

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.

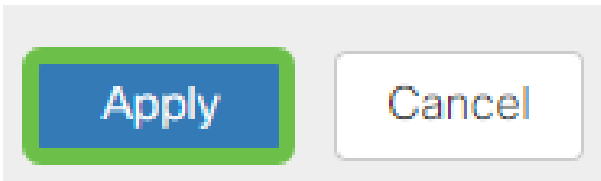
Server: Dies ist die am häufigsten verwendete Option.

- 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 - Wählen Sie aus der Dropdown-Liste aus, um einen DNS-Server als Proxy oder einen ISP 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.

The screenshot shows the top part of the 'VLAN Settings' page, including the 'Create new VLANs' section and the beginning of the table.

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.

Assign VLANs to ports

<input type="checkbox"/>	VLAN ID	LAN1	LAN2
<input checked="" type="checkbox"/>	1	Untagged	Excluded
<input checked="" type="checkbox"/>	200	Excluded	Untagged

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.

Assign VLANs to ports

<input type="checkbox"/>	VLAN ID	LAN1	LAN2
<input checked="" type="checkbox"/>	1	Untagged	Excluded
<input checked="" type="checkbox"/>	200	Excluded	Untagged

Schritt 11

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

Apply

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.

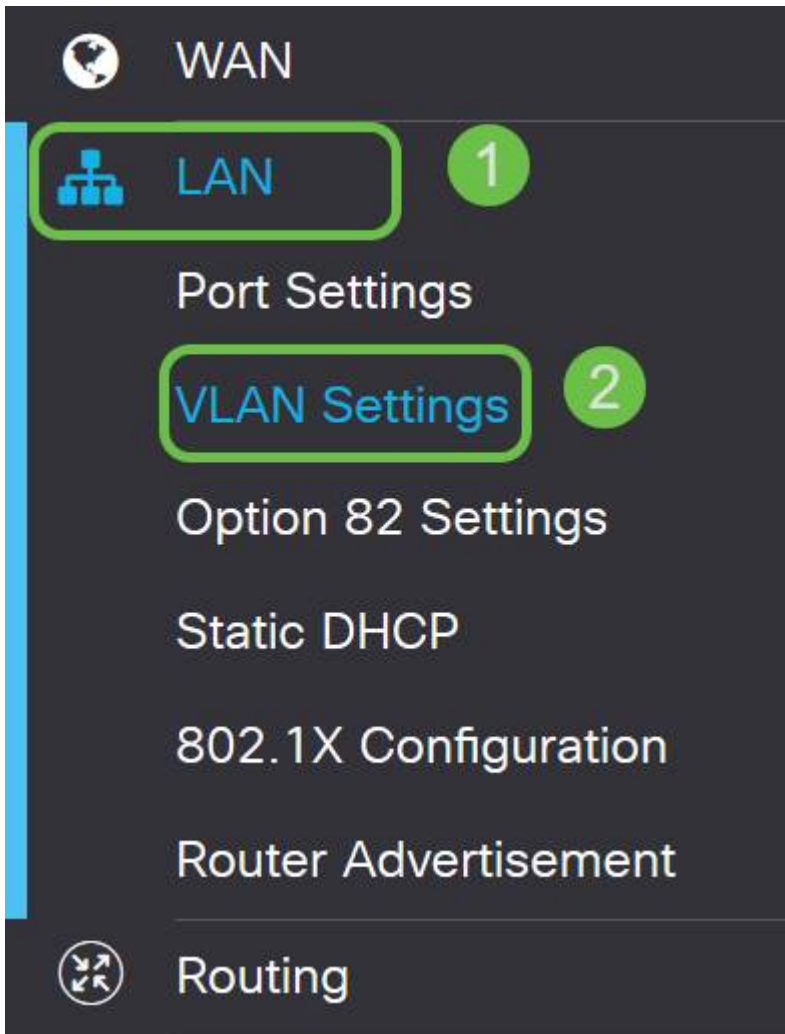
IP-Adresse bearbeiten (optional)

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 die **LAN**-Schaltfläche und klicken Sie dann auf **VLAN Settings**.



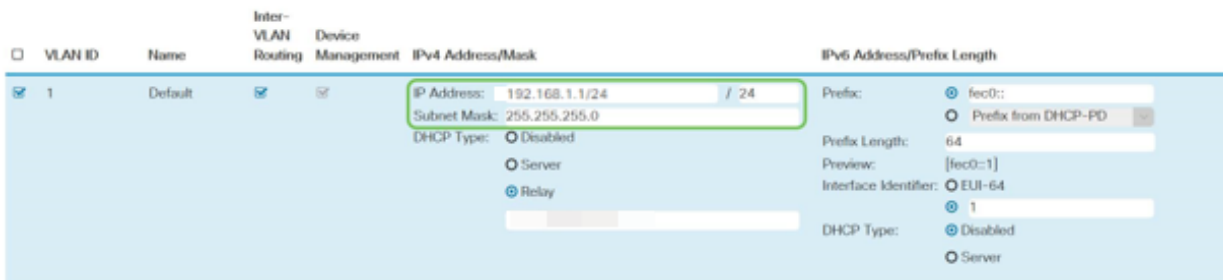
Schritt 2

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



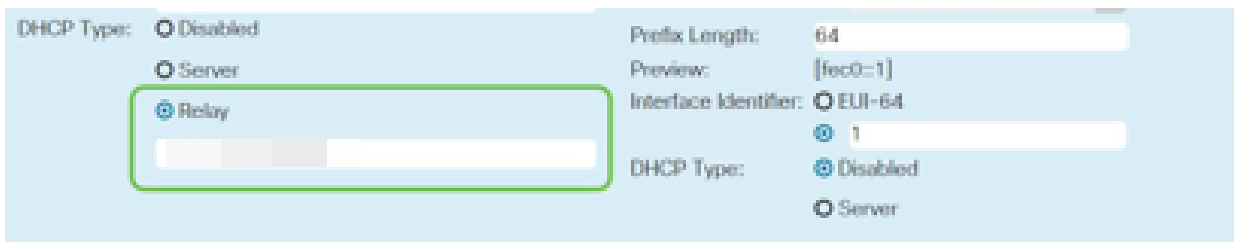
Schritt 3

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.



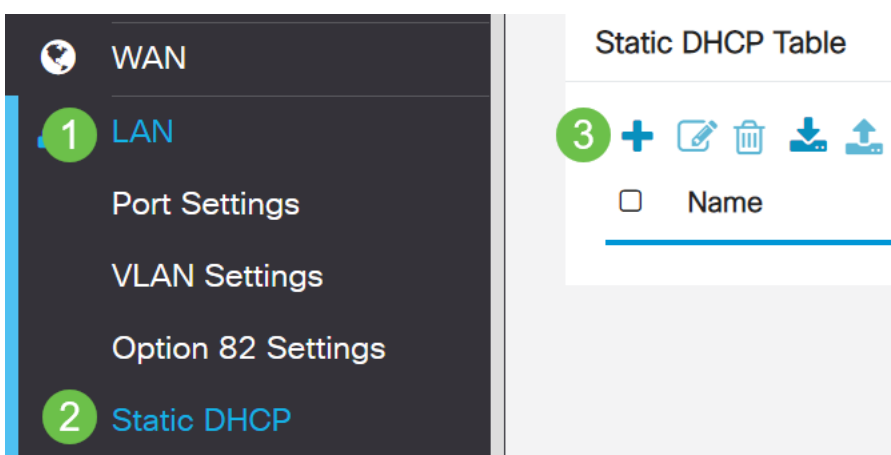
Hinzufügen einer statischen IP (optional)

Wenn Sie möchten, dass ein bestimmtes Gerät für andere VLANs erreichbar ist, können Sie diesem Gerät eine statische IP-Adresse zuweisen und eine Zugriffsregel erstellen, um darauf zuzugreifen. Dies funktioniert nur, wenn Inter-VLAN-Routing aktiviert ist.

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

Schritt 1

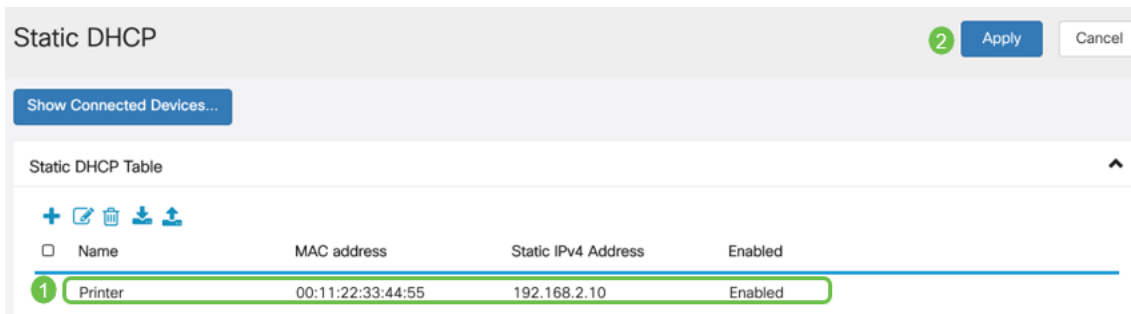
Navigieren Sie zu **LAN > Static DHCP (LAN > Static DHCP)**. Klicken Sie auf das **Pluszeichen**.



Schritt 2

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

ist das Gerät ein Drucker.



Weitere Informationen zum Einstellen statischer IP-Adressen finden Sie in den [Best Practices zum Einstellen statischer IP-Adressen auf Cisco Business Hardware](#).

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 den Routern RV160 und RV260](#).

Richten Sie den Wireless Access Point für mobile 140AC-Anwendungen ein.

In diesem Abschnitt richten Sie den Wireless Access Point für mobile Anwendungen ein.

Beachten Sie, dass die Anwendung häufig aktualisiert wird und sich das Aussehen/Layout im Laufe der Zeit ändern kann.

Stecken Sie das mitgelieferte Kabel auf der Rückseite des 140AC in den gelben PoE-Stecker Ihres 140 AC-Kabels. Schließen Sie das andere Ende an einen der RV260P-LAN-Ports an.

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

Schritt 1

Laden Sie die Cisco Business Wireless-App auf [Google Play](#) oder den [Apple App Store](#) auf Ihr Mobilgerät herunter. Sie benötigen eines der folgenden Betriebssysteme:

- Android Version 5.0 oder höher
- iOS Version 8.0 oder höher

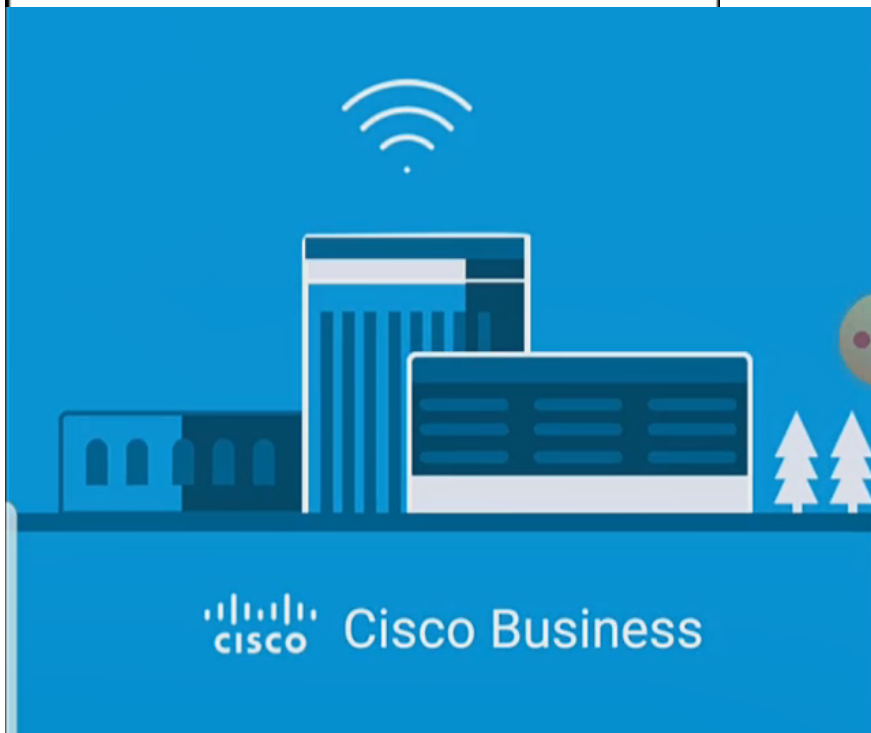
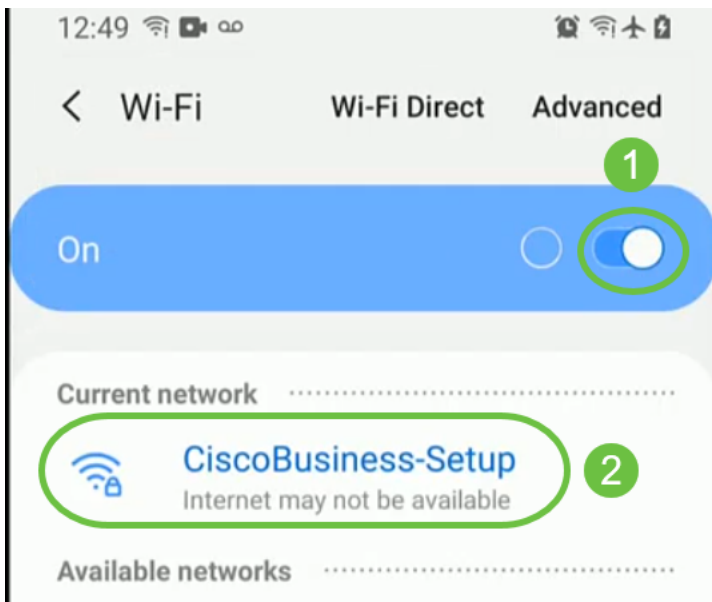
Schritt 2

Öffnen Sie die **Cisco Business Wireless**-Anwendung auf Ihrem Mobilgerät.



Schritt 3

Stellen Sie eine Verbindung zum **CiscoBusiness-Setup-Wireless-Netzwerk** auf Ihrem Mobilgerät her. Die Passphrase ist **cisco123**.



Schritt 4

Die App erkennt automatisch das mobile Netzwerk. Wählen Sie **Netzwerk einrichten aus**.



Monitor My Network



Set up My Network



Enter the name of the Primary AP / IP

Discovered Primary

Schritt 5

Um das Netzwerk einzurichten, geben Sie Folgendes ein:

- *Administratorbenutzername erstellen*
- *Administratorkennwort erstellen*
- *Administratorkennwort bestätigen*, indem Sie es erneut eingeben
- (Optional) Aktivieren Sie das Kontrollkästchen *Kennwort anzeigen*.

Wählen Sie **Erste Schritte aus**.




1 Name and Place




Primary AP Name

1 TestAP


Country

2 United States (US) 

Date and Time

3 04/09/2021 05:05:37 PM 

Timezone

4 Central Time (US and Canada) 



Mesh

Schritt 6

Um *Name und Ort* zu konfigurieren, geben Sie die folgenden Informationen präzise ein. Wenn Sie widersprüchliche Informationen eingeben, kann dies zu unvorhersehbarem Verhalten führen.

- *AP-Name* für *mobile Anwendungen* für Ihr Wireless-Netzwerk
- *Land*
- *Datum*
- *Zeit*
- *Zeitzone*

← Cisco Business Wireless 140AC Access Point

1 Name and Place ?

Primary AP Name

1 TestAP

Country

2 United States (US) ▼

Date and Time

3 04/09/2021 05:05:37 PM ▼

Timezone

4 Central Time (US and Canada) ▼

Mesh

Previous

Next

Schritt 7

Schalten Sie den Umschalter für *Mesh ein*. Klicken Sie auf **Weiter**.



1

Name and Place



Primary AP Name

TestAP

Country

United States (US)



Date and Time

04/09/2021 05:05:37 PM



Timezone

Central Time (US and Canada)



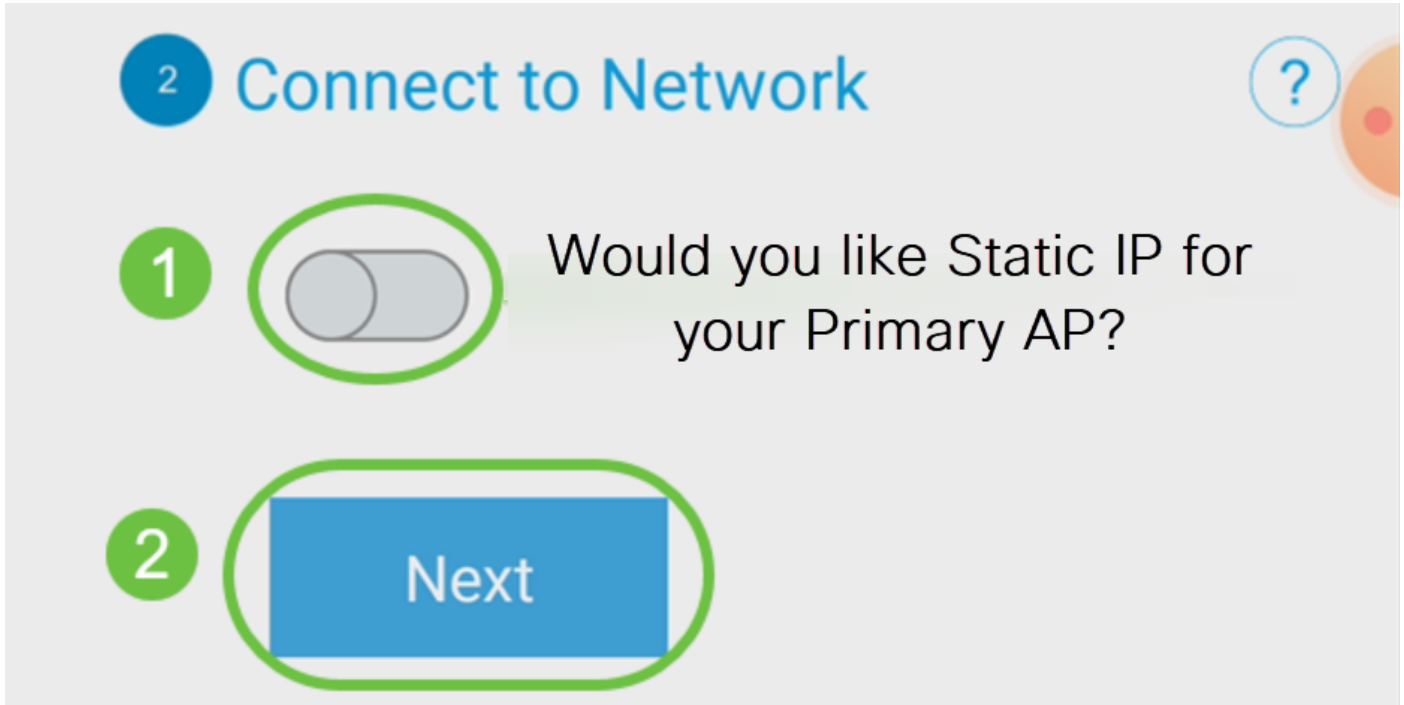
1



Mesh

Schritt 8

(Optional) Sie können die *statische IP-Adresse für Ihren mobilen Anwendungs-AP* zu Verwaltungszwecken aktivieren. Andernfalls weist der DHCP-Server eine IP-Adresse zu. Wenn Sie keine statische IP-Adresse für den Access Point konfigurieren möchten, klicken Sie auf **Weiter**.



Alternativ zum *Herstellen einer Netzwerkverbindung*:

Wählen Sie *Static IP (Statische IP) für Ihren AP für mobile Anwendungen* aus. Standardmäßig ist diese Option **deaktiviert**.

- Geben Sie die *Management-IP-Adresse* ein.
- *Subnetzmaske*
- *Standard-Gateway*

Klicken Sie auf **Speichern**.

2

Connect to Network

?

1



Would you like Static IP for your Primary AP?

MANAGEMENT IP ADDRESS

0.0.0.0

2

SUBNET MASK

0.0.0.0

3

DEFAULT GATEWAY

0.0.0.0

4

Save

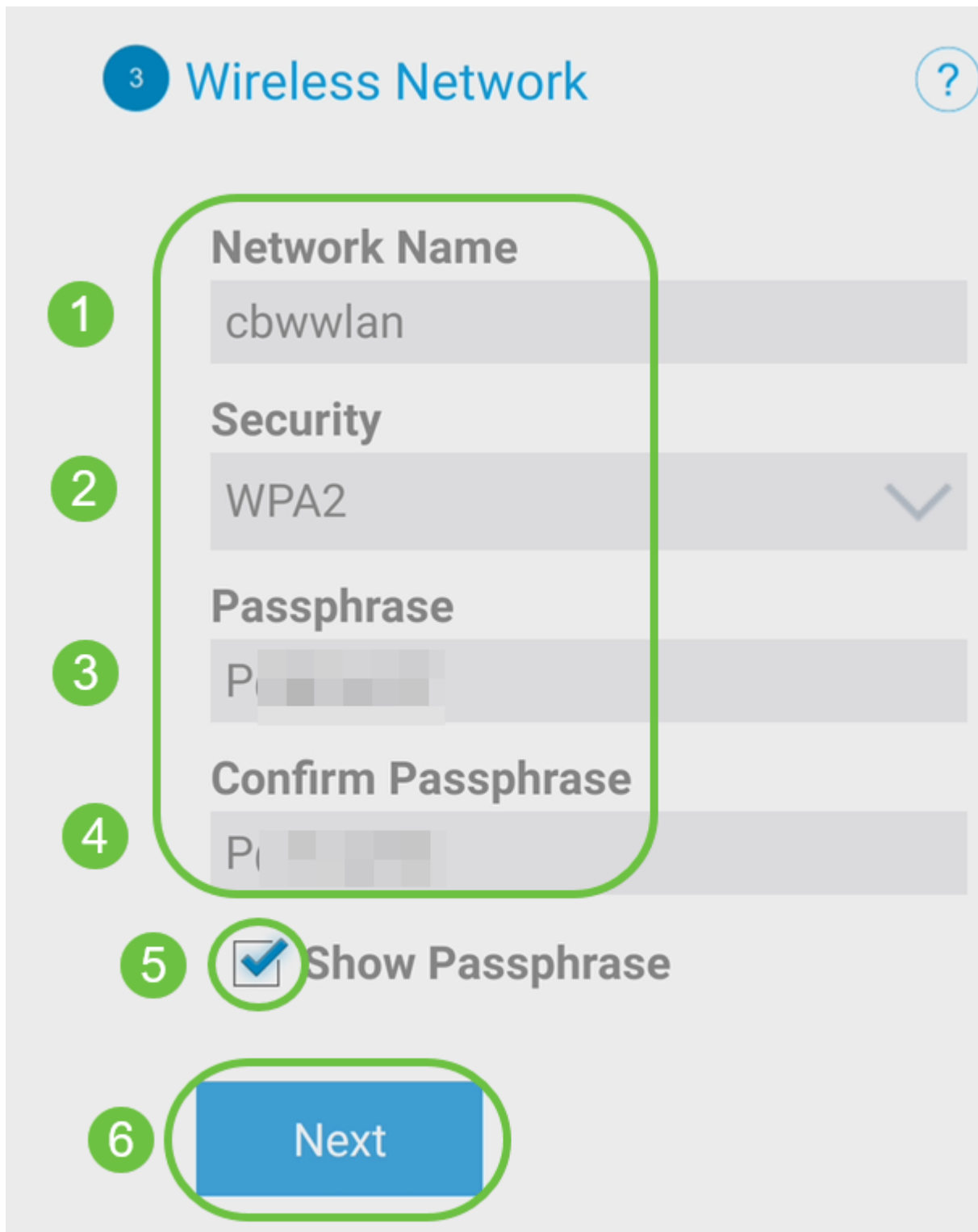
5

Schritt 9

Konfigurieren Sie das *Wireless-Netzwerk*, indem Sie Folgendes eingeben:

- *Netzwerkname/SSID*
- *Sicherheit*
- *Passphrase*
- *Passphrase bestätigen*
- (Optional) *Aktivieren Sie Passphrase anzeigen*

Klicken Sie auf **Weiter**.



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

Schritt 10

Um die Einstellungen im Bildschirm "An AP für mobile Anwendungen senden" zu bestätigen, klicken Sie auf **Senden**.



Cisco Business Wireless 140AC Access Point

- ✓ 1 Name and Place Edit ?
- ✓ 2 Connect to Network Edit ?
- ✓ 3 Wireless Network Edit ?
- 4 Submit to Primary AP

You have done all the configurations, please submit to Primary AP.

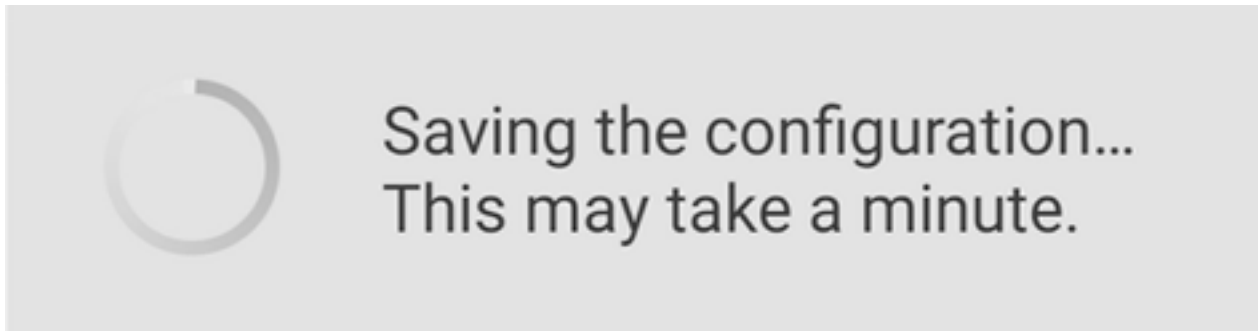
Note: After initial setup and reboot, the Primary AP needs to be connected to a DHCP server even if the management IP address was set to static (access point functionality and client connections use dynamically assigned

[Previous](#)

[Submit](#)

Schritt 11

Warten Sie, bis der Neustart abgeschlossen ist.



Der Neustart kann bis zu 10 Minuten dauern. Während eines 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 12

Sie sehen den folgenden Bildschirm *zur Bestätigung*. Klicken Sie auf **OK**.

Confirmation

The Primary AP has been fully configured and will restart in 6 minutes. After the Primary AP is restarted, it will be accessible from the network by going to this URL - <https://ciscobusiness.cisco> via browser or using Discovered Primary list in Cisco Business Mobile Application provided client should be connected to configured ' TestAP ' SSID.



Schritt 13

Schließen Sie die App, stellen Sie eine Verbindung zu Ihrem neu erstellten Wireless-Netzwerk her, und starten Sie sie neu, um den ersten Teil Ihres Wireless-Netzwerks erfolgreich abzuschließen.

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. Dies muss deaktiviert werden, um den Access Point für mobile Anwendungen zu finden.

- Melden Sie sich mit `https://<IP-Adresse des AP für mobile Anwendungen>` beim Access Point für mobile Anwendungen 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*.

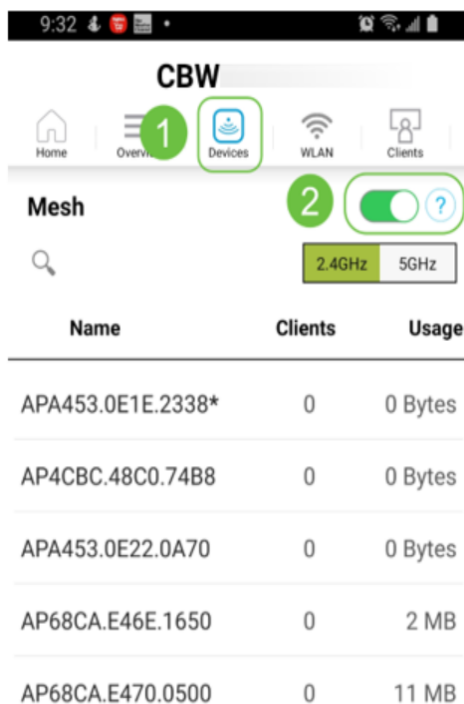
Konfigurieren der CBW142ACM-Mesh-Extender

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

Melden Sie sich bei der Cisco Business-App auf Ihrem Mobilgerät an.

Schritt 1

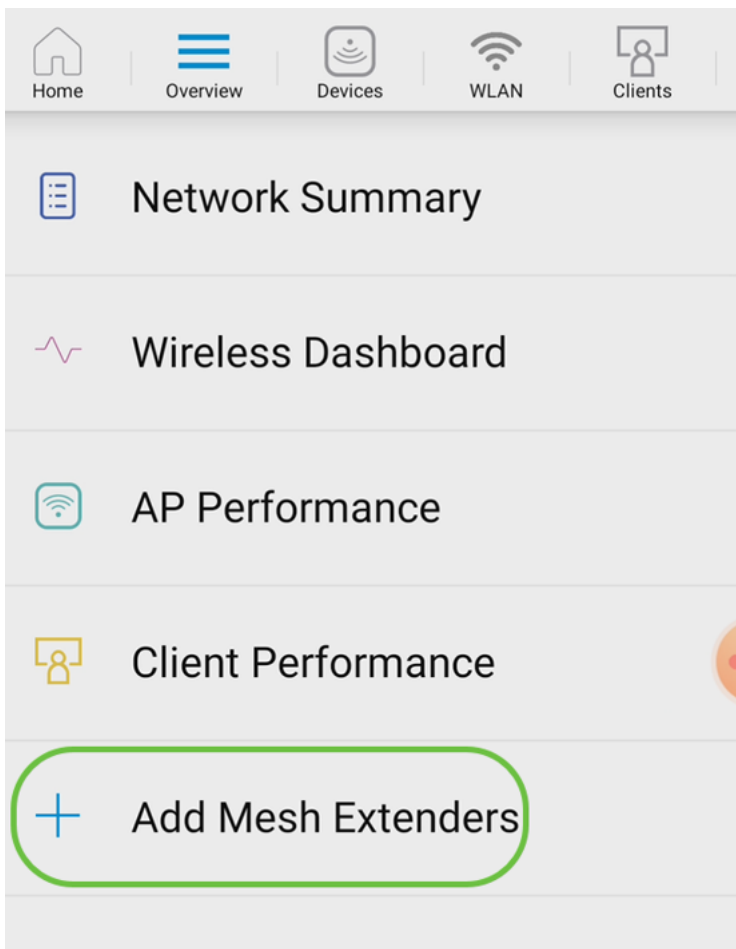
Navigieren Sie zu **Geräte**. Überprüfen Sie, ob *Mesh* aktiviert ist.



Schritt 2

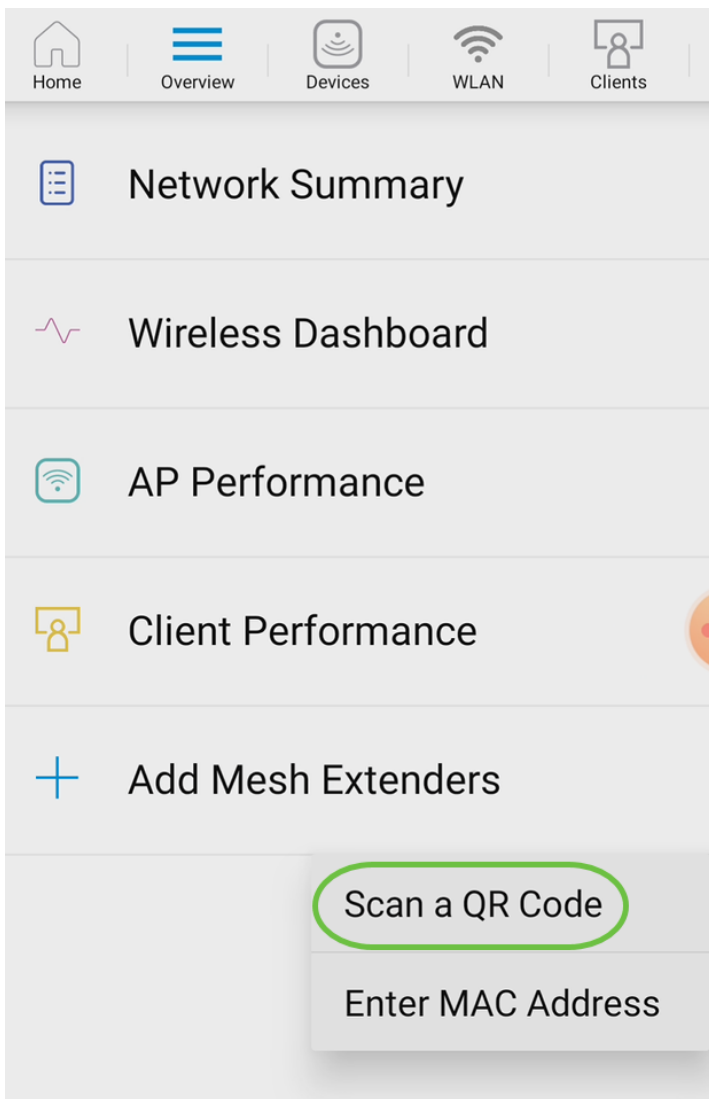
Sie müssen die MAC-Adresse aller Mesh Extenders eingeben, die Sie im Mesh-

Netzwerk mit dem Mobile Application AP verwenden möchten. Um die MAC-Adresse hinzuzufügen, klicken Sie im Menü auf **Add Mesh Extenders (Mesh-Extender hinzufügen)**.



Schritt 3

Sie können die MAC-Adresse entweder durch Scannen eines QR-Codes oder durch manuelle Eingabe der MAC-Adresse hinzufügen. In diesem Beispiel ist **Scannen eines QR-Codes** aktiviert.

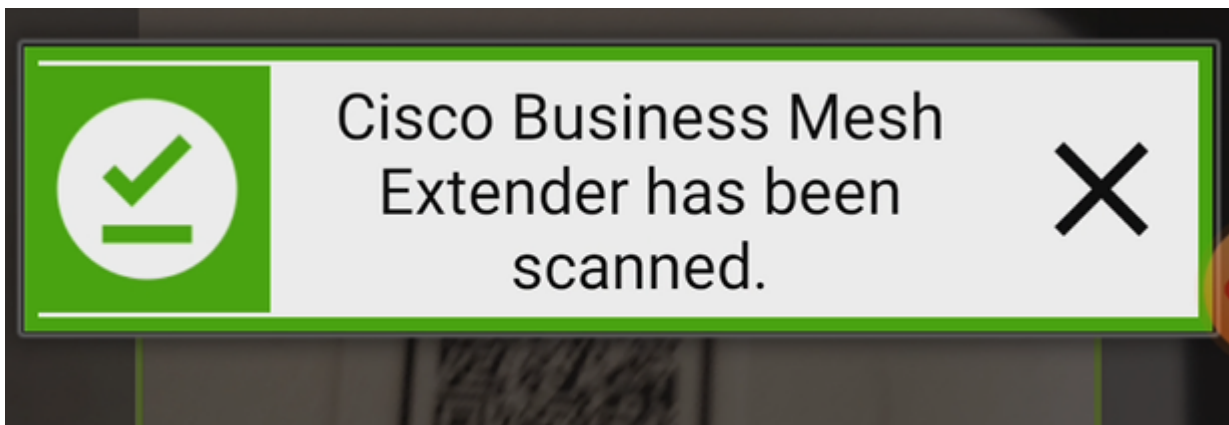


Schritt 4

Ein QR-Code-Reader wird angezeigt, um den QR-Code zu scannen.

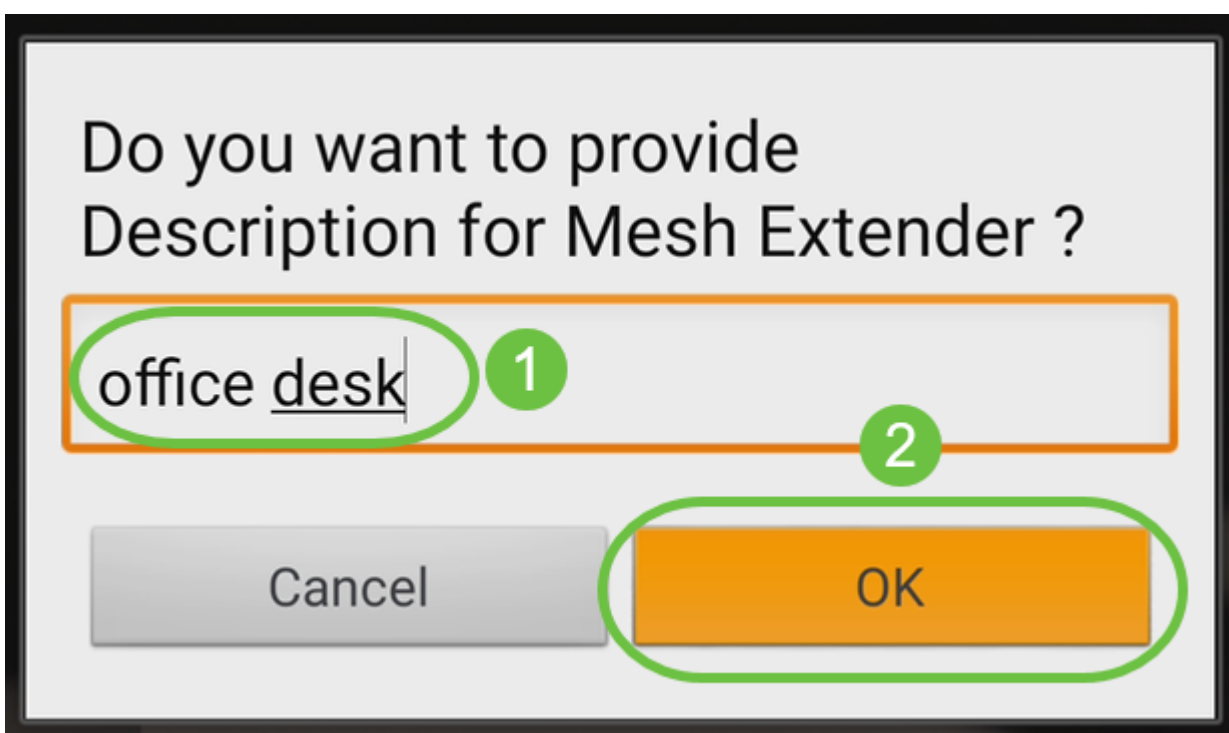


Sobald der QR-Code des Mesh Extender gescannt wurde, wird der folgende Bildschirm angezeigt.



Schritt 5 (optional)

Wenn Sie es vorziehen, geben Sie eine *Beschreibung für Mesh Extender ein*. Klicken Sie auf **OK**.



Schritt 6

Überprüfen Sie die *Zusammenfassung*, und klicken Sie auf **Senden**.

Summary

Almost done. The following Mesh Extenders will be added to your site. If you are done adding Mesh Extenders, click submit.

> Mesh Extenders To Be Added

Scanned MAC Address

A4 [redacted] 0

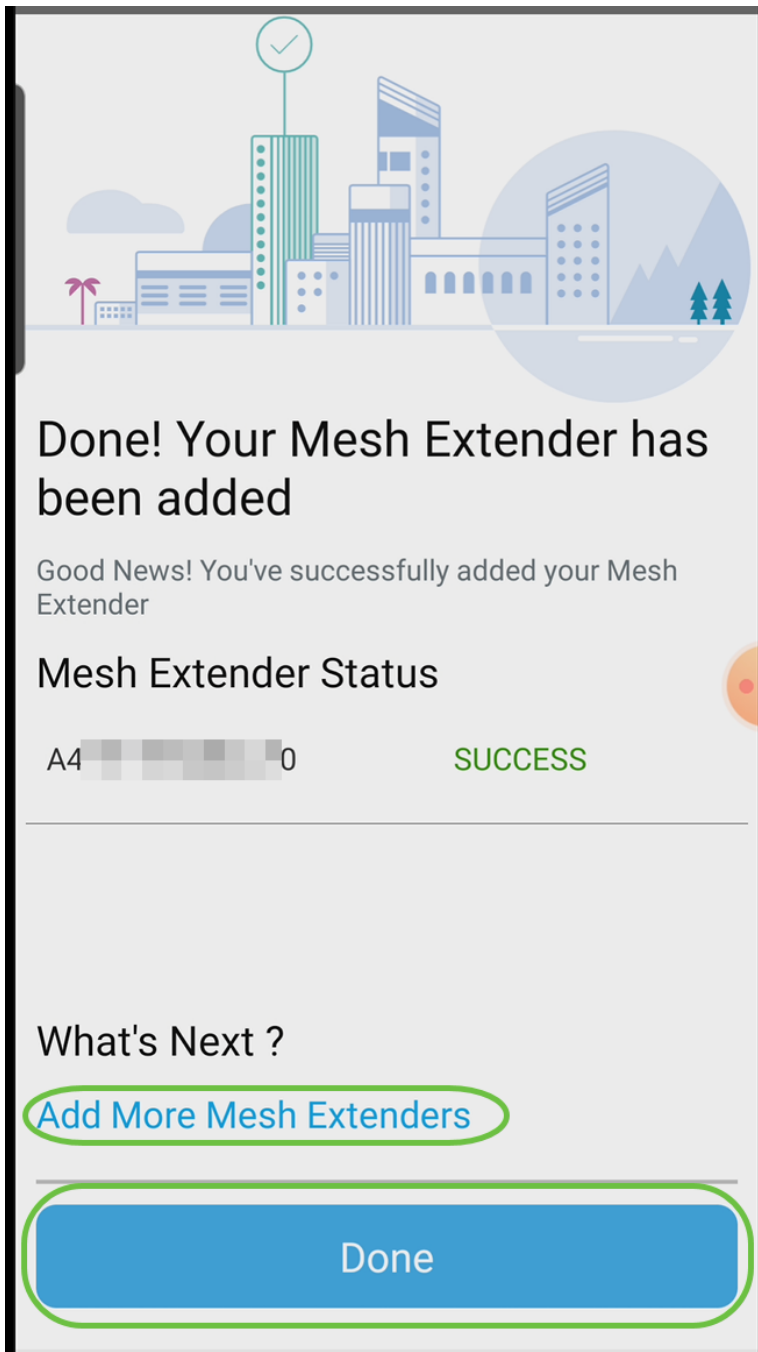
office desk



Submit

Schritt 7

Klicken Sie auf *Add More Mesh Extenders (Mehr Mesh-Extender hinzufügen)*, um weitere Mesh-Extender zum Netzwerk hinzuzufügen. Wenn alle Mesh-Extender hinzugefügt wurden, klicken Sie auf **Fertig**.



Wiederholen Sie diese Schritte für jeden Mesh-Extender.

Sie haben jetzt die Grundeinstellungen bereit zum Rollen. Bevor Sie fortfahren, überprüfen Sie, ob Sie die Software ggf. überprüfen und aktualisieren.

Überprüfen und Aktualisieren der Software auf der mobilen App

Die Aktualisierung der Software ist äußerst wichtig, überspringen Sie diesen Teil nicht!

Schritt 1

Klicken Sie auf Ihrer mobilen App unter der Registerkarte **More (Mehr)** auf die Schaltfläche **Check for update (Nach Aktualisierung suchen)**. Folgen Sie den Anweisungen, um die Software auf die neueste Version zu aktualisieren.



System Information



SYSTEM NAME:



1

Model

CBW140AC-B

Serial Number

FGL2419LCQN

2

Software Version

10.3.1.0

Check for update

Schritt 2

Der Download-Fortschritt wird beim Laden angezeigt.



Software Update


The upgrade has been initiated. When the Primary AP reboots, the app will be disconnected.

AP Name

Download Progress

*AP6C71.0D55.73C4

24%



AP6C71.0D55.5DA4

21%



Schritt 3

Eine Popup-Bestätigung benachrichtigt Sie über den Abschluss des Software-Upgrades. Klicken Sie auf **OK**.

Erstellen von WLANs mithilfe der mobilen App

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

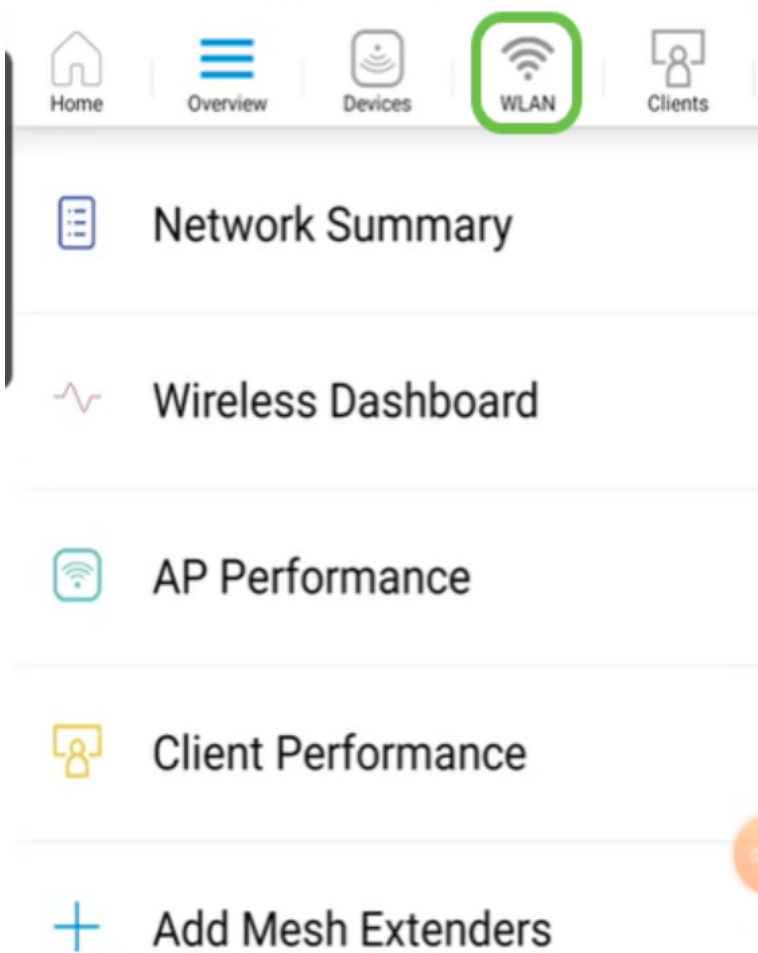
Schritt 1

Öffnen Sie die Cisco Business Wireless-App. _



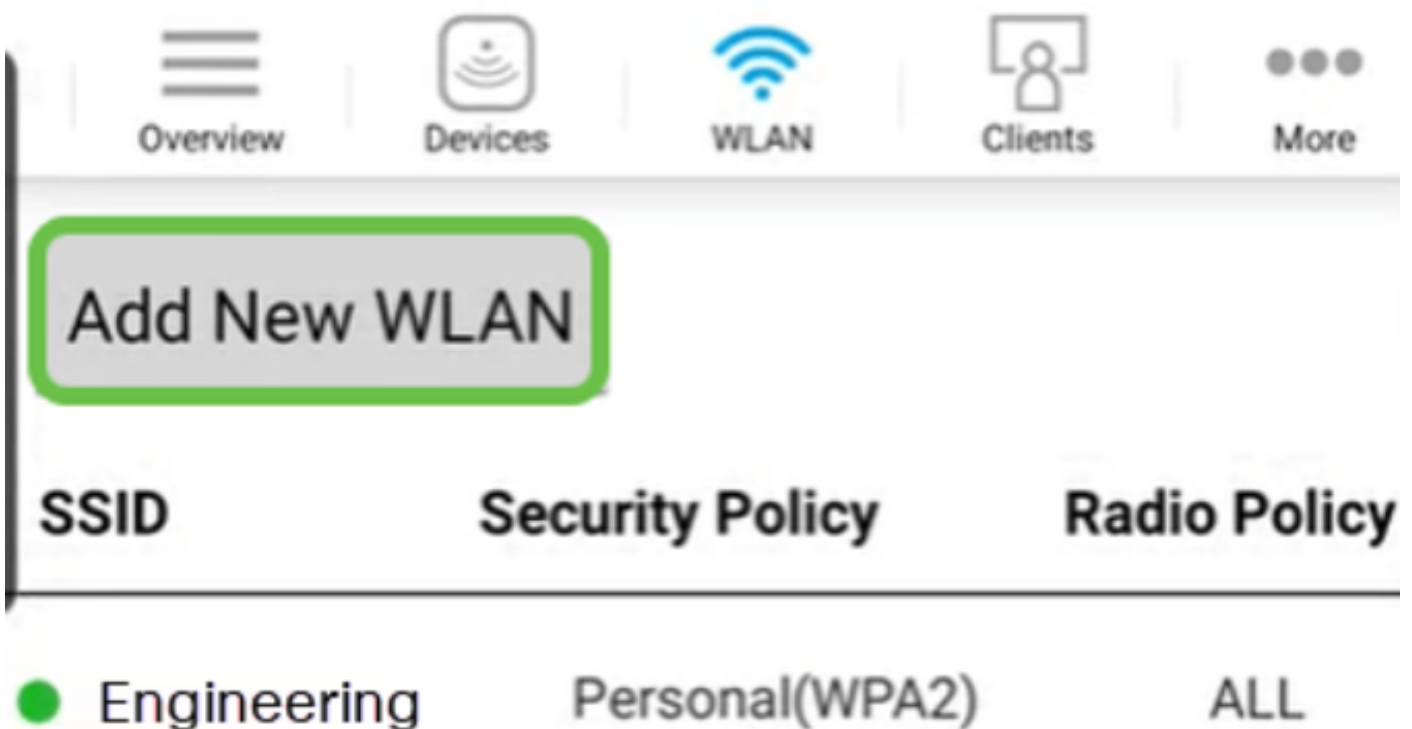
Schritt 2

Stellen Sie über Ihr Mobiltelefon eine Verbindung zu Ihrem Cisco Business Wireless-Netzwerk her. Melden Sie sich bei der Anwendung an. Klicken Sie auf das **WLAN-Symbol** oben auf der Seite.



Schritt 3

Der Bildschirm *Neues WLAN hinzufügen* wird geöffnet. Sie sehen die vorhandenen WLANs. Wählen Sie **Neues WLAN hinzufügen** aus.



Schritt 4

Geben Sie einen **Profilnamen** und eine **SSID ein**. Füllen Sie die übrigen Felder aus, oder belassen Sie die Standardeinstellungen. Wenn Sie Application Visibility Control aktiviert haben, werden in Schritt 6 weitere Konfigurationen erläutert. Klicken Sie auf **Weiter**.

The screenshot shows the 'WLAN' configuration page in a mobile application. At the top, there is a navigation bar with a back arrow, the title 'WLAN', and several icons: Overview, Devices, WLAN (selected), Clients, and More. Below the navigation bar is a 'General' section header. The configuration fields are as follows:

- WLAN ID: 3
- Profile Name*: labnet (marked with a green circle '1')
- SSID*: labnet (marked with a green circle '2')
- Admin State: Enabled
- Radio Policy: ALL
- Broadcast SSID: ON (toggle switch)
- Client Profiling: ON (toggle switch)
- Application Visibility Control: OFF (toggle switch)

At the bottom of the form, there is a 'Next' button (marked with a green circle '3').

Schritt 5 (optional)

Wenn Sie *Application Visibility Control* in Schritt 4 aktiviert haben, können Sie andere Einstellungen konfigurieren, einschließlich eines Gastnetzwerks. Die Details dazu finden Sie im nächsten Abschnitt. Auch hier können Sie *Captive Network Assistant*, *Security Type (Sicherheitstyp)*, *Passphrase* und *Password Expiry* hinzufügen. Wenn Sie alle Konfigurationen hinzugefügt haben, klicken Sie auf **Weiter**.

The screenshot displays the 'WLAN' configuration page, specifically the 'Security' section. At the top, there is a navigation bar with icons for Overview, Devices, WLAN, Clients, and More. Below this, the 'Security' section contains several settings:

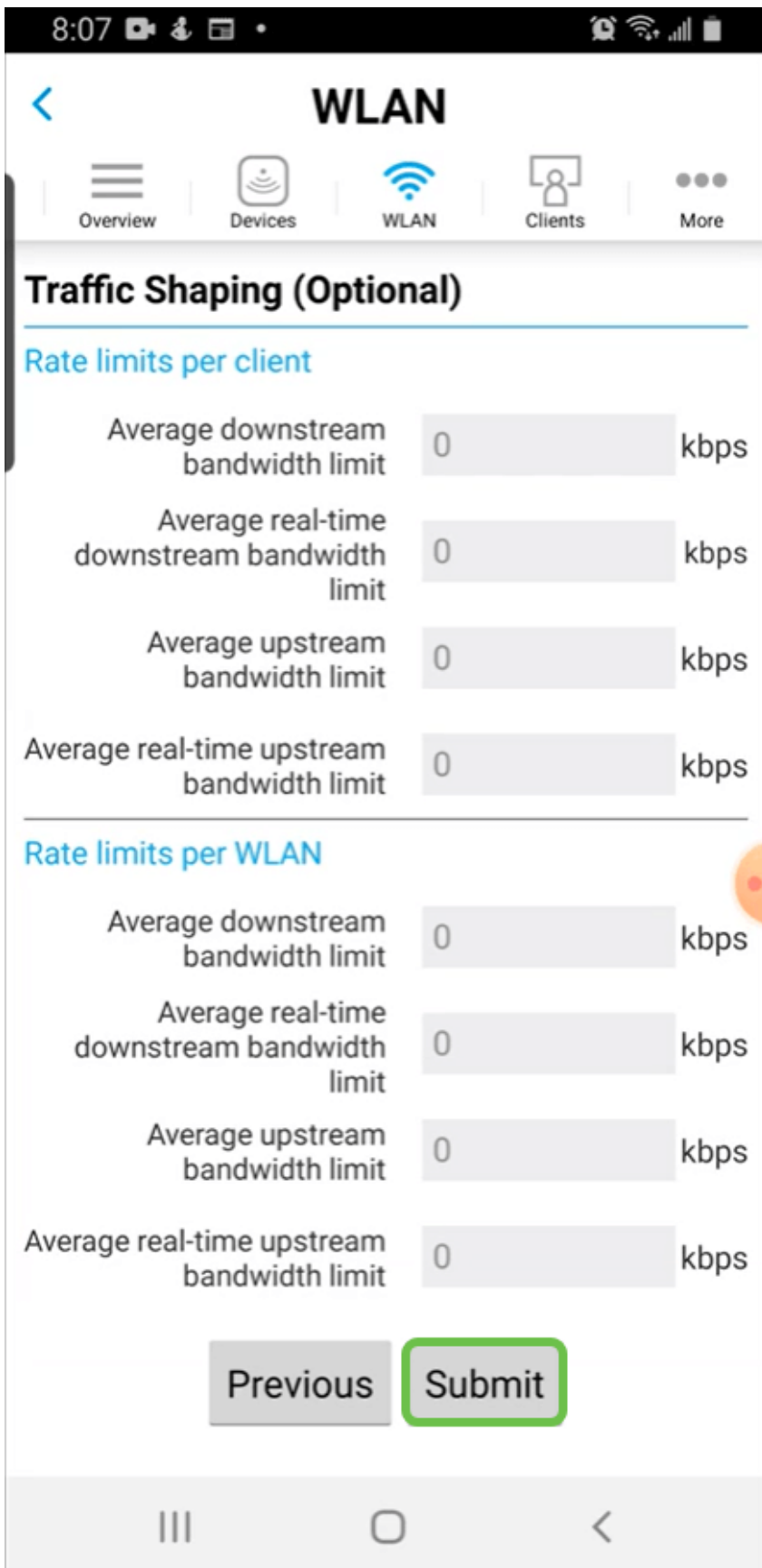
- Guest Network:** A toggle switch set to 'OFF'.
- Captive Network Assistant:** A toggle switch set to 'OFF'.
- Security Type:** A dropdown menu currently showing 'WPA2 Personal'.
- Passphrase Format:** A dropdown menu currently showing 'ASCII'.
- Passphrase*:** A text input field containing seven asterisks.
- Confirm Passphrase*:** A text input field containing seven asterisks.
- Show Passphrase:** A checkbox that is currently unchecked.
- Password Expiry:** A toggle switch set to 'OFF'.

At the bottom of the screen, there are two buttons: 'Previous' and 'Next'. The 'Next' button is highlighted with a green border, indicating it is the current step in the configuration process.

Bei Verwendung der mobilen Anwendung sind die einzigen Optionen für den *Sicherheitstyp* *Open* oder *WPA2 Personal*. Melden Sie sich für erweiterte Optionen stattdessen an der Webbenutzeroberfläche des AP für mobile Anwendungen an.

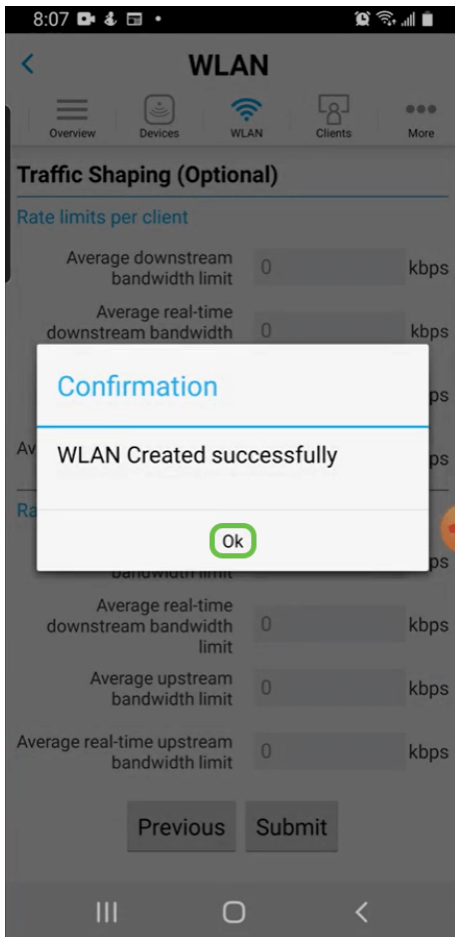
Schritt 6 (optional)

Auf diesem Bildschirm finden Sie die Optionen für *Traffic Shaping*. In diesem Beispiel wurde kein Traffic Shaping konfiguriert. Klicken Sie auf **Senden**.



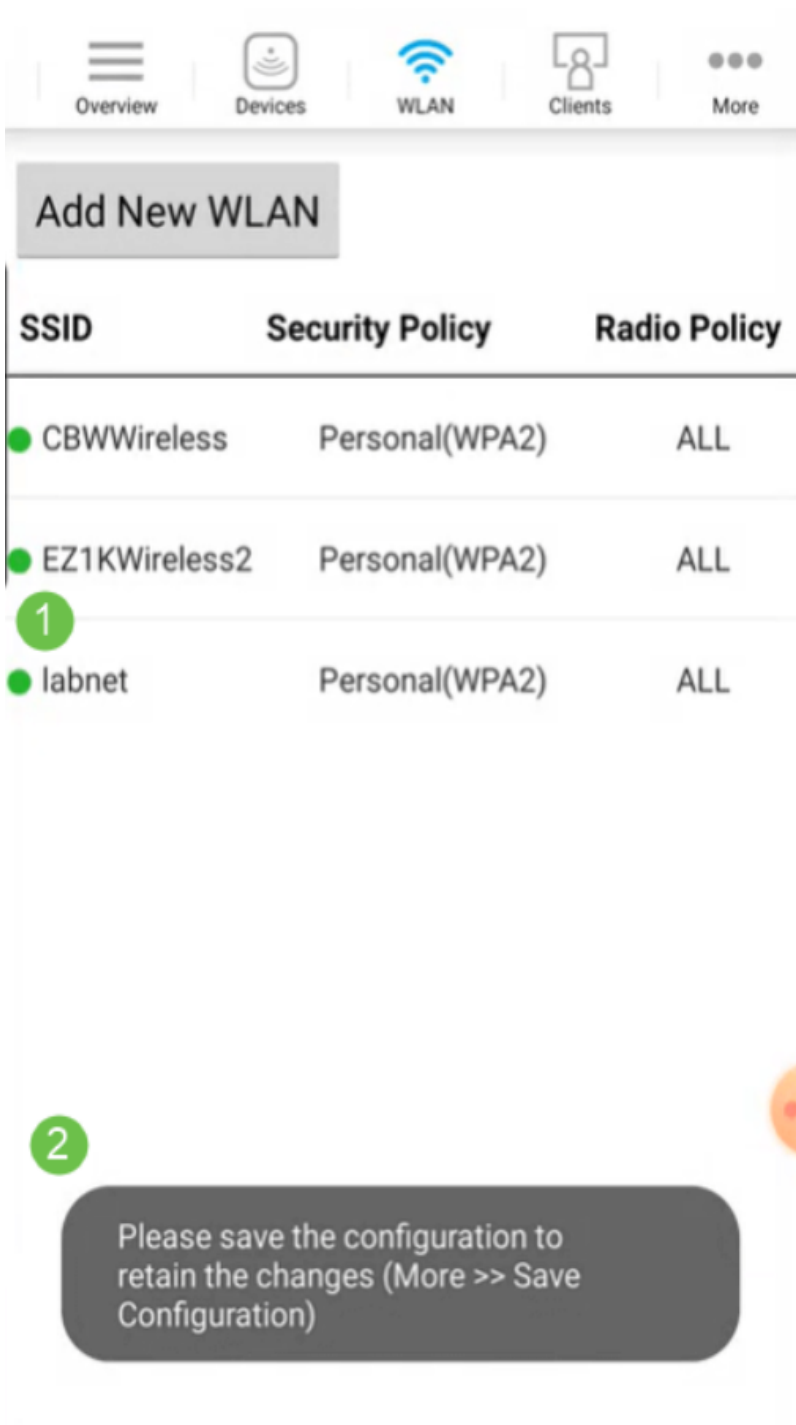
Schritt 7

Sie sehen ein Bestätigungs-Popup. Klicken Sie auf OK.



Schritt 8

Sie sehen das dem Netzwerk hinzugefügte neue WLAN sowie eine Erinnerung zum Speichern der Konfiguration.



Schritt 9

Speichern Sie Ihre Konfiguration, indem Sie auf die Registerkarte **More (Mehr)** klicken und dann im Dropdown-Menü **Save Configuration (Konfiguration speichern)** auswählen.



Erstellen eines Gast-WLAN mithilfe der mobilen App

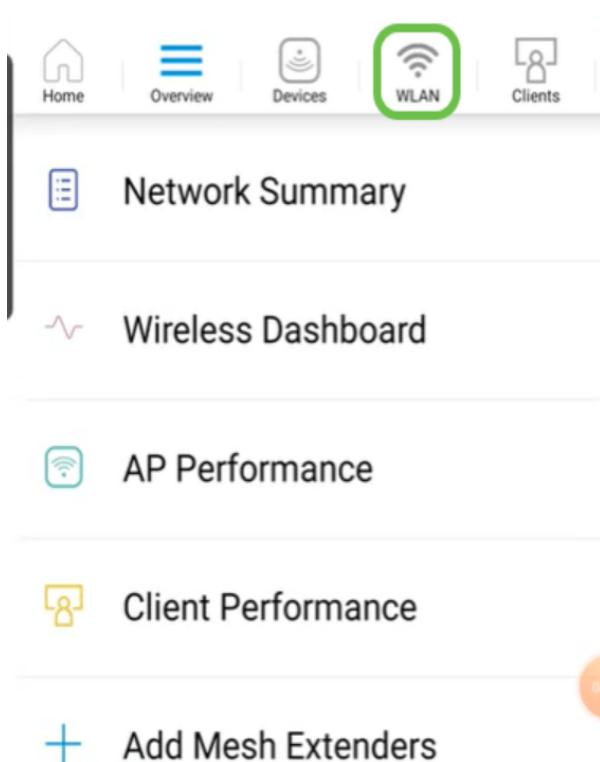
Schritt 1

Stellen Sie über Ihr Mobilgerät eine Verbindung zum Cisco Business Wireless-Netzwerk her. Melden Sie sich bei der Anwendung an.



Schritt 2

Klicken Sie auf das **WLAN-Symbol** oben auf der Seite.



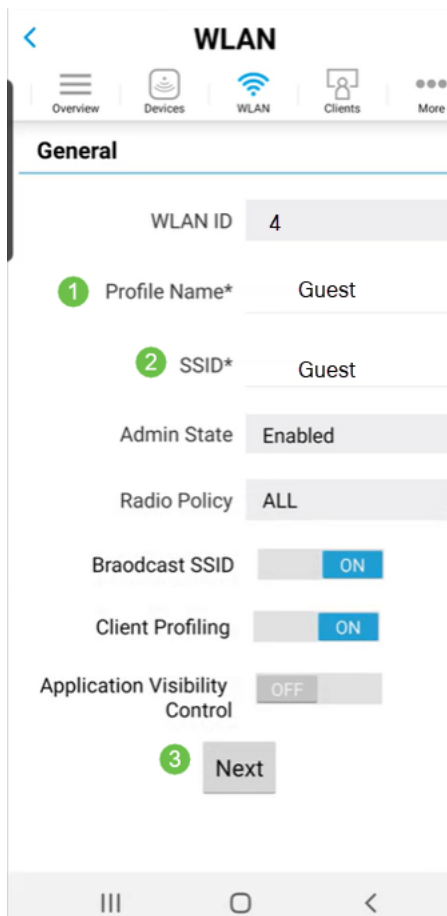
Schritt 3

Der Bildschirm *Neues WLAN hinzufügen* wird geöffnet. Es werden alle vorhandenen WLANs angezeigt. Wählen Sie **Neues WLAN hinzufügen** aus.



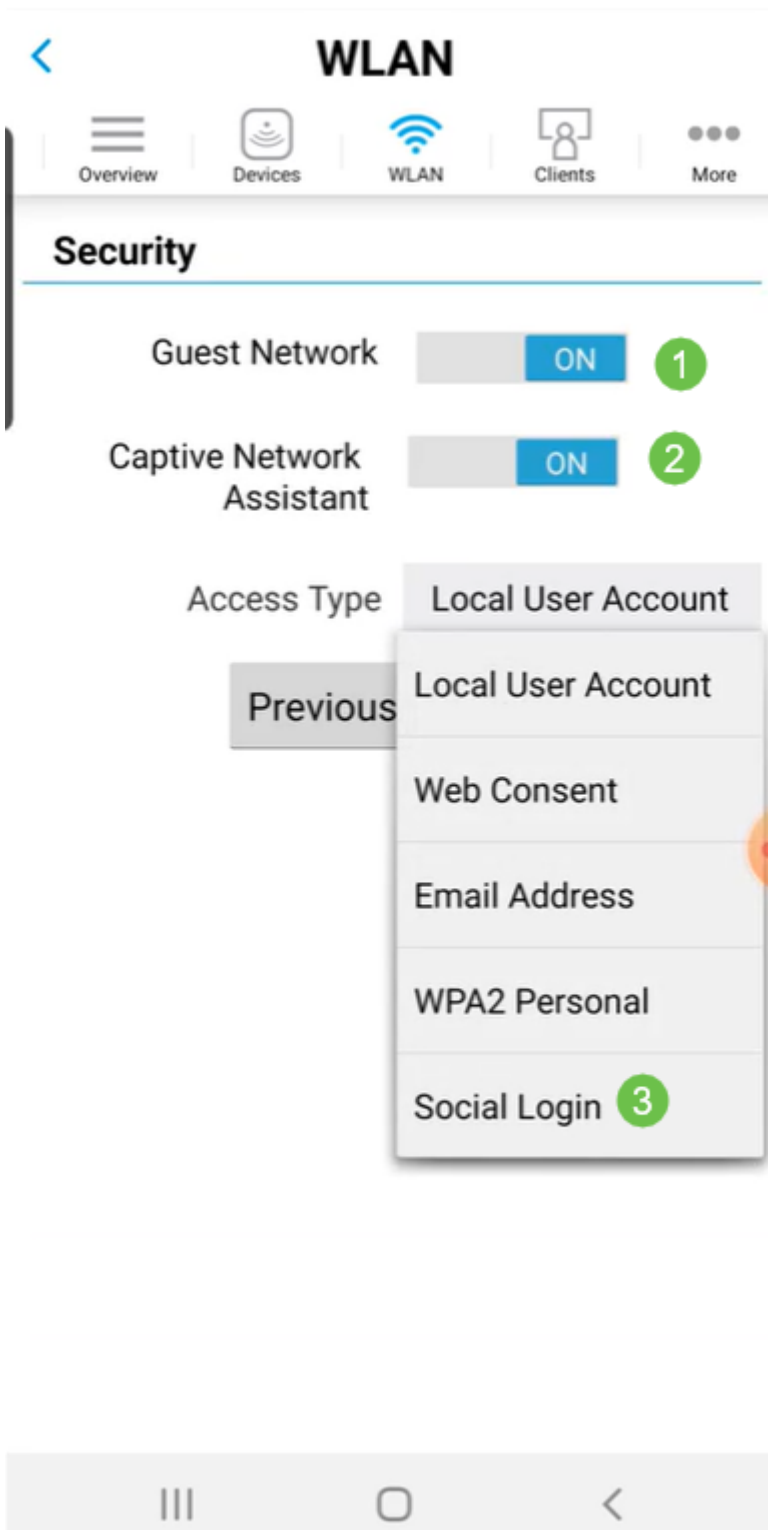
Schritt 4

Geben Sie einen **Profilnamen** und eine **SSID ein**. Füllen Sie die übrigen Felder aus, oder belassen Sie die Standardeinstellungen. Klicken Sie auf **Weiter**.





Schritt 5

Aktivieren Sie das *Gastnetzwerk*. In diesem Beispiel wird *Captive Network Assistant* ebenfalls aktiviert, dies ist jedoch optional. Sie haben Optionen für den *Zugriffstyp*. In diesem Fall ist **Social Login** ausgewählt.






Schritt 6

Auf diesem Bildschirm werden die Optionen für *Traffic Shaping (optional)* angezeigt. In diesem Beispiel wurde kein Traffic Shaping konfiguriert. Klicken Sie auf **Senden**.

8:07  

WLAN

Overview  **WLAN**  


Traffic Shaping (Optional)

Rate limits per client

Average downstream bandwidth limit	<input type="text" value="0"/>	kbps
Average real-time downstream bandwidth limit	<input type="text" value="0"/>	kbps
Average upstream bandwidth limit	<input type="text" value="0"/>	kbps
Average real-time upstream bandwidth limit	<input type="text" value="0"/>	kbps

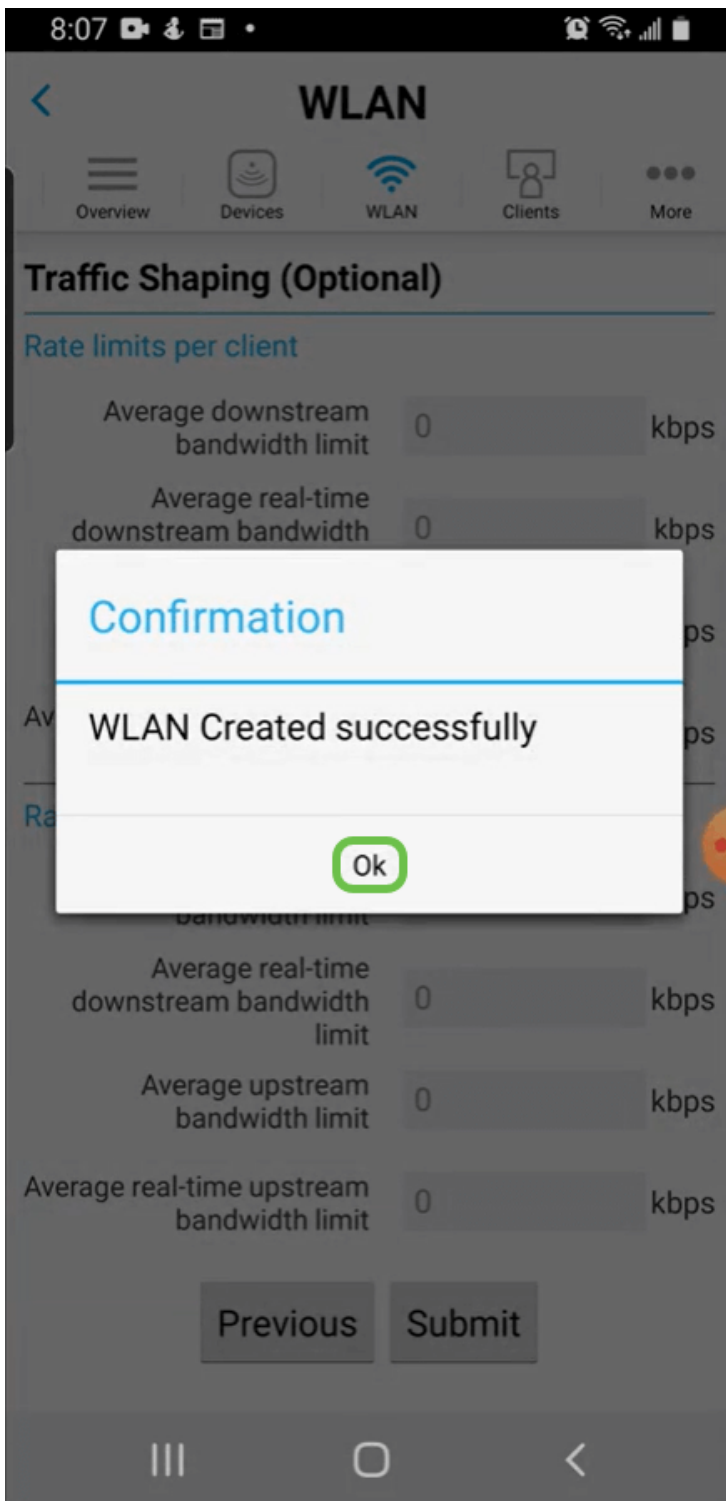
Rate limits per WLAN

Average downstream bandwidth limit	<input type="text" value="0"/>	kbps
Average real-time downstream bandwidth limit	<input type="text" value="0"/>	kbps
Average upstream bandwidth limit	<input type="text" value="0"/>	kbps
Average real-time upstream bandwidth limit	<input type="text" value="0"/>	kbps



Schritt 7

Sie sehen ein Bestätigungs-Popup. Klicken Sie auf OK.



Schritt 8

Speichern Sie Ihre Konfiguration, indem Sie auf die Registerkarte **More (Mehr)** klicken und dann im Dropdown-Menü **Save Configuration (Konfiguration speichern)** auswählen.



Schlussfolgerung

Sie haben nun eine vollständige Einrichtung für Ihr Netzwerk. Nehmen Sie sich eine Minute Zeit, um zu feiern und dann zur Arbeit zu kommen!

Wenn Sie dem Wireless-Mesh-Netzwerk die Funktion Anwendungsprofilierung oder Client Profiling hinzufügen möchten, sollten Sie die Webbenutzeroberfläche verwenden. [Klicken Sie, um diese Funktionen einzurichten](#).

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](#)