

Netzwerkkonfiguration gesamt: RV345P und Cisco Business Wireless mit der mobilen Anwendung

Ziel

In diesem Leitfaden wird die Konfiguration eines Wireless Mesh-Netzwerks mithilfe eines RV345P-Routers, eines CBW140AC-Access Points und zweier CBW142ACM-Mesh-Extender erläutert.

In diesem Artikel wird die mobile Anwendung verwendet, die für die einfache Einrichtung im vermaschten Wireless-Netzwerk empfohlen wird. Wenn Sie die Webbenutzeroberfläche (UI) für alle Konfigurationen verwenden möchten, [klicken Sie auf den Artikel, der die Webbenutzeroberfläche verwendet](#).

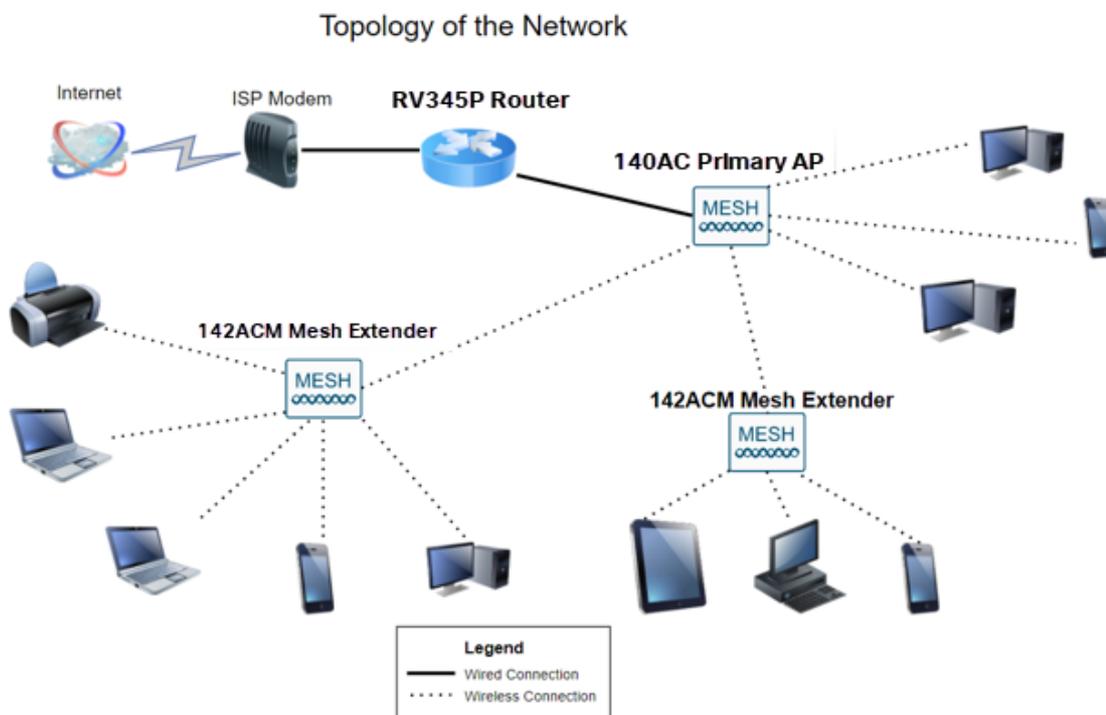
Inhalt

- [Voraussetzungen](#)
 - [Router vorbereiten](#)
 - [Cisco.com-Konto anfordern](#)
- [Konfigurieren des RV345P-Routers](#)
 - [RV345P sofort einsatzbereit](#)
 - [Router einrichten](#)
 - [Fehlerbehebung bei der Internetverbindung](#)
 - [Erstkonfiguration](#)
 - [Bearbeiten Sie ggf. eine IP-Adresse \(optional\).](#)
 - [Firmware aktualisieren, falls erforderlich](#)
 - [Konfigurieren automatischer Updates auf dem Router der Serie RV345P](#)
- [Sicherheitsoptionen](#)
 - [RV Security-Lizenz \(optional\)](#)
 - [Webfilterung auf dem RV345P-Router](#)
 - [Umbrella RV Branch License \(optional\)](#)
 - [Weitere Sicherheitsoptionen](#)
- [VPN-Optionen](#)
 - [VPN-Passthrough](#)
 - [AnyConnect VPN](#)
 - [Shrew Soft VPN](#)
 - [Weitere VPN-Optionen](#)
- [Zusätzliche Konfigurationen auf dem RV345P-Router](#)
 - [VLANs konfigurieren \(optional\)](#)
 - [VLANs Ports zuweisen \(optional\)](#)
 - [Hinzufügen einer statischen IP \(optional\)](#)
 - [Verwalten von Zertifikaten \(optional\)](#)
 - [Konfigurieren eines mobilen Netzwerks mit einem Dongle und einem Router](#)

der Serie RV345P (optional)

- Konfigurieren des Wireless Mesh-Netzwerks
 - Sofort einsatzbereiter CBW140AC
 - Richten Sie den 140AC Master Wireless Access Point auf der Webbenutzeroberfläche ein.
 - Tipps zur Wireless-Fehlerbehebung
 - Konfigurieren der CBW142ACM-Mesh-Extender mithilfe der Webbenutzeroberfläche
 - Überprüfen und Aktualisieren der Software mithilfe der Webbenutzeroberfläche
 - Erstellen von WLANs auf der Webbenutzeroberfläche
 - Erstellen eines Gast-WLAN mithilfe der Webbenutzeroberfläche (optional)

Topologie



Einführung

Alle Ihre Forschungsergebnisse sind zusammengekommen, und Sie haben Ihre Cisco Geräte gekauft - wie spannend! In diesem Szenario wird ein RV345P-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.

Dieser erweiterte Router bietet auch die Möglichkeit für zusätzliche Funktionen.

1. Mit der Anwendungskontrolle können Sie den Datenverkehr steuern. Diese Funktion kann so konfiguriert werden, dass Datenverkehr zugelassen, aber protokolliert, Datenverkehr blockiert und protokolliert oder einfach Datenverkehr blockiert wird.
2. Webfilterung wird verwendet, um Web-Datenverkehr zu unsicheren oder ungeeigneten

Websites zu verhindern. Diese Funktion wird nicht protokolliert.

3. AnyConnect ist ein Secure Sockets Layer (SSL) Virtual Private Network (VPN), das von Cisco zur Verfügung gestellt wird. VPNs ermöglichen es Remote-Benutzern und -Standorten, über ein sicheres Internet eine Verbindung zu Ihrem Firmenbüro oder Rechenzentrum herzustellen.

Wenn Sie diese Funktionen verwenden möchten, müssen Sie eine Lizenz erwerben. Router und Lizenzen werden online registriert. Diese Informationen werden in diesem Leitfaden behandelt.

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](#)

Unterstützte Geräte | Softwareversion

- RV345P | 1.0.03.21
- CBW140AC | 10.4.1.0
- CBW142ACM | 10.4.1.0 (Mindestens ein Mesh-Extender ist für das Mesh-Netzwerk erforderlich)

Voraussetzungen

Router vorbereiten

1. Stellen Sie sicher, dass Sie über eine aktuelle Internetverbindung verfügen.
2. Wenden Sie sich an Ihren Internetdienstanbieter (ISP), um spezielle Anweisungen für die Verwendung Ihres RV345P-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.

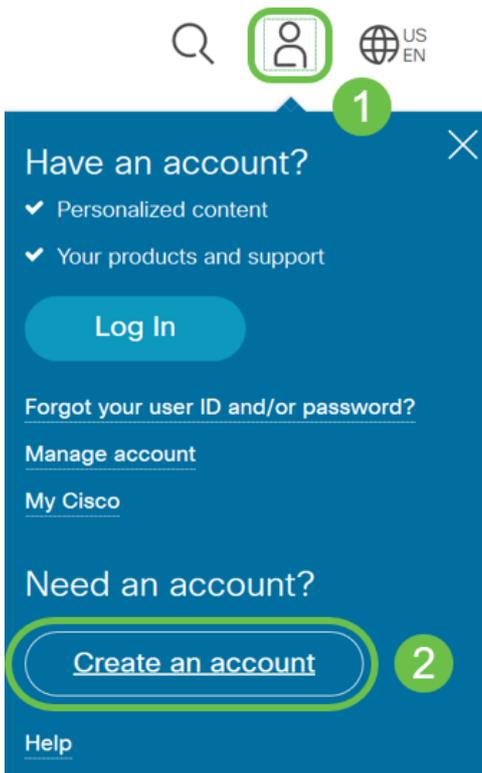
Cisco.com-Konto anfordern

Jetzt, da Sie Cisco Geräte besitzen, benötigen Sie ein Cisco.com-Konto, manchmal auch als Cisco Connection Online Identification (CCO-ID) bezeichnet. Für ein Konto ist keine Gebühr zu entrichten.

Wenn Sie bereits über ein Konto verfügen, können Sie [zum nächsten Abschnitt dieses Artikels wechseln](#).

Schritt 1

Rufen Sie [Cisco.com auf](#). Klicken Sie auf das **Personensymbol** und dann auf **Konto erstellen**.



Schritt 2

Geben Sie die erforderlichen Details zum Erstellen des Kontos ein, und klicken Sie auf **Registrieren**. Befolgen Sie die Anweisungen, um den Registrierungsprozess abzuschließen.

Create Account

1

Already have an account? [Sign In](#)

Email

First Name

Last Name

Country

Select a country or start typing for suggestions

Company

Password

Create a password

Confirm Password

Re-enter your password

Would you like updates about Cisco promotions, products and services?

Email Yes No

By clicking Register, I confirm that I have read and agree to the [Cisco Online Privacy Statement](#) and the [Cisco Web Site Terms and Conditions](#).

Register

2

Wenn Probleme auftreten, [klicken Sie auf die Hilfe-Seite zur Kontoregistrierung bei Cisco.com](#).

Konfigurieren des RV345P-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 RV345P verfügt über Standardeinstellungen, die für viele kleine und mittlere Unternehmen optimiert sind. Möglicherweise müssen Sie jedoch einige dieser Einstellungen ändern, um Netzwerkanforderungen oder Internetdienstanbieter (ISP) zu erfüllen. Nachdem Sie sich bezüglich der Anforderungen an Ihren ISP gewandt haben, können Sie Änderungen über die Webbenutzeroberfläche (UI) vornehmen.

Sind Sie bereit? Kommen wir dazu!

RV345P sofort einsatzbereit

Schritt 1

Verbinden Sie das Ethernetkabel von einem der RV345P-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 RV345P befinden, um die Erstkonfiguration durchzuführen.

Schritt 2

Stellen Sie sicher, dass Sie das mit dem RV345P gelieferte Netzteil verwenden. Die Verwendung eines anderen Netzadapters kann den RV345P beschädigen oder einen Ausfall der USB-Dongles verursachen. Der Netzschalter ist standardmäßig eingeschaltet.

Schließen Sie das Netzteil an den 12-V-Gleichstrom-Port des RV345P 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 RV345P anzuschließen.

Schritt 5

Schließen Sie das andere Ende des RV345P-Adapters an eine Steckdose an. Dadurch wird der RV345P 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 RV345P ist mit dem Booten fertig.

Router einrichten

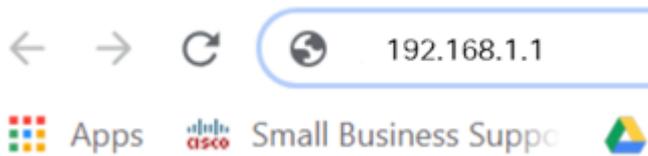
Jetzt ist es an der Zeit, einige Konfigurationen anzuzeigen! Führen Sie die folgenden Schritte aus, um die Webbenutzeroberfläche zu starten.

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 Adresleiste die Standard-IP-Adresse des RV345P, 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](#)



Schritt 4

Wenn die Anmeldeseite angezeigt wird, geben Sie den Standardbenutzernamen *cisco* und das Standardkennwort *cisco ein*.

Klicken Sie auf **Anmelden**.

Detaillierte Informationen erhalten Sie, wenn Sie auf [How to access the web-based setup page of Cisco VPN Router der Serie RV340](#) klicken.



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. Wenn der Navigationsbereich nicht geöffnet ist, können Sie ihn durch Klicken auf das **Menüsymbol** öffnen.



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

Wenn keine Verbindung hergestellt wird, können Sie sich den folgenden Artikel zur [Fehlerbehebung](#) ansehen.

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 RV345P) festgelegt ist. Um eine Verbindung herzustellen, müssen Sie möglicherweise die Netzwerkeinstellungen des RV345P 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 RV345P zurück, indem Sie beide Geräte ausschalten. Schalten Sie anschließend das Modem ein, und lassen Sie es etwa 2 Minuten untätig. Schalten Sie dann den RV345P 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 in diesem Abschnitt aufgeführten Schritte des *Assistenten für die Ersteinrichtung* zu durchlaufen. Sie können diese Einstellungen jederzeit ändern.

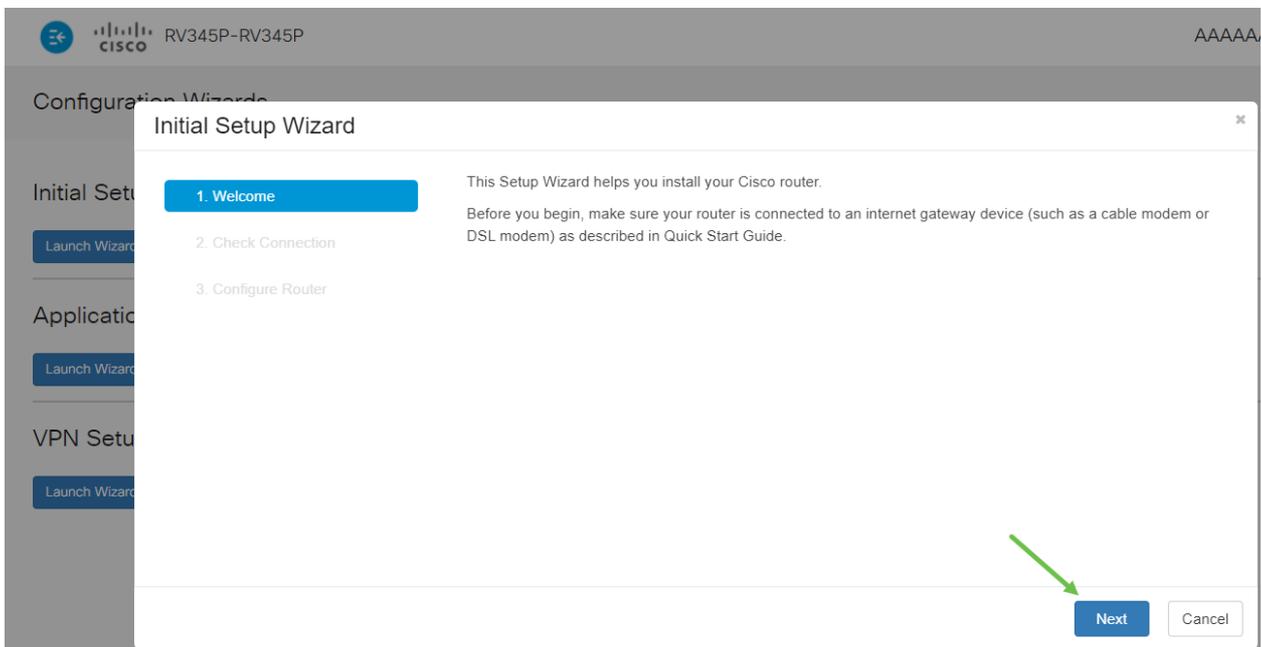
Schritt 1

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

The screenshot shows the Cisco RV345P web interface. The top navigation bar includes the Cisco logo, the device model 'RV345P-RV345P', and a language dropdown set to 'English'. A left-hand navigation menu lists various configuration categories. The main content area is titled 'Getting Started' and provides a list of links for quick configuration. The 'Initial Setup Wizard' link is highlighted with a green box, indicating it is the recommended starting point for initial configuration. Other links include 'VPN Setup Wizard', 'Application Control Wizard', 'Quick Access', 'Upgrade Router Firmware', 'Configure Remote Management Access', 'Backup Device Configuration', 'Initial Configuration', 'Change Administrator Password', 'Configure WAN Settings', 'Configure USB Settings', 'Configure VLAN Settings', 'Device Status', 'System Summary', 'VPN Status', 'Port Statistics', 'Traffic Statistics', and 'View System Log'.

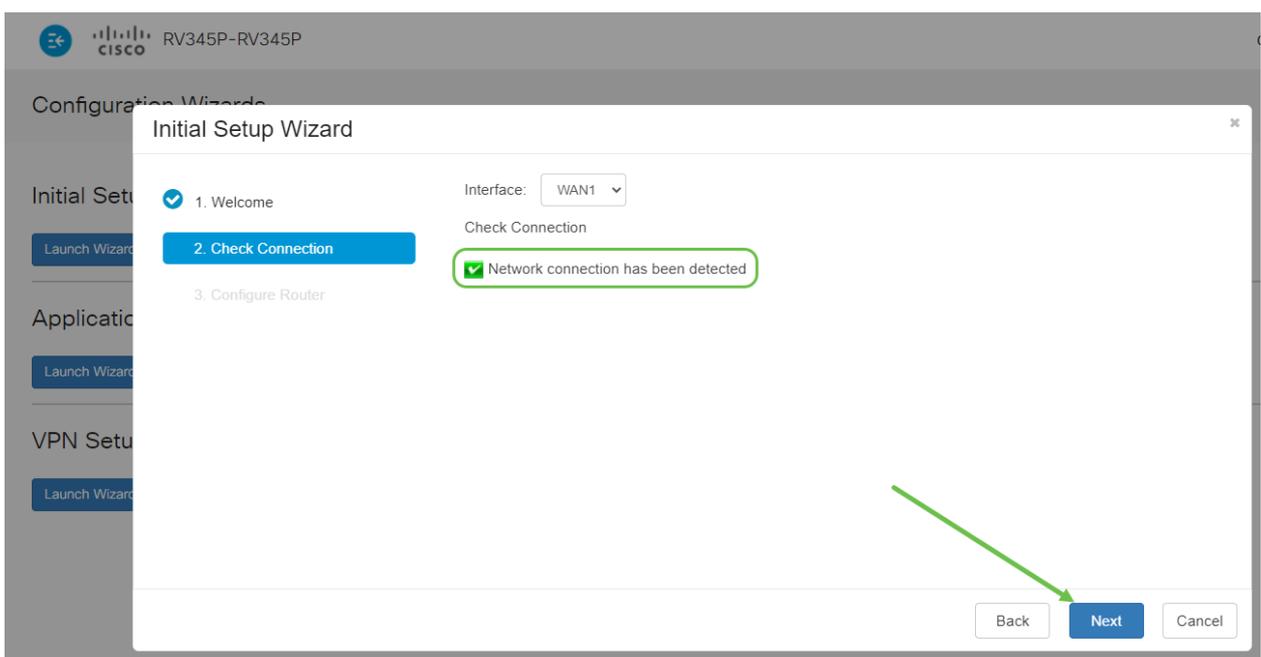
Schritt 2

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



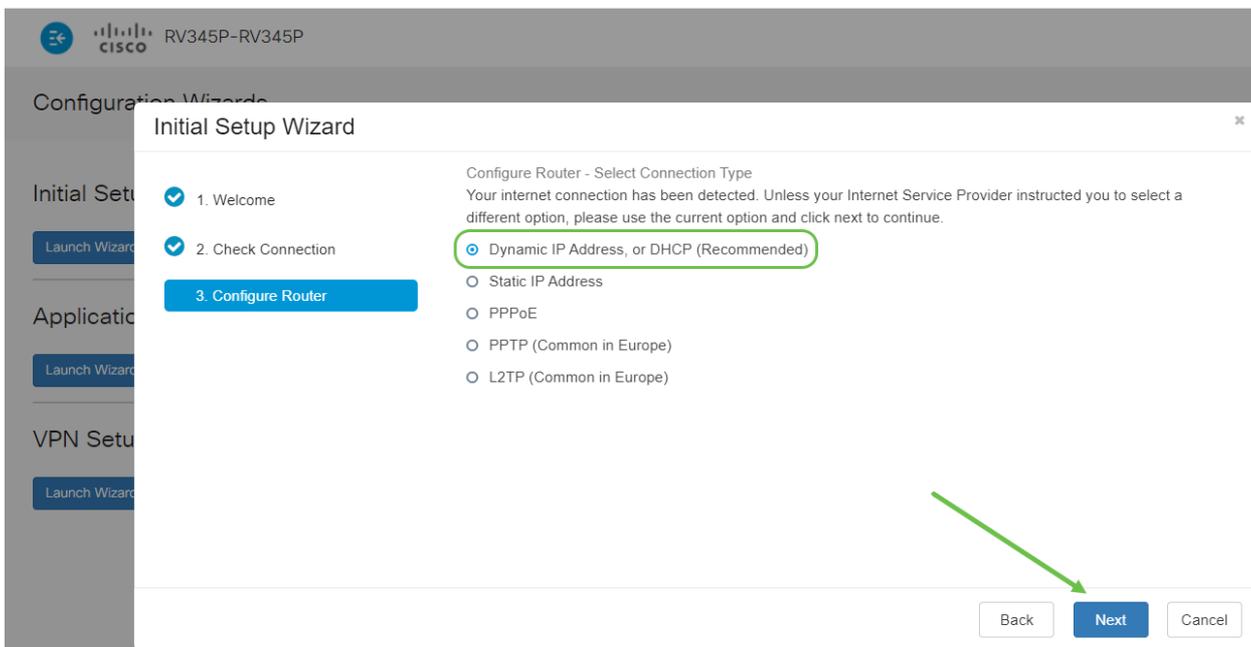
Schritt 3

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



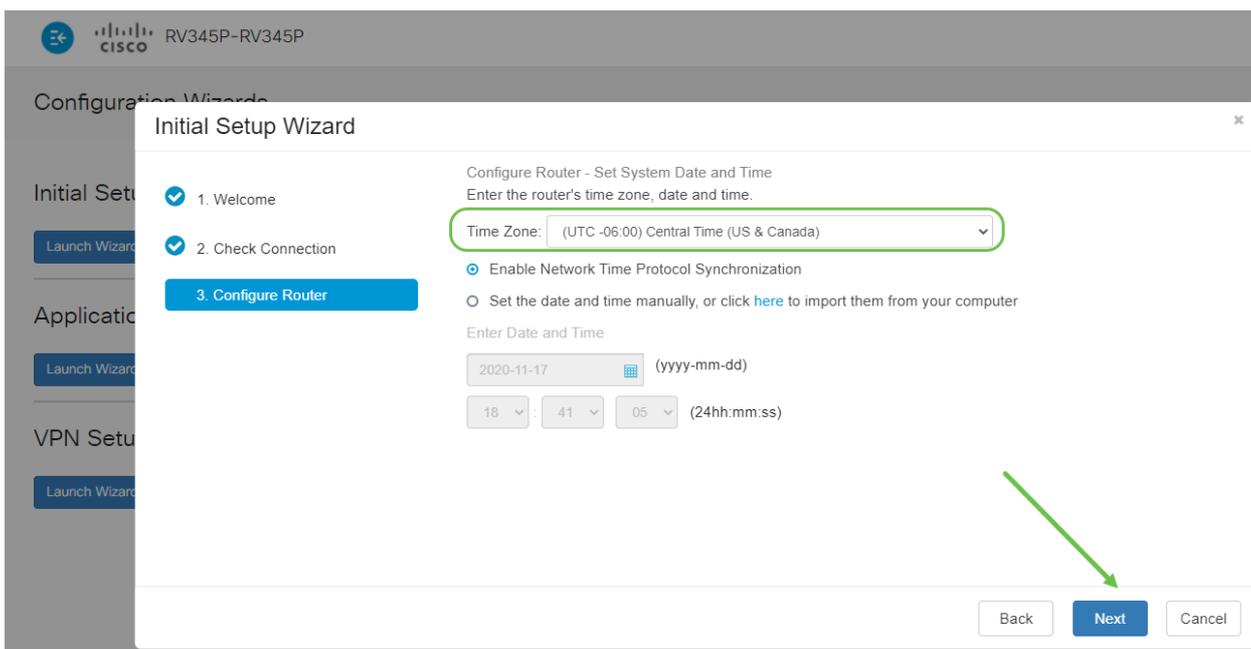
Schritt 4

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**.



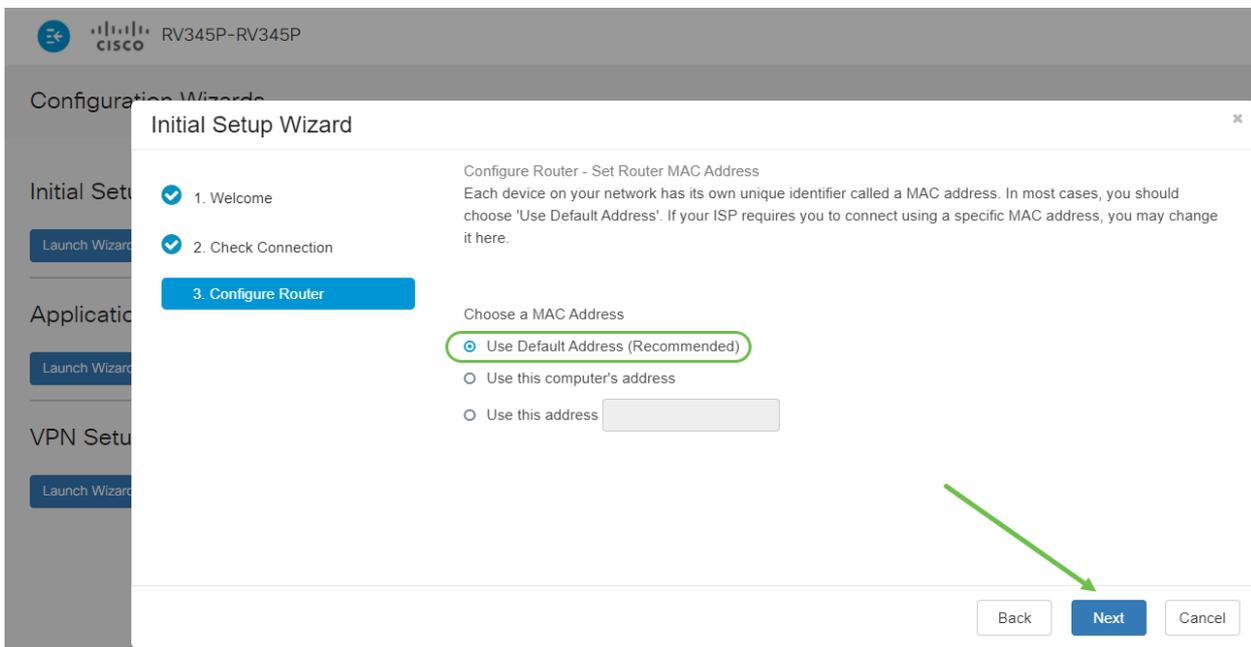
Schritt 5

Sie werden 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**.



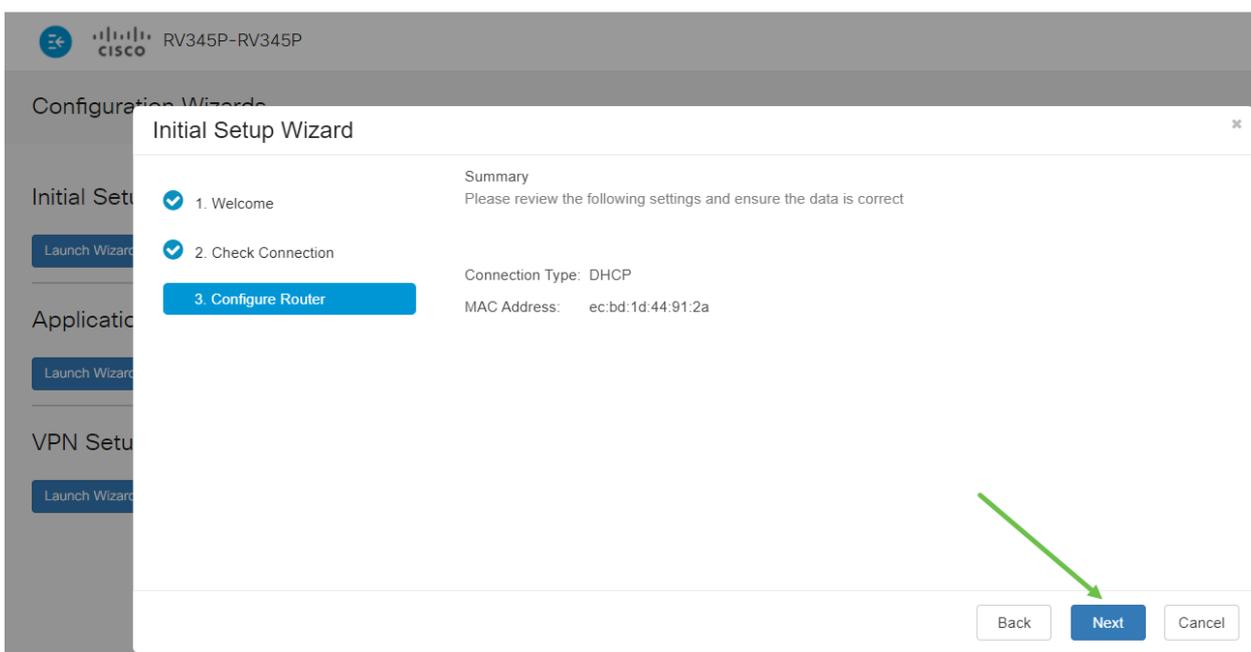
Schritt 6

Sie werden auswählen, welche MAC-Adressen Geräten zugewiesen werden sollen. In den meisten Fällen verwenden Sie die Standardadresse. Klicken Sie auf **Weiter**.



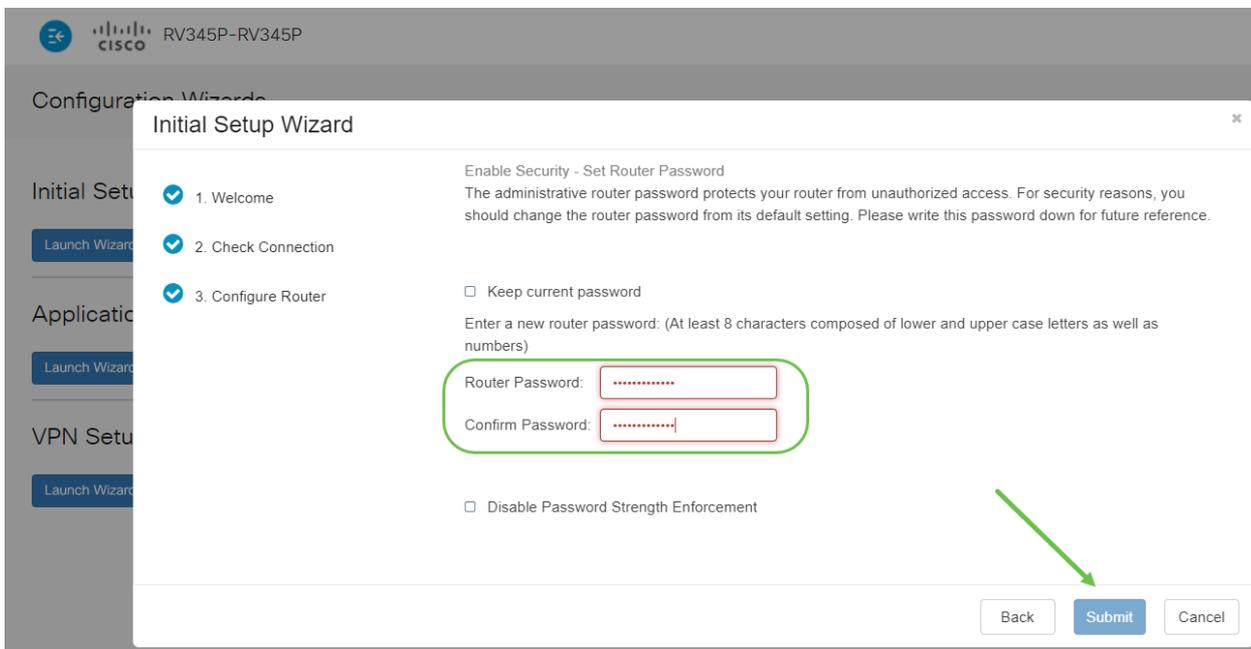
Schritt 7

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 **Speichersymbol**.



Wenn Sie weitere Informationen zu diesen Einstellungen benötigen, lesen Sie das Dokument [Konfigurieren der DHCP-WAN-Einstellungen auf dem RV34x-Router](#).

Auf dem RV345P ist standardmäßig Power over Ethernet (PoE) aktiviert. Sie können jedoch einige Anpassungen vornehmen. Wenn Sie die Einstellungen anpassen müssen, sehen Sie sich die [Option Configure Power over Ethernet \(PoE\) Settings \(PoE-Einstellungen konfigurieren\) auf dem RV345P-Router an](#).

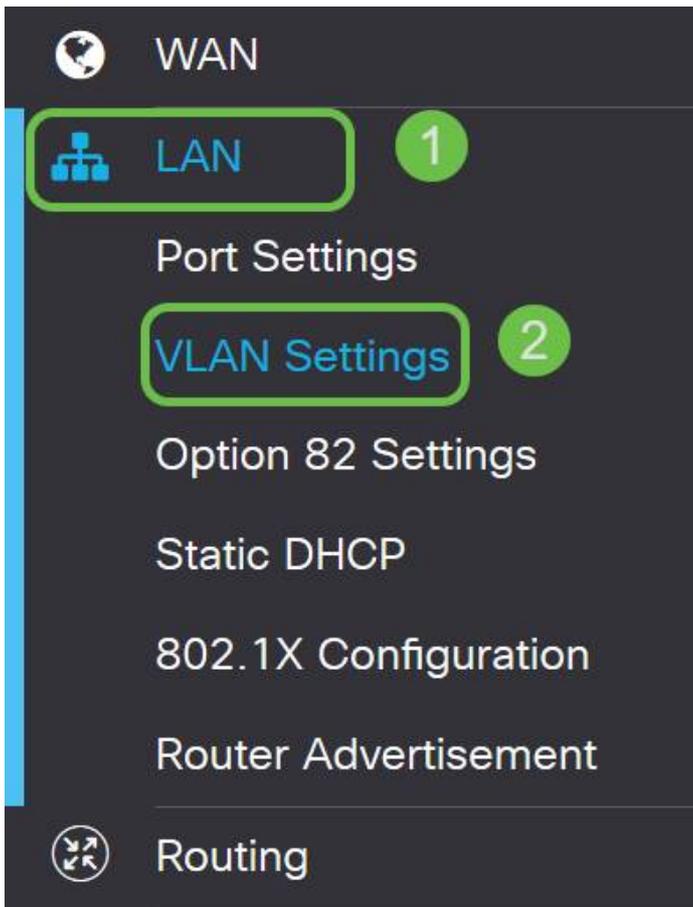
Bearbeiten Sie ggf. eine IP-Adresse (optional).

Nach Abschluss des *Assistenten für die Ersteinrichtung* können Sie eine statische IP-Adresse auf dem Router festlegen, indem Sie die VLAN-Einstellungen bearbeiten.

Dieser Prozess ist nur erforderlich, wenn der IP-Adresse Ihres Routers eine bestimmte Adresse in Ihrem vorhandenen Netzwerk zugewiesen werden muss. Wenn Sie keine IP-Adresse bearbeiten müssen, können Sie zum [nächsten Abschnitt](#) dieses Artikels wechseln.

Schritt 1

Klicken Sie im Menü auf der linken Seite auf **LAN > VLAN Settings**.



Schritt 2

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

VLAN Table

<input checked="" type="checkbox"/>	VLAN ID ↕	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input checked="" type="checkbox"/>	1	VLAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149

Schritt 3

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

VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask	IPv6 Address/Prefix Length
<input checked="" type="checkbox"/> 1	Default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IP Address: 192.168.1.1/24 Subnet Mask: 255.255.255.0 DHCP Type: <input type="radio"/> Disabled <input type="radio"/> Server <input checked="" type="radio"/> Relay	Prefix: <input checked="" type="radio"/> fec0: <input type="radio"/> Prefix from DHCP-PD Prefix Length: 64 Preview: [fec0::1] Interface Identifier: <input type="radio"/> EUI-64 <input checked="" type="radio"/> 1 DHCP Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Server

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.

DHCP Type: Disabled
 Server
 Relay

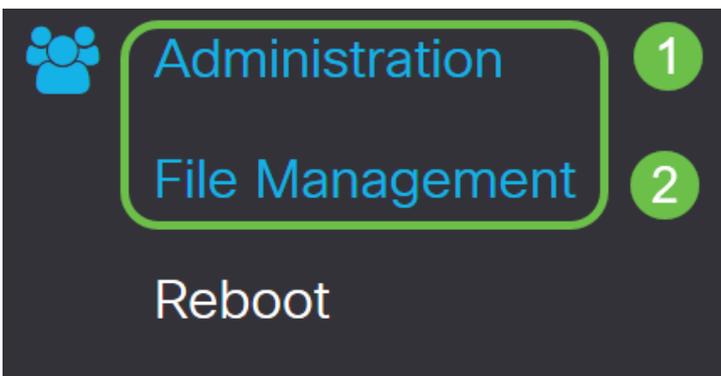
Prefix Length: 64
 Preview: [fec0::1]
 Interface Identifier: EUI-64
 1
 DHCP Type: Disabled
 Server

Firmware aktualisieren, falls erforderlich

Dies ist ein wichtiger Schritt, 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.

File Management

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 das 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.

Wenn Ihr Gerät nicht mit dem Internet verbunden ist oder die Internetverbindung unterbrochen wird, können Sie kein Upgrade von *cisco.com* durchführen. Wenn dies für Sie gilt, finden Sie [hier](#) alternative Optionen.

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

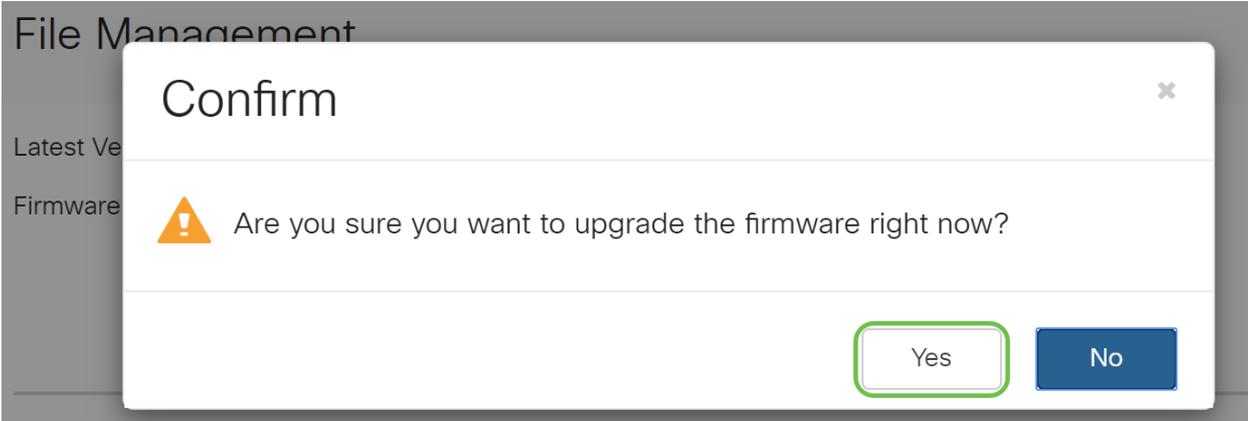
Upgrade

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

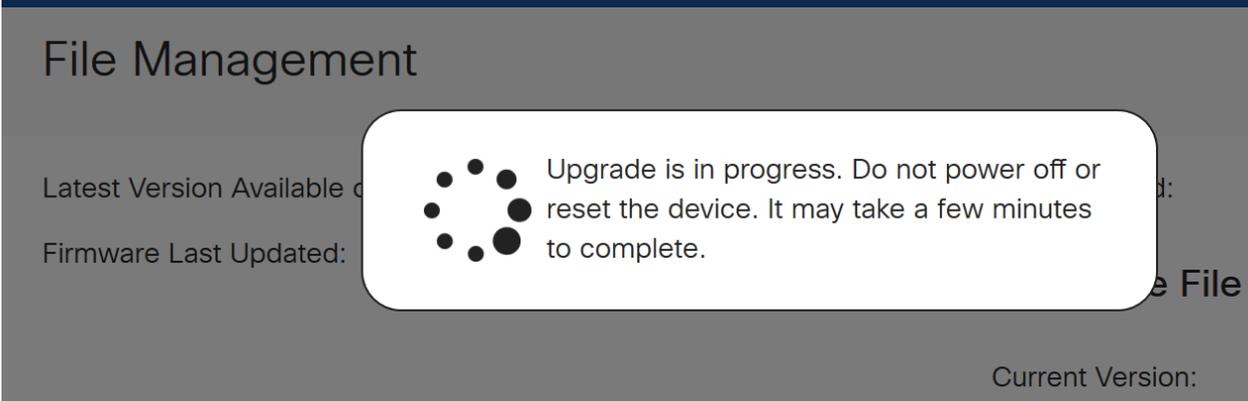
Download to USB

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 *Systeminformationen*. Im Bereich *Aktuelle Firmware-Version* sollte jetzt die aktualisierte Firmware-Version angezeigt werden.

File Management

System Information

Device Model:	RV345P
PID VID:	RV345P-K9 V01
Current Firmware Version:	1.0.03.20
Last Updated:	2020-Oct-02, 11:10:50 GMT
Last Version Available on Cisco.com:	1.0.03.20
Last Checked:	2020-Nov-11, 14:16:01 GMT

Konfigurieren automatischer Updates auf dem Router der Serie RV345P

Da Updates so wichtig sind und Sie sehr beschäftigt sind, ist es sinnvoll, automatische Updates von hier aus zu konfigurieren!

Schritt 1

Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Systemkonfiguration > Automatische Updates** aus.

1 System Configuration

System

Time

Log

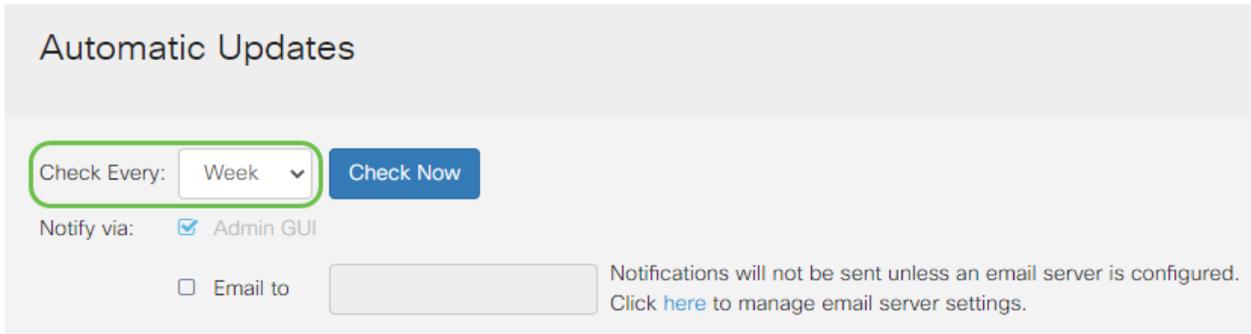
Email

User Accounts

User Groups

Schritt 2

Wählen Sie aus der Dropdown-Liste *Check Every (Alle prüfen)* aus, wie oft der Router nach Updates suchen soll.



Automatic Updates

Check Every: Week

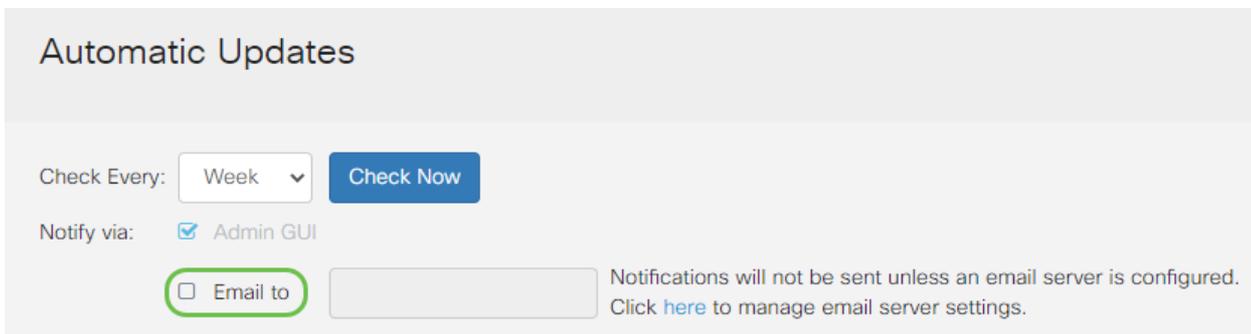
Notify via: Admin GUI

Email to Notifications will not be sent unless an email server is configured. Click [here](#) to manage email server settings.

Schritt 3

Aktivieren Sie im Bereich *Benachrichtigung über* das Kontrollkästchen **E-Mail an**, um Aktualisierungen per E-Mail zu erhalten. Das Kontrollkästchen *Admin GUI* ist standardmäßig aktiviert und kann nicht deaktiviert werden. Sobald eine Aktualisierung verfügbar ist, wird eine Benachrichtigung in der webbasierten Konfiguration angezeigt.

Wenn Sie E-Mail-Servereinstellungen einrichten möchten, klicken Sie [hier](#), um mehr darüber zu erfahren.



Automatic Updates

Check Every: Week

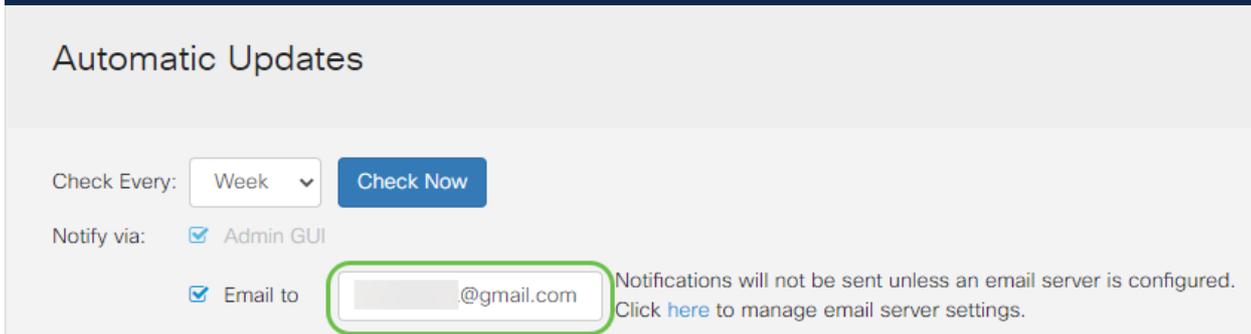
Notify via: Admin GUI

Email to Notifications will not be sent unless an email server is configured. Click [here](#) to manage email server settings.

Schritt 4

Geben Sie eine E-Mail-Adresse in das Feld *E-Mail an Adresse* ein.

Es wird dringend empfohlen, ein separates E-Mail-Konto zu verwenden, anstatt Ihre persönliche E-Mail-Adresse zu verwenden, um die Privatsphäre zu wahren.



Automatic Updates

Check Every: Week

Notify via: Admin GUI

Email to Notifications will not be sent unless an email server is configured. Click [here](#) to manage email server settings.

Schritt 5

Aktivieren Sie im Bereich *Automatisch aktualisieren* die Kontrollkästchen **Benachrichtigen** für die Art von Aktualisierungen, über die Sie benachrichtigt werden möchten. Folgende Optionen sind verfügbar:

- System-Firmware - Das Hauptsteuerungsprogramm für das Gerät.
- USB Modem Firmware (USB-Modem-Firmware): Das Steuerungsprogramm oder der Treiber für den USB-Port.
- Sicherheitssignatur - Diese Signaturen enthalten Signaturen für die Anwendungssteuerung, um Anwendungen, Gerätetypen, Betriebssysteme usw. zu identifizieren.

Automatic Updates

Check Every:

Notify via: Admin GUI

Email to Notifications will not be sent unless an email address is provided. Click [here](#) to manage email server settings.

Automatic Update	Notify	Update (hh:mm)	Status
System Firmware	<input checked="" type="checkbox"/>	<input type="text" value="Never"/>	Version 1.0.03.20
USB Modem Firmware	<input checked="" type="checkbox"/>	<input type="text" value="Never"/>	Version 1.0.00.02
Security Signature	<input checked="" type="checkbox"/>	<input type="text" value="23:00"/>	Version 2.0.0.0015

Schritt 6

Wählen Sie aus der Dropdown-Liste *Automatic Update (Automatische Aktualisierung)* eine Uhrzeit für den Tag aus, an dem die automatische Aktualisierung durchgeführt werden soll. Einige Optionen können je nach gewähltem Aktualisierungstyp variieren. Die einzige Option für eine sofortige Aktualisierung ist die Sicherheitssignatur. Es wird empfohlen, einen Zeitpunkt festzulegen, zu dem Ihr Büro geschlossen ist, damit der Dienst nicht zu einem ungünstigen Zeitpunkt unterbrochen wird.

Automatic Updates

Check Every:

Notify via: Admin GUI
 Email to

Never
00:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
Never

Automatic Update	
	Notify 
System Firmware <input checked="" type="checkbox"/>	<input type="text" value="Never"/>
USB Modem Firmware <input checked="" type="checkbox"/>	<input type="text" value="Never"/>
Security Signature <input checked="" type="checkbox"/>	<input type="text" value="23:00"/>

Der Status zeigt die aktuell ausgeführte Version der Firmware oder Sicherheitssignatur an.

Schritt 7

Klicken Sie auf Apply (Anwenden).



Schritt 8

Um die Konfiguration dauerhaft zu speichern, rufen Sie die Seite "Copy/Save Configuration" (Konfiguration kopieren/speichern) auf, oder klicken Sie auf das **Speichersymbol** oben auf der Seite.



Toll, Ihre Grundeinstellungen auf Ihrem Router sind abgeschlossen! Jetzt stehen Ihnen einige Konfigurationsoptionen zur Verfügung.

Sicherheitsoptionen

Natürlich möchten Sie, dass Ihr Netzwerk sicher ist. Es gibt einige einfache Optionen, wie z. B. ein komplexes Passwort, aber wenn Sie die Schritte für ein noch sichereres Netzwerk ergreifen möchten, lesen Sie diesen Abschnitt zur Sicherheit.

RV Security-Lizenz (optional)

Diese RV Security-Lizenzfunktionen schützen Ihr Netzwerk vor Angriffen aus dem Internet:

- **Intrusion Prevention System (IPS):** Inspiziert Netzwerkpakete, Protokolle und/oder blockiert eine Vielzahl von Netzwerkangriffen. Sie bietet eine höhere Netzwerkverfügbarkeit, schnellere Problembeseitigung und umfassenden Schutz vor Bedrohungen.
- **Antivirus:** Schutz vor Viren durch Scannen der Anwendungen auf verschiedene Protokolle wie HTTP, FTP, SMTP-E-Mail-Anhänge, POP3-E-Mail-Anhänge und IMAP-E-Mail-Anhänge, die den Router durchlaufen.
- **Web-Sicherheit:** Ermöglicht geschäftliche Effizienz und Sicherheit bei der Verbindung mit dem Internet, ermöglicht Internetzugriffsrichtlinien für Endgeräte und Internetanwendungen und gewährleistet so Leistung und Sicherheit. Sie ist Cloud-basiert und umfasst mehr als 80 Kategorien mit mehr als 450 Millionen klassifizierten Domänen.
- **Anwendungserkennung:** Identifizieren und Zuweisen von Richtlinien für Internetanwendungen 500 individuelle Anwendungen werden automatisch identifiziert.
- **Client-Identifizierung:** Clients dynamisch identifizieren und kategorisieren. Möglichkeit zum Zuweisen von Richtlinien basierend auf Endgerätekategorie und Betriebssystem.

Die RV Security-Lizenz bietet Webfilterung. Die Webfilterung ist eine Funktion, mit der Sie den Zugriff auf unangemessene Websites verwalten können. Sie kann die Webzugriffsanfragen eines Kunden prüfen, um festzustellen, ob diese Website zugelassen oder abgelehnt werden soll.

Die lizenzierten Sicherheitsfunktionen können 90 Tage lang kostenlos getestet werden. Wenn Sie die erweiterten Sicherheitsfunktionen Ihres Routers auch nach der Testphase weiterhin verwenden möchten, müssen Sie eine Lizenz erwerben und aktivieren.

Eine weitere Sicherheitsoption ist Cisco Umbrella. [Klicken Sie hier, um zum Umbrella-Bereich zu springen.](#)

Wenn Sie keine der Sicherheitslizenzen benötigen, [klicken Sie, um zum Abschnitt VPN dieses Dokuments zu springen.](#)

Einführung in Smart Accounts

Zum Erwerb der RV Security-Lizenz benötigen Sie einen Smart Account.

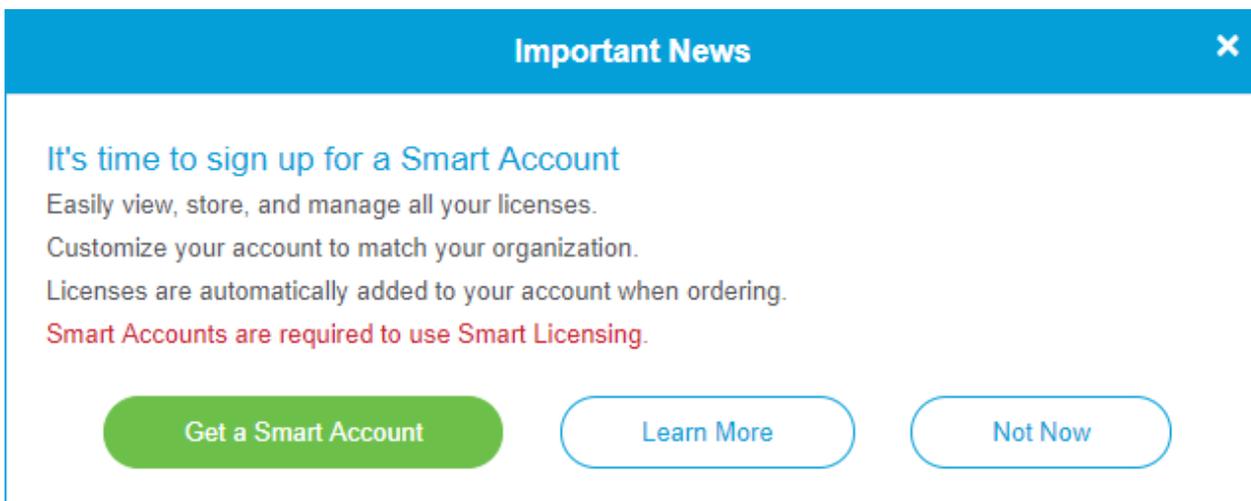
Indem Sie die Aktivierung dieses Smart Accounts genehmigen, stimmen Sie zu, dass

Sie zur Erstellung von Konten und zur Verwaltung von Produkt- und Serviceansprüchen, Lizenzvereinbarungen und Benutzerzugriff auf Konten im Namen Ihres Unternehmens autorisiert sind. Cisco Partner dürfen die Erstellung von Konten nicht im Namen von Kunden genehmigen.

Die Erstellung eines neuen Smart Accounts ist ein einmaliges Ereignis, und die Verwaltung erfolgt von diesem Zeitpunkt an über das Tool.

Smart Account erstellen

Wenn Sie über Ihr Cisco.com-Konto oder Ihre CCO-ID (die CCO-ID, die Sie zu Beginn dieses Dokuments erstellt haben) auf Ihr allgemeines Cisco Konto zugreifen, werden Sie möglicherweise durch eine Nachricht zur Erstellung eines Smart Accounts begrüßt.



Important News ✕

It's time to sign up for a Smart Account

Easily view, store, and manage all your licenses.

Customize your account to match your organization.

Licenses are automatically added to your account when ordering.

Smart Accounts are required to use Smart Licensing.

Get a Smart Account Learn More Not Now

Wenn Sie dieses Popup-Fenster noch nicht gesehen haben, können Sie auf die [Seite "Smart Account Creation"](#) klicken, um zur [Seite "Smart Account Creation"](#) zu gelangen. Möglicherweise müssen Sie sich mit Ihren Cisco.com-Anmeldeinformationen anmelden.

Klicken Sie [hier](#), um weitere Informationen zu den Schritten für die Anforderung Ihres Smart Accounts zu erhalten.

Notieren Sie sich Ihren Kontonamen und weitere Registrierungsdetails.

Schneller Tipp: Wenn Sie eine Domäne eingeben müssen und keine haben, können Sie Ihre E-Mail-Adresse in Form von *name@domain.com* eingeben. Gängige Domänen sind gmail, yahoo, etc., je nach Ihrem Unternehmen oder Anbieter.

Es ist sehr wichtig, dass Sie vor dem Erwerb der RV Security-Lizenz über ein Konto bei Cisco.com (CCO-ID) und ein Cisco Smart Account verfügen.

Erwerb der RV Security-Lizenz

Sie müssen eine Lizenz bei Ihrem Cisco Distributor oder Ihrem Cisco Partner erwerben. Klicken Sie [hier](#), um einen Cisco Partner zu finden.

In der Tabelle unten wird die Teilenummer der Lizenz angezeigt.

Typ	Produkt-ID	Beschreibung
RV Security-Lizenz	LS-RV34X-SEC-1YR=	RV-Sicherheit: 1 Jahr: Dynamic Web Filter, Application Visibility, Client Identification and Statistics, Gateway Antivirus und Intrusion Prevention System IPS.

Der Lizenzschlüssel wird nicht direkt in den Router eingegeben, sondern nach Bestellung der Lizenz Ihrem Cisco Smart Account zugewiesen. Der Zeitraum, in dem die Lizenz für Ihr Konto angezeigt wird, hängt davon ab, wann der Partner die Bestellung annimmt und wann der Reseller die Lizenzen mit Ihrem Konto verknüpft (normalerweise 24-48 Stunden).

Lizenz in Smart Account bestätigen

Navigieren Sie zur Seite für Ihr Smart License-Konto, und klicken Sie dann auf **Smart Software-Lizenzseite > Bestand > Lizenzen**.

The screenshot shows the Cisco Software Central interface for Smart Software Licensing. The 'Licenses' tab is active, and a table displays the following data:

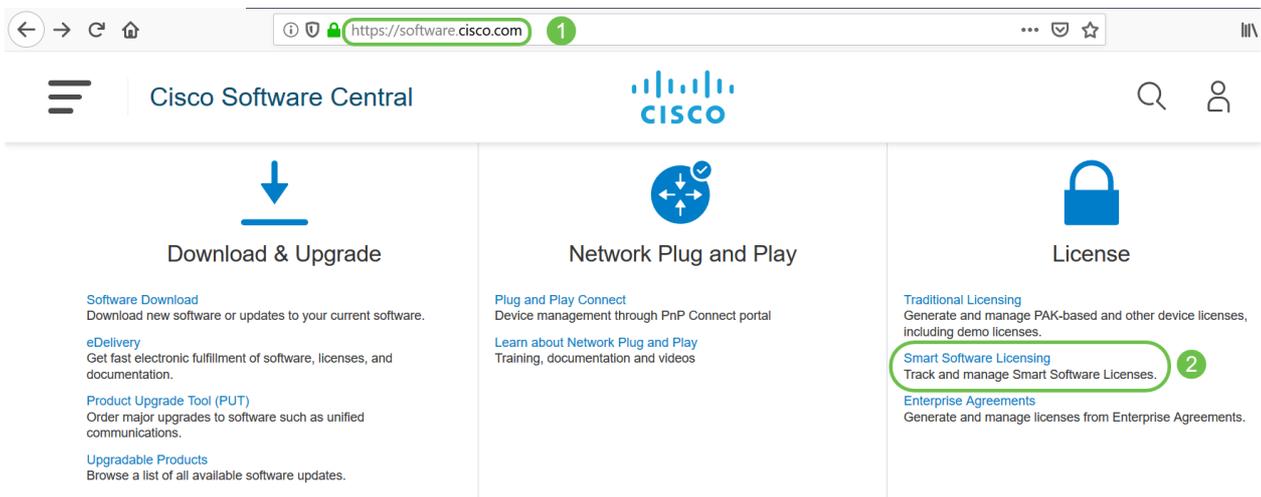
License	Billing	Purchased	In Use	Balance	Alerts	Actions
[Redacted]	Prepaid		0			Actions
RV-Series Security Services License	Prepaid		0			Actions
[Redacted]	Prepaid		0			Actions

Wenn Ihre Lizenz nicht in Ihrem Smart Account angezeigt wird, wenden Sie sich an Ihren Cisco Partner.

Konfigurieren der RV Security-Lizenz auf dem Router der Serie RV345P

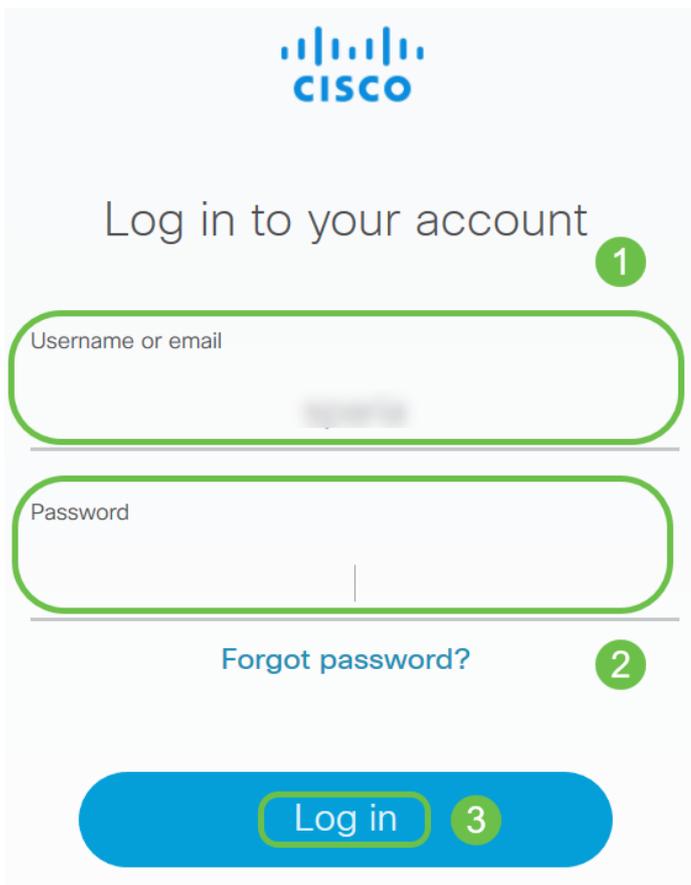
Schritt 1

Greifen Sie auf [Cisco Software](#) zu, und navigieren Sie zu **Smart Software Licensing**.



Schritt 2

Geben Sie Ihren *Benutzernamen*, Ihre *E-Mail-Adresse* und Ihr *Passwort* ein, um sich bei Ihrem Smart Account anzumelden. Klicken Sie auf **Anmelden**.



Schritt 3

Navigieren Sie zu **Inventory > Licenses (Bestand > Lizenzen)**, und überprüfen Sie, ob die *Security Services-Lizenz der RV-Serie* auf Ihrem Smart Account aufgeführt ist. Wenn die Lizenz nicht aufgeführt ist, wenden Sie sich an Ihren Cisco Partner.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing



Schritt 4

Navigieren Sie zu **Bestand > Allgemein**. Klicken Sie unter *Product Instance Registration Tokens* auf **New Token**.

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts | **Inventory** | Convert to Smart Licensing | Reports | Preferences | Satellites | Activity

1

Virtual Account:

General

Licenses

Product Instances

Event Log

2

Virtual Account

Description:

Default Virtual Account:

No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

3

Schritt 5

Das Fenster Registrierungstoken erstellen wird angezeigt. Im Bereich *Virtuelles Konto* wird das virtuelle Konto angezeigt, unter dem das Registrierungstoken erstellt wird. Gehen Sie auf der Seite *Registrierungstoken erstellen wie folgt vor*.

- Geben Sie im Feld Description (Beschreibung) eine eindeutige Beschreibung für das Token ein. In diesem Beispiel wird Security License - Web Filtering eingegeben.
- Geben Sie im Feld Ablaufdatum einen Wert zwischen 1 und 365 Tagen ein. Cisco empfiehlt für dieses Feld den Wert 30 Tage. Sie können den Wert jedoch an Ihre Anforderungen anpassen.
- Im Feld Max. Number of Uses field (Anzahl der verwendeten Felder) gibt einen Wert ein, um die Anzahl der Verwendungszwecke dieses Tokens festzulegen. Das Token läuft ab, wenn entweder die Anzahl der Tage oder die maximale Anzahl der Verwendungen erreicht ist.
- Aktivieren Sie das Kontrollkästchen Exportgesteuerte Funktionen für die mit diesem Token registrierten Produkte zulassen, um die exportgesteuerte Funktionalität für Token einer Produktinstanz in Ihrem virtuellen Konto zu aktivieren. Deaktivieren Sie das Kontrollkästchen, wenn Sie nicht zulassen möchten, dass die exportgesteuerte

Funktionalität für die Verwendung mit diesem Token verfügbar gemacht wird. Verwenden Sie diese Option nur, wenn Sie die exportgesteuerte Funktionalität einhalten. Einige exportkontrollierte Funktionen sind durch das US-Handelsministerium eingeschränkt. Diese Funktionen sind auf Produkte beschränkt, die mit diesem Token registriert wurden, wenn Sie das Kontrollkästchen deaktivieren. Verstöße werden mit Strafen und Verwaltungsgebühren belegt.

- Klicken Sie auf **Token erstellen**, um das Token zu generieren.

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description : 1

* Expire After: Days 2
Between 1 - 365, 30 days recommended

Max. Number of Uses: 3
The token will be expired when either the expiration or the maximum uses is reached

Allow export-controlled functionality on the products registered with this token 4

5

Sie haben nun erfolgreich ein Produktinstanzregistrierungstoken generiert.

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
<input type="text" value="ITMGZIN..."/>	2019-Sep-08 09:46:20 (in 30...)	0 of 10	Allowed	security license - web filtering		Actions

The token will be expired when either the expiration or the maximum uses is reached

Schritt 6

Klicken Sie auf das **Pfeilsymbol** in der Spalte *Token*, um das Token in die Zwischenablage zu kopieren. Drücken Sie **Strg + c** auf Ihrer Tastatur.

Token

Press ctrl + c to copy selected text to clipboard. 2

1

The token will be expired when either the expiration or the maximum uses is reached

Schritt 7 (optional)

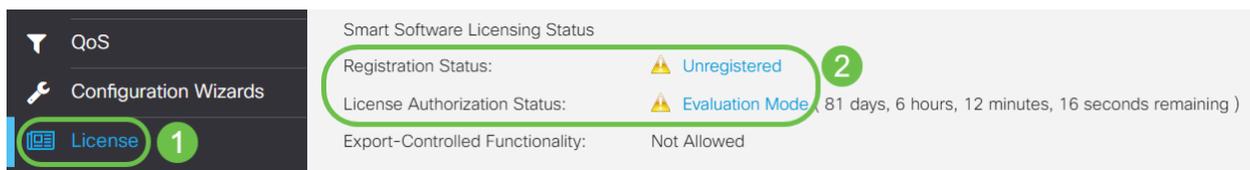
Klicken Sie auf das Dropdown-Menü **Aktionen**, und wählen Sie **Kopieren aus**, um das Token in die Zwischenablage zu kopieren oder **herunterzuladen...**, um eine Textdatei

des Tokens herunterzuladen, von dem Sie kopieren können.



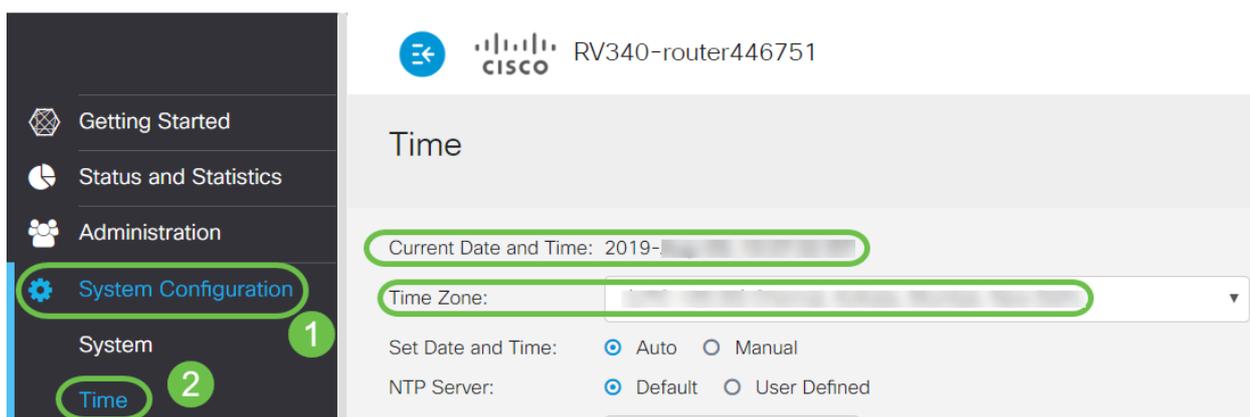
Schritt 8

Navigieren Sie zu **License (Lizenz)**, und überprüfen Sie, ob der *Registrierungsstatus* als *Nicht registriert* angezeigt wird und der *Lizenzautorisierungsstatus* als *Evaluierungsmodus* angezeigt wird.



Schritt 9

Navigieren Sie zu **Systemkonfiguration > Zeit**, und überprüfen Sie, ob *Datum*, *Uhrzeit* und *Zeitzone* entsprechend Ihrer Zeitzone korrekt reflektiert werden.



Schritt 10

Navigieren Sie zu **Lizenz**. Fügen Sie das kopierte Token in Schritt 6 im Textfeld unter der Registerkarte *Lizenz ein*, indem Sie auf Ihrer Tastatur **Strg + v** auswählen. Klicken Sie auf **Registrieren**.

Getting Started
 Status and Statistics
 Administration
 System Configuration
 WAN
 LAN
 Routing
 Firewall
 VPN
 Security
 QoS
 Configuration Wizards
License 1

License

You are currently running in evaluation mode, to register an account:

- Ensure this product has internet access.
- Click [here](#) to access your Cisco Smart Account.
- Navigate to the Virtual Account section which contains licenses.
- Generate and copy a token for the specific license to be applied to this device.
- Paste the token into the box below.

2

3E4LTE1Njc5MzU5%0AODA4MTh8dFh0

* Click **Register 3**

Learn More about [Smart Software Licensing](#)

Smart Software Licensing Status

Registration Status: ⚠ Unregistered

License Authorization Status: ⚠ Evaluation Mode (81 days, 6 hours, 12 minutes, 14 seconds remaining)

Export-Controlled Functionality: Not Allowed

Die Registrierung kann einige Minuten in Anspruch nehmen. Verlassen Sie die Seite nicht, da der Router versucht, den Lizenzserver zu kontaktieren.

Schritt 11

Sie sollten jetzt Ihren Router der Serie RV345P mit Smart License erfolgreich registriert und autorisiert haben. Sie erhalten eine Benachrichtigung auf dem Bildschirm *Registrierung erfolgreich abgeschlossen*. Außerdem können Sie sehen, dass der *Registrierungsstatus* als *Registriert* angezeigt wird und der *Lizenzautorisierungsstatus* als *Autorisiert* angezeigt wird.

RV340-router446751

Registration completed successfully

License

To view and manage Smart Software Licenses for your Cisco Smart Account, go to [Smart Licensing Manager](#) **Actions**

Smart Software Licensing Status

Registration Status: ✔ Registered (, 2019)

License Authorization Status: ✔ Authorized (, 2019)

Smart Account: Cisco Demo Customer Smart Account

Virtual Account:

PID: RV340-K9

Export-Controlled Functionality: Allowed

Schritt 12 (optional)

Wenn Sie weitere Informationen zum *Registrierungsstatus* der Lizenz anzeigen möchten, bewegen Sie den Mauszeiger über den *Registrierten* Status. Es wird eine Dialogmeldung mit folgenden Informationen angezeigt:

License

To view and manage Smart Software Licenses for your Cisco Smart Account, go to [Smart Licensing Manager](#) Actions

Smart Software Licensing Status

Registration Status: **Registered**

License Authorization Status: **Authorized (A)**

Smart Account: [Redacted]

Virtual Account: [Redacted]

PID: RV340-K9

Export-Controlled Functionality: Allowed

This product is registered for Smart Software Licensing

Initial Registration: [Redacted] 2019 11:01:37 (Succeed)

Next Renewal Attempt: [Redacted] 2020 11:01:36

Registration Expire: [Redacted] 2020 10:55:01

- Erstregistrierung: In diesem Bereich werden Datum und Uhrzeit der Lizenzregistrierung angezeigt.
- Nächster Verlängerungsversuch: In diesem Bereich werden das Datum und die Uhrzeit angezeigt, zu dem der Router versucht, die Lizenz zu verlängern.
- Registrierung abgelaufen - In diesem Bereich werden das Datum und die Uhrzeit der Registrierung angezeigt.

Schritt 13

Überprüfen Sie auf der *Lizenzseite*, ob der Status *Sicherheitslizenz Authorized (Autorisiert)* angezeigt wird. Sie können auch auf die Schaltfläche **Lizenz auswählen** klicken, um zu überprüfen, ob die *Sicherheitslizenz* aktiviert ist.

Wenn bei diesem Schritt Probleme auftreten, müssen Sie den Router möglicherweise neu starten.

Choose Smart Licenses

Choose Smart Licenses to be used by this product. Ensure you have a sufficient number of licenses in the Virtual Account associated with this product, otherwise it will be out of compliance.

Enable	Name (Version)	Description	Count
<input checked="" type="checkbox"/>	Security-License	Anti Threat Services: IPS, ApplID, Dynamic Web...	--

Save and Authorize Cancel

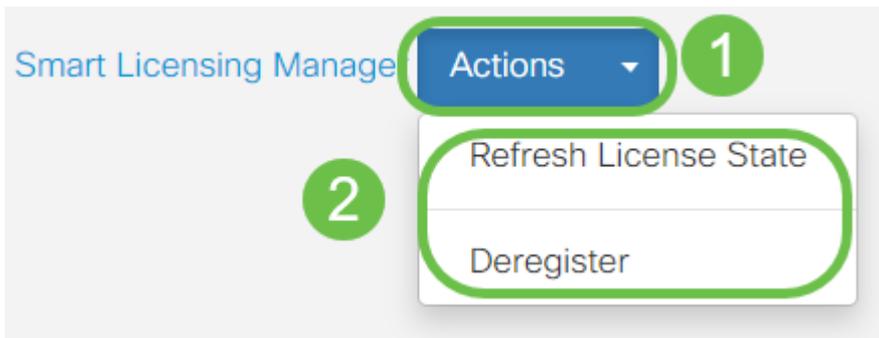
Choose Licenses

Name	Description	Count	Status
Security-License	Anti Threat Services: IPS, ApplID, Dynamic Web Filter, G...	--	Authorized

Schritt 14 (optional)

Um den *Lizenzstatus* zu aktualisieren oder die *Registrierung* der Lizenz vom Router zu löschen, klicken Sie auf das *Smart Licensing Manager-Aktionen*-Dropdown-Menü und

wählen Sie eine Aktion aus.



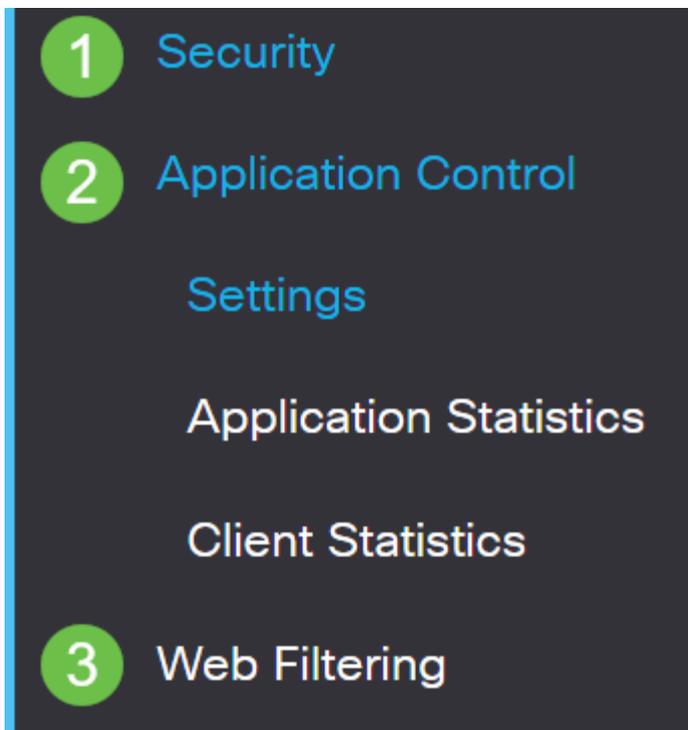
Nachdem Sie Ihre Lizenz auf dem Router installiert haben, müssen Sie die Schritte im nächsten Abschnitt ausführen.

Webfilterung auf dem RV345P-Router

Sie haben 90 Tage nach der Aktivierung Zeit, um kostenlos eine Webfilterung zu verwenden. Nach der kostenlosen Testversion müssen Sie eine Lizenz erwerben, wenn Sie diese Funktion weiterhin verwenden möchten. [Klicken Sie, um zu diesem Abschnitt zurückzukehren.](#)

Schritt 1

Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Sicherheit > Anwendungskontrolle > Webfilterung** aus.



Schritt 2

Wählen Sie das Optionsfeld **Ein**.

Web Filtering

Web Filtering: On Off

Schritt 3

Klicken Sie auf das **Symbol Hinzufügen**.

Web Filtering Policies



Policies

Schritt 4

Geben Sie einen *Richtliniennamen*, eine *Beschreibung* und das Kontrollkästchen *Aktivieren ein*.

Policy Profile-Add/Edit

Policy Name:

1

Weekdays

Description:

2

Default-High

Enable:

3



Wenn die Inhaltsfilterung auf Ihrem Router aktiviert ist, wird eine Benachrichtigung angezeigt, die Sie darüber informiert, dass die Inhaltsfilterung deaktiviert wurde und dass die beiden Funktionen nicht gleichzeitig aktiviert werden können. Klicken Sie auf **Apply**, um

mit der Konfiguration fortzufahren.

Schritt 5

Aktivieren Sie das Kontrollkästchen Webreputation, um die Filterung auf Grundlage eines Webreputations-Index zu aktivieren.

Web Reputation



Die Filterung der Inhalte erfolgt nach dem Bekanntheitsgrad einer Website oder einer URL basierend auf einem Web-Reputationsindex. Wenn die Punktzahl unter 40 fällt, wird die Website blockiert. Weitere Informationen zur Web-Reputationstechnologie finden Sie [hier](#).

Schritt 6

Wählen Sie aus der Dropdown-Liste *Device Type (Gerätetyp)* die Quelle/das Ziel der zu filternden Pakete aus. Es kann jeweils nur eine Option ausgewählt werden. Folgende Optionen sind verfügbar:

- BELIEBIG - Wählen Sie diese Option, um die Richtlinie auf jedes Gerät anzuwenden.
- Kamera: Wählen Sie diese Option aus, um die Richtlinie auf Kameras (z. B. IP-Sicherheitskameras) anzuwenden.
- Computer - Wählen Sie diese Option aus, um die Richtlinie auf Computer anzuwenden.
- Game_Console: Wählen Sie diese Option aus, um die Richtlinie auf Spielekonsolen anzuwenden.
- Media_Player: Wählen Sie diese Option, um die Richtlinie auf Media Player anzuwenden.
- Mobile - Wählen Sie diese Option, um die Richtlinie auf mobile Geräte anzuwenden.
- VoIP: Wählen Sie diese Option aus, um die Richtlinie auf Voice over Internet Protocol-Geräte anzuwenden.

Policy Profile-Add/Edit

IP Group:

Any



Device Type:

ANY



OS Type:

ANY

Camera

Computer

Game_Console

Schritt 7

Wählen Sie aus der Dropdown-Liste *OS Type (Betriebssystemtyp)* ein Betriebssystem aus, für das die Richtlinie gelten soll. Es kann jeweils nur eine Option ausgewählt werden. Folgende Optionen sind verfügbar:

- BELIEBIG - Wendet die Richtlinie auf jeden Betriebssystemtyp an. Dies ist die Standardeinstellung.
- Android - Diese Richtlinie gilt nur für Android-Betriebssysteme.
- BlackBerry - Wendet die Richtlinie nur auf Blackberry-Betriebssysteme an.
- Linux — Anwendung der Richtlinie nur auf Linux-Betriebssysteme.
- Mac_OS_X — Wendet die Richtlinie nur auf Mac OS an.
- Other (Andere) - Wendet die Richtlinie auf ein Betriebssystem an, das nicht aufgeführt ist.
- Windows — Wendet die Richtlinie auf das Windows-Betriebssystem an.
- iOS - Gilt nur für iOS-Betriebssysteme.

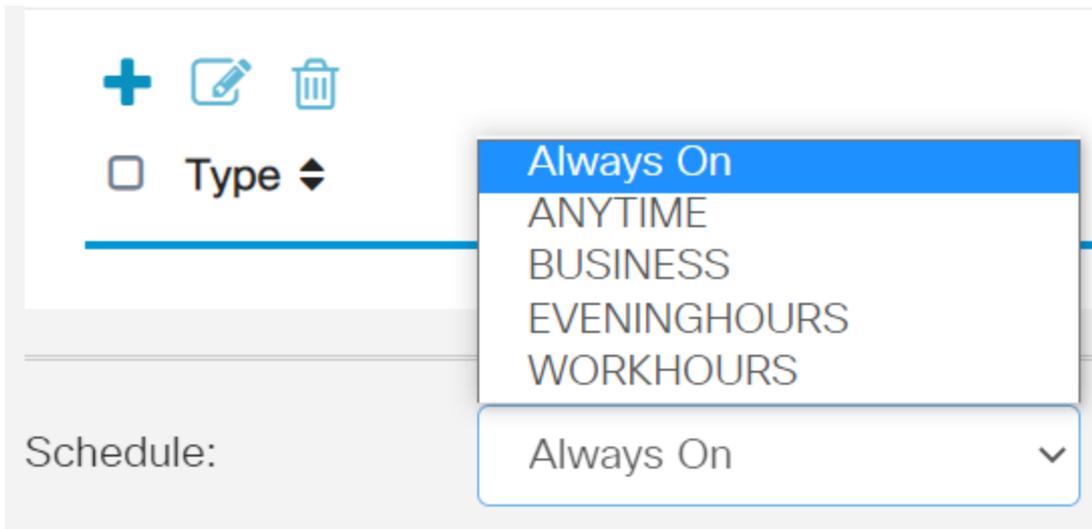
The screenshot shows a configuration interface with the following elements:

- Application:** A label followed by a blue **Edit** button.
- Application List Table:** A table header.
- Category:** A dropdown menu with a double-headed arrow icon, currently showing **ANY**.
- IP Group:** A label.
- Device Type:** A label.
- OS Type:** A dropdown menu with a downward arrow icon, currently showing **ANY**.

The dropdown menu for **OS Type** is open, displaying the following options: **ANY**, **Android**, **BlackBerry**, **Linux**, **Mac_OS_X**, **Other**, **Windows**, and **iOS**.

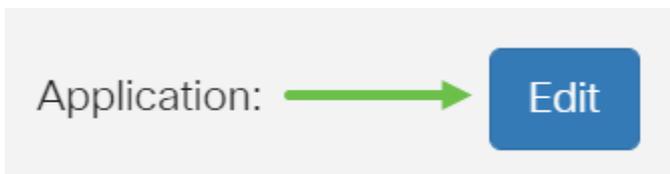
Schritt 8

Blättern Sie nach unten zum Abschnitt *Zeitplan*, und wählen Sie die Option aus, die Ihren Anforderungen am besten entspricht.



Schritt 9

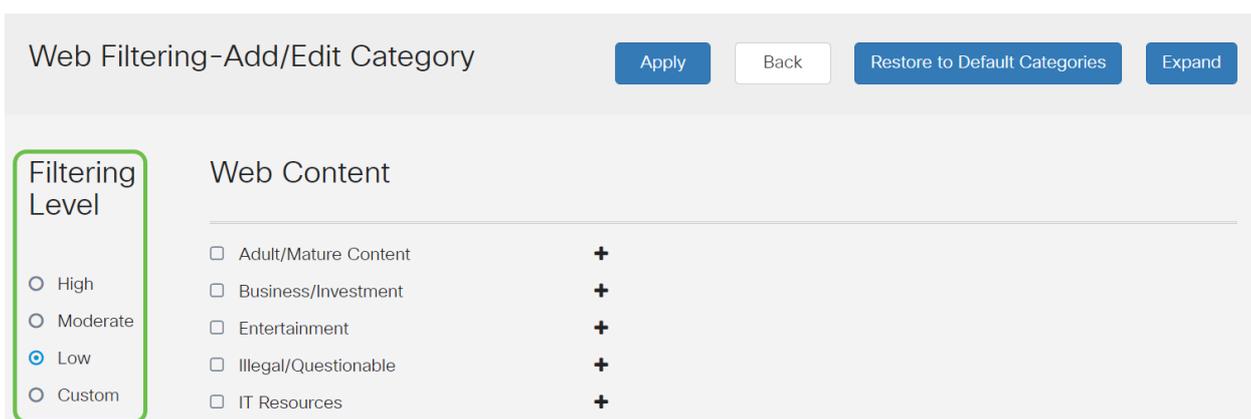
Klicken Sie auf das **Bearbeitungssymbol**.



Schritt 10

Klicken Sie in der Spalte Filterebene auf ein Optionsfeld, um schnell das Filtervolumen zu definieren, das den Netzwerkrichtlinien am besten entspricht. Die Optionen sind Hoch, Mittel, Niedrig und Benutzerdefiniert. Klicken Sie auf eine der unten stehenden Filterebenen, um die vordefinierten Unterkategorien zu erfahren, die jeweils für die jeweilige aktivierte Web Content-Kategorie gefiltert wurden. Vordefinierte Filter können nicht mehr geändert werden und sind ausgegraut.

- **Niedrig** - Dies ist die Standardoption. Mit dieser Option wird die Sicherheit aktiviert.
- **Mäßig** - Erwachsene/Erwachsene-Inhalte, rechtswidrig/fraglich und Sicherheit sind mit dieser Option aktiviert.
- **Hoch** - Erwachsene/ausgereifte Inhalte, Business/Investitionen, Illegal/Fraglich, IT-Ressourcen und Sicherheit sind mit dieser Option aktiviert.
- **Benutzerdefiniert**: Es sind keine Standardeinstellungen festgelegt, um benutzerdefinierte Filter zuzulassen.



Schritt 11

Geben Sie die Webinhalte ein, die gefiltert werden sollen. Klicken Sie auf das **Pluszeichen**, wenn Sie weitere Details zu einem Bereich wünschen.

Web Filtering-Add/Edit Category

Apply Back Restore to Default Categories Expand

Filtering Level

High
Moderate
Low
Custom

Web Content

- Adult/Mature Content +
- Business/Investment +
- Entertainment +
- Illegal/Questionable +
- IT Resources +
- Lifestyle/Culture +
- Other +
- Security +

Schritt 12 (optional)

Um alle Unterkategorien und Beschreibungen von Webinhalten anzuzeigen, können Sie auf die Schaltfläche **Erweitern** klicken.

Apply Back Restore to Default Categories Expand

Schritt 13 (optional)

Klicken Sie auf **Collapse**, um die Unterkategorien und Beschreibungen zu reduzieren.

Apply Back Restore to Default Categories Collapse

Schritt 14 (optional)

Um zu den Standardkategorien zurückzukehren, klicken Sie auf **Wiederherstellen zu Standardkategorien**.

Apply Back Restore to Default Categories Collapse

Schritt 15

Klicken Sie auf **Apply**, um die Konfiguration zu speichern und zur Seite Filter zurückzukehren, um mit der Einrichtung fortzufahren.

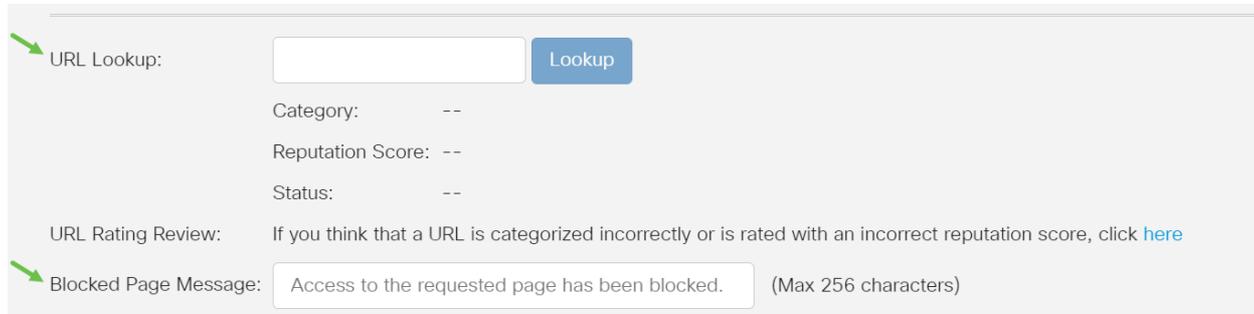
Apply Cancel

In der Anwendungslistentabelle füllen die entsprechenden Unterkategorien basierend auf

der gewählten Filterebene die Tabelle aus.

Schritt 16 (optional)

Weitere Optionen sind die URL-Suche und die Meldung, die anzeigt, wann eine angeforderte Seite blockiert wurde.



The screenshot shows a configuration panel with the following elements:

- URL Lookup:** A text input field followed by a blue "Lookup" button. A green arrow points to the input field.
- Category:** --
- Reputation Score:** --
- Status:** --
- URL Rating Review:** Text: "If you think that a URL is categorized incorrectly or is rated with an incorrect reputation score, click [here](#)".
- Blocked Page Message:** A text input field containing "Access to the requested page has been blocked." and a "(Max 256 characters)" label. A green arrow points to the input field.

Schritt 17 (optional)

Klicken Sie auf Apply (Anwenden).



The screenshot shows two buttons: a blue "Apply" button with a green border and a white "Cancel" button with a grey border.

Schritt 18

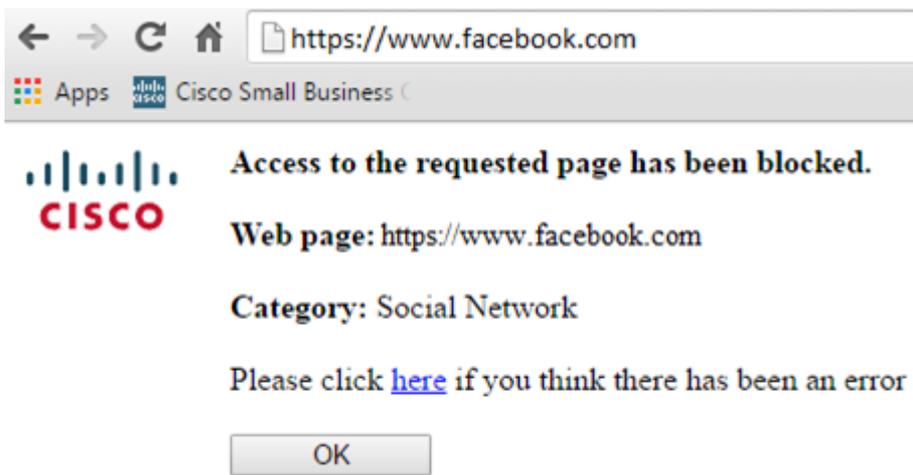
Um die Konfiguration dauerhaft zu speichern, rufen Sie die Seite *Konfiguration kopieren/speichern auf*, oder klicken Sie auf das **Speichersymbol** oben auf der Seite.



Schritt 19 (optional)

Um zu überprüfen, ob eine Website oder URL gefiltert oder blockiert wurde, starten Sie einen Webbrowser oder öffnen Sie eine neue Registerkarte in Ihrem Browser. Geben Sie den Domain-Namen ein, den Sie aufgelistet haben oder dessen Blockierung blockiert oder abgelehnt wurde.

In diesem Beispiel haben wir www.facebook.com verwendet.



Sie sollten jetzt die Webfilterung auf Ihrem RV345P-Router erfolgreich konfiguriert haben. Da Sie die RV Security-Lizenz für die Webfilterung verwenden, benötigen Sie Umbrella wahrscheinlich nicht. Wenn Sie Umbrella auch möchten, [klicken Sie hier](#). Wenn Sie über genügend Sicherheit verfügen, [klicken Sie auf, um zum nächsten Abschnitt zu wechseln](#).

Fehlerbehebung

Wenn Sie eine Lizenz erworben haben, diese jedoch nicht in Ihrem virtuellen Konto aufgeführt ist, haben Sie zwei Möglichkeiten:

1. Setzen Sie sich mit dem Händler in Verbindung, um ihn zu bitten, die Weiterleitung vorzunehmen.
2. Kontaktieren Sie uns, und wir werden uns mit dem Händler in Verbindung setzen.

Im Idealfall müssten Sie das auch nicht tun, aber wenn Sie an dieser Kreuzung ankommen, helfen wir Ihnen gerne weiter! Um den Prozess so schnell wie möglich zu gestalten, benötigen Sie die Anmeldeinformationen in der obigen Tabelle sowie die unten aufgeführten.

Erforderliche Informationen	Suchen von Informationen
Lizenzrechnung Cisco Verkaufsauftragsnummer	Sie erhalten diese E-Mail nach Abschluss des Erwerbs der Lizenzen. Um dies zu erhalten, müssen Sie möglicherweise zum Händler zurückkehren. Mit einem Screenshot können Sie den Inhalt Ihres Bildschirms für unser Team freigeben.
Screenshot Ihrer Smart Account-Lizenzseite	Wenn Sie mit Screenshots nicht vertraut sind, können Sie die folgenden Methoden verwenden.

Screenshots

Wenn Sie über ein Token verfügen oder eine Fehlerbehebung durchführen, sollten Sie einen Screenshot erstellen, um den Inhalt des Bildschirms zu erfassen.

Aufgrund der Unterschiede in der Vorgehensweise zum Erfassen eines Screenshots

finden Sie im Folgenden Links speziell zu Ihrem Betriebssystem.

- [Windows](#)
- [MAC](#)
- [iPhone/iPad](#)
- [Android](#)

Umbrella RV Branch License (optional)

Umbrella ist eine einfache, aber sehr effektive Cloud-Sicherheitsplattform von Cisco.

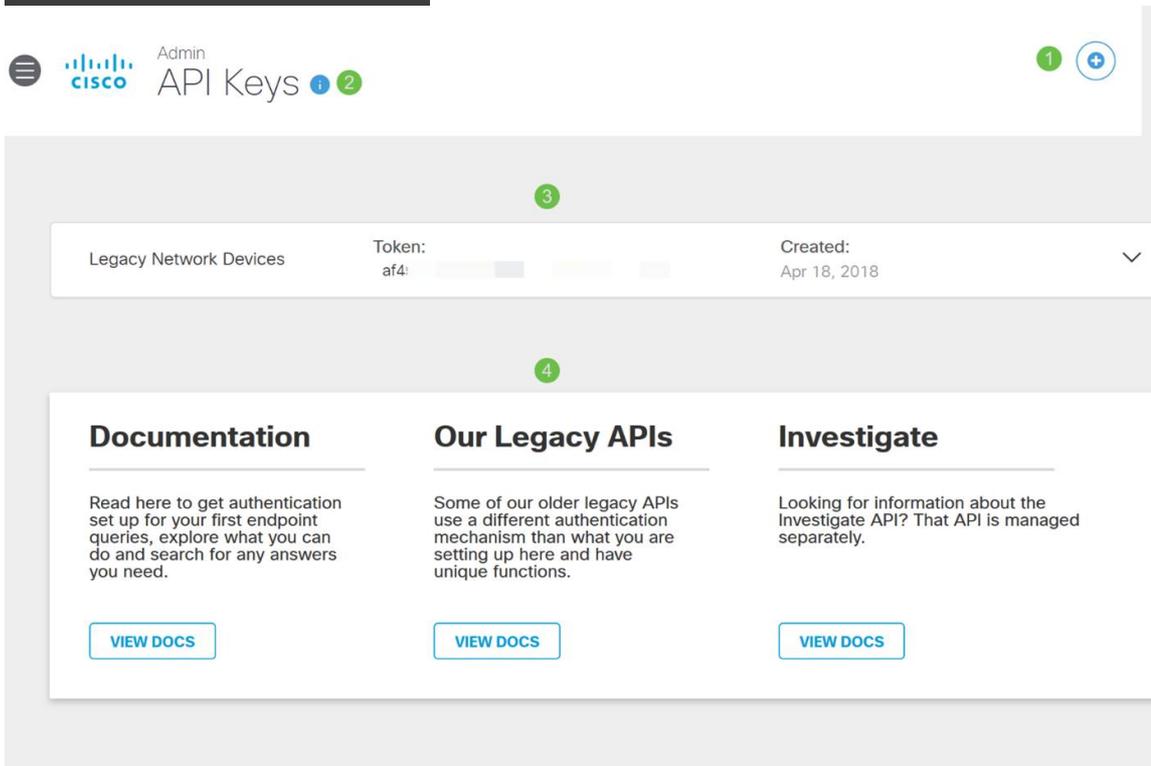
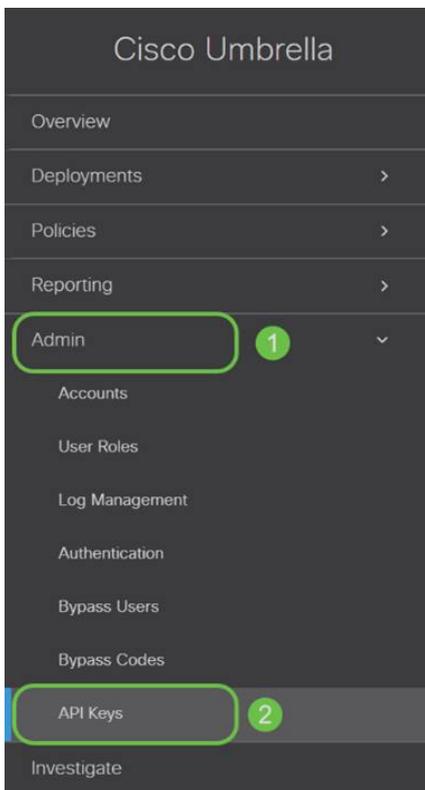
Umbrella arbeitet in der Cloud und führt viele sicherheitsrelevante Services durch. Von der Bedrohung bis zur Untersuchung nach einem Ereignis. Umbrella erkennt und verhindert Angriffe über alle Ports und Protokolle hinweg.

Umbrella verwendet DNS als Hauptvektor für die Verteidigung. Wenn Benutzer eine URL in ihre Browser-Leiste eingeben und auf *Enter* drücken, nimmt Umbrella an der Übertragung teil. Diese URL wird an den DNS-Resolver von Umbrella weitergeleitet. Wenn eine Sicherheitswarnung mit der Domäne verknüpft ist, wird die Anforderung blockiert. Diese Telemetriedaten werden in Mikrosekunden analysiert, wodurch eine Latenz nahezu vermieden wird. Die Telemetriedaten nutzen Protokolle und Instrumente, um weltweit Milliarden von DNS-Anfragen zu verfolgen. Wenn diese Daten allgegenwärtig sind, können sie weltweit korreliert werden, um schnell auf Angriffe reagieren zu können, sobald diese beginnen. Weitere Informationen finden Sie in den Datenschutzrichtlinien von Cisco: [vollständige Richtlinie](#), [Kurzfassung](#). Telemetriedaten sind Daten, die von Tools und Protokollen abgeleitet wurden.

Besuchen Sie [Cisco Umbrella](#), um mehr zu erfahren und ein Konto einzurichten. Wenn Probleme auftreten, [finden Sie hier Dokumentation](#) und [hier die Support-Optionen für Umbrella](#).

Schritt 1

Wenn Sie sich bei Ihrem Umbrella Account angemeldet haben, klicken Sie im *Dashboard*-Bildschirm auf **Admin > API Keys (Admin > API-Schlüssel)**.



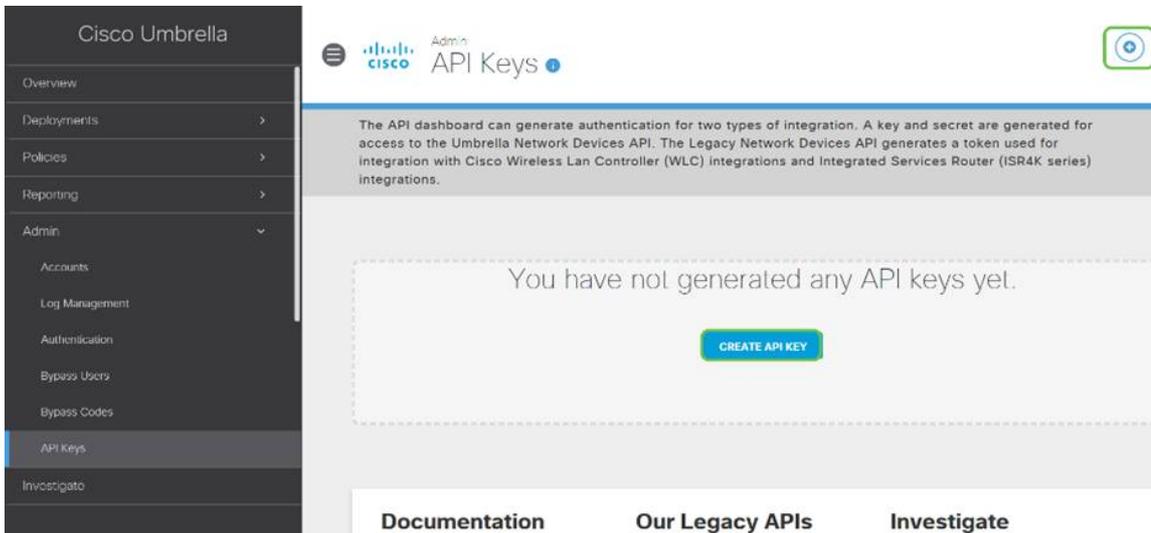
Anatomie des Bildschirms "API Keys" (API-Schlüssel) (mit bereits vorhandenem API-Schlüssel)

1. Add API Key (API-Schlüssel hinzufügen): Initiiert die Erstellung eines neuen Schlüssels für die Verwendung mit der Umbrella API.
2. Zusätzliche Informationen: Hiermit wird ein Explorer für diesen Bildschirm nach unten bzw. nach oben verschoben.
3. Token Well - Enthält alle Schlüssel und Token, die von diesem Konto erstellt wurden. (Fügt nach dem Erstellen eines Schlüssels ein)

4. Support-Dokumente - Links zu Dokumentationen auf der übergeordneten Website zu den Themen in den einzelnen Abschnitten.

Schritt 2

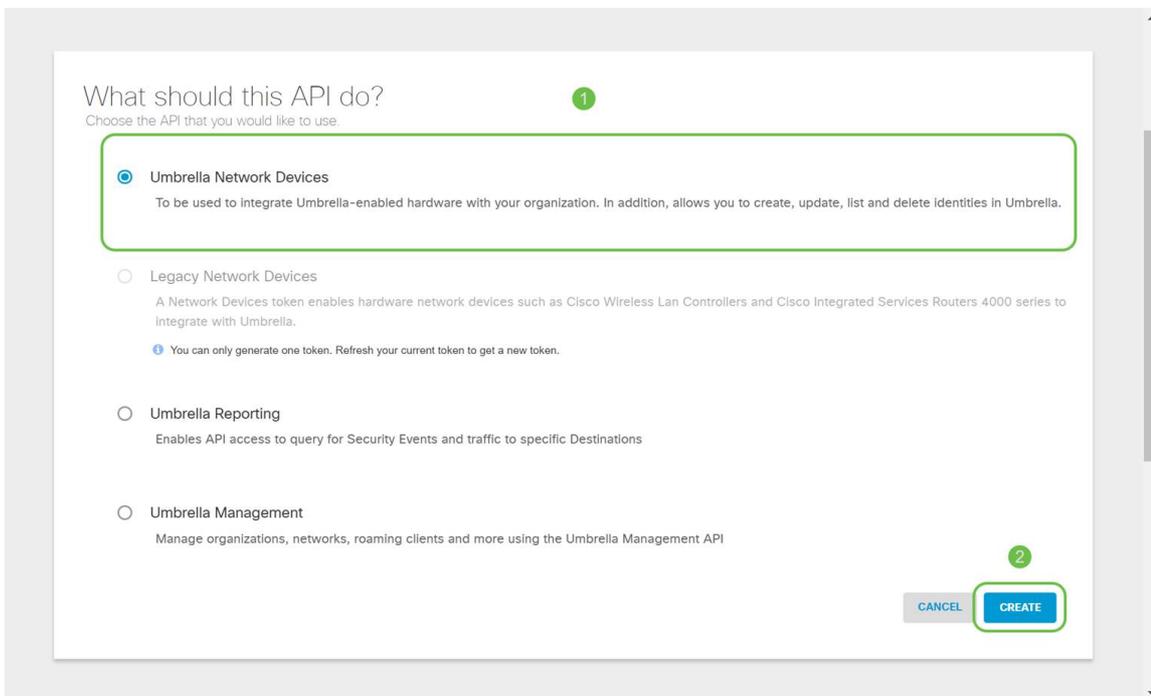
Klicken Sie in der rechten oberen Ecke auf die Schaltfläche **API-Schlüssel hinzufügen**, oder klicken Sie auf die Schaltfläche **API-Schlüssel erstellen**. Beide funktionieren gleich.



Der obige Screenshot entspricht dem, was Sie zum ersten Mal sehen würden, wenn Sie dieses Menü öffnen.

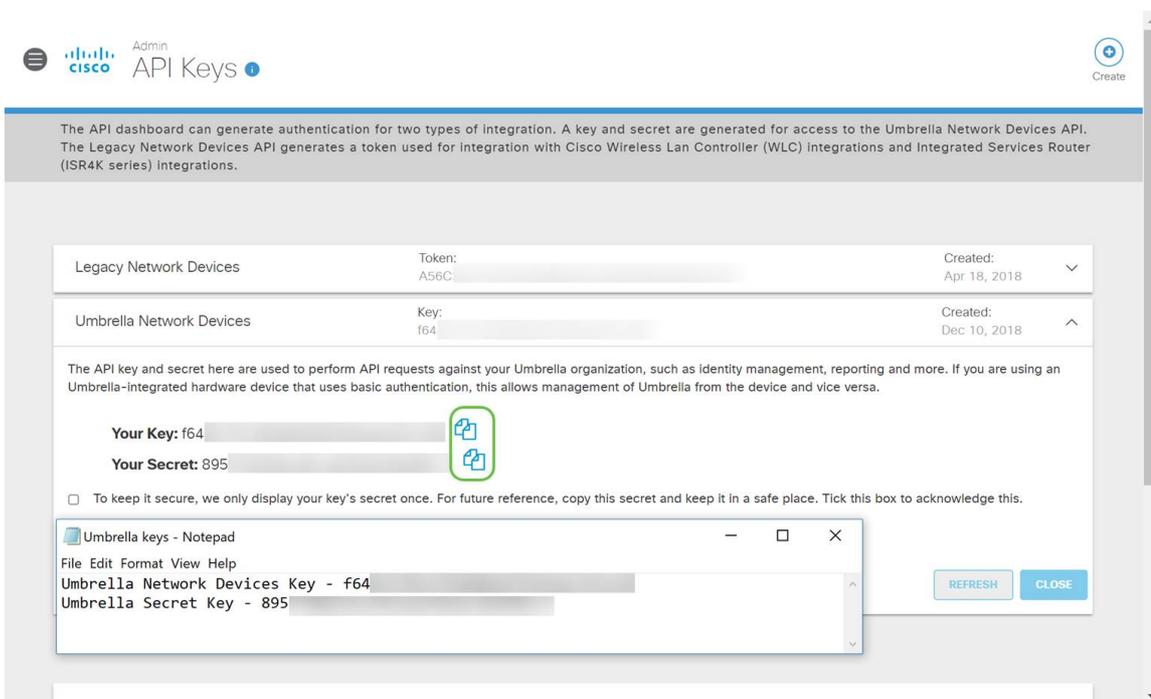
Schritt 3

Wählen Sie **Umbrella Network Devices** und klicken Sie dann auf die Schaltfläche **Create** (Erstellen).



Schritt 4

Öffnen Sie einen Text-Editor wie notepad, und klicken Sie dann auf das **Kopiersymbol** rechts neben der API und dem API-*Geheimschlüssel*. Eine Popup-Benachrichtigung bestätigt, dass der Schlüssel in die Zwischenablage kopiert wird. Fügen Sie jeweils Ihren geheimen und API-Schlüssel in das Dokument ein, und kennzeichnen Sie ihn als zukünftige Referenz. In diesem Fall ist die Bezeichnung "Umbrella network devices key" (Netzwerkgeräteschlüssel für Umbrella). Speichern Sie die Textdatei an einem sicheren Ort, der später leicht zugänglich ist.



Schritt 5

Nachdem Sie den Schlüssel und geheimen Schlüssel in einen sicheren Bereich kopiert haben, klicken Sie im *Bildschirm Umbrella API* auf das **Kontrollkästchen**, um die Bestätigung der temporären Anzeige des geheimen Schlüssels abzuschließen, und klicken Sie dann auf die Schaltfläche **Schließen**.

To keep it secure, we only display your key's secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

1 Check out the [documentation](#) for step by step instructions.

DELETE

REFRESH

CLOSE

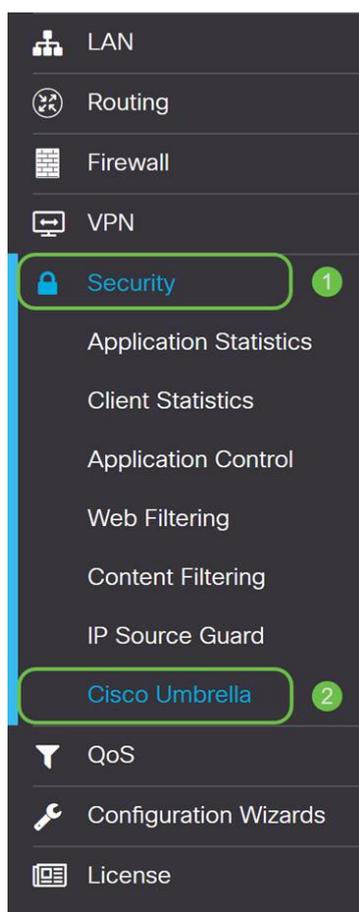
Wenn Sie den geheimen Schlüssel verlieren oder versehentlich löschen, gibt es keine Funktion oder Support-Nummer, um diesen Schlüssel abzurufen. Wenn der Schlüssel verloren geht, müssen Sie den Schlüssel löschen und den neuen API-Schlüssel mit jedem Gerät, das Sie mit Umbrella schützen möchten, erneut autorisieren.

Konfigurieren von Umbrella auf dem RV345P

Nachdem wir API-Schlüssel in Umbrella erstellt haben, können Sie diese Schlüssel auf Ihrem RV345P installieren.

Schritt 1

Nachdem Sie sich bei Ihrem RV345P-Router angemeldet haben, klicken Sie im Seitenleistenmenü auf **Sicherheit > Umbrella**.



Schritt 2

Der Bildschirm Umbrella API bietet eine Reihe von Optionen. Klicken Sie auf das Kontrollkästchen **Enable (Aktivieren)**, um Umbrella zu aktivieren.

Cisco Umbrella

Apply Cancel

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

Enable
 Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

If you use "Network" as this router's identity.

- Go to [DNS-O-MATIC](#) website, create an account and add your OpenDNS account to it.
- Go to [DNS-O-MATIC Settings](#) to enable DNS-O-MATIC so your WAN IP change can be propagated to OpenDNS/Umbrella.

Advanced Configuration

Local Domain To Bypass (Optional): +

DNSCrypt: Enable

Public Key:

If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

Schritt 3 (optional)

Standardmäßig ist das Feld *LAN-DNS-Abfragen blockieren* aktiviert. Diese tolle Funktion erstellt automatisch Zugriffskontrolllisten auf Ihrem Router, die verhindern, dass DNS-Datenverkehr ins Internet gelangt. Diese Funktion erzwingt, dass alle Anfragen zur Domänenübersetzung über den RV345P weitergeleitet werden. Dies ist für die meisten Benutzer eine gute Idee.

Schritt 4

Der nächste Schritt wird auf zwei verschiedene Arten ausgeführt. Beide hängen von der Einrichtung Ihres Netzwerks ab. Wenn Sie einen Dienst wie DynDNS oder NoIP verwenden, lassen Sie das Standardnamensschema "Network" (Netzwerk). Sie müssen sich bei diesen Konten anmelden, um sicherzustellen, dass Umbrella-Schnittstellen mit diesen Diensten verbunden sind, da sie Schutz bieten. Für unsere Zwecke nutzen wir "Netzwerkgerät", also klicken wir auf das untere Optionsfeld.

Cisco Umbrella

Apply Cancel

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

Enable
 Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

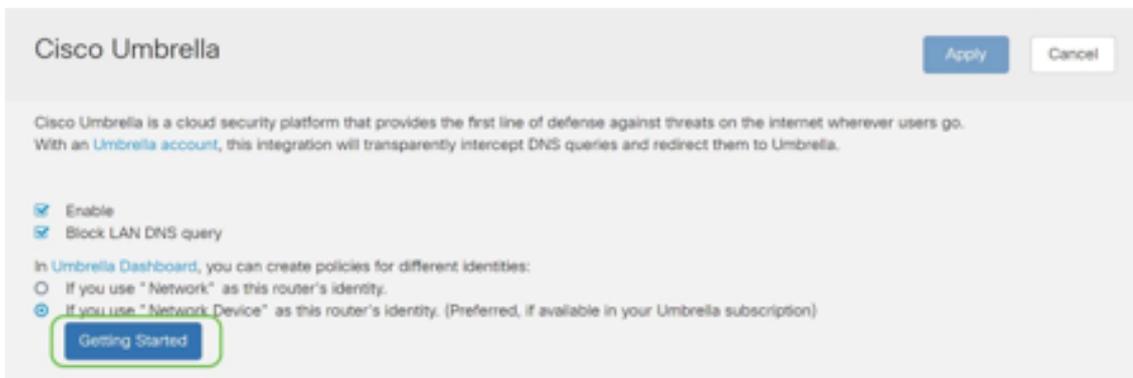
If you use "Network" as this router's identity.

If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

Getting Started

Schritt 5

Klicken Sie auf **Erste Schritte**.



Cisco Umbrella

Apply Cancel

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.

Enable
 Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

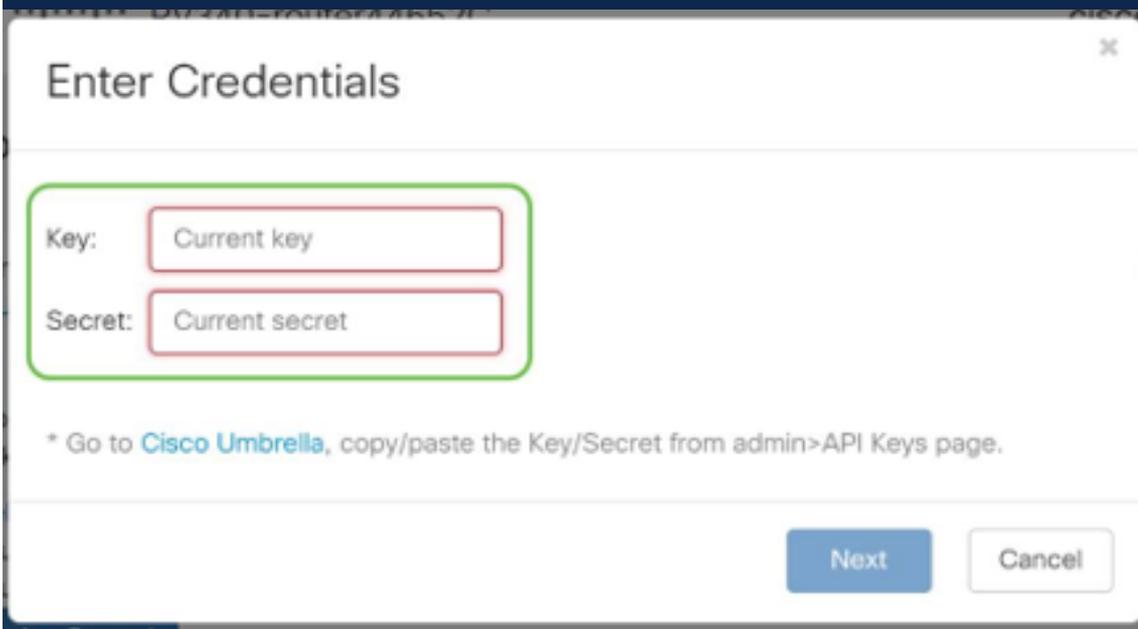
If you use "Network" as this router's identity.
 If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

Getting Started

Schritt 6

Geben Sie den **API-Schlüssel** und den **Geheimschlüssel** in die Textfelder ein.

Zweimal anrufen, um zu wissen, dass es wichtig ist! Wenn Sie den geheimen Schlüssel verlieren oder versehentlich löschen, gibt es keine Funktion oder Support-Nummer, um diesen Schlüssel abzurufen. Halte es geheim und sicher. Wenn der Schlüssel verloren geht, müssen Sie den Schlüssel löschen und den neuen API-Schlüssel mit jedem Gerät, das Sie mit Umbrella schützen möchten, erneut autorisieren.



Enter Credentials

Key:

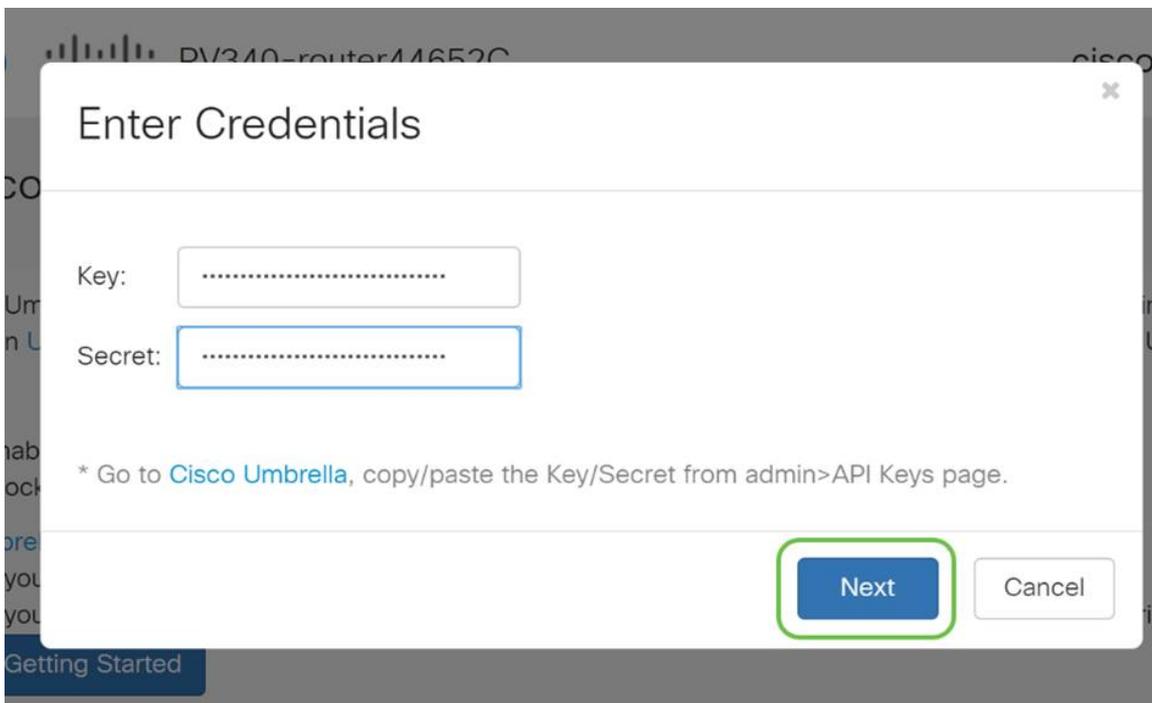
Secret:

* Go to [Cisco Umbrella](#), copy/paste the Key/Secret from admin>API Keys page.

Next Cancel

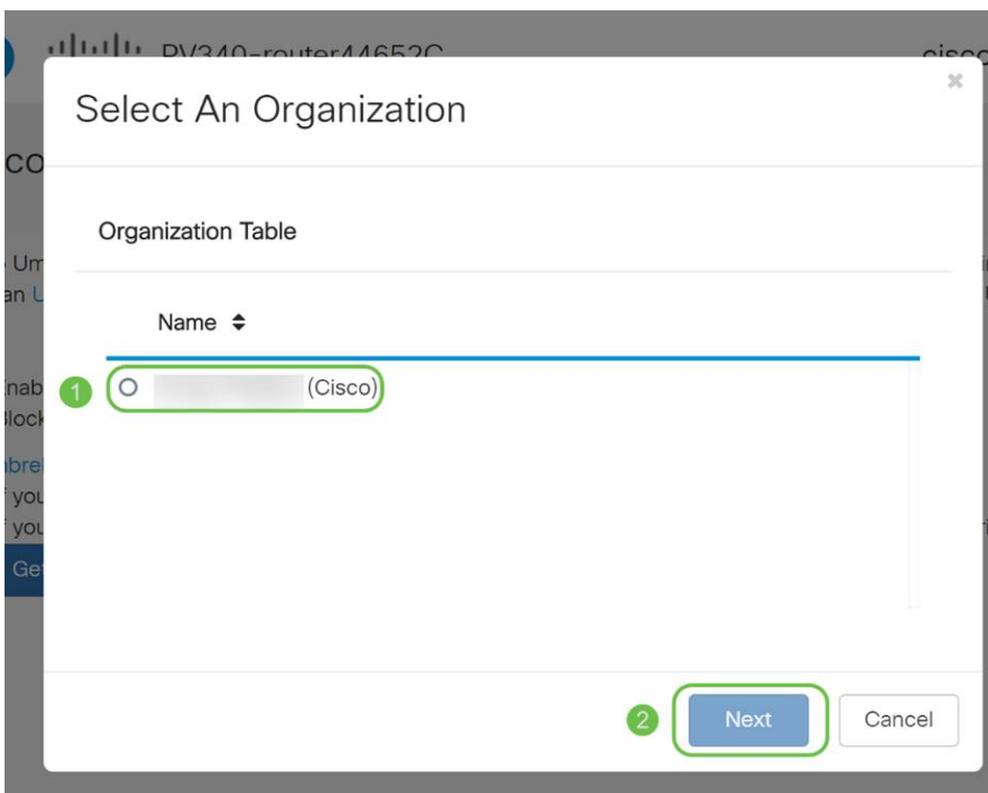
Schritt 7

Klicken Sie nach Eingabe der API und des Geheimschlüssels auf die Schaltfläche **Weiter**.



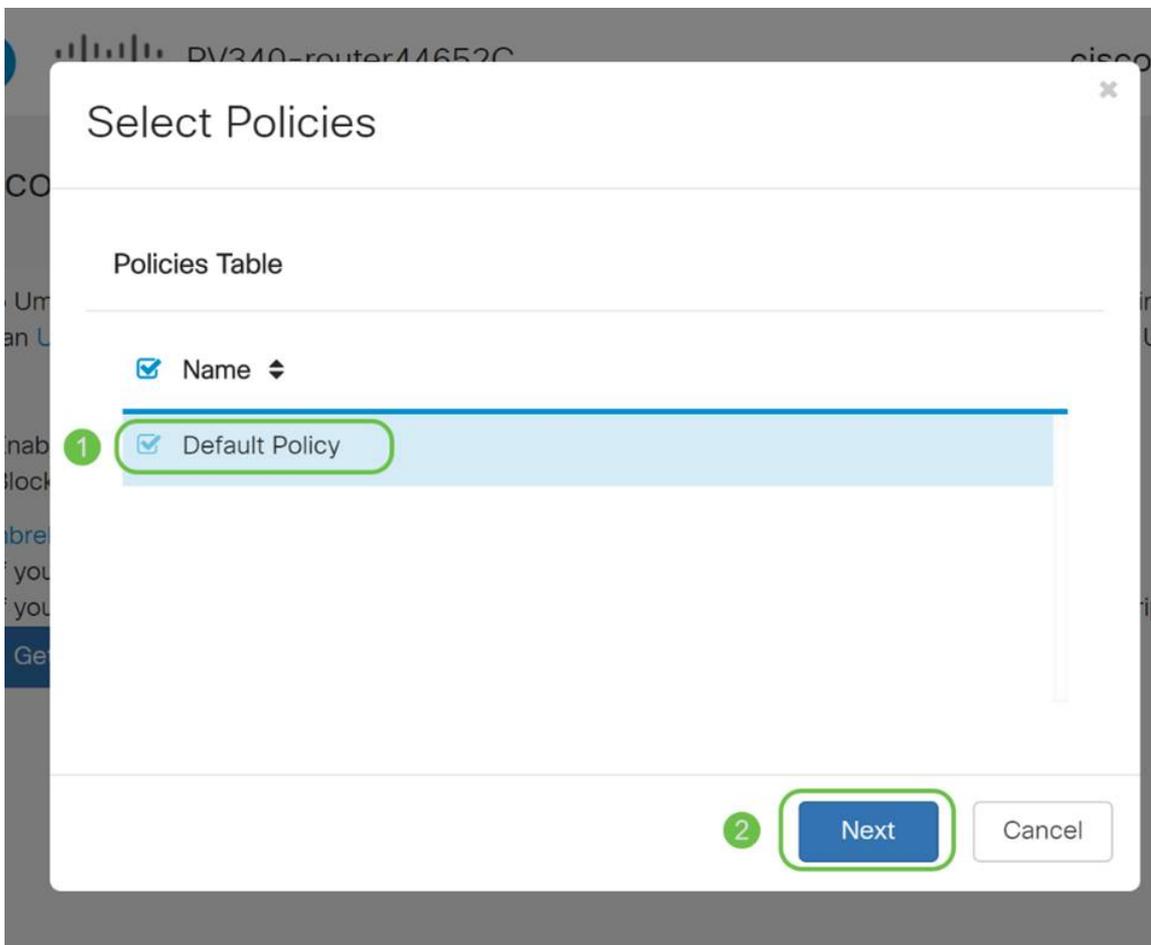
Schritt 8

Wählen Sie im nächsten Bildschirm die **Organisation** aus, die Sie dem Router zuordnen möchten. Klicken Sie auf **Weiter**.



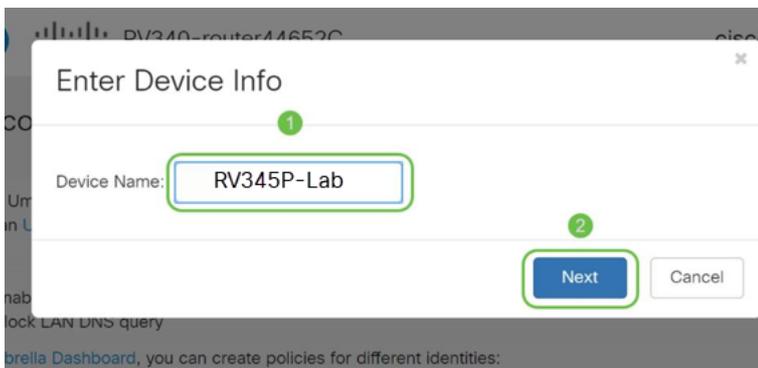
Schritt 9

Wählen Sie die Richtlinie aus, die auf den vom RV345P weitergeleiteten Datenverkehr angewendet werden soll. Für die meisten Benutzer bietet die Standardrichtlinie eine ausreichende Abdeckung.



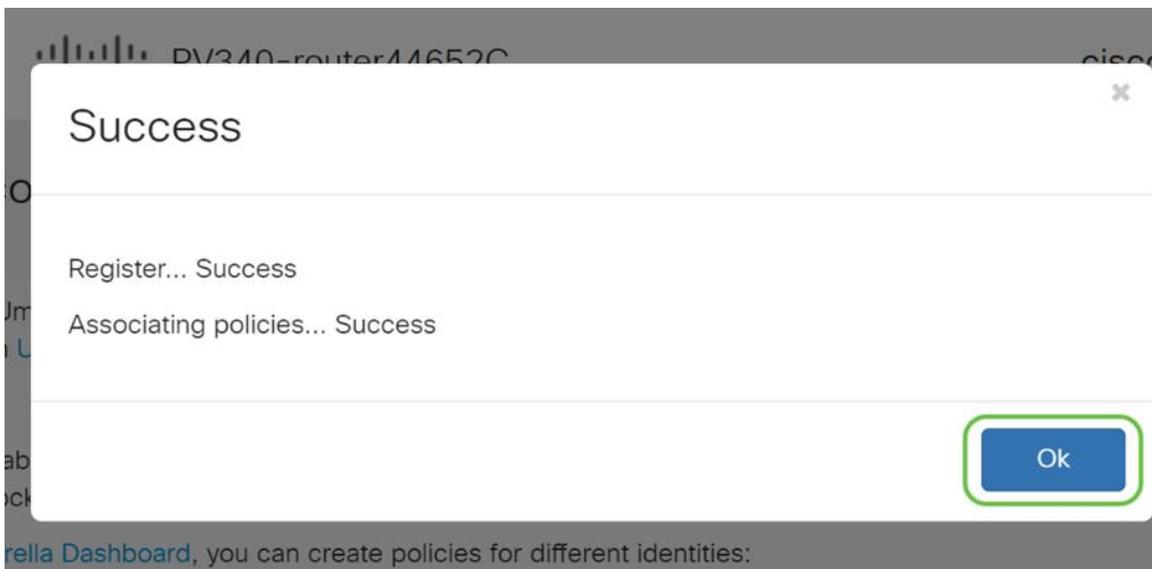
Schritt 10

Weisen Sie dem Gerät einen Namen zu, damit es in der Umbrella-Berichterstattung bezeichnet werden kann. In unserer Konfiguration haben wir sie *RV345P-Lab* genannt.



Schritt 11

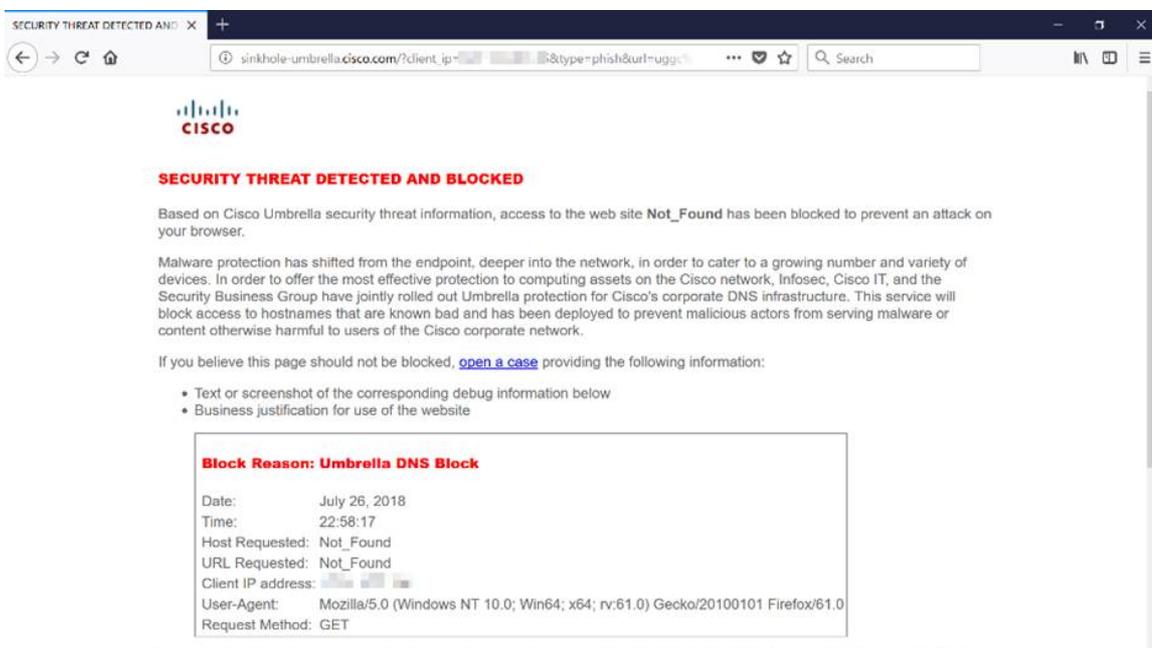
Im nächsten Bildschirm werden die von Ihnen ausgewählten Einstellungen validiert und eine Aktualisierung angezeigt, wenn diese erfolgreich zugeordnet wurde. Klicken Sie auf **OK**.



Bestätigung

Herzlichen Glückwunsch! Sie sind jetzt durch Cisco Umbrella geschützt. Oder sind Sie es? Lassen Sie uns sicherstellen, dass Sie das Beispiel durch eine Doppelprüfung überprüfen. Cisco hat eine Website erstellt, auf der Sie genau festlegen können, wie schnell die Seite geladen wird. [Klicken Sie hier](#), oder geben Sie <https://InternetBadGuys.com> in die Browserleiste ein.

Wenn Umbrella korrekt konfiguriert ist, werden Sie von einem Bildschirm ähnlich wie diesem begrüßt.



Weitere Sicherheitsoptionen

Befürchten Sie, dass jemand versuchen würde, einen unbefugten Zugriff auf das Netzwerk zu erlangen, indem er ein Ethernet-Kabel von einem Netzwerkgerät abzieht und eine Verbindung mit diesem herstellt? In diesem Fall ist es wichtig, eine Liste der zulässigen Hosts zu registrieren, die direkt mit dem Router eine Verbindung mit den entsprechenden IP- und MAC-Adressen herstellen können. Anweisungen finden Sie im Artikel [Configure IP Source Guard on the RV34x Series Router](#).

VPN-Optionen

Über eine VPN-Verbindung (Virtual Private Network) können Benutzer auf ein privates Netzwerk (z. B. das Internet) zugreifen, Daten an ein privates Netzwerk senden und von diesem empfangen. Dabei wird eine sichere Verbindung zu einer zugrunde liegenden Netzwerkinfrastruktur zum Schutz des privaten Netzwerks und seiner Ressourcen sichergestellt.

Ein VPN-Tunnel richtet ein privates Netzwerk ein, das Daten sicher mit Verschlüsselung und Authentifizierung senden kann. Die meisten Firmenbüros verwenden eine VPN-Verbindung, da es sowohl nützlich als auch notwendig ist, den Mitarbeitern den Zugriff auf ihr privates Netzwerk zu ermöglichen, selbst wenn sie sich außerhalb des Büros befinden.

Mit dem VPN kann ein Remote-Host so agieren, als ob er sich im selben lokalen Netzwerk befinde. Der Router unterstützt bis zu 50 Tunnel. Nachdem der Router für die Internetverbindung konfiguriert wurde, kann zwischen dem Router und einem Endpunkt eine VPN-Verbindung eingerichtet werden. Der VPN-Client ist vollständig von den Einstellungen des VPN-Routers abhängig, um eine Verbindung herstellen zu können.

Wenn Sie nicht sicher sind, welches VPN am besten zu Ihren Anforderungen passt, sehen Sie sich die [Cisco Business VPN Übersicht und Best Practices an](#).

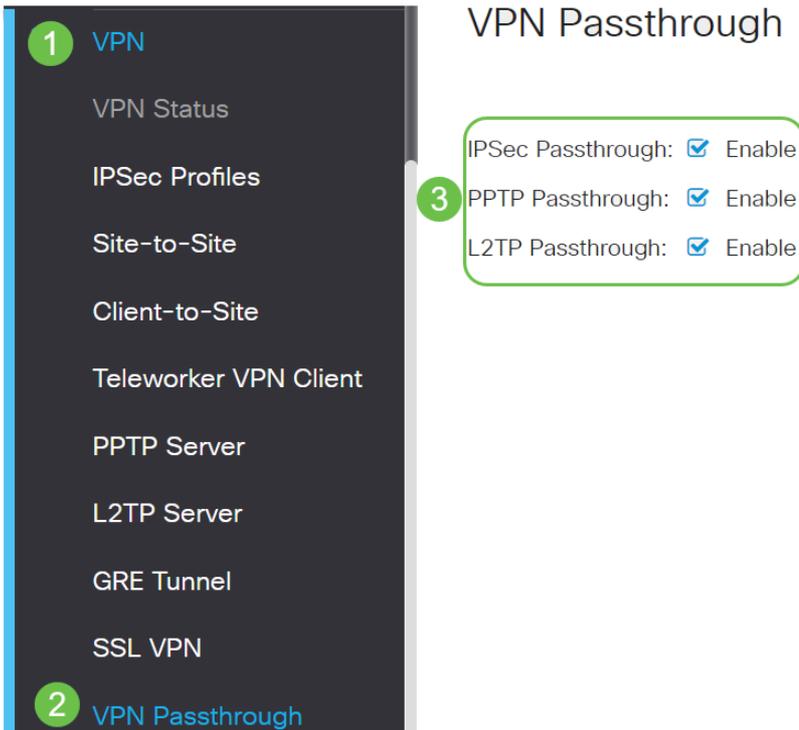
AnyConnect VPN ist das einzige von Cisco VPN unterstützte Produkt, das in diesem Konfigurationsleitfaden aufgeführt ist. Produkte von Drittanbietern, die nicht von Cisco stammen, einschließlich TheGreenBow und Shrew Soft, werden von Cisco nicht unterstützt. Sie werden ausschließlich zu Orientierungszwecken aufgenommen. Wenn Sie Support zu diesen benötigen, die über den Artikel hinausgehen, sollten Sie sich an diesen Drittanbieter wenden, um Unterstützung zu erhalten.

Wenn Sie keine VPN-Einrichtung planen, können Sie [mit einem Klick zum nächsten Abschnitt wechseln](#).

VPN-Passthrough

Im Allgemeinen unterstützt jeder Router Network Address Translation (NAT), um IP-Adressen zu sparen, wenn Sie mehrere Clients mit derselben Internetverbindung unterstützen möchten. Point-to-Point Tunneling Protocol (PPTP) und Internet Protocol Security (IPsec) VPN unterstützen NAT jedoch nicht. Hier kommt der VPN-Passthrough ins Spiel. Ein VPN-Passthrough ist eine Funktion, mit der VPN-Datenverkehr, der von mit diesem Router verbundenen VPN-Clients generiert wird, durch diesen Router geleitet und mit einem VPN-Endpunkt verbunden werden kann. Mit dem VPN-Passthrough können PPTP und IPsec VPN nur an das Internet weitergeleitet werden, das von einem VPN-Client aus initiiert wird. Anschließend wird das Remote-VPN-Gateway erreicht. Diese Funktion wird häufig auf Heim-Routern verwendet, die NAT unterstützen.

Standardmäßig sind IPsec, PPTP und L2TP-Passthrough aktiviert. Wenn Sie diese Einstellungen anzeigen oder anpassen möchten, wählen Sie **VPN > VPN Passthrough aus**. Anzeige oder Anpassung nach Bedarf.



AnyConnect VPN

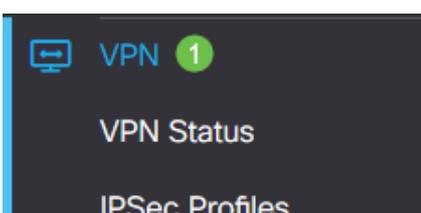
Die Verwendung von Cisco AnyConnect bietet mehrere Vorteile:

1. Sichere und persistente Verbindungen
2. Durchgängige Sicherheit und Richtliniendurchsetzung
3. Bereitstellung über die Adaptive Security Appliance (ASA) oder Enterprise Software Deployment Systems
4. Anpassbar und übersetzbar
5. Einfache Konfiguration
6. Unterstützt IPsec- (Internet Protocol Security) und SSL-Verbindungen (Secure Sockets Layer)
7. Unterstützt das IKEv2.0-Protokoll (Internet Key Exchange Version 2.0)

Konfigurieren von AnyConnect SSL VPN auf dem RV345P

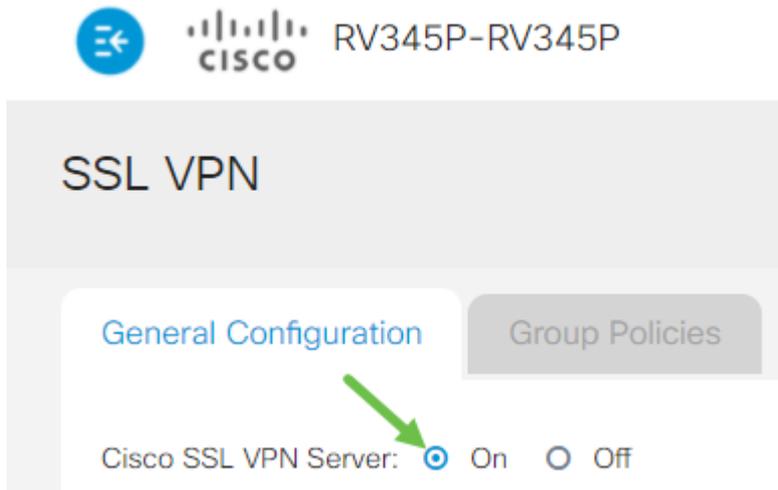
Schritt 1

Rufen Sie das webbasierte Dienstprogramm des Routers auf, und wählen Sie **VPN > SSL VPN aus**.



Schritt 2

Klicken Sie auf das **Optionsfeld On** (Ein), um Cisco SSL VPN Server zu aktivieren.



Obligatorische Gateway-Einstellungen

Schritt 1

Die folgenden Konfigurationseinstellungen sind obligatorisch:

1. Wählen Sie in der Dropdown-Liste die Gateway-Schnittstelle aus. Dies ist der Port, der für die Weiterleitung von Datenverkehr über die SSL VPN-Tunnel verwendet wird. Folgende Optionen sind verfügbar: WAN1, WAN2, USB1, USB2
2. Geben Sie die Portnummer für das SSL VPN-Gateway im Feld Gateway-Port zwischen 1 und 65535 ein.
3. Wählen Sie die Zertifikatsdatei aus der Dropdown-Liste aus. Dieses Zertifikat authentifiziert Benutzer, die versuchen, über die SSL VPN-Tunnel auf die Netzwerkressource zuzugreifen. Die Dropdown-Liste enthält ein Standardzertifikat und die importierten Zertifikate.
4. Geben Sie die IP-Adresse des Client-Adresspools im Feld *Client Address Pool (Client-Adresspool)* ein. Dieser Pool ist der Bereich von IP-Adressen, die Remote-VPN-Clients zugewiesen werden.

Stellen Sie sicher, dass sich der IP-Adressbereich nicht mit einer der IP-Adressen im lokalen Netzwerk überschneidet.

6. Wählen Sie die Client Netmask aus der Dropdown-Liste aus.
7. Geben Sie den Client-Domännennamen in das Feld *Client Domain* ein. Dies ist der Domänenname, der an SSL VPN-Clients gesendet werden soll.
8. Geben Sie im Feld *Anmeldebanner* den Text ein, der als Anmeldebanner angezeigt

wird. Dies ist das Banner, das bei jeder Anmeldung eines Clients angezeigt wird.

Mandatory Gateway Settings

Gateway Interface:	<input type="text" value="WAN1"/>
Gateway Port:	<input type="text" value="8443"/>
Certificate File:	<input type="text" value="Default"/>
Client Address Pool:	<input type="text" value="192.168.0.0"/>
Client Netmask:	<input type="text" value="255.255.255.0"/>
Client Domain:	<input type="text" value="yourdomain.com"/>
Login Banner:	<input type="text" value="Welcome to WideDomain!"/>

Schritt 2

Klicken Sie auf Apply (Anwenden).

<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>
--------------------------------------	---------------------------------------

Optionale Gateway-Einstellungen

Schritt 1

Die folgenden Konfigurationseinstellungen sind optional:

1. Geben Sie einen Wert in Sekunden für das Leerlaufzeitlimit zwischen 60 und 86400 ein. Dies ist die Zeitdauer, die die SSL VPN-Sitzung inaktiv bleiben kann.
2. Geben Sie in das Feld *Sitzungs-Timeout* einen Wert in Sekunden ein. Dies ist die Zeit, die erforderlich ist, damit die Transmission Control Protocol (TCP)- oder User Datagram Protocol (UDP)-Sitzung nach der angegebenen Leerlaufzeit das Zeitlimit überschreitet. Der Bereich liegt zwischen 60 und 12.09.600.
3. Geben Sie im Feld *ClientDPD Timeout* einen Wert in Sekunden zwischen 0 und 3600 ein. Dieser Wert gibt das regelmäßige Senden von HELLO/ACK-Nachrichten an, um den Status des VPN-Tunnels zu überprüfen. Diese Funktion muss an beiden Enden des VPN-Tunnels aktiviert werden.
4. Geben Sie im Feld *GatewayDPD Timeout (Gateway-Zeitüberschreitung)* einen Wert in Sekunden zwischen 0 und 3600 ein. Dieser Wert gibt das regelmäßige Senden von HELLO/ACK-Nachrichten an, um den Status des VPN-Tunnels zu überprüfen. Diese Funktion muss an beiden Enden des VPN-Tunnels aktiviert werden.
5. Geben Sie in das Feld *Keep Alive (Erhaltungsdosis in Sekunden)* einen Wert zwischen 0 und 600 ein. Diese Funktion stellt sicher, dass Ihr Router immer mit dem Internet verbunden ist. Wenn die VPN-Verbindung getrennt wird, versucht sie, sie wieder

herzustellen.

6. Geben Sie in das Feld *Leasedauer* einen Wert in Sekunden für die Dauer des Tunnels ein. Der Bereich liegt zwischen 600 und 12.09.600.
7. Geben Sie die Paketgröße in Byte ein, die über das Netzwerk gesendet werden können. Der Bereich liegt zwischen 576 und 1406.
8. Geben Sie die Relay-Intervallzeit in das Feld *Rekey Interval* ein. Mit der Funktion "Schlüssel neu eingeben" können die SSL-Schlüssel nach der Einrichtung der Sitzung neu verhandelt werden. Der Bereich liegt zwischen 0 und 43.200.

Optional Gateway Settings

Idle Timeout:	<input type="text" value="3000"/>	sec. (Range: 60-86400)
Session Timeout:	<input type="text" value="60"/>	sec. (Range: 0,60-1209600)
Client DPD Timeout:	<input type="text" value="350"/>	sec. (Range: 0-3600)
Gateway DPD Timeout:	<input type="text" value="360"/>	sec. (Range: 0-3600)
Keep Alive:	<input type="text" value="40"/>	sec. (Range: 0-600)
Lease Duration:	<input type="text" value="43500"/>	sec. (Range: 600-1209600)
Max MTU:	<input type="text" value="1406"/>	bytes (Range: 576-1406)
Rekey Interval:	<input type="text" value="3600"/>	sec. (Range: 0-43200)

Schritt 2

Klicken Sie auf Apply (Anwenden).

Gruppenrichtlinien konfigurieren

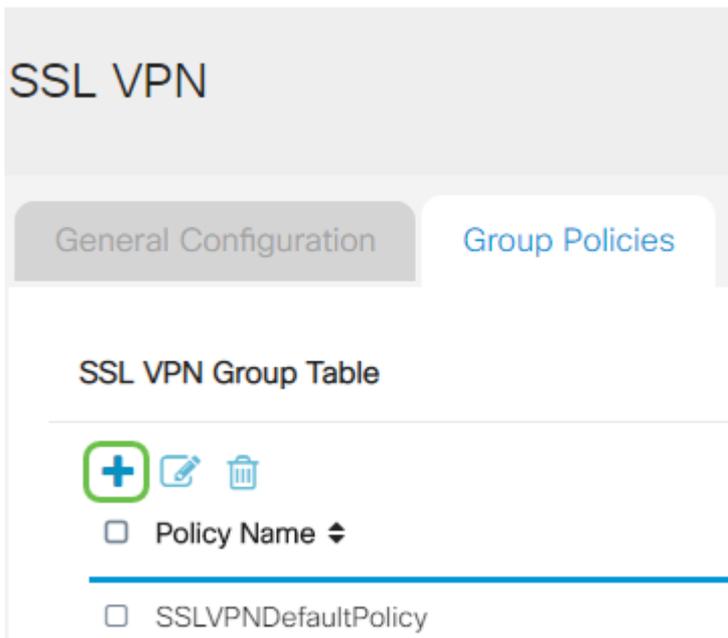
Schritt 1

Klicken Sie auf die Registerkarte **Gruppenrichtlinien**.

SSL VPN

Schritt 2

Klicken Sie unter der Tabelle für die SSL VPN-Gruppe auf das **Symbol Add** (Hinzufügen), um eine Gruppenrichtlinie hinzuzufügen.



Die Tabelle der SSL VPN-Gruppen zeigt die Liste der Gruppenrichtlinien auf dem Gerät. Sie können auch die erste Gruppenrichtlinie in der Liste bearbeiten, die SSLVPNDefaultPolicy heißt. Dies ist die vom Gerät bereitgestellte Standardrichtlinie.

Schritt 3

1. Geben Sie den bevorzugten Richtliniennamen in das Feld *Policy Name* (*Richtliniennamen*) ein.
2. Geben Sie die IP-Adresse des primären DNS in das angegebene Feld ein. Standardmäßig wird diese IP-Adresse bereits angegeben.
3. (Optional) Geben Sie die IP-Adresse des sekundären DNS in das angegebene Feld ein. Dies dient als Backup für den Fall, dass der primäre DNS ausfällt.
4. (Optional) Geben Sie in das Feld die IP-Adresse des primären WINS ein.
5. (Optional) Geben Sie die IP-Adresse des sekundären WINS in das angegebene Feld ein.
6. (Optional) Geben Sie im Feld *Beschreibung* eine Beschreibung der Richtlinie ein.

SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:	<input type="text" value="Group 1 Policy"/>
Primary DNS:	<input type="text" value="192.168.1.1"/>
Secondary DNS:	<input type="text" value="192.168.1.2"/>
Primary WINS:	<input type="text" value="192.168.1.1"/>

Schritt 4 (optional)

Klicken Sie auf ein Optionsfeld, um die IE-Proxy-Richtlinie auszuwählen, um die Microsoft Internet Explorer (MSIE)-Proxyeinstellungen für die Einrichtung des VPN-Tunnels zu aktivieren. Folgende Optionen sind verfügbar:

- None (Keine): Der Browser kann keine Proxy-Einstellungen verwenden.
- Auto (Automatisch): Ermöglicht dem Browser, die Proxy-Einstellungen automatisch zu erkennen.
- Bypass-local - Ermöglicht dem Browser, die auf dem Remote-Benutzer konfigurierten Proxy-Einstellungen zu umgehen.
- Disabled (Deaktiviert): Deaktiviert die MSIE-Proxyeinstellungen.

IE Proxy Settings

IE Proxy Policy: None Auto Bypass-local Disabled

Schritt 5 (optional)

Aktivieren Sie im Bereich Getrennte Tunneling-Einstellungen das Kontrollkästchen **Enable Split Tunneling**, um das unverschlüsselte Senden von Internetdatenverkehr an das Internet zu ermöglichen. Full Tunneling sendet den gesamten Datenverkehr an das Endgerät, wo er dann an die Ziel-Ressourcen weitergeleitet wird, sodass das Unternehmensnetzwerk nicht mehr über den Pfad für den Internetzugriff verfügt.

Split Tunneling Settings

Enable Split Tunneling

Schritt 6 (optional)

Klicken Sie auf ein Optionsfeld, um festzulegen, ob beim Anwenden des Split-Tunneling Datenverkehr eingeschlossen oder ausgeschlossen werden soll.

Include Traffic Exclude Traffic

Schritt 7

Klicken Sie in der Tabelle Split Network (Netzwerk teilen) auf das **Symbol Add (Hinzufügen)**, um eine geteilte Netzwerkausnahme hinzuzufügen.

Split Network Table



Schritt 8

Geben Sie die IP-Adresse des Netzwerks in das angegebene Feld ein.

Split Tunneling Settings

Enable Split Tunneling

Split Selection Include Traffic Exclude Traffic

Split Network Table



IP ⇅

192.168.1.0

Schritt 9

Klicken Sie in der Split DNS Table (DNS-Tabelle aufteilen) auf das **Symbol Add (Hinzufügen)**, um eine DNS-Trennung hinzuzufügen.

Split DNS Table



Domain ⇅

Schritt 10

Geben Sie den Domännennamen in das entsprechende Feld ein, und klicken Sie dann auf **Übernehmen**.

Split DNS Table



Domain ⇅

WideDomain.com

Der Router wird standardmäßig mit 2 AnyConnect-Serverlizenzen ausgeliefert. Das bedeutet, dass Sie nach der Verfügbarkeit von AnyConnect Client-Lizenzen 2 VPN-Tunnel gleichzeitig mit jedem anderen Router der Serie RV340 einrichten können.

Kurz gesagt, der RV345P-Router benötigt keine Lizenz, aber alle Clients benötigen eine. AnyConnect Client-Lizenzen ermöglichen Desktop- und mobilen Clients den Remote-Zugriff auf das VPN-Netzwerk.

Im nächsten Abschnitt wird beschrieben, wie Sie Lizenzen für Ihre Kunden erhalten.

AnyConnect Mobility Client

Ein VPN-Client ist eine Software, die auf einem Computer installiert und ausgeführt wird, der eine Verbindung zum Remote-Netzwerk herstellen möchte. Diese Client-Software muss mit der Konfiguration des VPN-Servers wie IP-Adresse und Authentifizierungsinformationen konfiguriert werden. Diese Authentifizierungsinformationen enthalten den Benutzernamen und den Pre-Shared Key, der zur Verschlüsselung der Daten verwendet wird. Je nach physischem Standort der zu verbindenden Netzwerke kann ein VPN-Client auch ein Hardwaregerät sein. Dies geschieht in der Regel, wenn die VPN-Verbindung verwendet wird, um zwei Netzwerke an unterschiedlichen Standorten miteinander zu verbinden.

Der Cisco AnyConnect Secure Mobility Client ist eine Softwareanwendung für die Verbindung mit einem VPN, das auf verschiedenen Betriebssystemen und Hardwarekonfigurationen funktioniert. Mit dieser Softwareanwendung können Remote-Ressourcen eines anderen Netzwerks so zugänglich gemacht werden, als ob der Benutzer direkt mit seinem Netzwerk verbunden wäre, aber auf sichere Weise.

Sobald der Router registriert und mit AnyConnect konfiguriert ist, kann der Client aus Ihrem vorhandenen Lizenzpool, den Sie erwerben, Lizenzen auf dem Router installieren. Diese werden im nächsten Abschnitt erläutert.

Lizenz erwerben

Sie müssen eine Lizenz bei Ihrem Cisco Distributor oder Ihrem Cisco Partner erwerben. Bei der Bestellung einer Lizenz müssen Sie Ihre Cisco Smart Account-ID oder Domänen-ID in Form von [name@domain.com](#) angeben.

Wenn Sie keinen Cisco Distributor oder Partner haben, können Sie einen [hier](#) finden.

Zum Zeitpunkt der Erstellung dieses Dokuments können die folgenden Produkt-SKUs zum Erwerb zusätzlicher Lizenzen in Paketen mit 25 Lizenzen verwendet werden. Beachten Sie, dass es weitere Optionen für die AnyConnect Client-Lizenzen gibt, wie in der Cisco AnyConnect-Bestellanleitung beschrieben. Die angegebene Produkt-ID ist jedoch die Mindestanforderung für die volle Funktionalität.

Bitte beachten Sie, dass die zuerst aufgeführte AnyConnect-Client-Lizenz-Produkt-SKU Lizenzen für einen Zeitraum von 1 Jahr bereitstellt und einen Mindestkauf von 25 Lizenzen erfordert. Andere Produkt-SKUs, die für die Router der Serie RV340 gelten, sind auch mit unterschiedlichen Abonnementstufen erhältlich:

- **LS-AC-PLS-1Y-S1** - Cisco AnyConnect Plus-Client-Lizenz für 1 Jahr
- **LS-AC-PLS-3Y-S1** - Cisco AnyConnect Plus-Client-Lizenz, 3 Jahre
- **LS-AC-PLS-5Y-S1** - Cisco AnyConnect Plus Client-Lizenz, 5 Jahre
- **LS-AC-PLS-P-25-S** - Cisco AnyConnect Plus-Lizenz, 25 Stück
- **LS-AC-PLS-P-50-S** - Cisco AnyConnect Plus-Lizenz, unbefristet, 50 Stück

Kundeninformationen

Wenn Ihr Client einen der folgenden Links eingerichtet hat, sollten Sie diesen folgende Links senden:

- Windows: [AnyConnect auf einem Windows-Computer](#)
- Mac: [Installieren Sie AnyConnect auf Mac](#).
- Ubuntu-Desktop: [Installieren und Verwenden von AnyConnect auf Ubuntu Desktop](#)
- Bei Problemen können Sie unter [Informationen zur grundlegenden Fehlerbehebung bei Fehlern des Cisco AnyConnect Secure Mobility Client](#) aufrufen.

Überprüfen der AnyConnect VPN-Verbindung

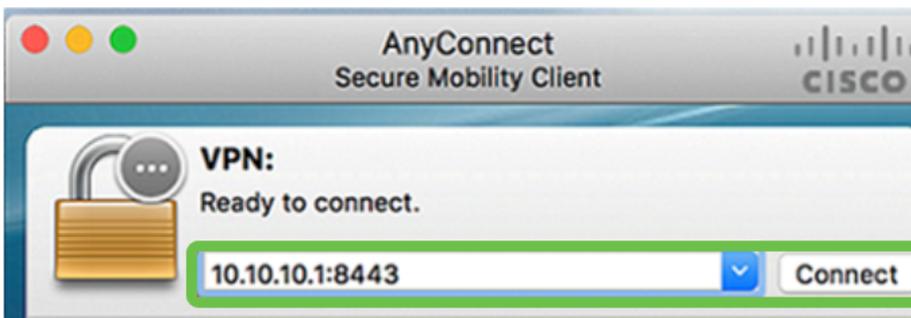
Schritt 1

Klicken Sie auf das **Symbol AnyConnect Secure Mobility Client**.

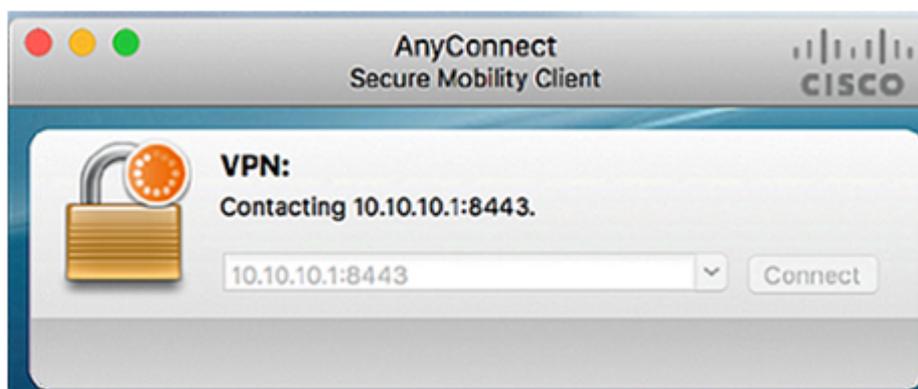


Schritt 2

Geben Sie im Fenster des AnyConnect Secure Mobility Client die Gateway-IP-Adresse und die Gateway-Portnummer getrennt durch einen Doppelpunkt (:) ein, und klicken Sie dann auf **Verbinden**.

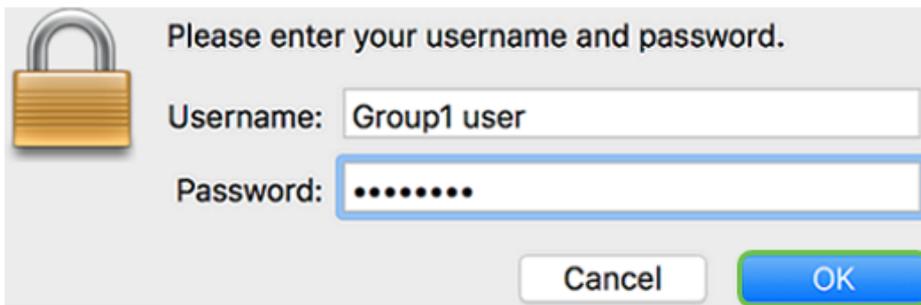


Die Software zeigt nun an, dass sie mit dem Remote-Netzwerk Kontakt aufnimmt.



Schritt 3

Geben Sie Ihren Server-Benutzernamen und Ihr Kennwort in die entsprechenden Felder ein und klicken Sie auf **OK**.



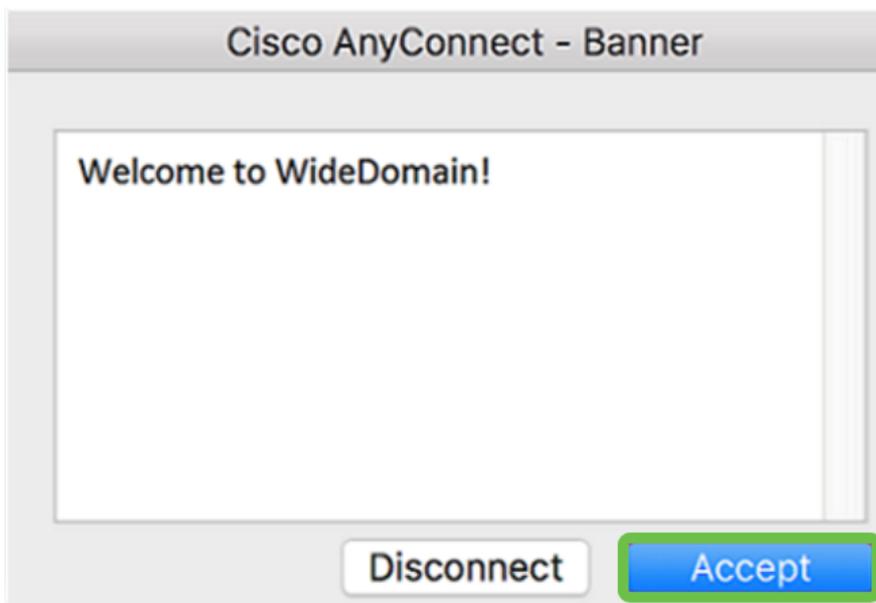
Please enter your username and password.

Username:

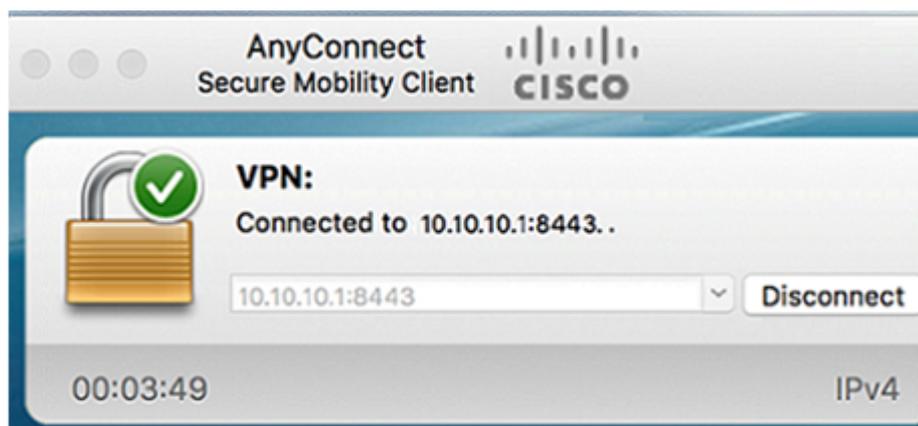
Password:

Schritt 4

Sobald die Verbindung hergestellt ist, wird das Anmeldebanner angezeigt. Klicken Sie auf **Akzeptieren**.



Das Fenster AnyConnect sollte jetzt die erfolgreiche VPN-Verbindung mit dem Netzwerk anzeigen.



Wenn Sie jetzt AnyConnect VPN verwenden, können Sie andere VPN-Optionen überspringen und mit dem [nächsten Abschnitt](#) fortfahren.

Shrew Soft VPN

Mit einem IPsec-VPN können Sie Remote-Ressourcen sicher abrufen, indem Sie im Internet einen verschlüsselten Tunnel einrichten. Die Router der Serie RV34X arbeiten als IPsec-VPN-Server und unterstützen den Shrew Soft VPN-Client. In diesem

Abschnitt wird beschrieben, wie Sie Ihren Router und den Shrew Soft Client konfigurieren, um eine Verbindung mit einem VPN zu sichern.

Shrew Soft wird von Cisco nicht unterstützt. Dieses Beispiel dient lediglich zu Demonstrationszwecken. Wenn Sie Probleme mit Shrew Soft haben, wenden Sie sich bitte an die entsprechenden Stellen.

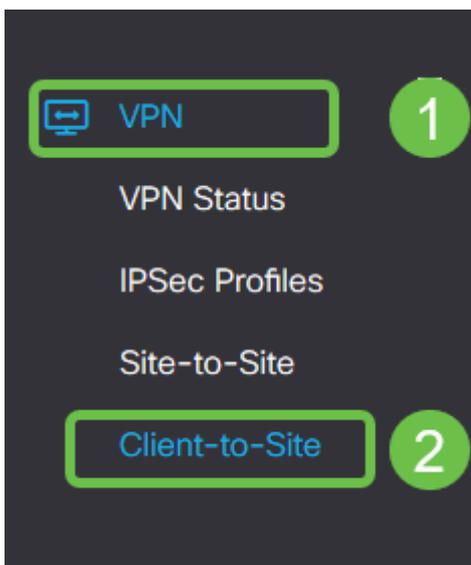
Sie können die neueste Version der Shrew Soft VPN-Clientsoftware hier herunterladen: <https://www.shrew.net/download/vpn>

Konfigurieren von Shrew Soft auf dem Router der Serie RV345P

Zunächst konfigurieren Sie das **Client-to-Site-VPN** auf dem RV345P.

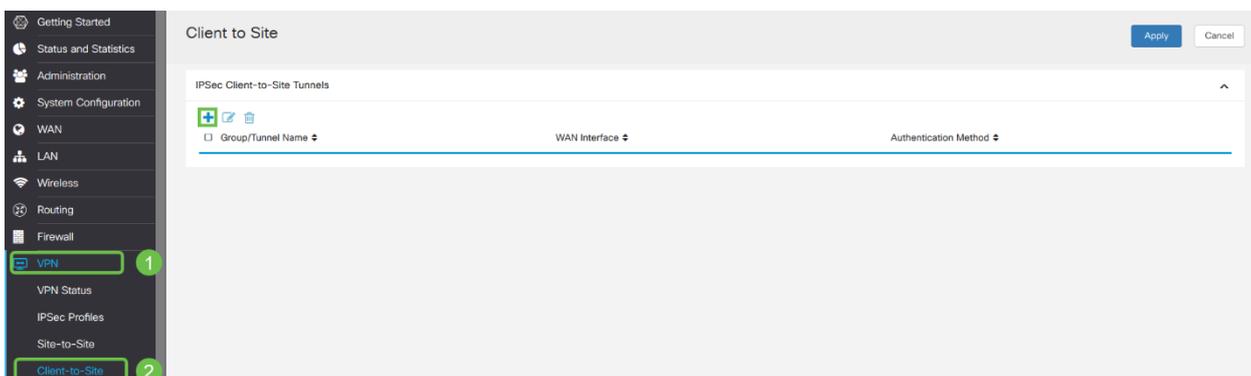
Schritt 1

Navigieren Sie zu **VPN > Client-to-Site**.



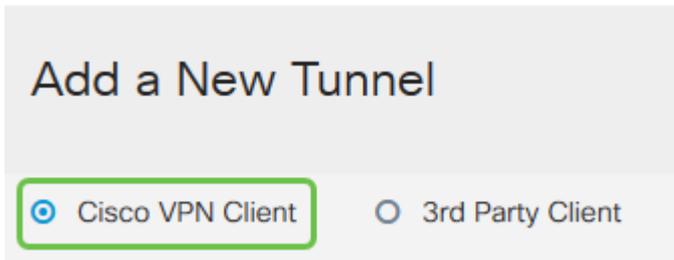
Schritt 2

Fügen Sie ein **Client-to-Site-VPN-Profil** hinzu.



Schritt 3

Wählen Sie die Option **Cisco VPN Client** aus.



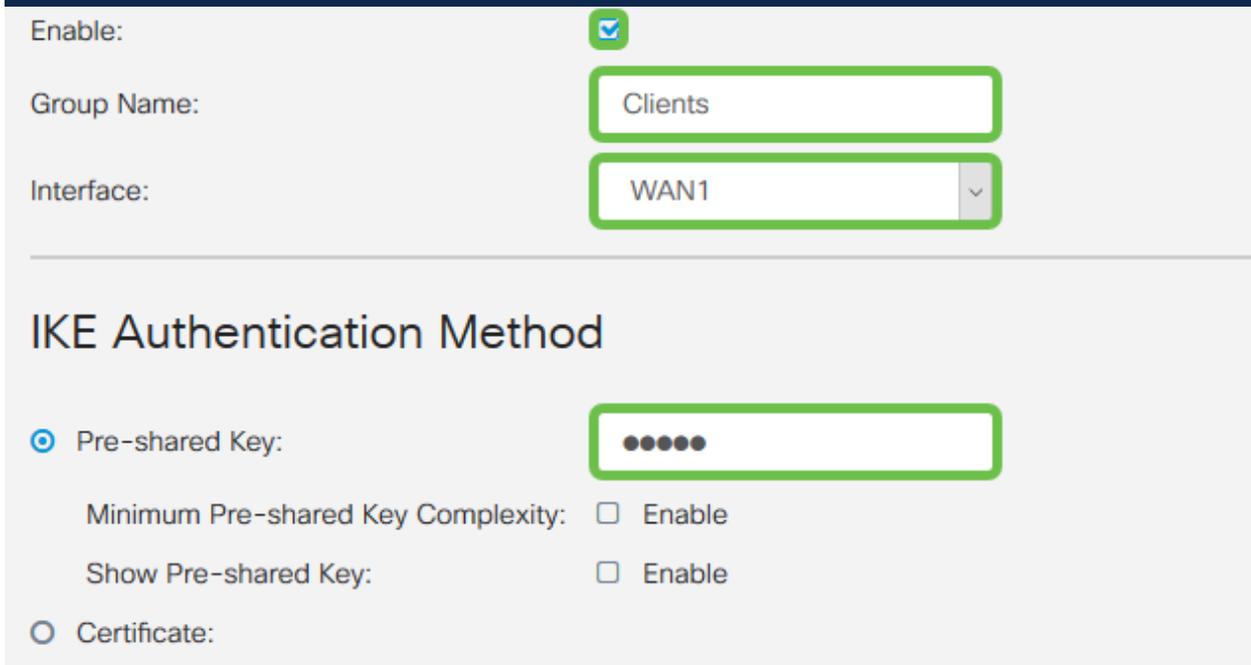
Add a New Tunnel

Cisco VPN Client 3rd Party Client

Schritt 4

Aktivieren Sie das **Kontrollkästchen Aktivieren**, um das VPN-Clientprofil zu aktivieren. Außerdem konfigurieren Sie den *Gruppennamen*, wählen die **WAN-Schnittstelle** aus und geben einen **Pre-shared Key** ein.

Bitte beachten Sie den *Gruppennamen* und den *Pre-shared Key*, wie sie später bei der Konfiguration des Clients verwendet werden.



Enable:

Group Name:

Interface:

IKE Authentication Method

Pre-shared Key:

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

Schritt 5

Lassen Sie die **Benutzergruppentabelle** jetzt leer. Dies gilt für die *Benutzergruppe* auf dem Router, wurde jedoch noch nicht konfiguriert. Stellen Sie sicher, dass der **Modus** auf **Client** eingestellt ist. Geben Sie den **Pool-Bereich für Client-LAN** ein. Wir verwenden die Nummern 172.16.10.1 bis 172.16.10.10.

Der Pool-Bereich sollte ein eindeutiges Subnetz verwenden, das an keiner anderen Stelle im Netzwerk verwendet wird.

User Group:

User Group Table

+ 

Group Name 

Mode: Client NEM

Pool Range for Client LAN

Start IP:

End IP:

Schritt 6

Hier konfigurieren Sie die Einstellungen für die **Moduskonfiguration**. Hier sind die Einstellungen, die wir verwenden werden:

- **Primärer DNS-Server:** Wenn Sie einen internen DNS-Server haben oder einen externen DNS-Server verwenden möchten, können Sie diesen hier eingeben. Andernfalls wird der Standardwert auf die RV345P LAN-IP-Adresse festgelegt. In unserem Beispiel verwenden wir die Standardeinstellung.
- **Split Tunnel (Tunnel teilen):** Aktivieren Sie Split Tunneling. Mit diesem Parameter wird festgelegt, welcher Datenverkehr über den VPN-Tunnel geleitet wird. In unserem Beispiel wird Split Tunnel verwendet.
- **Split Tunnel Table:** Geben Sie die Netzwerke ein, auf die der VPN-Client über das VPN zugreifen soll. In diesem Beispiel wird das LAN-Netzwerk RV345P verwendet.

Mode Configuration

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

Default Domain:

Backup Server 1: (IP Address or Domain Name)

Backup Server 2: (IP Address or Domain Name)

Backup Server 3: (IP Address or Domain Name)

Split Tunnel:

Split Tunnel Table

+  

IP Address  Netmask 

<input checked="" type="checkbox"/>	<input type="text" value="192.168.1.0"/>	<input type="text" value="255.255.255.0"/>
-------------------------------------	--	--

Schritt 7

Wenn Sie auf **Speichern** klicken, wird das Profil in der Liste **IPsec-Client-to-Site-Gruppen** angezeigt.

Client to Site		
IPSec Client-to-Site Tunnels		
Group/Tunnel Name ↕	WAN Interface ↕	Authentication Method ↕
Clients	WAN1	Pre-shared Key

Schritt 8

Konfigurieren Sie eine **Benutzergruppe** für die Authentifizierung von VPN-Client-Benutzern. Klicken Sie unter **Systemkonfiguration > Benutzergruppen** auf das **Pluszeichen**, um eine Benutzergruppe hinzuzufügen.

User Groups

User Groups Table

Group ↕	Web Login/NETCONF/RESTCONF ↕
admin	Admin
guest	Disabled

Schritt 9

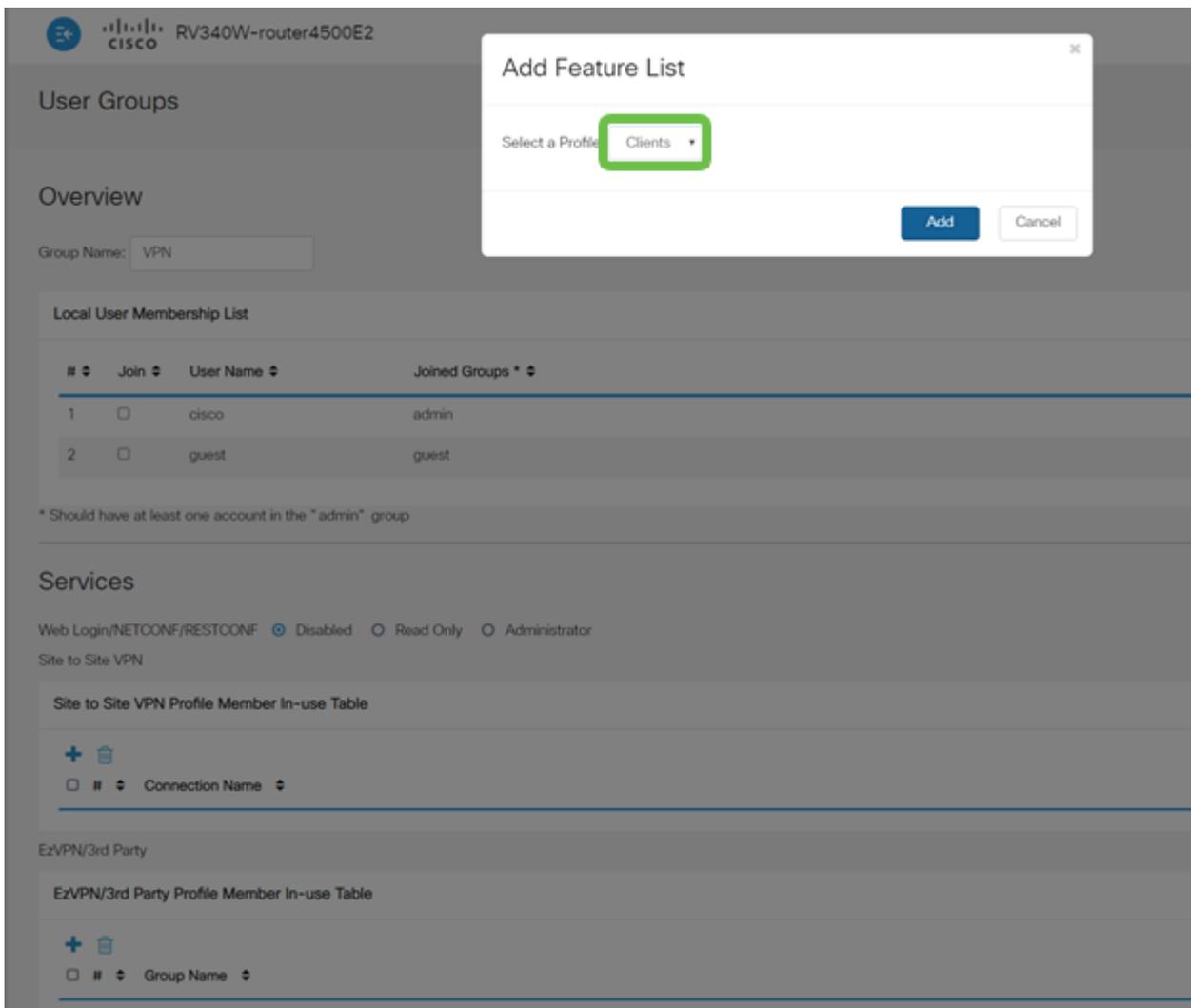
Geben Sie einen **Gruppennamen** ein.

Overview

Group Name:

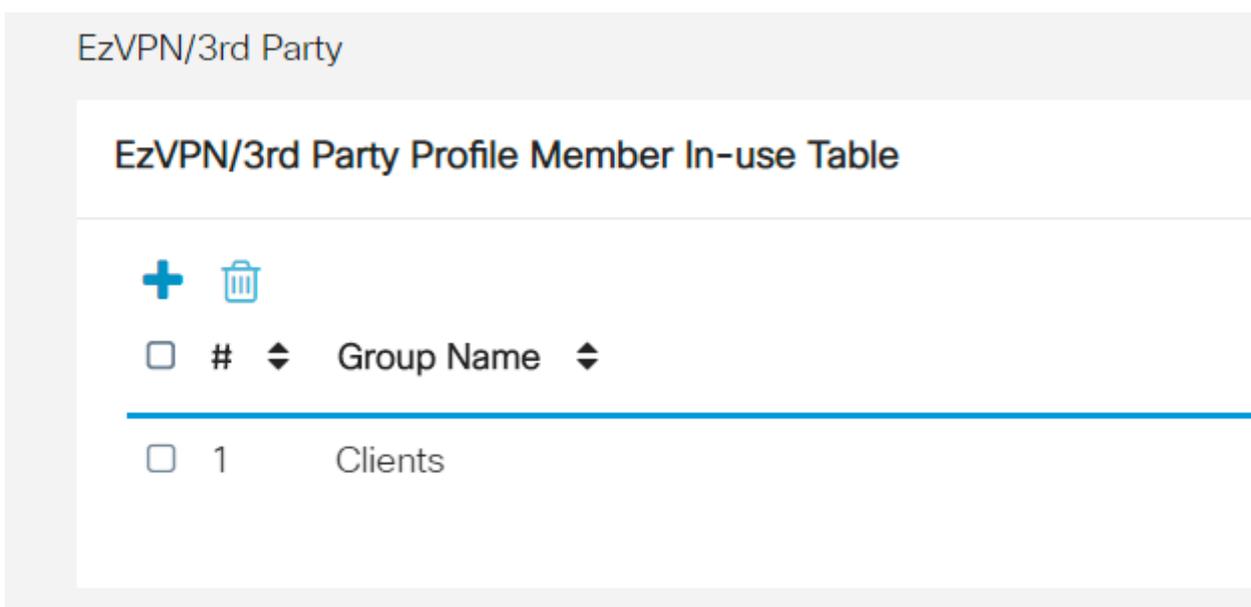
Schritt 10

Klicken Sie unter **Services > EzVPN/Drittanbieter** auf **Hinzufügen**, um diese Benutzergruppe mit dem **Client-to-Site**-Profil zu verknüpfen, das zuvor konfiguriert wurde.



Schritt 11

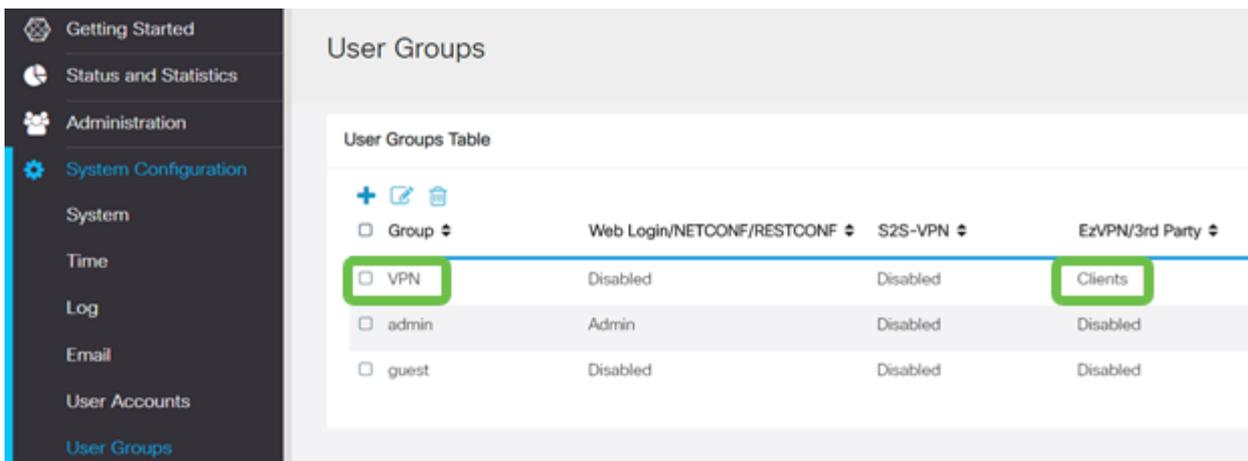
Sie sollten nun den **Client-to-Site**-Gruppennamen in der Liste für **EzVPN/Drittanbieter** sehen.



Schritt 12

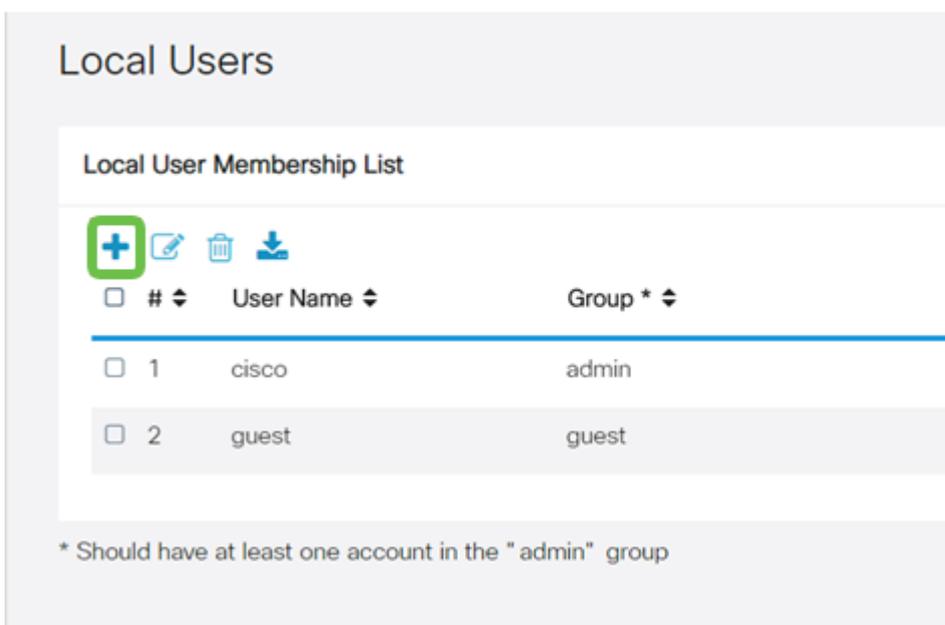
Nachdem Sie die Benutzergruppenkonfiguration **angewendet** haben, wird diese in der Liste der **Benutzergruppen** angezeigt und die neue Benutzergruppe wird mit dem zuvor

erstellten Client-to-Site-Profil verwendet.



Schritt 13

Konfigurieren eines neuen Benutzers in **Systemkonfiguration > Benutzerkonten**. Klicken Sie auf das **Pluszeichen**, um einen neuen Benutzer zu erstellen.



Schritt 14

Geben Sie den neuen **Benutzernamen** zusammen mit dem **neuen Kennwort ein**. Stellen Sie sicher, dass die **Gruppe** auf die neue **Benutzergruppe** festgelegt ist, die Sie gerade konfiguriert haben. Klicken Sie abschließend auf **Übernehmen**.

User Accounts

Add User Account

User Name	<input type="text" value="vpnuser"/>	
New Password	<input type="password" value="....."/>	(Range: 0 - 127)
New Password Confirm	<input type="password" value="....."/>	
Group	<input type="text" value="VPN"/>	

Schritt 15

Der neue **Benutzer** wird in der Liste der **lokalen Benutzer** angezeigt.

Local Users

Local User Membership List



<input type="checkbox"/>	#	User Name	Group *
--------------------------	---	-----------	---------

<input type="checkbox"/>	1	cisco	admin
--------------------------	---	-------	-------

<input type="checkbox"/>	2	guest	guest
--------------------------	---	-------	-------

<input type="checkbox"/>	3	vpnuser	VPN
--------------------------	---	---------	-----

* Should have at least one account in the "admin" group

Damit ist die Konfiguration des Routers der Serie RV345P abgeschlossen. Als Nächstes konfigurieren Sie den Shrew Soft VPN-Client.

Konfigurieren des Shrew Soft VPN-Clients

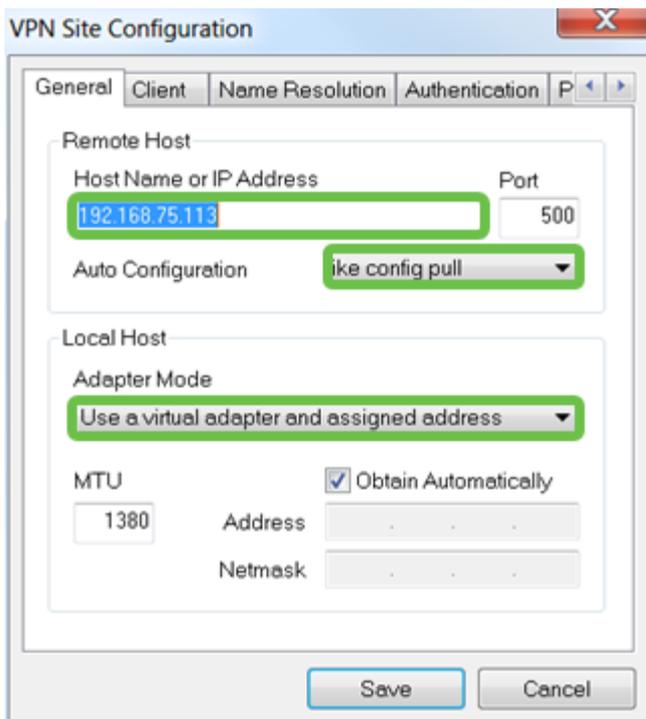
Führen Sie die folgenden Schritte aus.

Schritt 1

Öffnen Sie den Shrew Soft *VPN Access Manager*, und klicken Sie auf **Hinzufügen**, um ein Profil hinzuzufügen. Im sich öffnenden Fenster *VPN Site Configuration* konfigurieren Sie die Registerkarte **General**:

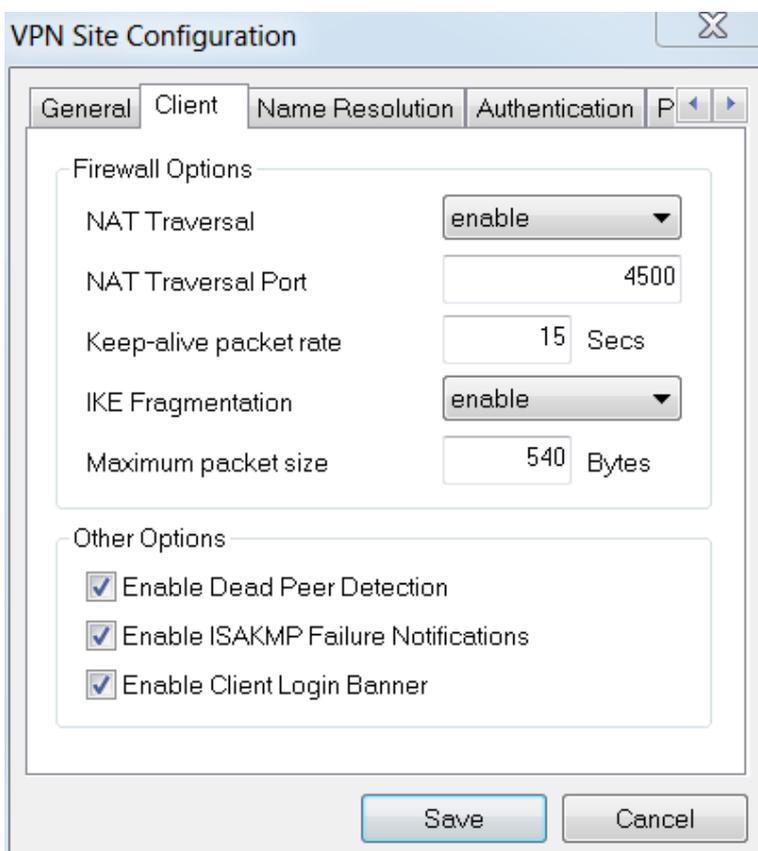
- **Hostname oder IP-Adresse:** Verwenden Sie die WAN-IP-Adresse (oder den Hostnamen des RV345P).

- **Automatische Konfiguration:** Wählen Sie die Option Konfigurationsanfrage aus.
- **Adaptermodus:** Wählen Sie **Einen virtuellen Adapter und zugewiesene Adresse** verwenden.



Schritt 2

Konfigurieren Sie die Registerkarte **Client**. In diesem Beispiel haben wir die Standardeinstellungen beibehalten.



Schritt 3

Aktivieren Sie unter **Namensauflösung > DNS** das **Kontrollkästchen DNS aktivieren**, und lassen Sie die Kontrollkästchen **Automatisch beziehen** aktiviert.

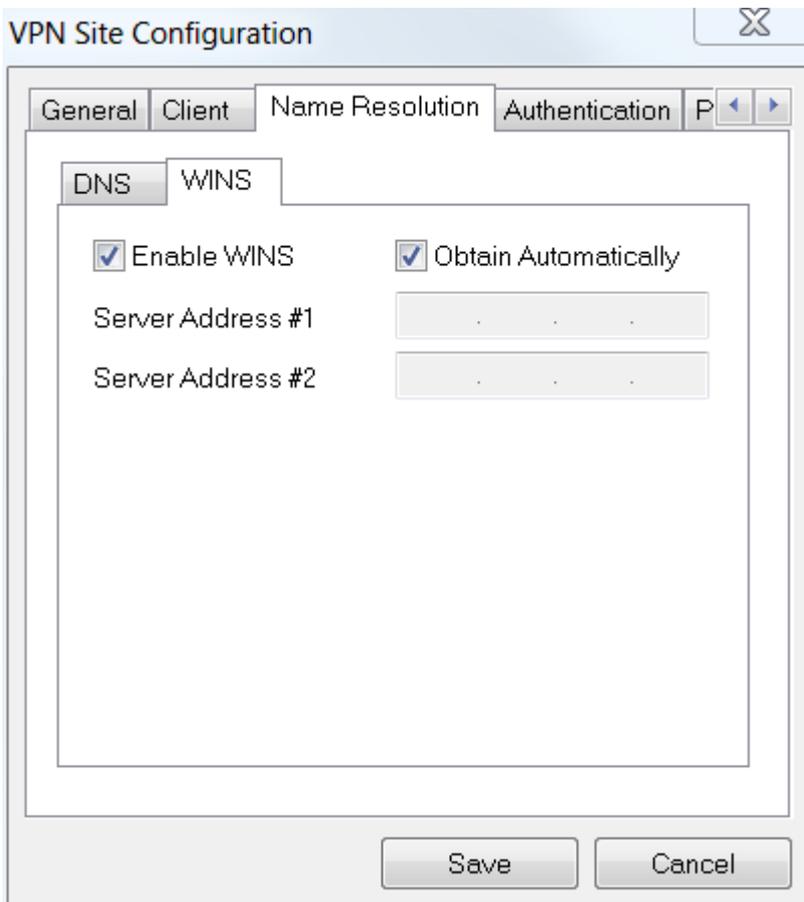
The image shows a screenshot of the 'VPN Site Configuration' dialog box. The 'Name Resolution' tab is selected, and the 'DNS' sub-tab is active. The 'WINS' sub-tab is also visible. The 'DNS' section contains the following controls:

- Enable DNS
- Obtain Automatically
- Server Address #1: [. . .]
- Server Address #2: [. . .]
- Server Address #3: [. . .]
- Server Address #4: [. . .]
- Obtain Automatically
- DNS Suffix: []

At the bottom of the dialog box, there are 'Save' and 'Cancel' buttons.

Schritt 4

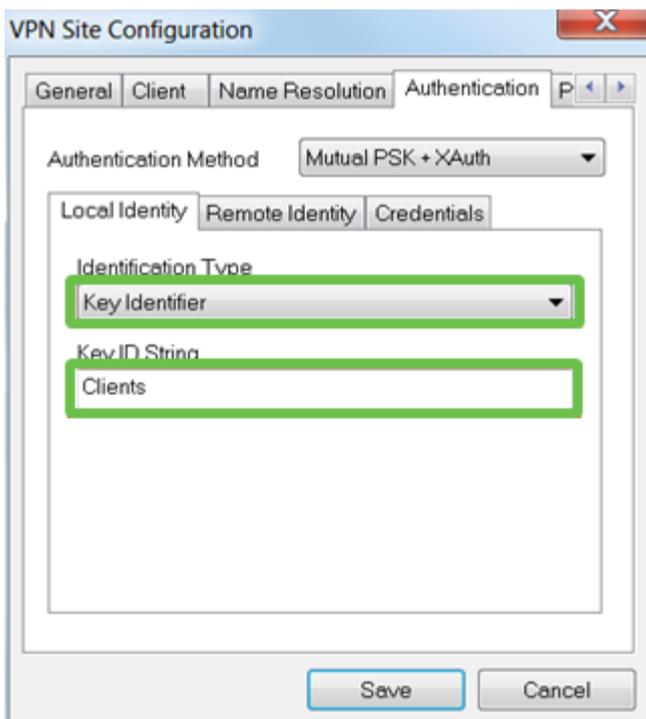
Aktivieren Sie unter **Namensauflösung > WINS-Registerkarte** das Kontrollkästchen **WINS aktivieren**, und lassen Sie das **Kontrollkästchen Automatisch beziehen** aktiviert.



Schritt 5

Klicken Sie auf **Authentifizierung > Lokale Identität**.

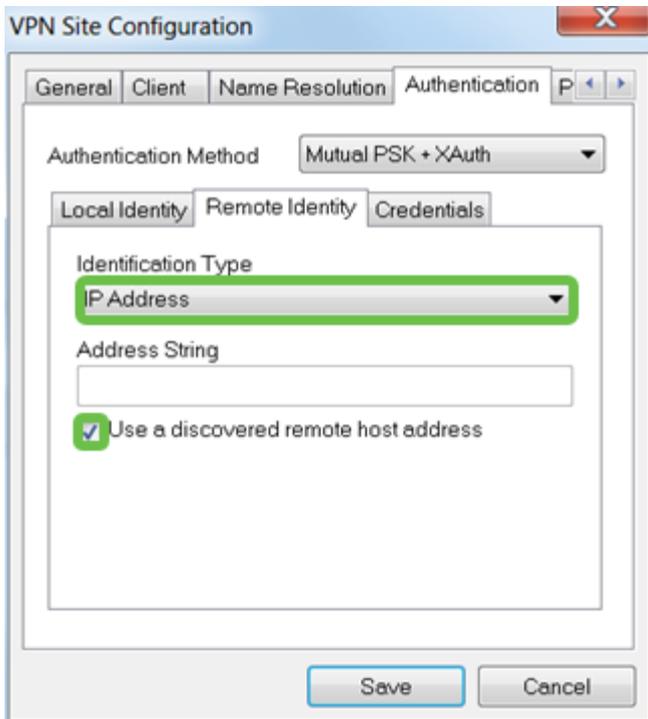
- **Identifizierungstyp:** Schlüsselkennung auswählen
- **Schlüssel-ID-Zeichenfolge:** Geben Sie den **Gruppennamen** ein, der auf dem RV345P konfiguriert wurde.



Schritt 6

Unter **Authentifizierung > Remote Identity**. In diesem Beispiel haben wir die Standardeinstellungen beibehalten.

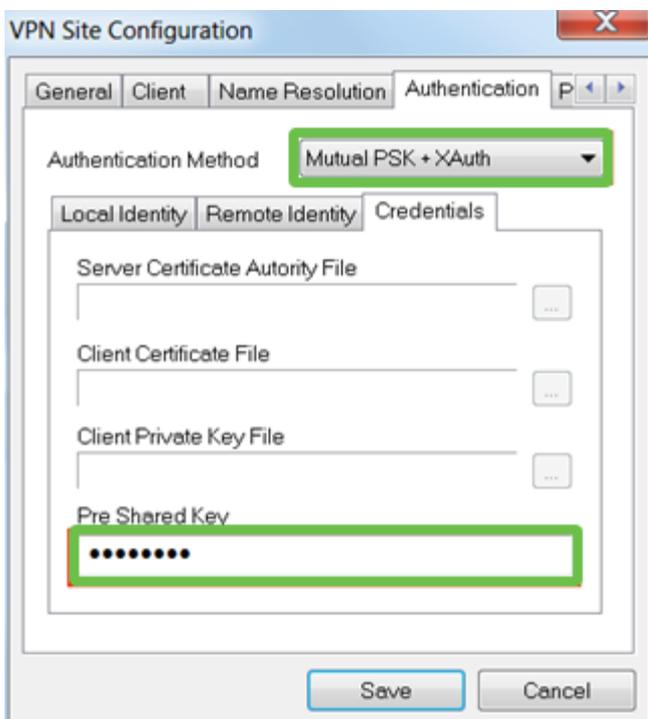
- **Identifizierungstyp:** IP-Adresse
- **Adresszeichenfolge:** <leer>
- **Verwenden Sie ein erkanntes Adressfeld des Remotehosts:** Aktiviert



Schritt 7

Konfigurieren Sie unter **Authentication > Credentials** (Authentifizierung > Anmeldeinformationen) Folgendes:

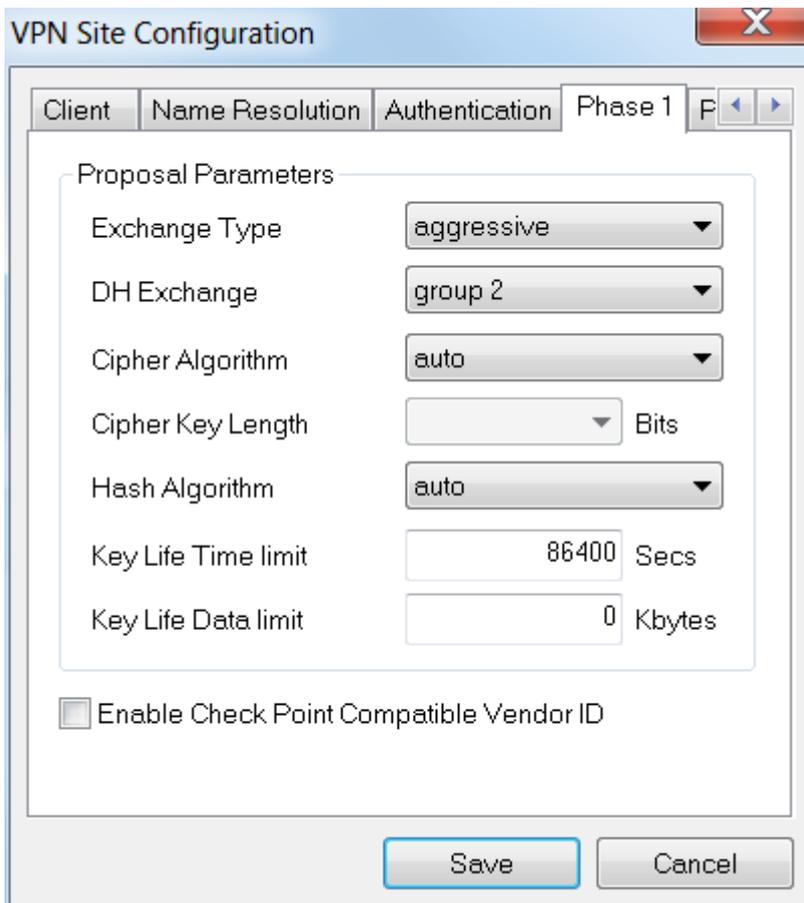
- **Authentifizierungsmethode:** Wählen Sie **Mutual PSK + XAuth** aus
- **Vorinstallierter Schlüssel:** Geben Sie den im RV345P-Clientprofil konfigurierten **Pre-shared Key** ein.



Schritt 8

Für die Registerkarte **Phase 1**. In diesem Beispiel wurden die Standardeinstellungen beibehalten:

- **Exchange-Typ:** Aggressive
- **DH Exchange:** Gruppe 2
- **Cipher Algorithm:** Auto
- **Hash-Algorithmus:** Auto



The screenshot shows the 'VPN Site Configuration' dialog box with the 'Phase 1' tab selected. The 'Proposal Parameters' section is visible, containing the following settings:

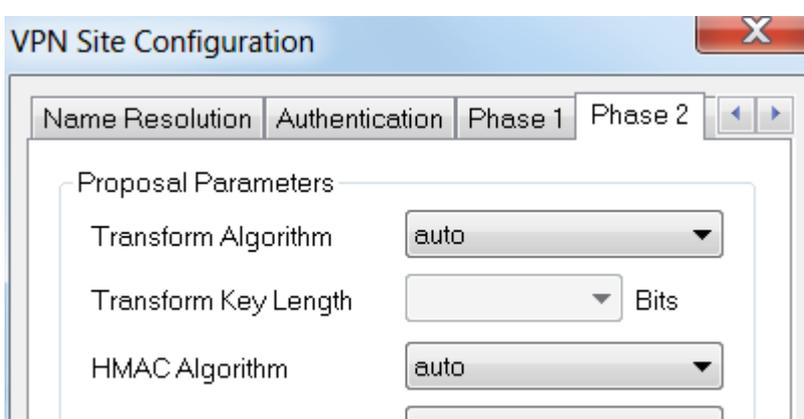
Parameter	Value
Exchange Type	aggressive
DH Exchange	group 2
Cipher Algorithm	auto
Cipher Key Length	[] Bits
Hash Algorithm	auto
Key Life Time limit	86400 Secs
Key Life Data limit	0 Kbytes

Below the parameters, there is an unchecked checkbox labeled 'Enable Check Point Compatible Vendor ID'. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

Schritt 9

In diesem Beispiel wurden die Standardwerte für die Registerkarte **Phase 2** beibehalten.

- **Umwandlungsalgorithmus:** Auto
- **HMAC-Algorithmus:** Auto
- **PFS-Exchange:** Deaktiviert
- **Komprimierungsalgorithmus:** Deaktiviert



The screenshot shows the 'VPN Site Configuration' dialog box with the 'Phase 2' tab selected. The 'Proposal Parameters' section is visible, containing the following settings:

Parameter	Value
Transform Algorithm	auto
Transform Key Length	[] Bits
HMAC Algorithm	auto

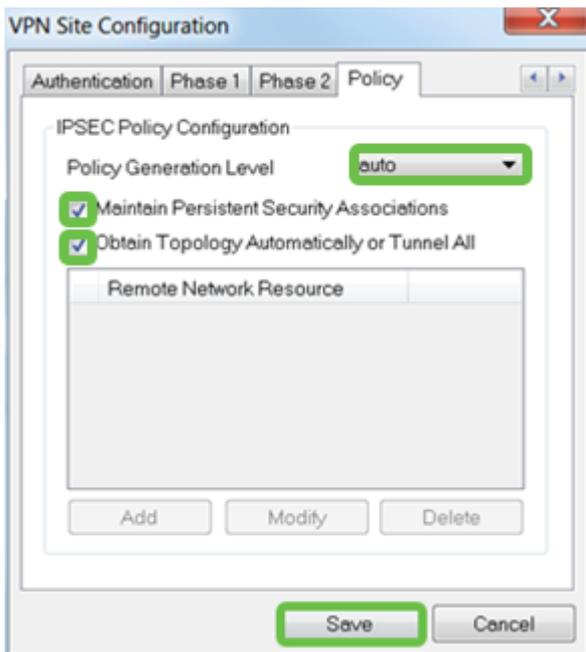
At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

Schritt 10

Für das Beispiel der **Policy**-Registerkarte wurden die folgenden Einstellungen verwendet:

- Richtlinienerstellungsstufe: Auto
- Beibehaltung permanenter Sicherheitszuordnungen: geprüft
- Topologie automatisch oder Tunnel All abrufen: Aktiviert

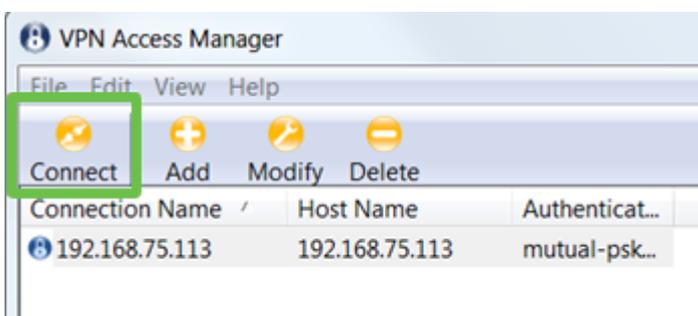
Da **Split-Tunneling** auf dem RV345P konfiguriert wurde, muss er hier nicht konfiguriert werden.



Klicken Sie abschließend auf **Speichern**.

Schritt 11

Sie sind jetzt bereit, die Verbindung zu testen. Markieren Sie im *VPN Access Manager* das Verbindungsprofil, und klicken Sie auf die Schaltfläche **Connect**.



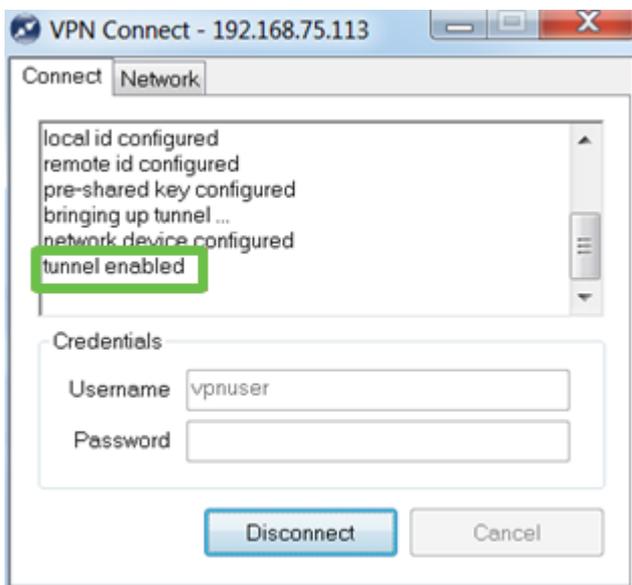
Schritt 12

Geben Sie im **VPN Connect**-Fenster, das angezeigt wird, den **Benutzernamen** und das **Kennwort** mit den Anmeldeinformationen für das **Benutzerkonto ein**, das Sie auf dem RV345P erstellt haben (Schritte 13 und 14). Wenn Sie fertig sind, klicken Sie auf **Verbinden**.



Schritt 13

Überprüfen Sie, ob der Tunnel angeschlossen ist. Der Tunnel sollte **aktiviert sein**.



Shrew Soft wurde in dieser Konfiguration als Beispiel verwendet. Da Shrew Soft kein Cisco Produkt ist, wenden Sie sich bitte an diesen Dritten, wenn Sie technische Unterstützung benötigen.

Weitere VPN-Optionen

Für die Verwendung eines VPN gibt es noch eine Reihe weiterer Optionen. Klicken Sie auf die folgenden Links, um weitere Informationen zu erhalten:

- [Verwenden des GreenBow VPN-Clients für die Verbindung mit dem Router der Serie RV34x](#)
- [Konfigurieren eines Telearbeiter-VPN-Clients auf dem Router der Serie RV34x](#)
- [Konfigurieren eines PPTP-Servers \(Point-to-Point Tunneling Protocol\) auf dem Router der Serie Rv34x](#)

- [Konfigurieren eines IPsec-Profiles \(Internet Protocol Security\) auf einem Router der Serie RV34x](#)
- [Konfigurieren der L2TP-WAN-Einstellungen auf dem RV34x-Router](#)
- [Konfigurieren des Site-to-Site-VPN auf dem RV34x](#)

Zusätzliche Konfigurationen auf dem RV345P-Router

VLANs konfigurieren (optional)

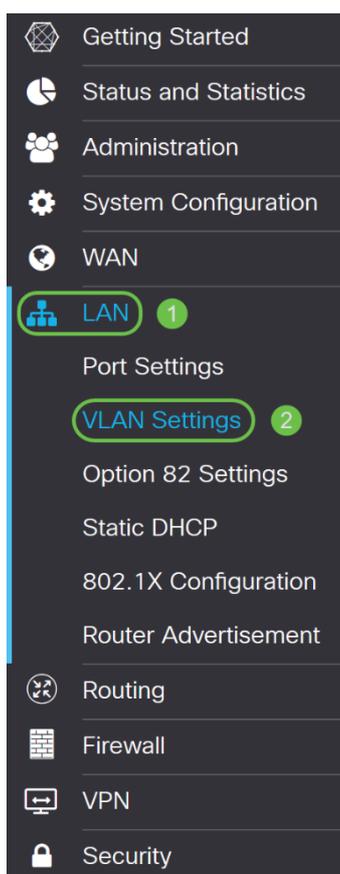
Mit einem Virtual Local Area Network (VLAN) können Sie ein Local Area Network (LAN) logisch in verschiedene Broadcast-Domänen segmentieren. In Umgebungen, in denen über das Netzwerk möglicherweise vertrauliche Daten übertragen werden, kann durch die Erstellung von VLANs die Sicherheit verbessert werden. 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.

Weitere Hinweise finden Sie unter [VLAN Best Practices und Security Tips](#).

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 das **Symbol Hinzufügen**, um ein neues VLAN zu erstellen.

VLAN Table



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.

VLAN Table



<input type="checkbox"/>	VLAN ID ↕	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	VLAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ⓘ	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input checked="" type="checkbox"/>	200	VLAN200	<input type="checkbox"/>	<input type="checkbox"/> ⓘ	IPv4 Address: 192.168.2.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Server <input type="radio"/> Relay

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 RV345P vom VLAN aus anmelden und den RV345P 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.

VLAN Table



<input type="checkbox"/>	VLAN ID ↕	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	VLAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ⓘ	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input checked="" type="checkbox"/>	<input type="text" value="200"/>	VLAN200	<input type="checkbox"/>	<input type="checkbox"/> ⓘ	IPv4 Address: <input type="text" value="192.168.2.1"/> / <input type="text" value="24"/> Subnet Mask: <input type="text" value="255.255.255.0"/> DHCP Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Server <input type="radio"/> Relay

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.

VLAN Table



<input type="checkbox"/>	VLAN ID ↕	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	VLAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ⓘ	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input checked="" type="checkbox"/>	<input type="text" value="200"/>	VLAN200	<input type="checkbox"/>	<input type="checkbox"/> ⓘ	IPv4 Address: <input type="text" value="192.168.2.1"/> / <input type="text" value="24"/> Subnet Mask: <input type="text" value="255.255.255.0"/> DHCP Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Server <input type="radio"/> Relay

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**.

VLAN Table



<input type="checkbox"/>	VLAN ID ↕	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
<input type="checkbox"/>	1	VLAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.1/24 255.255.255.0 DHCP Server: 192.168.1.100-192.168.1.149
<input checked="" type="checkbox"/>	<input type="text" value="200"/>	VLAN200	<input type="checkbox"/>	<input type="checkbox"/>	IPv4 Address: <input type="text" value="192.168.2.1"/> / <input type="text" value="24"/> <input type="text" value="255.255.255.0"/> DHCP Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Server <input type="radio"/> Relay

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.

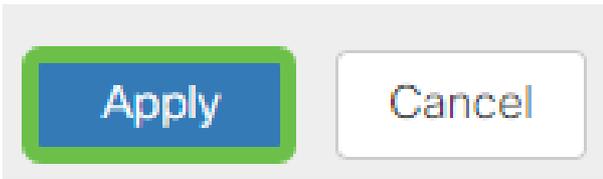
Server: Dies ist die am häufigsten verwendete Option.

- 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.

<input checked="" type="checkbox"/>	<input type="text" value="200"/>	VLAN200	<input type="checkbox"/>	<input type="checkbox"/>	IPv4 Address: <input type="text" value="192.168.2.1"/> / <input type="text" value="24"/>
					Subnet Mask: <input type="text" value="255.255.255.0"/>
					DHCP Type: <input type="radio"/> Disabled <input checked="" type="radio"/> Server <input type="radio"/> Relay
					Lease Time: <input type="text" value="1440"/> min.
					Range Start: <input type="text" value="192.168.2.100"/>

Schritt 8

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



VLANs Ports zuweisen (optional)

Auf dem RV345P 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. Mit dem 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 diesem Port zugewiesene VLAN muss 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.

In diesem Beispiel gibt es keine Trunks.

Schritt 1

Wählen Sie die zu bearbeitenden *VLAN-IDs* aus.

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 2

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 3

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

Apply **Cancel**

Sie sollten jetzt erfolgreich ein neues VLAN erstellt und VLANs für die Ports des RV345P 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.

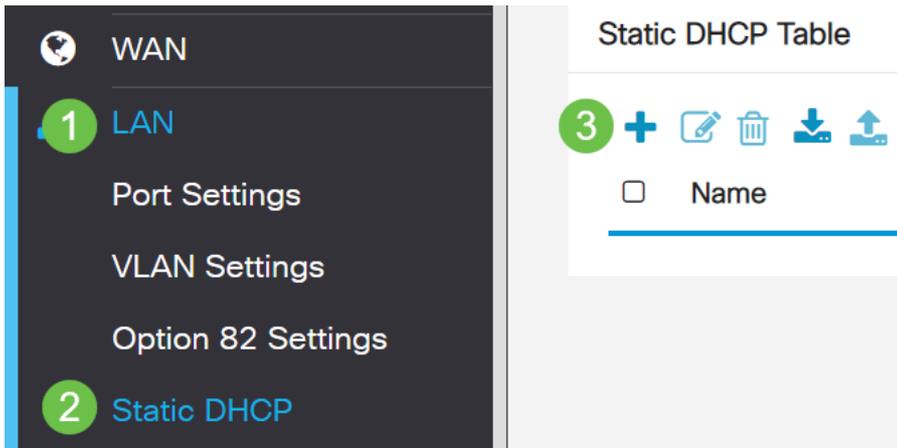
Hinzufügen einer statischen IP (optional)

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 zum [nächsten Abschnitt](#) dieses Artikels wechseln.

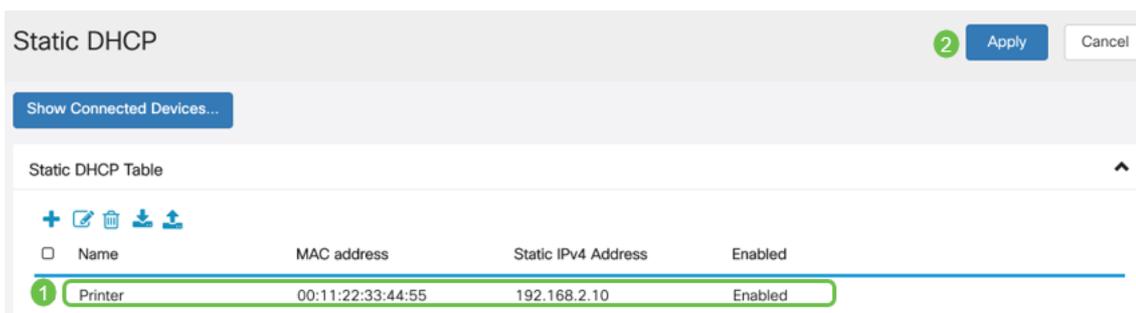
Schritt 1

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.



Verwalten von Zertifikaten (optional)

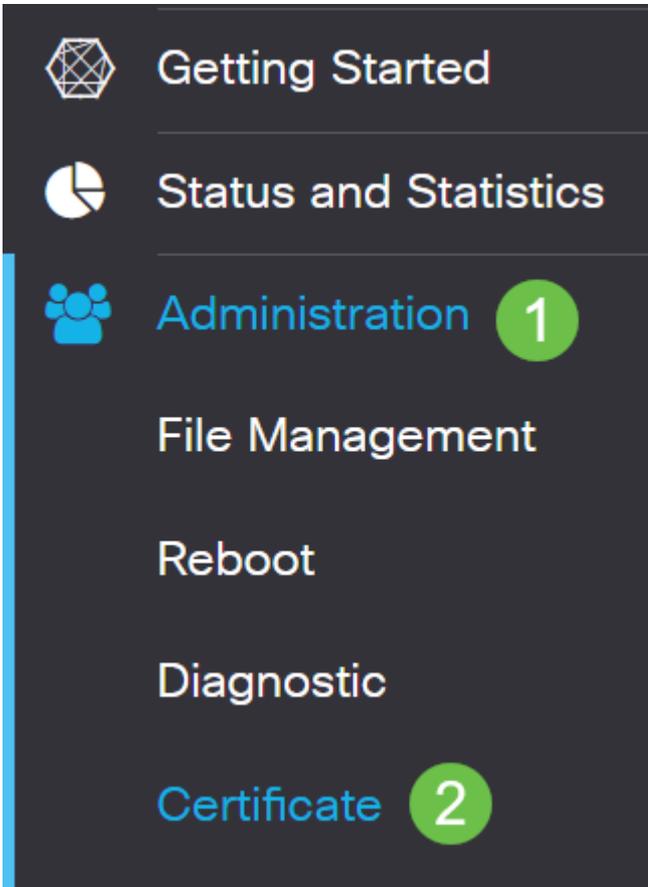
Ein digitales Zertifikat bescheinigt das Eigentum an einem öffentlichen Schlüssel durch den benannten Subjekt des Zertifikats. Dadurch können sich die Parteien auf Signaturen oder Behauptungen des privaten Schlüssels verlassen, der dem öffentlichen Schlüssel entspricht, der zertifiziert ist. Ein Router kann ein selbstsigniertes Zertifikat generieren, ein Zertifikat, das von einem Netzwerkadministrator erstellt wurde. Sie kann auch Anfragen an Zertifizierungsstellen (Certificate Authority, CA) senden, um ein digitales Identitätszertifikat zu beantragen. Es ist wichtig, legitime Zertifikate von Drittanbieteranwendungen zu erhalten.

Für die Authentifizierung wird eine Zertifizierungsstelle (Certificate Authority, CA) verwendet. Zertifikate können von einer beliebigen Anzahl von Websites Dritter erworben werden. Es ist eine offizielle Methode, zu beweisen, dass Ihre Website sicher ist. Im Wesentlichen ist die CA eine vertrauenswürdige Quelle, die sicherstellt, dass Sie ein legitimes Unternehmen sind und vertrauenswürdig sind. Je nach Ihren Bedürfnissen, ein Zertifikat zu minimalen Kosten. Sie werden von der Zertifizierungsstelle ausgecheckt, und sobald diese Ihre Informationen überprüft hat, wird Ihnen das Zertifikat ausgestellt. Dieses Zertifikat kann als Datei auf Ihren Computer heruntergeladen werden. Sie können dann zu Ihrem Router (oder VPN-Server) gehen und ihn dort hochladen.

CSR/Zertifikat erstellen

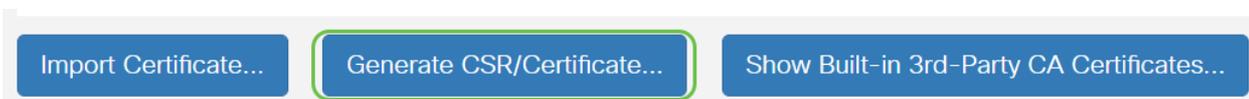
Schritt 1

Melden Sie sich beim webbasierten Dienstprogramm des Routers an, und wählen Sie **Administration > Certificate** aus.



Schritt 2

Klicken Sie auf **CSR/Zertifikat generieren**. Sie werden zur Seite "CSR/Zertifikat generieren" weitergeleitet.



Schritt 3

Füllen Sie die Felder mit folgenden Angaben aus:

- Wählen Sie den entsprechenden Zertifikatstyp aus.
 - Self-Signing Certificate - Dies ist ein SSL-Zertifikat (Secure Socket Layer), das vom eigenen Ersteller signiert wird. Dieses Zertifikat ist weniger vertrauenswürdig, da es nicht abgebrochen werden kann, wenn der private Schlüssel durch einen Angreifer kompromittiert wird.
 - Certified Signing Request - Dies ist eine Public Key Infrastructure (PKI), die an die Zertifizierungsstelle gesendet wird, um ein digitales Identitätszertifikat zu beantragen. Sie ist sicherer als selbstsignierte Schlüssel, da der private

Schlüssel geheim gehalten wird.

- Geben Sie im Feld Zertifikatname einen Namen für das Zertifikat ein, um die Anforderung zu identifizieren. Dieses Feld darf nicht leer sein und keine Leerzeichen und Sonderzeichen enthalten.
- (Optional) Klicken Sie im Bereich "Betreff-Alternative Name" auf ein Optionsfeld. Folgende Optionen sind verfügbar:
 - IP-Adresse - Geben Sie eine IP-Adresse (Internet Protocol) ein.
 - FQDN - Geben Sie einen vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) ein.
 - E-Mail - E-Mail-Adresse eingeben
- Geben Sie im Feld Subject Alternative Name (Betreffalternative Namen) den FQDN ein.
- Wählen Sie in der Dropdown-Liste Ländername einen Ländernamen aus, in dem Ihre Organisation legal registriert ist.
- Geben Sie einen Namen oder eine Abkürzung für das Bundesland, die Provinz, die Region oder das Gebiet ein, in dem sich Ihr Unternehmen im Feld "Bundesland/Region" befindet.
- Geben Sie im Feld "Locality Name" (Ortsname) den Namen des Ortes oder der Stadt ein, in dem Ihre Organisation registriert ist oder sich befindet.
- Geben Sie einen Namen ein, unter dem Ihr Unternehmen rechtlich registriert ist. Wenn Sie sich als kleines Unternehmen oder alleiniger Eigentümer anmelden, geben Sie den Namen des Zertifikatsanforderers in das Feld Organisationsname ein. Sonderzeichen können nicht verwendet werden.
- Geben Sie im Feld Name der Organisationseinheit einen Namen ein, um zwischen den Abteilungen innerhalb einer Organisation zu unterscheiden.
- Geben Sie im Feld "Allgemeiner Name" einen Namen ein. Dieser Name muss der vollqualifizierte Domännename der Website sein, für die Sie das Zertifikat verwenden.
- Geben Sie die E-Mail-Adresse der Person ein, die das Zertifikat generieren möchte.
- Wählen Sie aus der Dropdown-Liste Key Encryption Length (Schlüssellänge) eine Schlüssellänge aus. Die Optionen sind 512, 1024 und 2048. Je größer die Schlüssellänge, desto sicherer ist das Zertifikat.
- Geben Sie im Feld Gültige Dauer die Anzahl der Tage ein, für die das Zertifikat gültig ist. Der Standardwert ist 360.
- Klicken Sie auf **Generieren**.

Certificate

2

Generate

Cancel

Generate CSR/Certificate

Type: Self-Signing Certificate

Certificate Name: TestCACertificate

Subject Alternative Name: spprtfrms

IP Address FQDN Email

Country Name(C): US - United States

State or Province Name(ST): Wisconsin

Locality Name(L): Oconomowoc

Organization Name(O): Cisco

Organization Unit(OU): Cisco Business

Common Name(CN): cisco.com

Email Address(E): @cisco.com

Key Encryption Length: 2048

Valid Duration: 360 days (Range: 1-10950, Default: 360)

Das generierte Zertifikat sollte nun in der Zertifikatstabelle angezeigt werden.

Certificate Table

Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		

Import Certificate...

Generate CSR/Certificate...

Show Built-in 3rd-Party CA Certificates...

Select as Primary Certificate...

Sie sollten jetzt erfolgreich ein Zertifikat auf dem RV345P-Router erstellt haben.

Zertifikat exportieren

Schritt 1

Aktivieren Sie in der Zertifikatstabelle das Kontrollkästchen des zu exportierenden Zertifikats, und klicken Sie auf das **Exportsymbol**.

Certificate Table ^

Index Certificate Used By Type Signed By Duration Details Action

Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
<input type="checkbox"/> 1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
<input type="checkbox"/> 2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
<input type="checkbox"/> 3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
<input checked="" type="checkbox"/> 4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		

1 2

Schritt 2

- Klicken Sie auf ein Format, um das Zertifikat zu exportieren. Folgende Optionen sind verfügbar:
 - PKCS #12 - Public Key Cryptography Standards (PKCS) #12 ist ein exportiertes Zertifikat, das in der Erweiterung .p12 enthalten ist. Um die Datei zu verschlüsseln, ist ein Kennwort erforderlich, um sie beim Exportieren, Importieren und Löschen zu schützen.
 - PEM — Privacy Enhanced Mail (PEM) wird häufig für Webserver verwendet, um mithilfe eines einfachen Texteditors wie Notepad leicht in lesbare Daten übersetzt werden zu können.
- Wenn Sie PEM ausgewählt haben, klicken Sie einfach auf **Exportieren**.
- Geben Sie im Feld Kennwort eingeben ein Kennwort ein, um die zu exportierende Datei zu sichern.
- Geben Sie das Kennwort erneut im Feld Kennwort bestätigen ein.
- Im Bereich "Select Destination" (Ziel auswählen) wurde PC ausgewählt und ist die einzige derzeit verfügbare Option.
- Klicken Sie auf **Exportieren**.

Export Certificate x

1

Export as PKCS#12 format

Enter Password

.....

2

Confirm Password

.....

Export as PEM format

Schritt 3

Unter der Schaltfläche Download wird eine Meldung angezeigt, die den Erfolg des Downloads anzeigt. Eine Datei wird in Ihrem Browser heruntergeladen. Klicken Sie auf OK.

Information



Success



Ok

Sie sollten jetzt erfolgreich ein Zertifikat für den Router der Serie RV345P exportiert haben.

Importieren eines Zertifikats

Schritt 1

Klicken Sie auf **Zertifikat importieren....**

Certificate Table

Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		

Import Certificate... Generate CSR/Certificate... Show Built-in 3rd-Party CA Certificates...
Select as Primary Certificate...

Schritt 2

- Wählen Sie aus der Dropdown-Liste den zu importierenden Zertifikattyp aus. Folgende Optionen sind verfügbar:
 - Local Certificate (Lokales Zertifikat): Ein auf dem Router generiertes Zertifikat.
 - Zertifizierungsstellenzertifikat - Ein Zertifikat, das von einer vertrauenswürdigen Drittbehörde zertifiziert wurde und bestätigt hat, dass die

im Zertifikat enthaltenen Informationen korrekt sind.

- PKCS #12 Encoded file — Public Key Cryptography Standards (PKCS) #12 ist ein Format zum Speichern eines Serverzertifikats.
- Geben Sie im Feld Zertifikatname einen Namen für das Zertifikat ein.
- Wenn PKCS #12 ausgewählt wurde, geben Sie im Feld Importpasswort ein Kennwort für die Datei ein. Fahren Sie andernfalls mit Schritt 3 fort.
- Klicken Sie auf eine Quelle, um das Zertifikat zu importieren. Folgende Optionen sind verfügbar:
 - Importieren aus PC
 - Importieren über USB
- Wenn der Router kein USB-Laufwerk erkennt, wird die Option Import from USB (Von USB importieren) deaktiviert.
- Wenn Sie Import From USB (Aus USB importieren) ausgewählt haben und Ihr USB vom Router nicht erkannt wird, klicken Sie auf Refresh (Aktualisieren).
- Klicken Sie auf die Schaltfläche Choose File (Datei auswählen), und wählen Sie die entsprechende Datei aus.
- Klicken Sie auf **Hochladen**.

Certificate 3 Upload Cancel

Import Certificate

Type: PKCS#12 encoded file

Certificate Name: cisco 1

Import Password:

Upload certificate file

Import From PC 2 Browse... TestCACertificate

Import From USB Refresh

Nach dem erfolgreichen Abschluss werden Sie automatisch zur Hauptseite für Zertifikate weitergeleitet. Die Zertifikatstabelle wird mit dem kürzlich importierten Zertifikat gefüllt.

Certificate Table

Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		

Sie sollten jetzt erfolgreich ein Zertifikat auf Ihrem RV345P-Router importiert haben.

Konfigurieren eines mobilen Netzwerks mit einem Dongle und einem Router der Serie RV345P (optional)

Vielleicht möchten Sie ein mobiles Backup-Backup-Netzwerk mit einem Dongle und Ihrem RV345P-Router konfigurieren. In diesem Fall sollten Sie das Dokument [Konfigurieren eines mobilen Netzwerks mithilfe eines Dongle und eines Routers der Serie RV34x lesen](#).

Herzlichen Glückwunsch! Sie haben die Konfiguration Ihres RV345P-Routers abgeschlossen! Sie konfigurieren jetzt Ihre Cisco Business Wireless-Geräte.

Konfigurieren des Wireless Mesh-Netzwerks

Sofort einsatzbereiter CBW140AC

Schließen Sie zunächst ein Ethernetkabel vom PoE-Port Ihres CBW140AC an einen PoE-Port des RV345P an. Die ersten vier Ports des RV345P 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 Master-AP kann NUR zur Bereitstellung eines Uplink zum LAN und NICHT zur Verbindung mit anderen Master-fähigen oder 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 RV345x-Routern](#).

Einrichten des 140AC Master Wireless Access Point

In diesem Abschnitt richten Sie mithilfe der mobilen Anwendung den Master Wireless Access Point 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 RV345P-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 auf [Google Play](#) verfügbare Cisco Business Mobile App 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

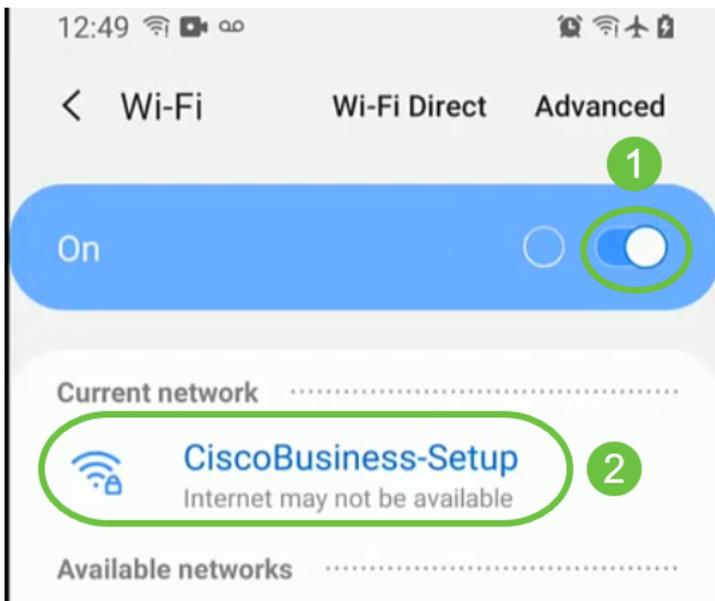
Schritt 2

Öffnen Sie die **Cisco Business** Application auf Ihrem Mobilgerät.



Schritt 3

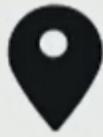
Stellen Sie eine Verbindung zum **CiscoBusiness-Setup-Wireless-Netzwerk** auf Ihrem Mobilgerät her. Die Passphrase ist **cisco123**.





Schritt 4

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



Monitor My Network



Set up My Network

Discovered Master

Master (192.168.1.1)

 *Enter the name of the master AP*

No Master AP Added.

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**.

Cisco Business Wireless 140AC Access Point

Welcome

Please start by creating an admin account.

admin 1

P 2

P 3

Show Password 4

5

Cancel Get Started

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.

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

Cisco Business Wireless 140AC Access Point

1 Name and Place ?

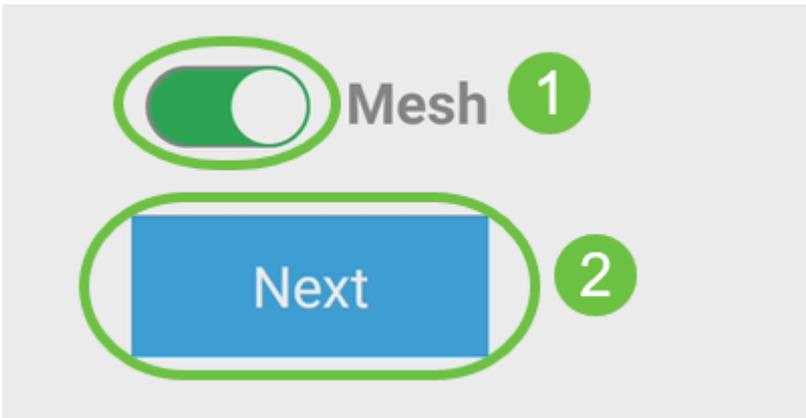
1 cbwmaster

2 United States

Date

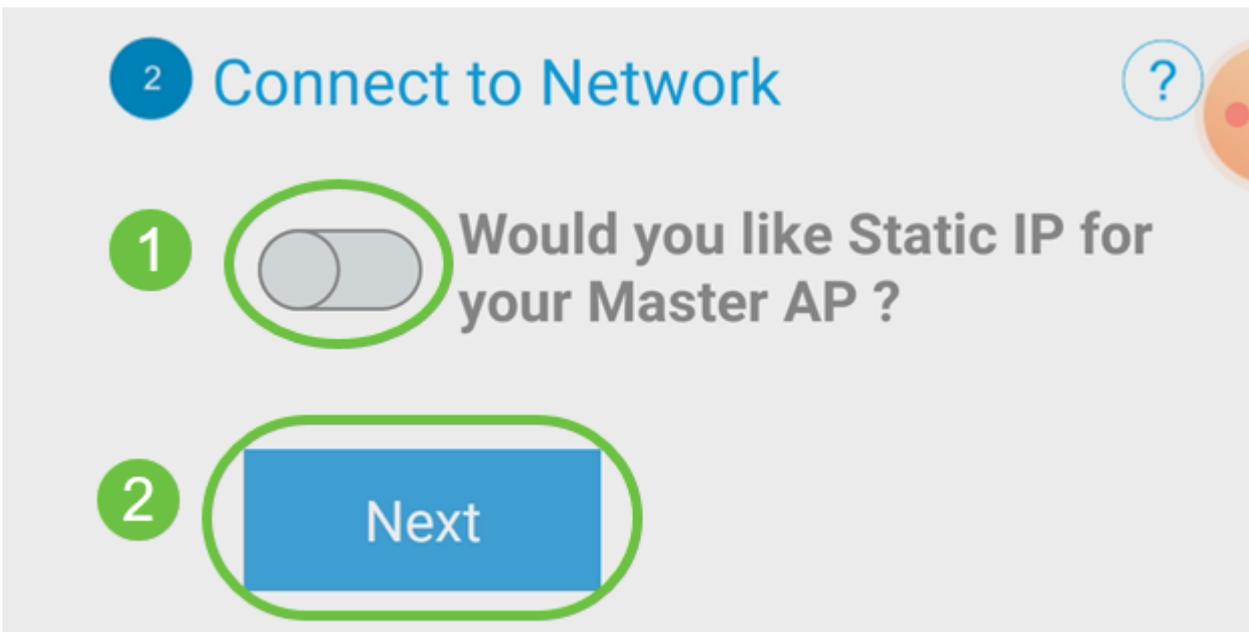
Schritt 7

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



Schritt 8

(Optional) Sie können die *statische IP für Ihren Master-Access* 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 Master-AP* aus. Standardmäßig ist diese Option **deaktiviert**.

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

Klicken Sie auf **Speichern**.

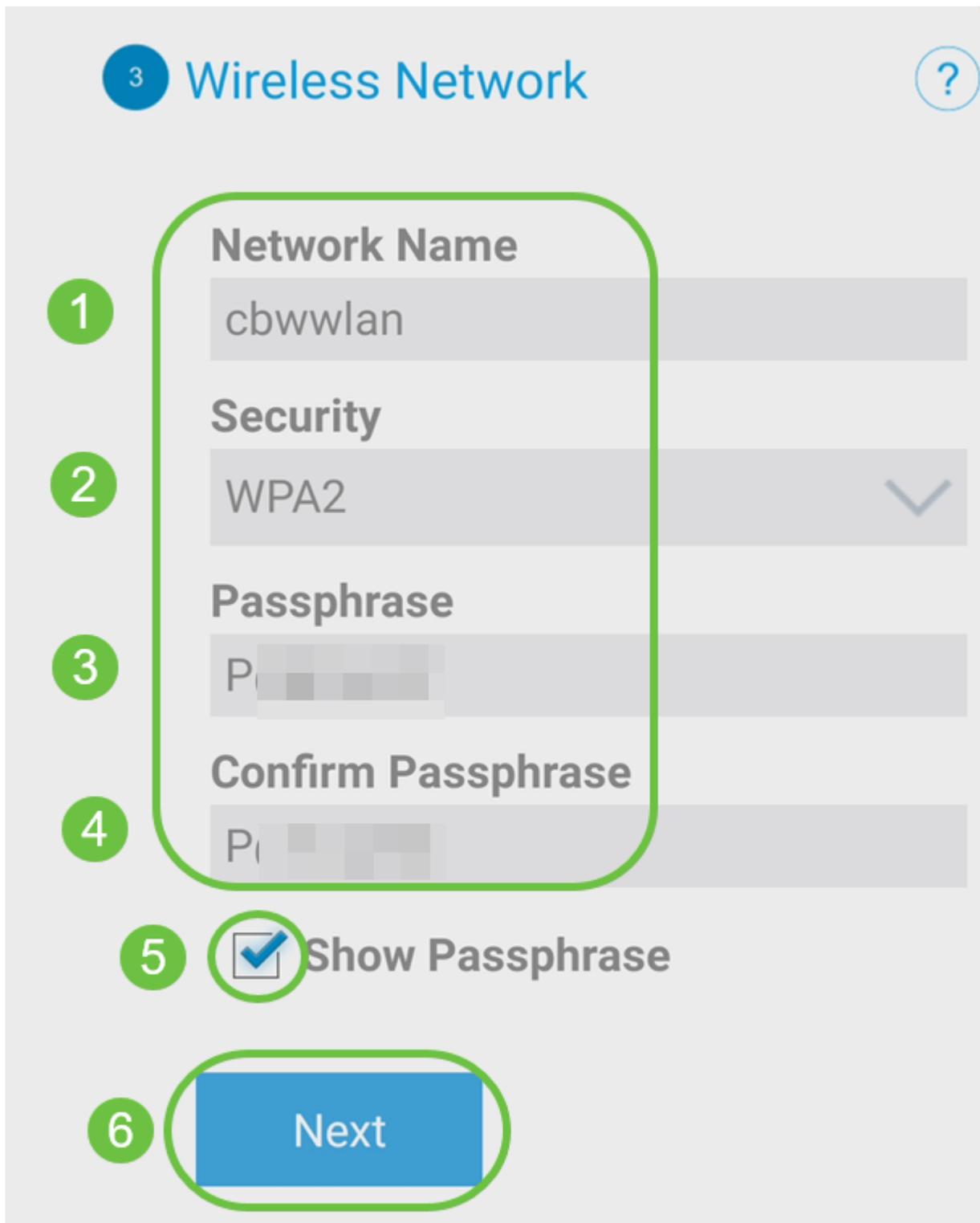


Schritt 9

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

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

Klicken Sie auf **Weiter**.



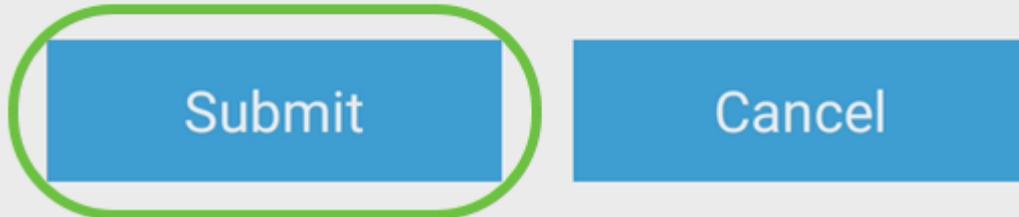
Wi-Fi Protected Access (WPA) Version 2 (WPA2) ist der aktuelle Standard für die Wi-Fi-Sicherheit.

Schritt 10

Um die Einstellungen im Bildschirm *An Master Access senden* zu bestätigen, klicken Sie auf **Submit (Senden)**.

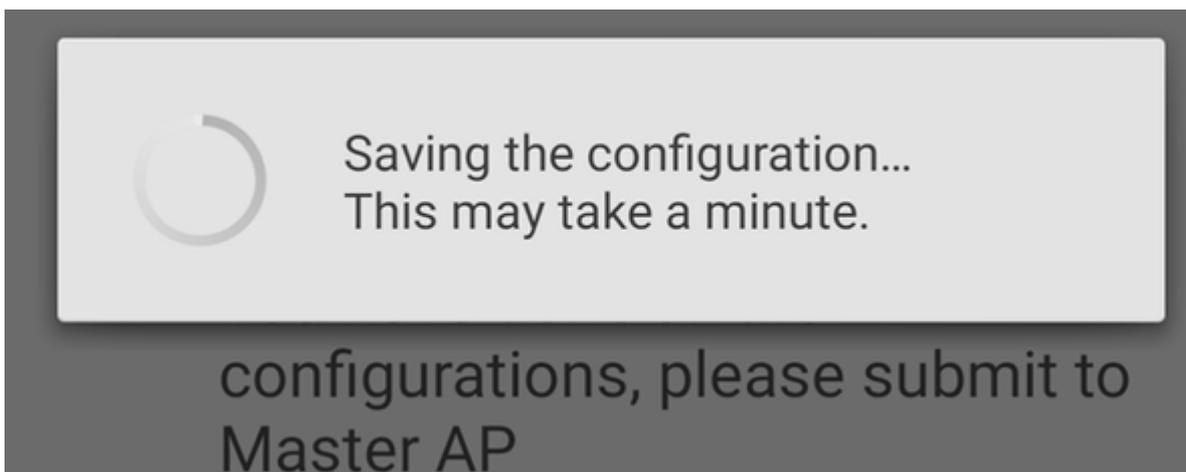
4 Submit to Master AP

You have done all the configurations, please submit to Master AP



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 Access Point mit einem Switch oder Router mit einem DHCP-Server verbunden ist.

Schritt 12

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

Confirmation

The Master AP has been fully configured and will restart in 6 minutes.

After the Master AP is restarted, it will be accessible from the network by going to this URL - <https://ciscobusiness.cisco> via browser or using Discovered Master list in Cisco Business Mobile Application provided client should be connected to configured network " cbwwlan "

Yes

Schritt 13

Schließen Sie die App, stellen Sie eine Verbindung zu Ihrem neu erstellten Wireless-Netzwerk her, und starten Sie sie erneut, um die Einrichtung von Day Zero erfolgreich abzuschließen und mit der Verwaltung Ihres Netzwerks zu beginnen.

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 Master-Access-Point zu finden.
- Melden Sie sich mit `https://<IP-Adresse des Master AP>` beim Master AP 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*.

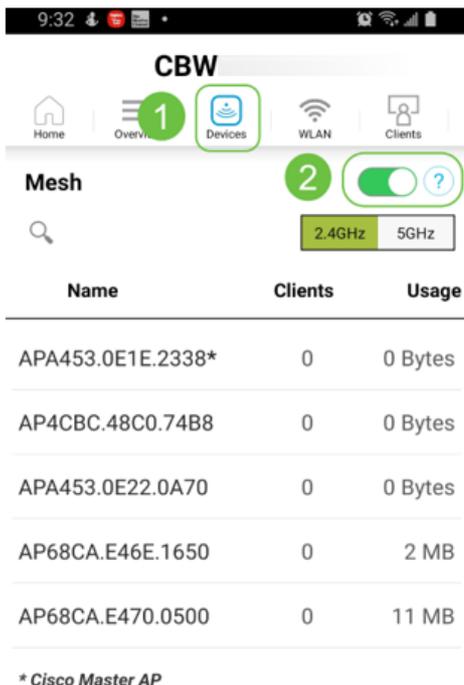
Konfigurieren der CBW142ACM-Mesh-Extender

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.

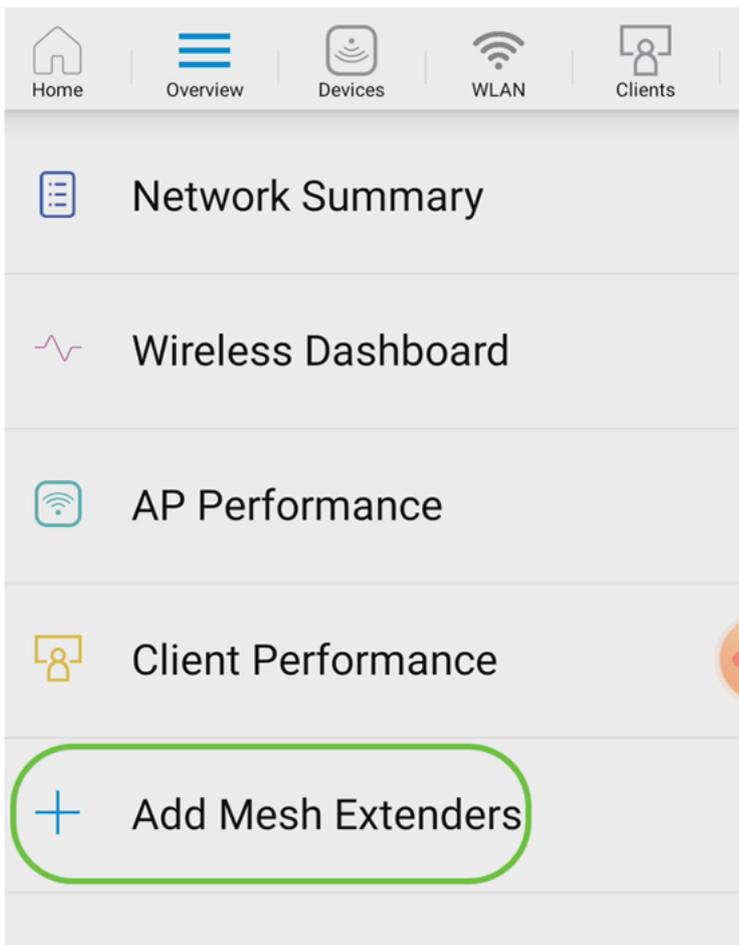
Schritt 1

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



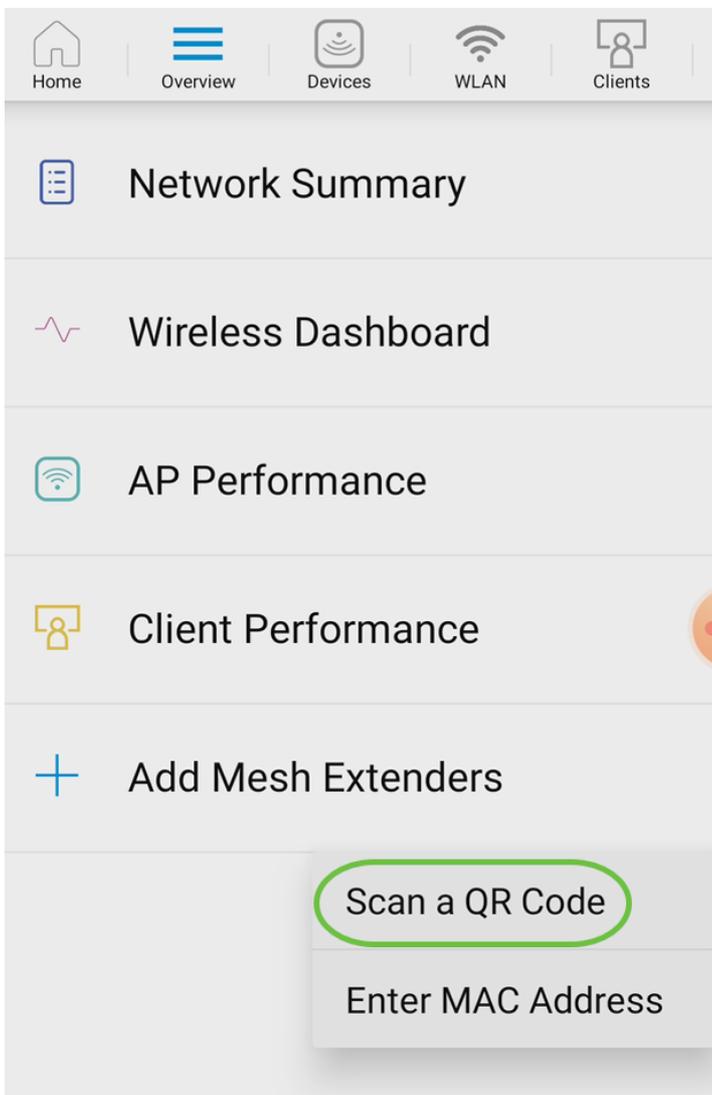
Schritt 2

Sie müssen die MAC-Adresse aller Mesh-Extender eingeben, die Sie im Mesh-Netzwerk mit dem Master-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.

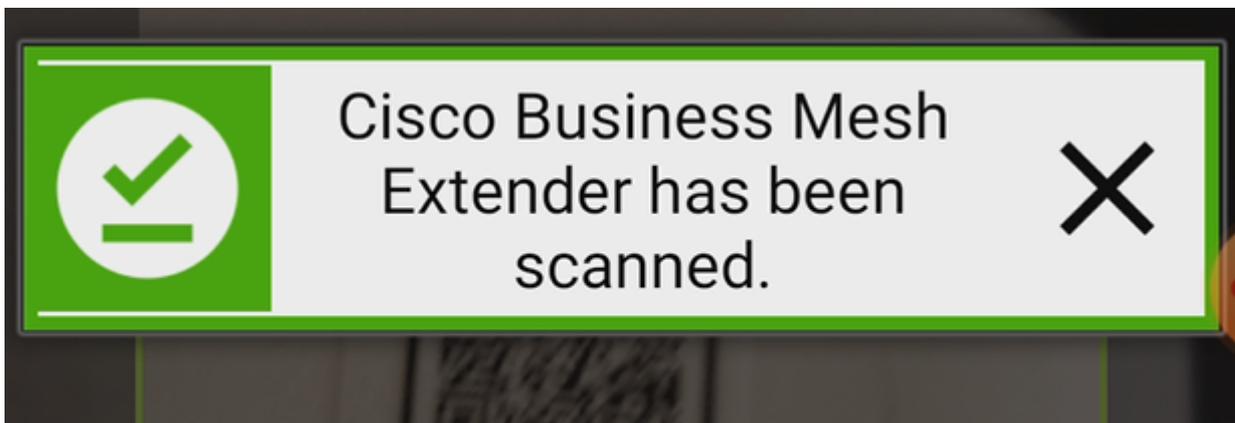


Schritt 4

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

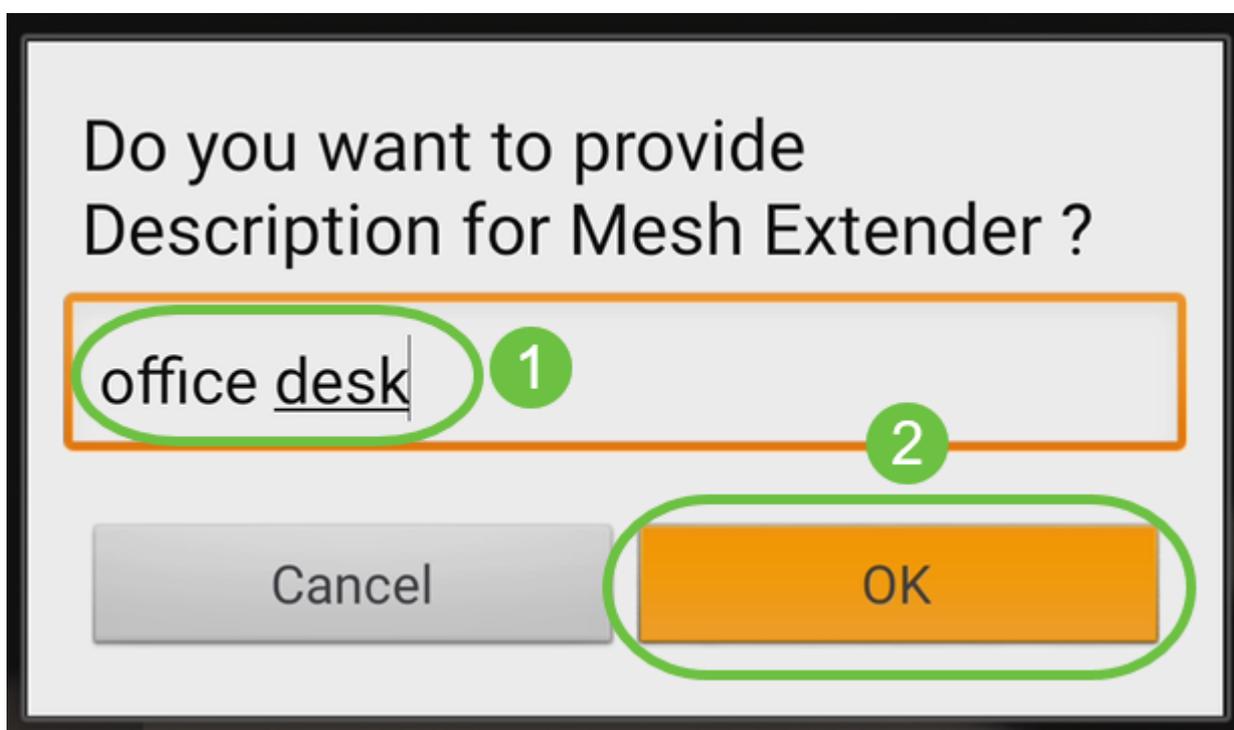


Sobald der QR-Code des Mesh Extender gescannt wurde, wird der folgende Bildschirm angezeigt.



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

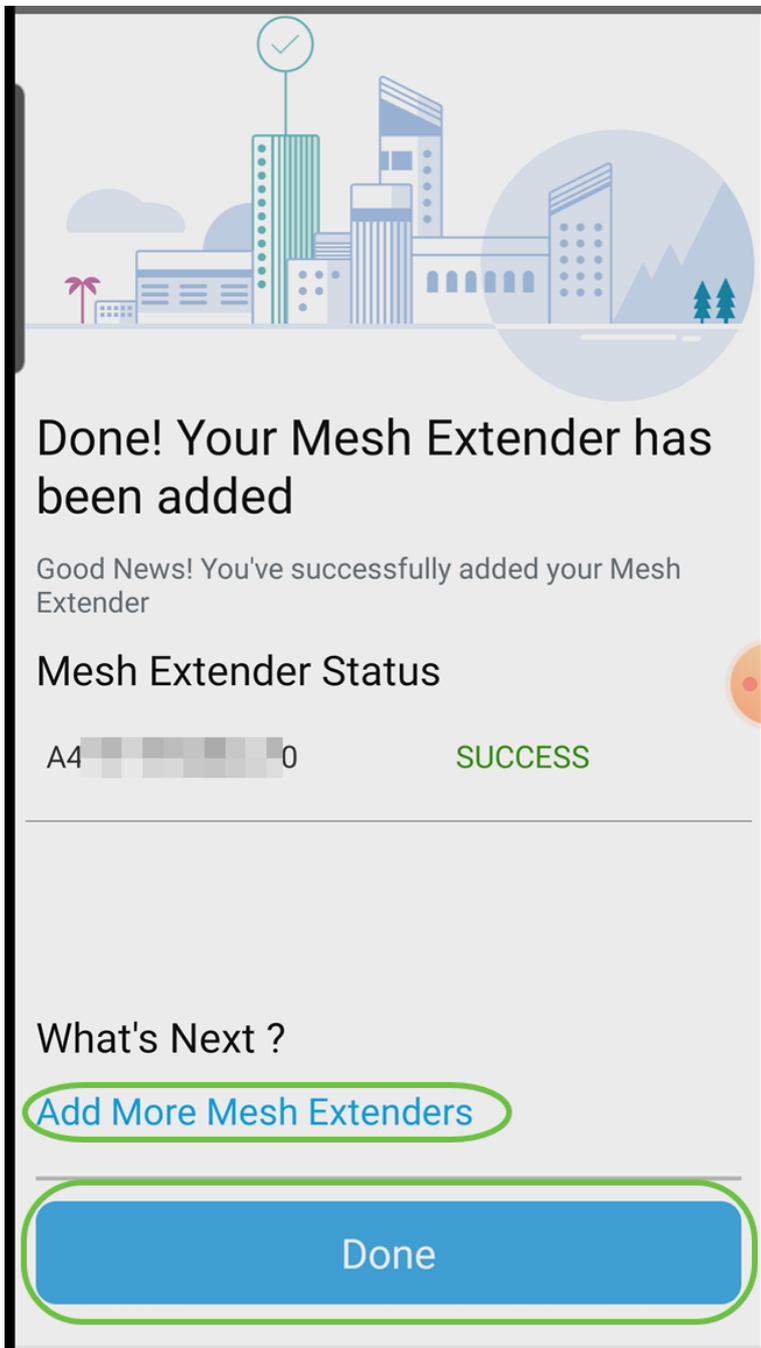
office desk



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



Home



Overview



Devices



WLAN



Clients



More

SYSTEM NAME:



1

Model

CBW140AC-B

Serial Number

FGL2419LCQN

2

Software Version

10.3.1.0

[Check for update](#)

Schritt 2



Software Update

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

AP Name	Download Progress
*AP6C71.0D55.73C4	24%
AP6C71.0D55.5DA4	21%



Home



Overview



Devices



WLAN



Clients



More

Schritt 3



Software Update

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

Erstellen von WLANs mithilfe der mobilen App

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

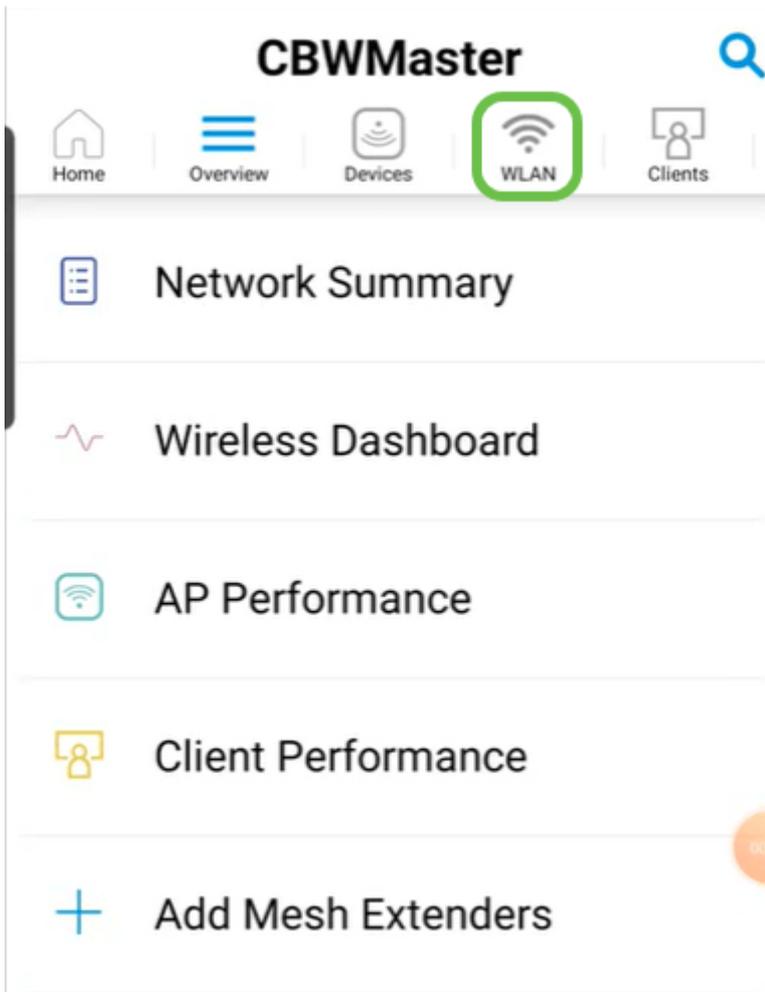
Schritt 1

Öffnen Sie die Cisco Business App. _



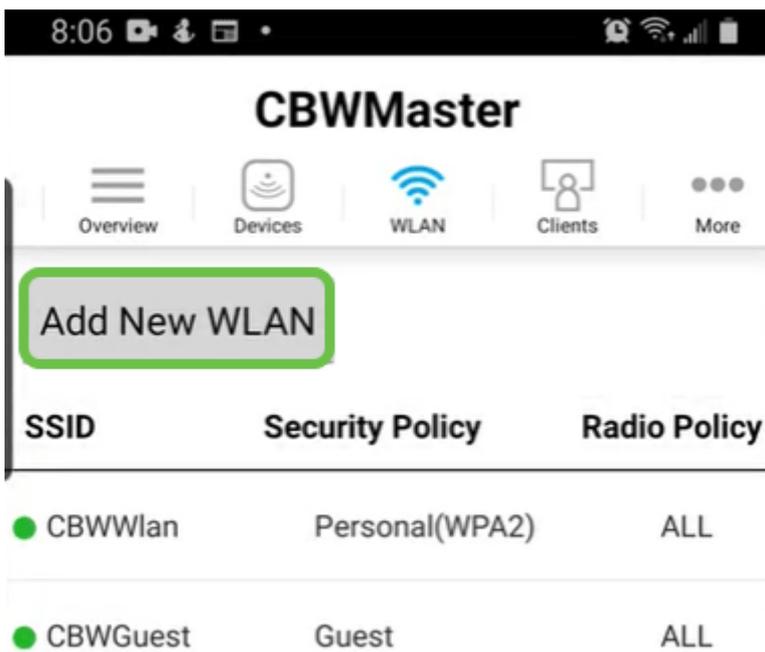
Schritt 2

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**.

WLAN

Overview Devices WLAN Clients More

General

WLAN ID 3

1 Profile Name* labnet

2 SSID* labnet

Admin State Enabled

Radio Policy ALL

Broadcast SSID ON

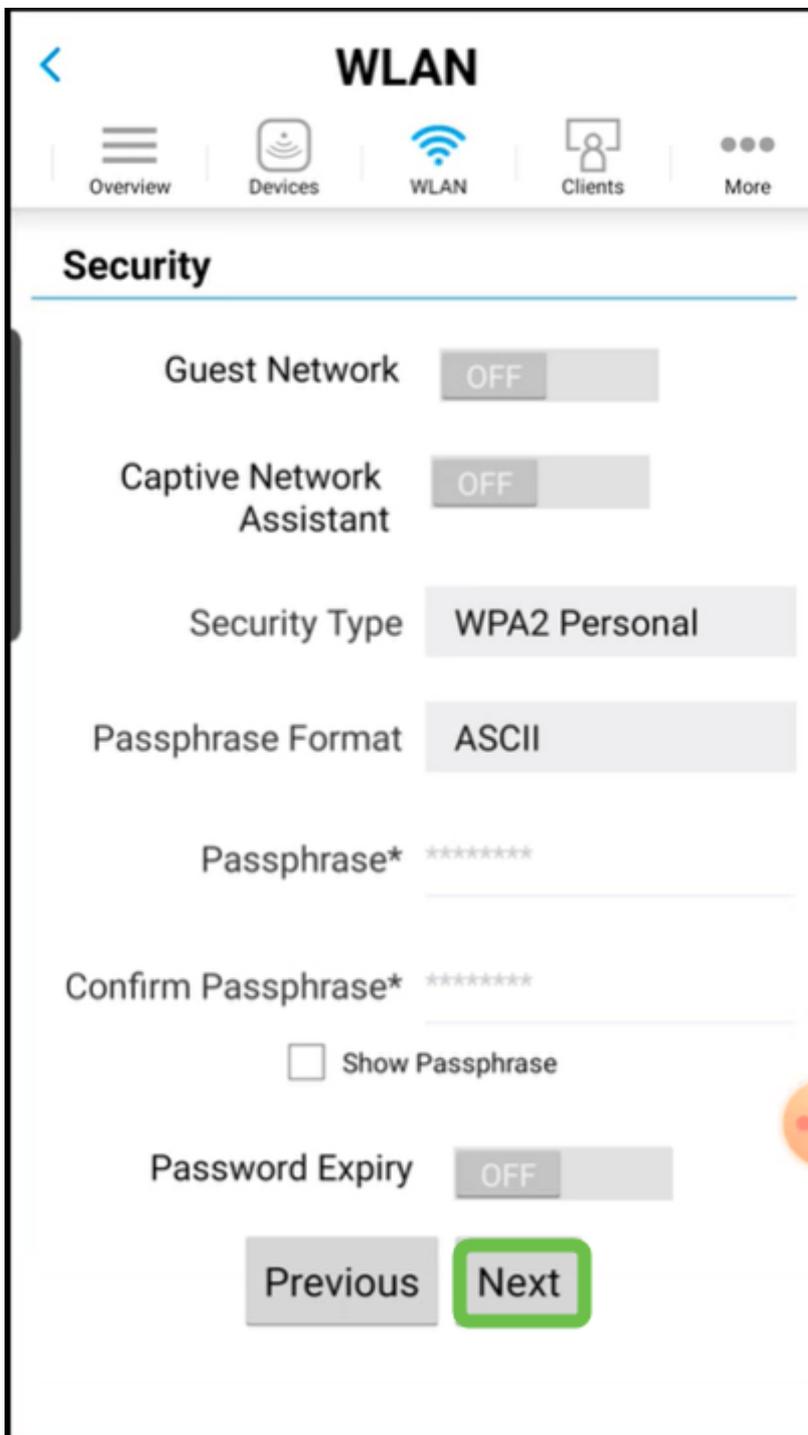
Client Profiling ON

Application Visibility Control OFF

3 Next

Schritt 5 (optional)

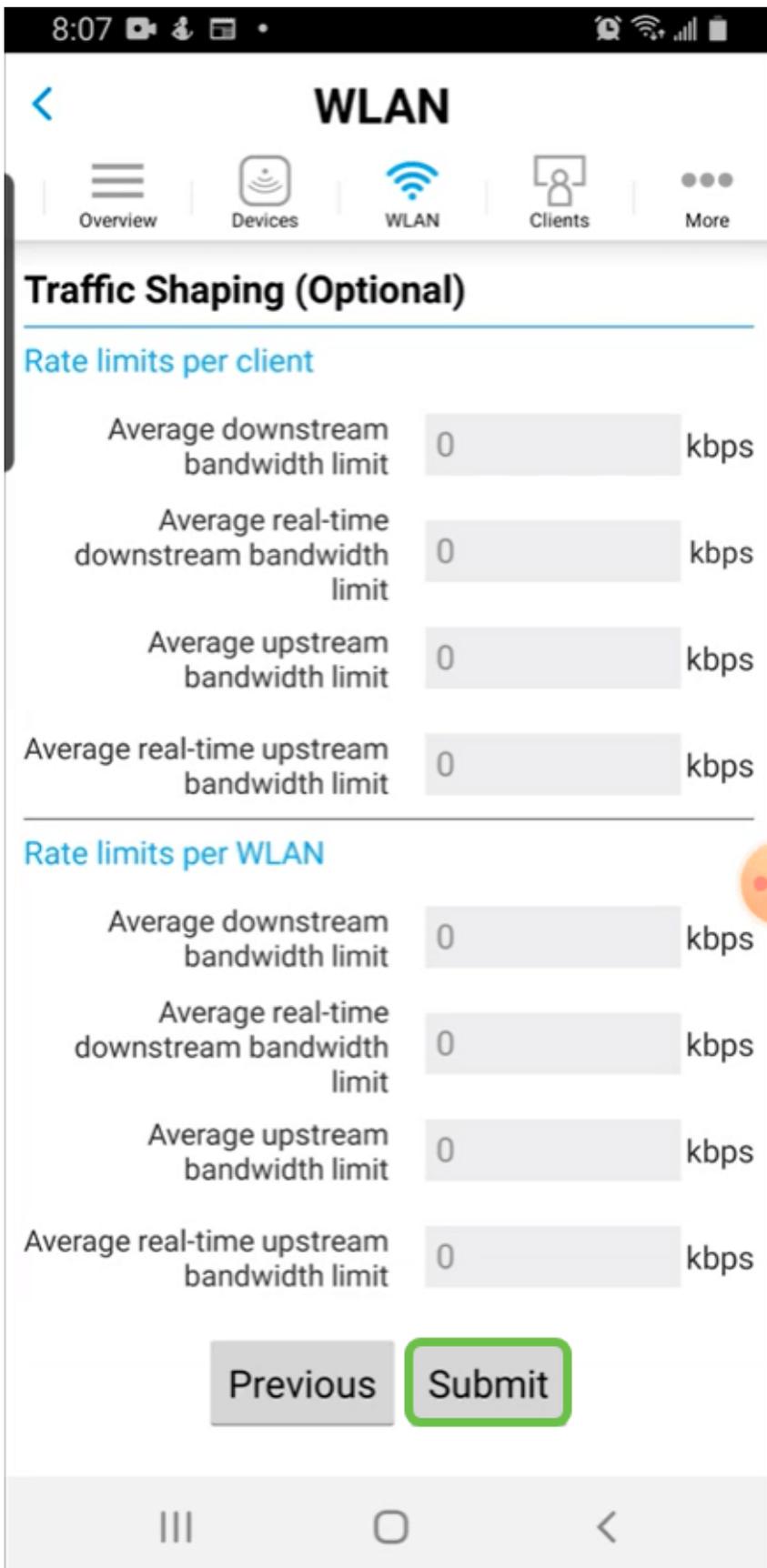
Wenn Sie *Application Visibility Control* in Schritt 4 aktiviert haben, können Sie andere Einstellungen konfigurieren, einschließlich eines Gastnetzwerks. Die Details dazu finden Sie im nächsten Abschnitt. Auch hier können Sie *Captive Network Assistant*, *Security Type (Sicherheitstyp)*, *Password Expiry*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



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 Master Access Points an.

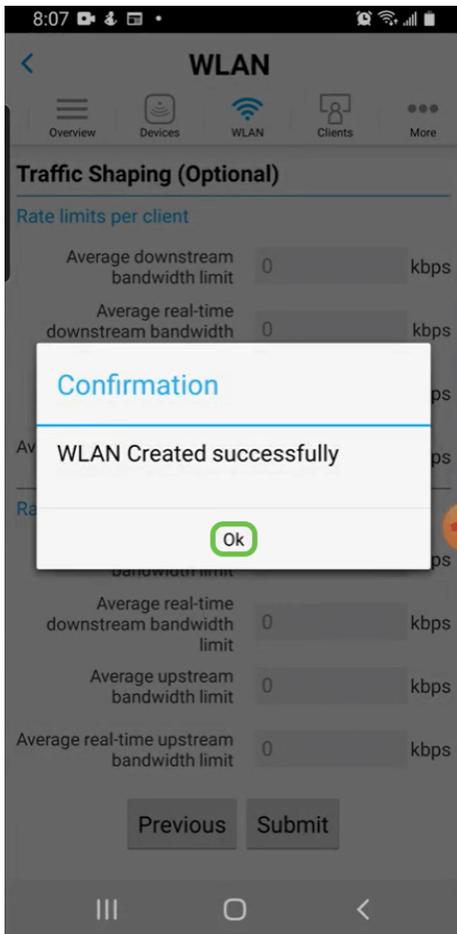
Schritt 6 (optional)

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



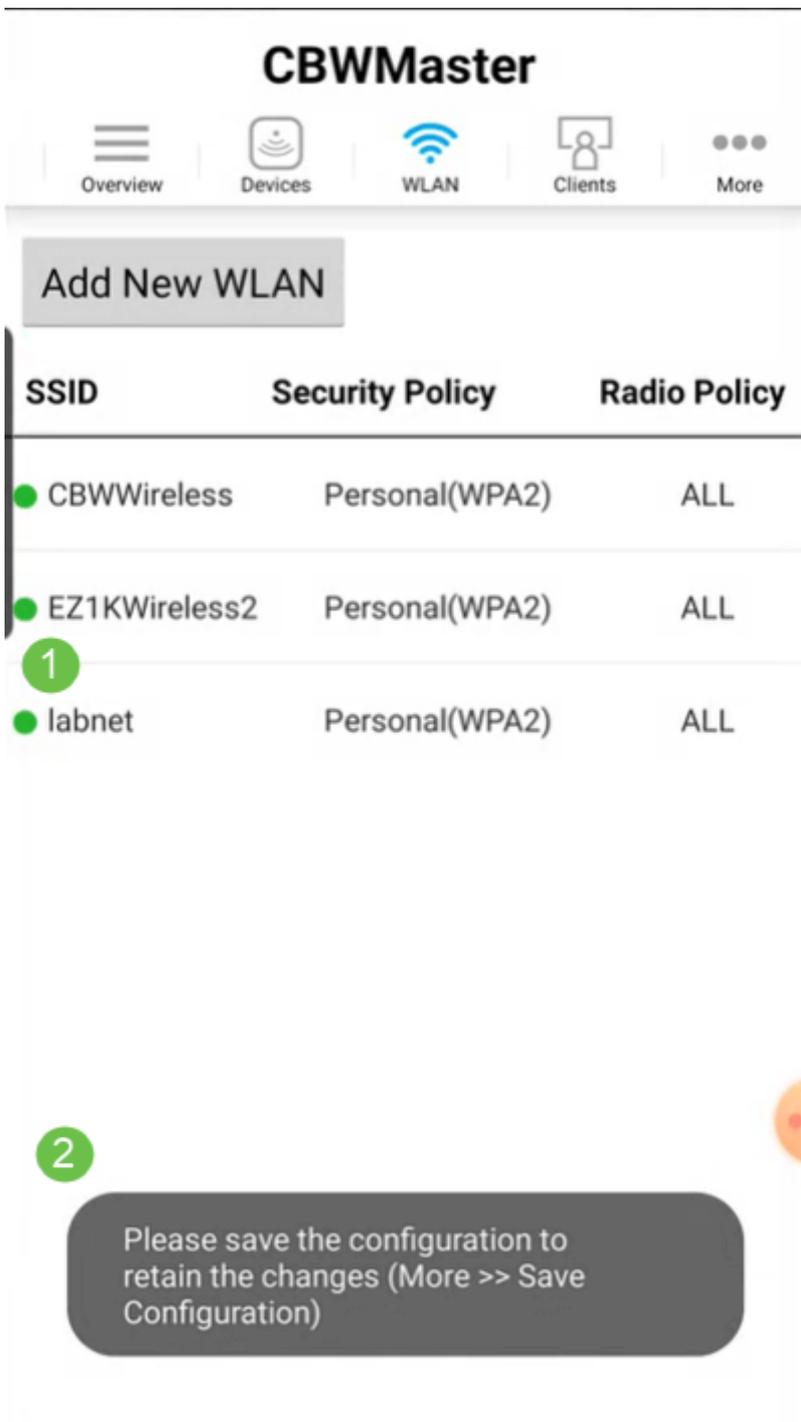
Schritt 7

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

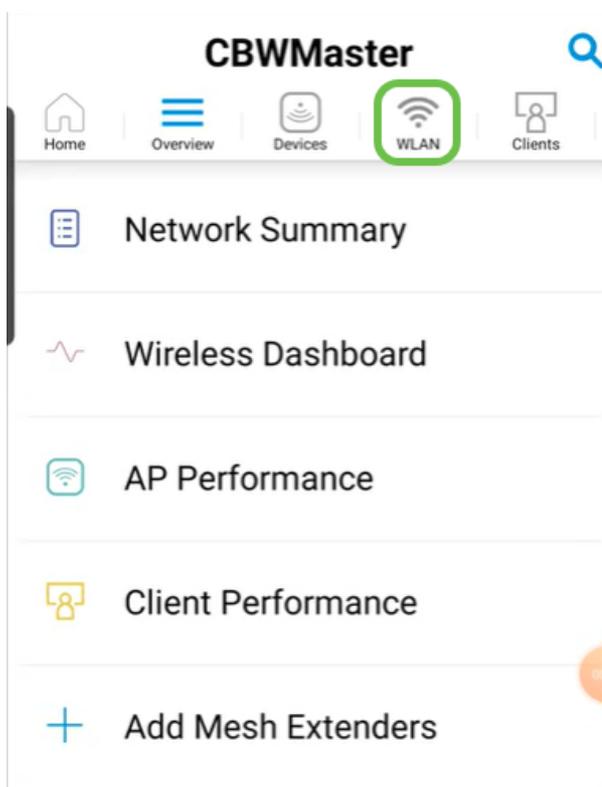
Schritt 1

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



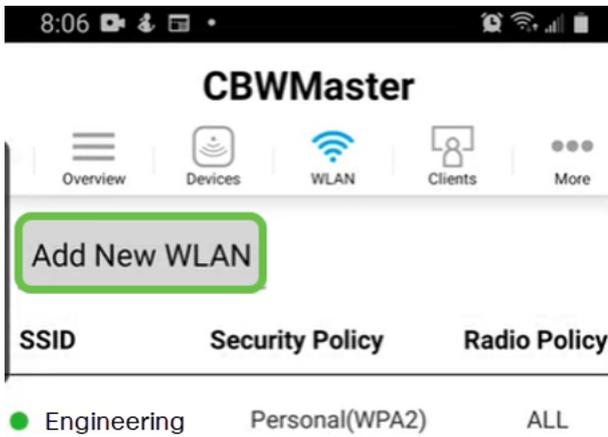
Schritt 2

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



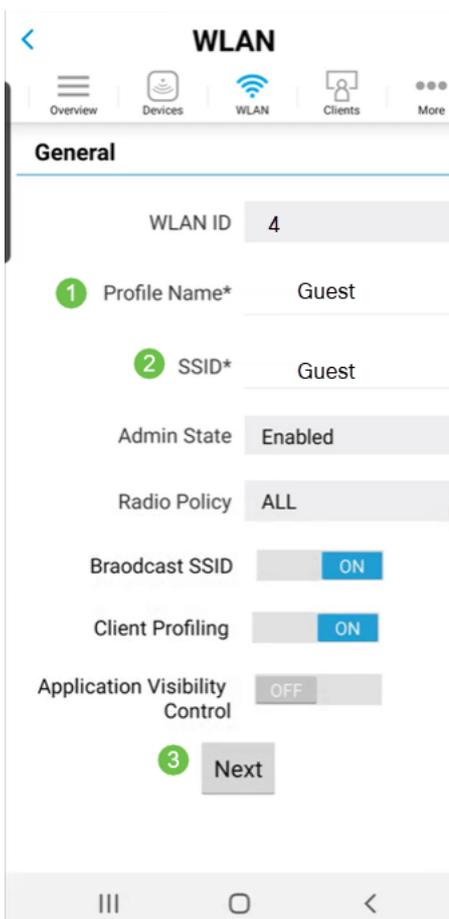
Schritt 3

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



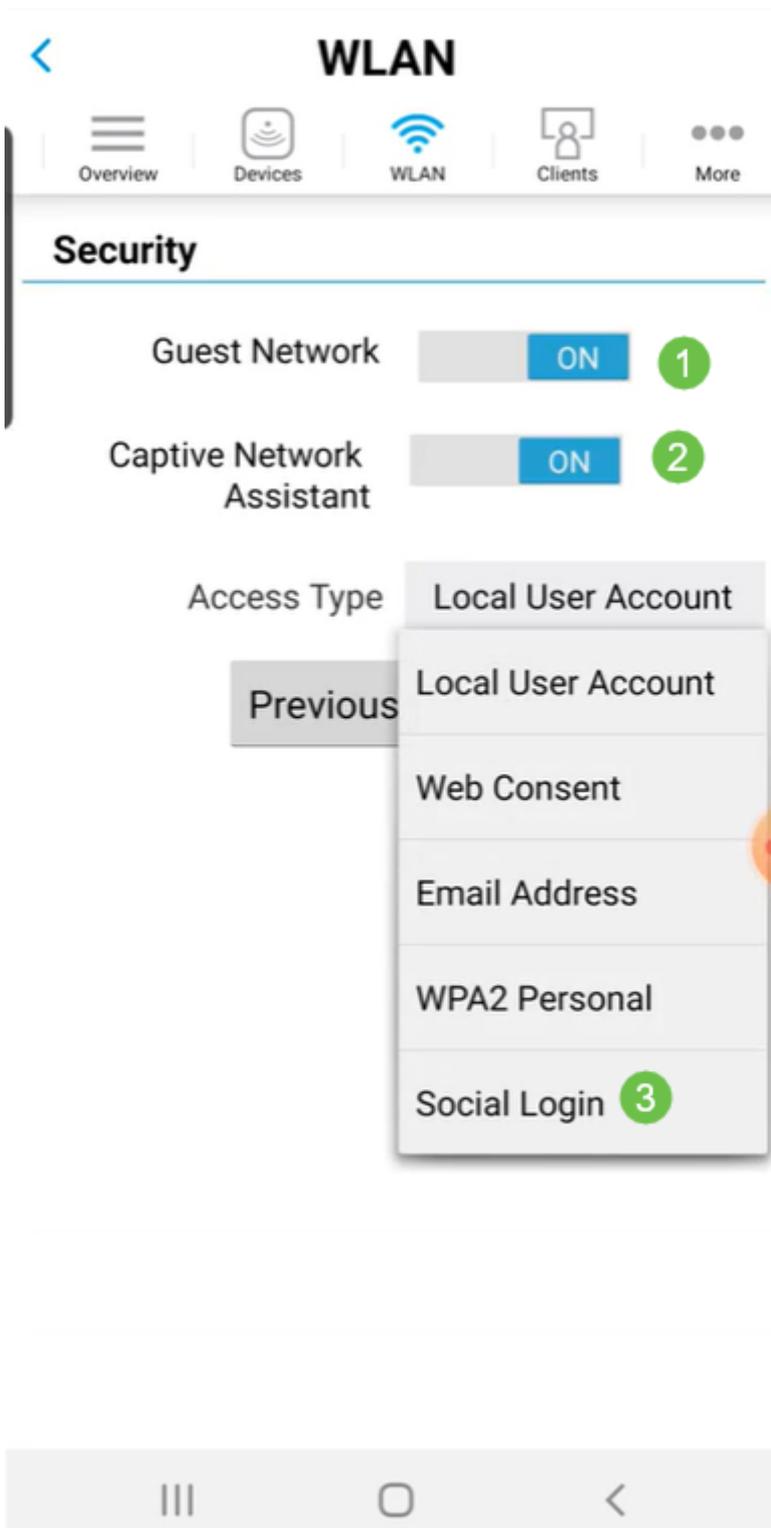
Schritt 4

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 kbps

Average real-time downstream bandwidth limit kbps

Average upstream bandwidth limit kbps

Average real-time upstream bandwidth limit kbps

Rate limits per WLAN

Average downstream bandwidth limit kbps

Average real-time downstream bandwidth limit kbps

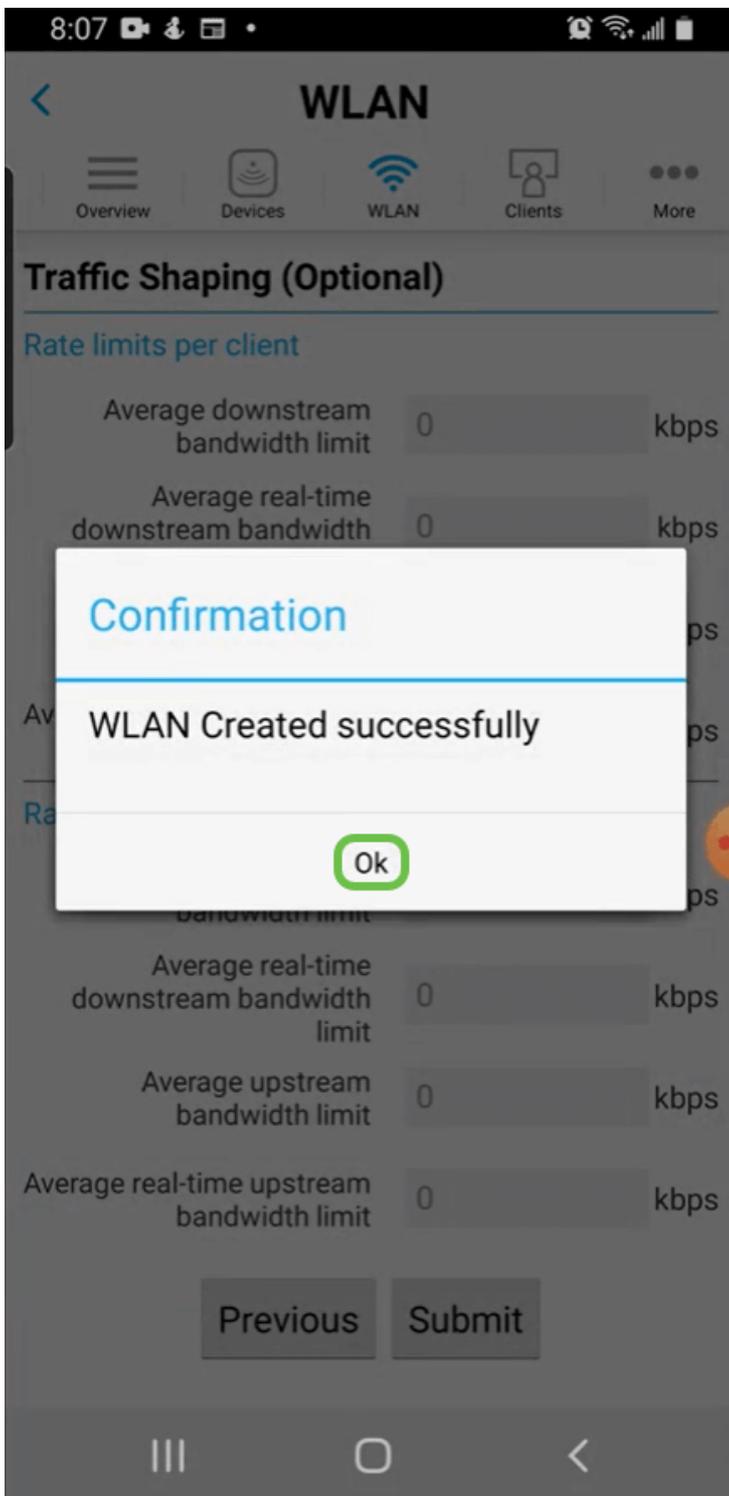
Average upstream bandwidth limit kbps

Average real-time upstream bandwidth limit 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.



Fazit

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 RV345P VPN-Router mit PoE](#)
- [Cisco Business Access Point der Serie 140AC](#)
- [Cisco Business 142ACM Mesh Extender](#)