Netzwerkkonfiguration gesamt: RV345P und Cisco Business Wireless über die Webbenutzeroberfläche

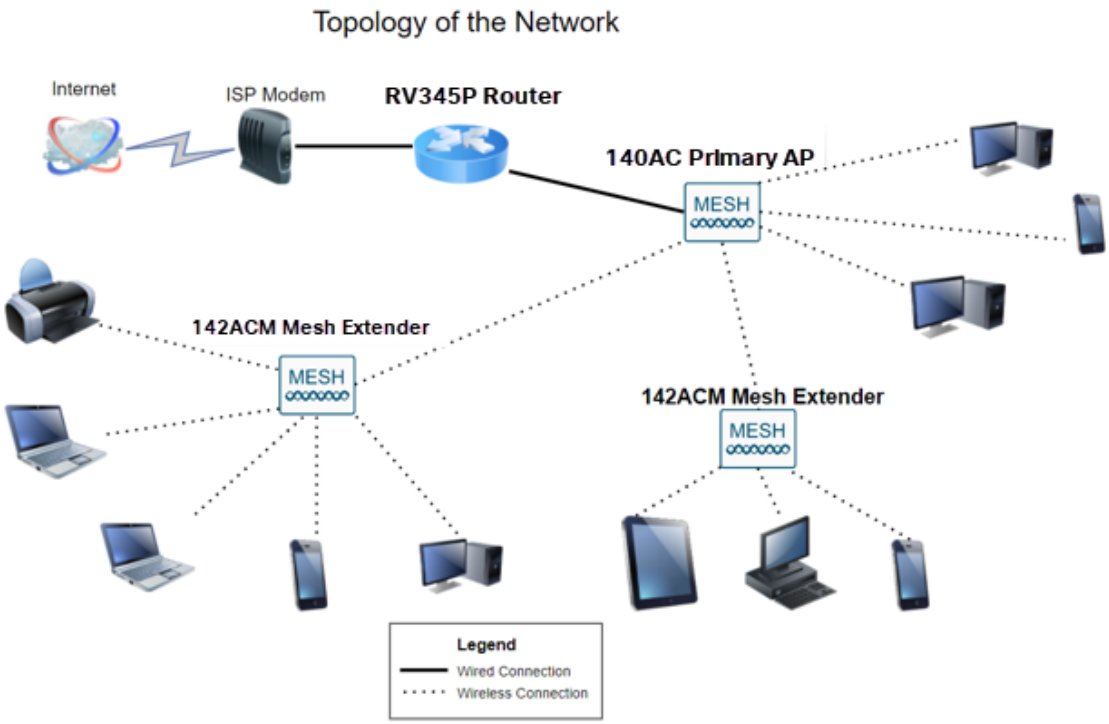
Ziel

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

Inhalt

Topologie



Einleitung

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.

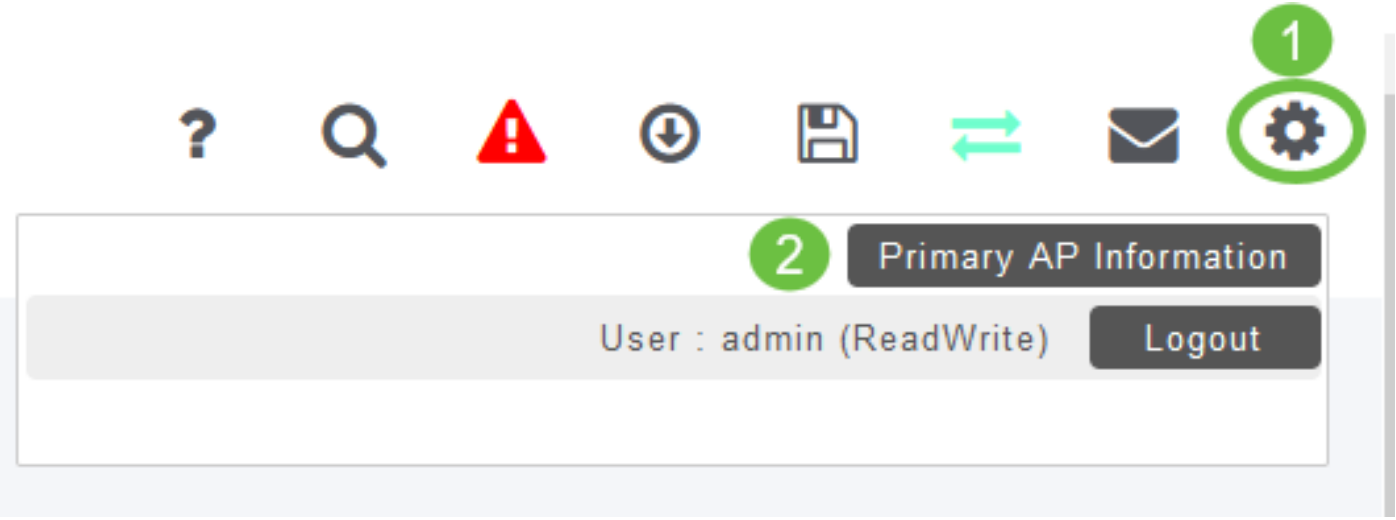
Cisco.com-Konto anfordern

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.

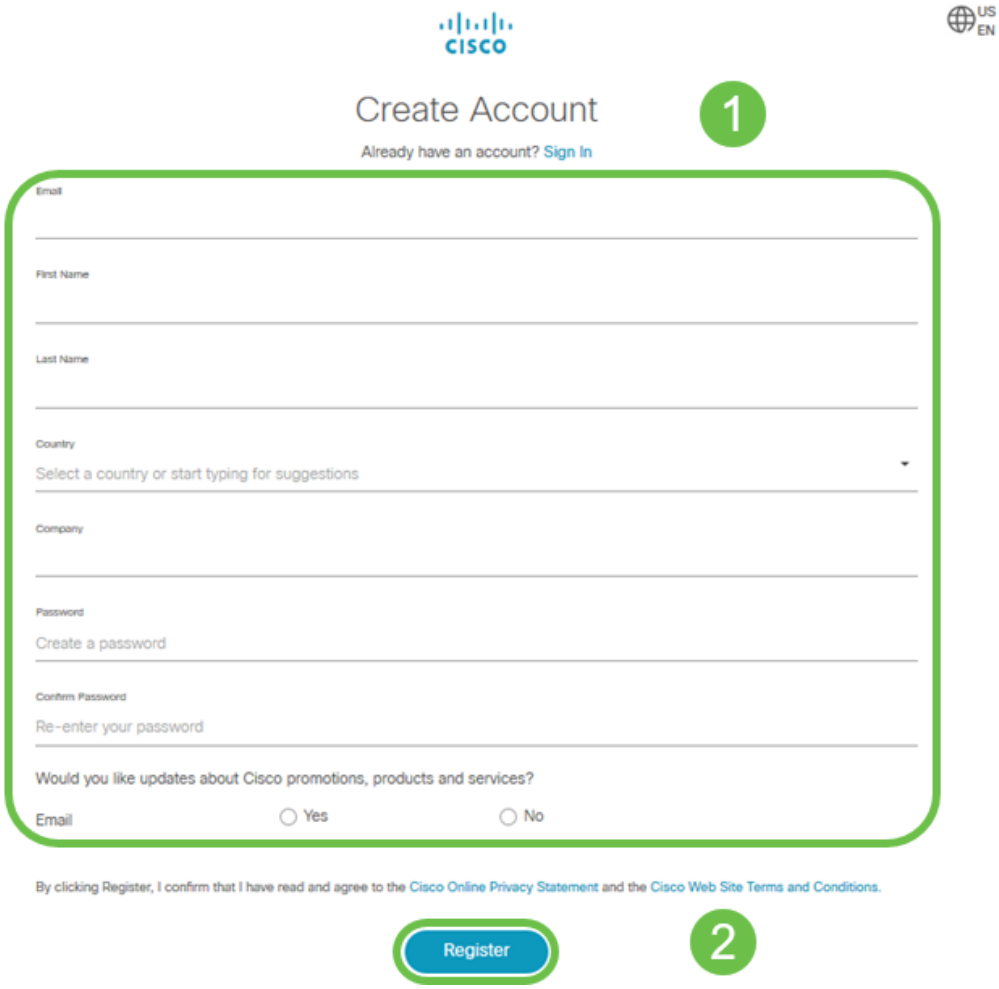
Schritt 1

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.



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

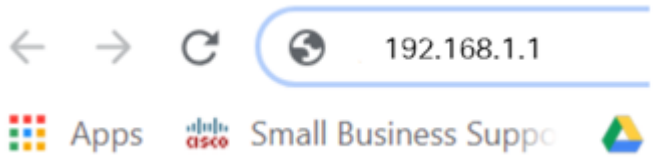
Jetzt ist es an der Zeit, einige Konfigurationen anzuzeigen! Führen Sie die folgenden Schritte aus, um die Webbenutzeroberfläche zu starten.

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.

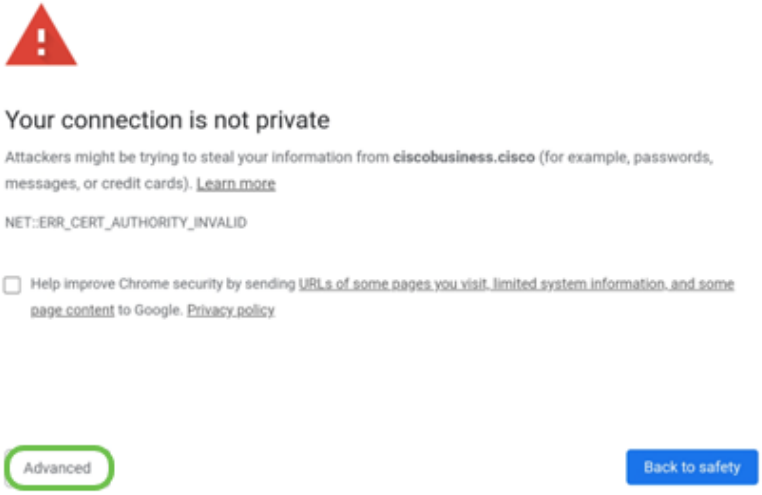
Schritt 2

Öffnen Sie einen Webbrowser wie Safari, Internet Explorer oder Firefox. Geben Sie in die Adressleiste 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.

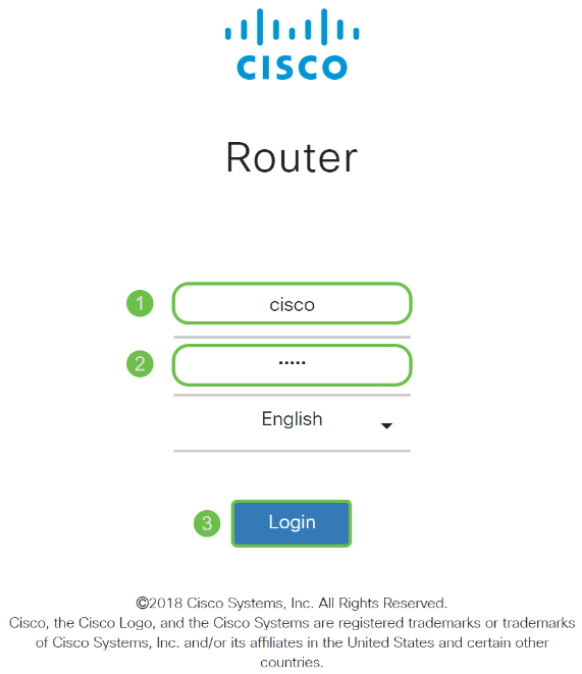


Schritt 4

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.



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.

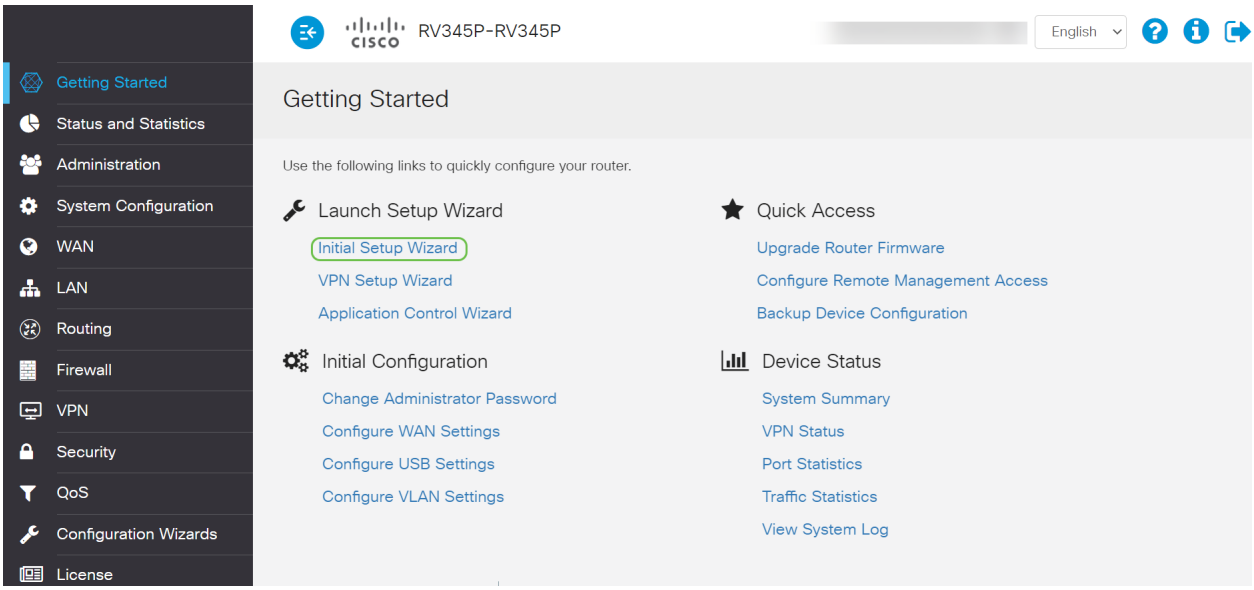
3. Wenn Sie bereits Geräte mit der IP-Adresse 192.168.1.1 besitzen, müssen Sie diesen Konflikt beheben, damit das Netzwerk funktioniert. Mehr dazu am Ende dieses Abschnitts, oder klicken Sie hier direkt dorthin.
4. Setzen Sie das Modem und den RV345P zurück, indem Sie beide Geräte ausschalten. Schalten 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.

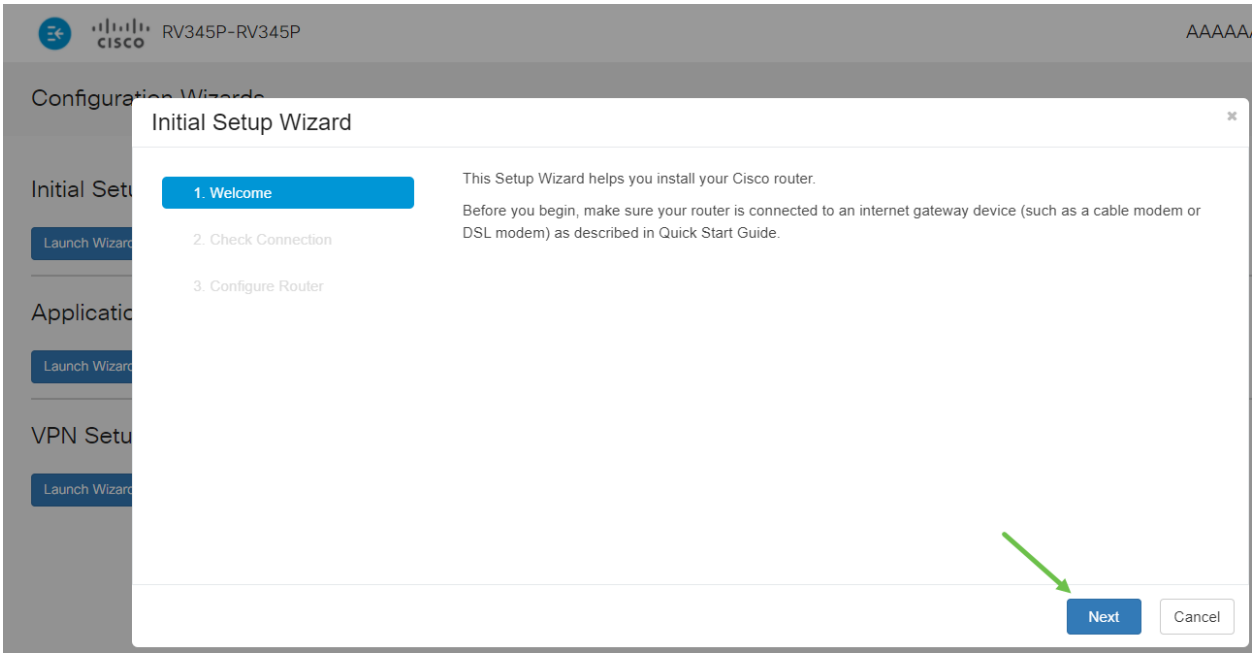
Schritt 1

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



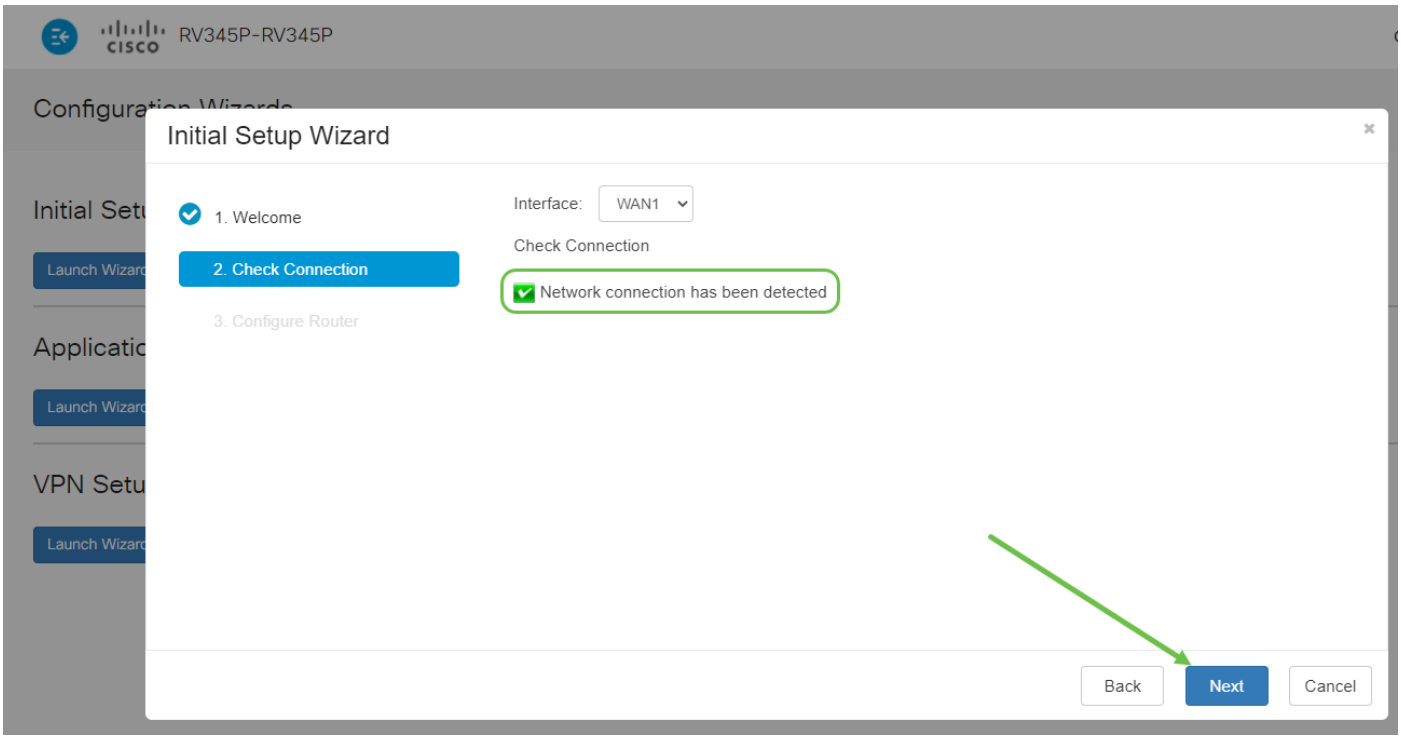
Schritt 2

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



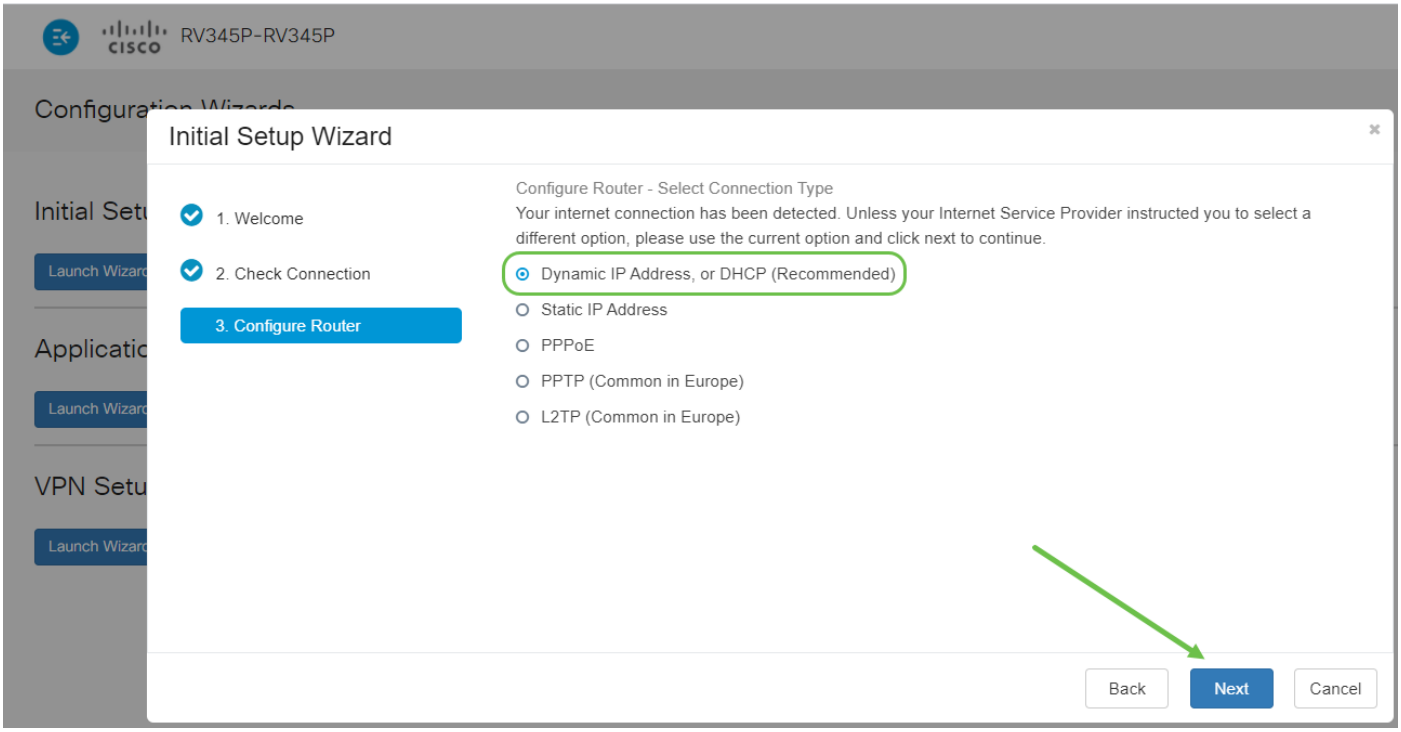
Schritt 3

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



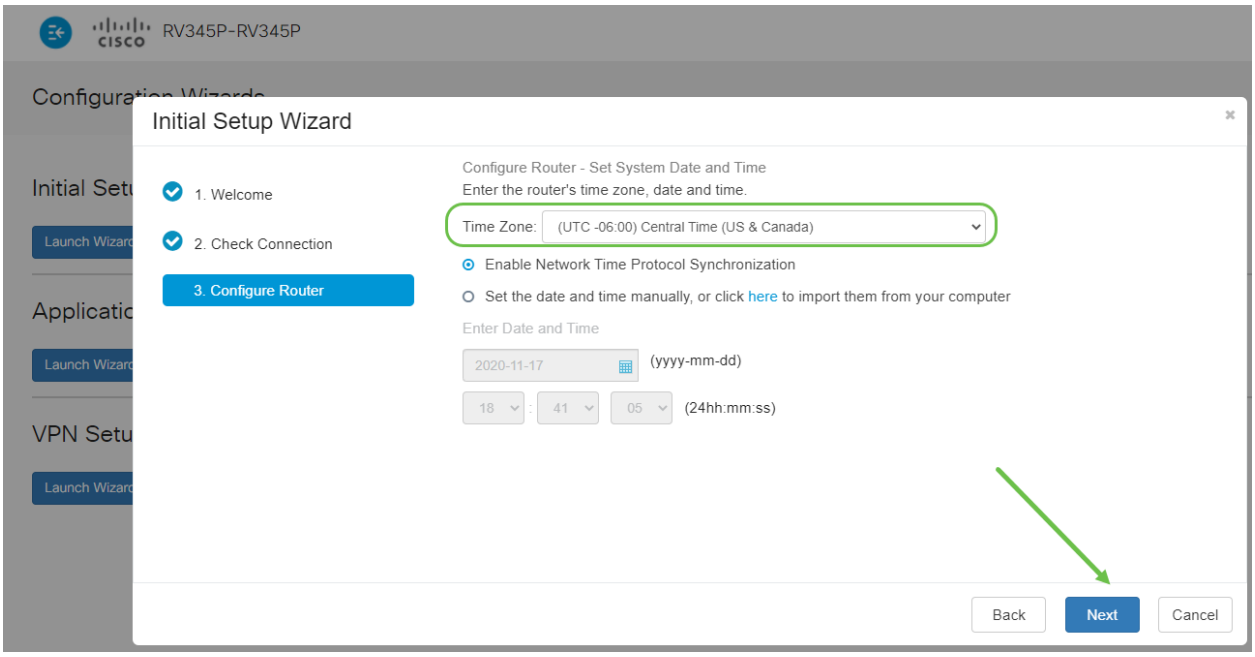
Schritt 4

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**.



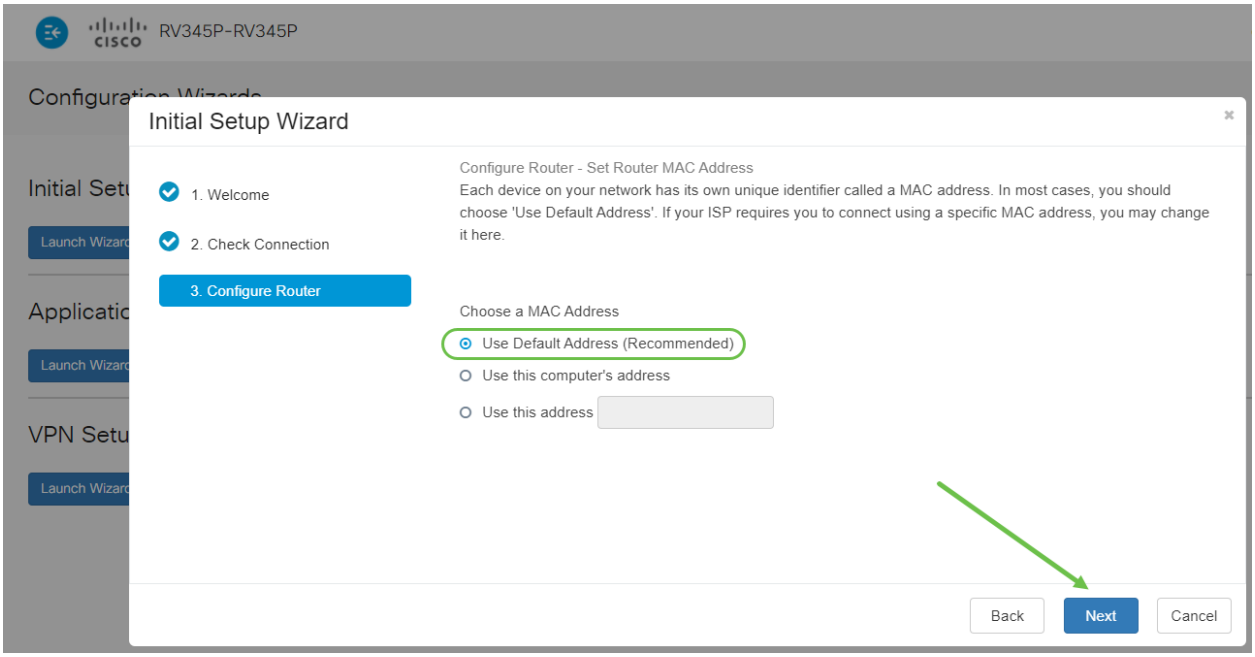
Schritt 5

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**.



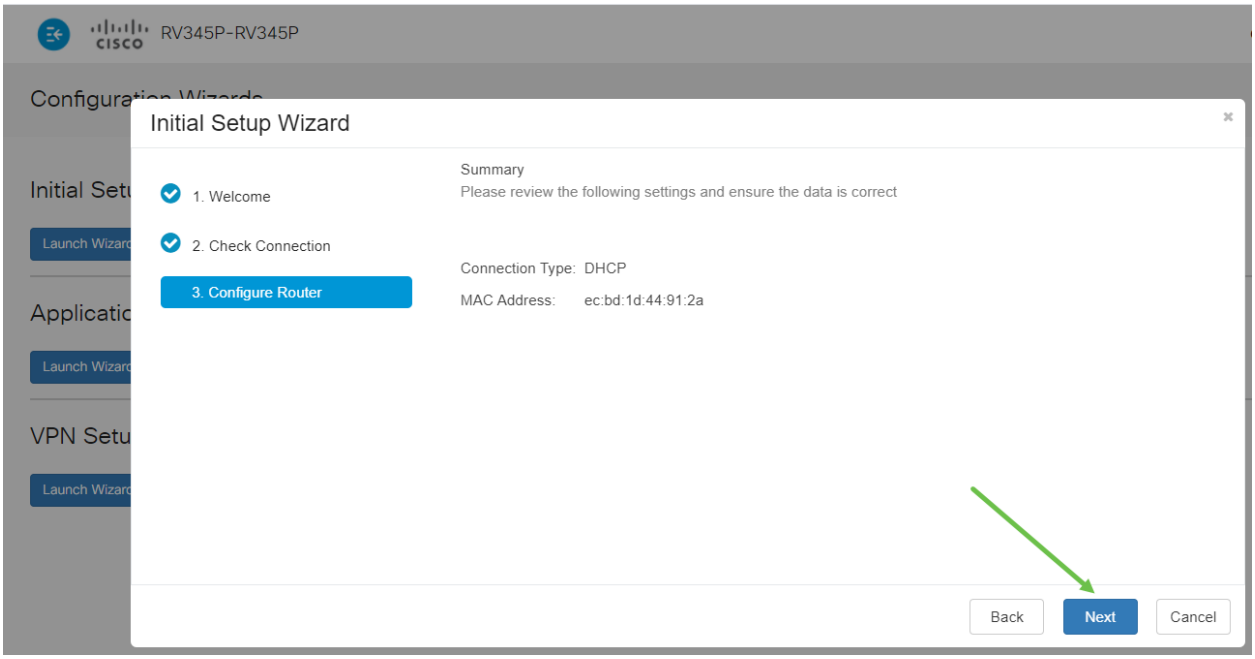
Schritt 6

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



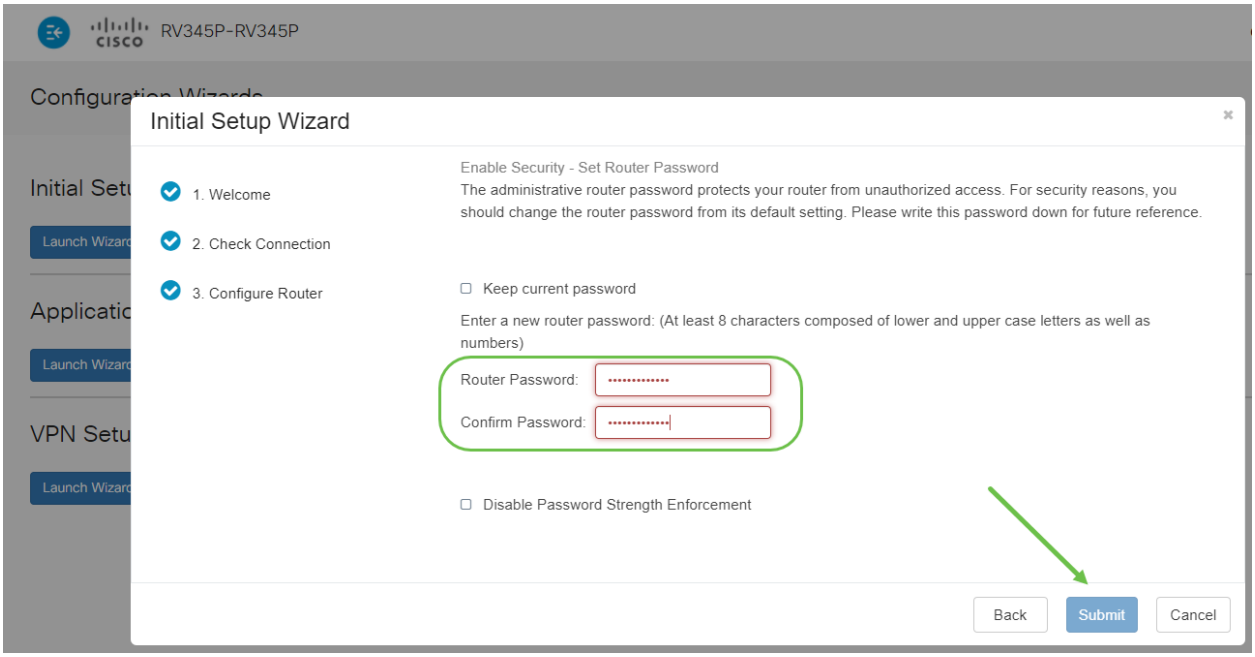
Schritt 7

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.

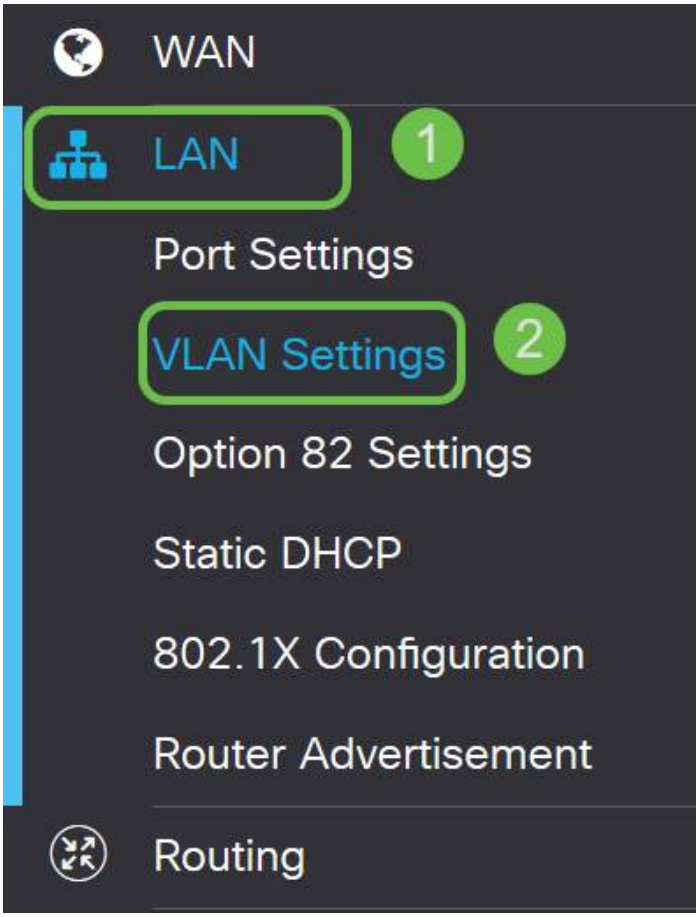
Bearbeiten Sie ggf. eine IP-Adresse (optional).

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.

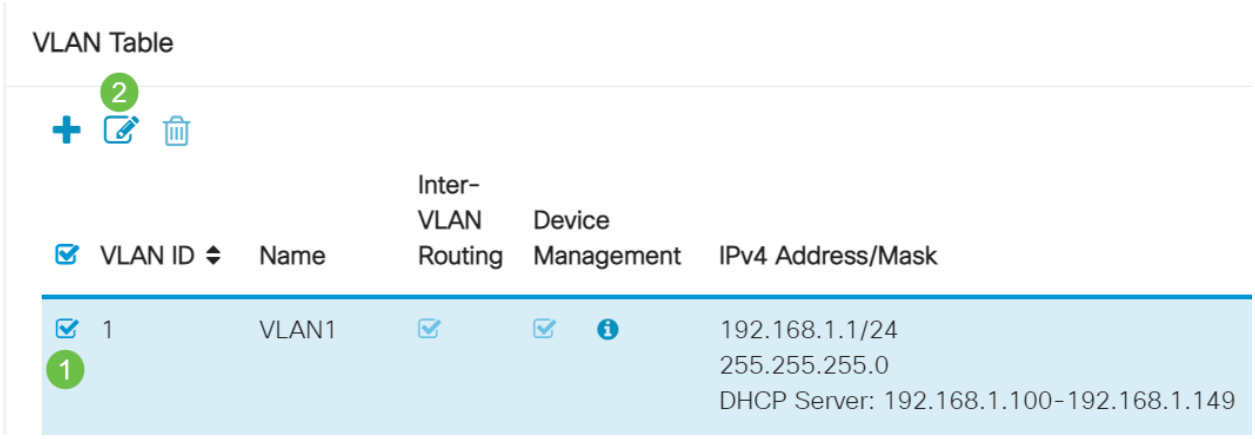
Schritt 1

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



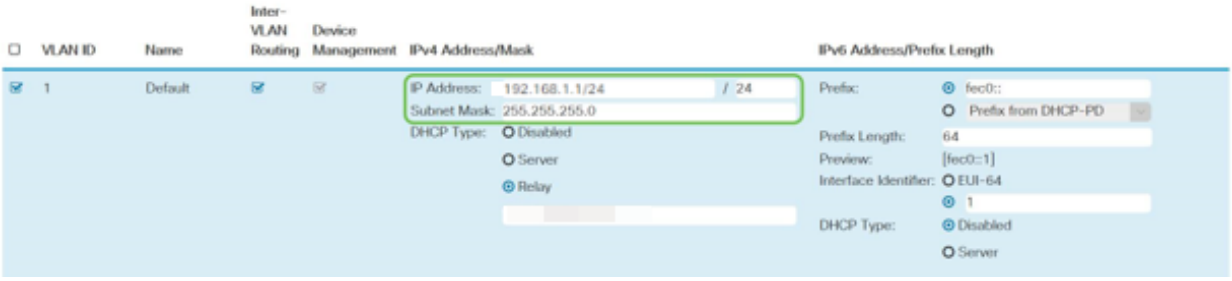
Schritt 2

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



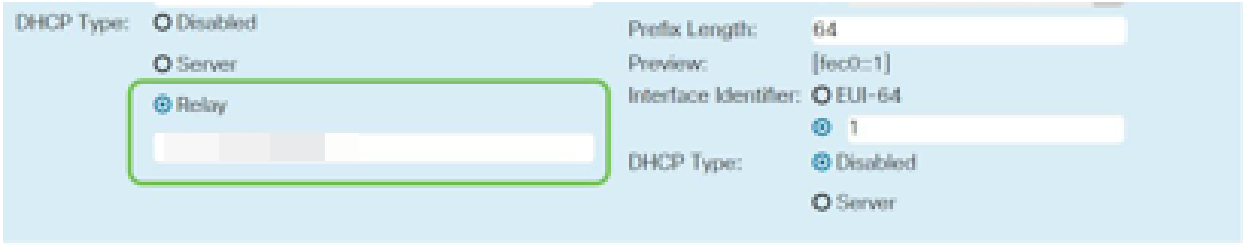
Schritt 3

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



Schritt 4 (optional)

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

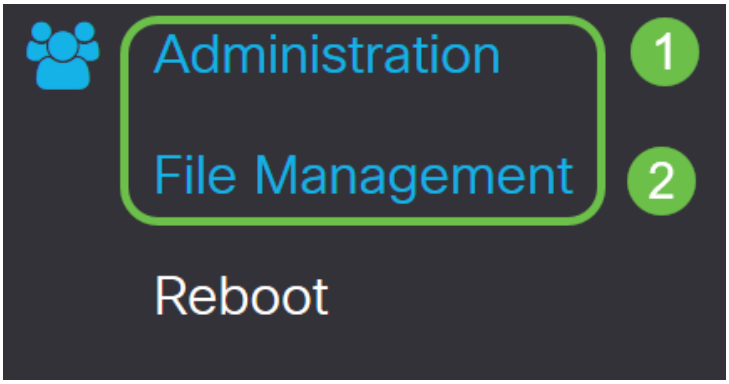


Firmware aktualisieren, falls erforderlich

Dies ist ein wichtiger Schritt, überspringen Sie ihn nicht!

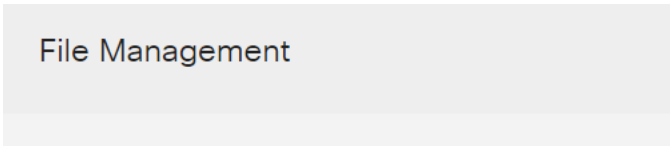
Schritt 1

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



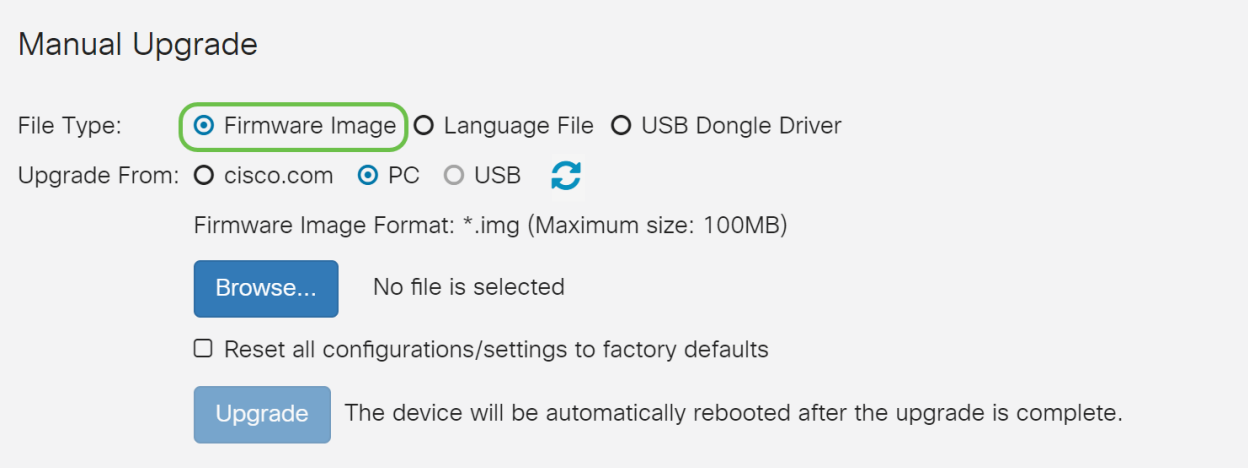
Im Bereich *Systeminformationen* beschreiben die folgenden Unterbereiche Folgendes:

- 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.



Schritt 2

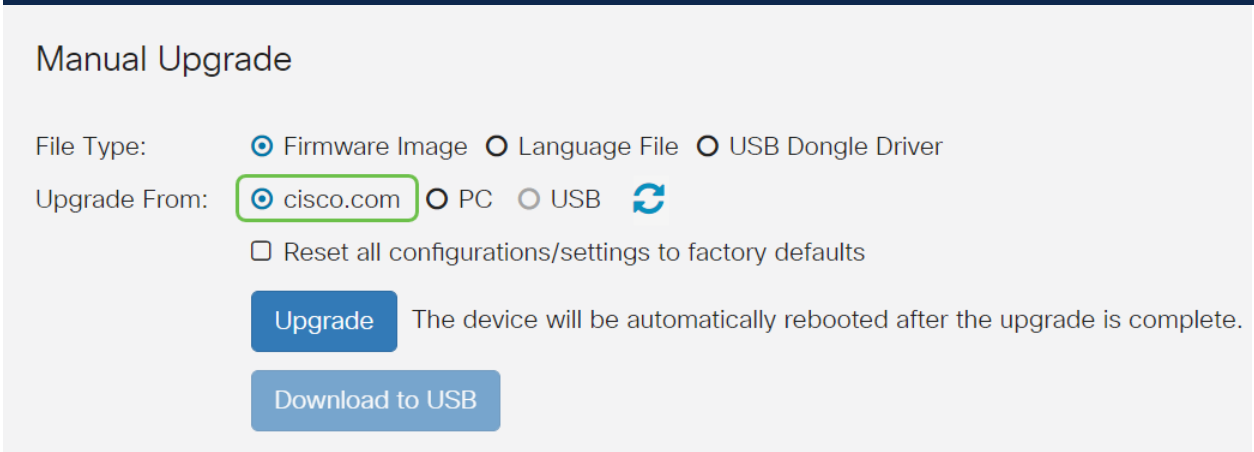
Klicken Sie im Abschnitt *Manuelle Aktualisierung* auf das Optionsfeld **Firmware-Image** für *Dateityp*.



Schritt 3

Klicken Sie auf der Seite *Manuelle Aktualisierung* auf 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.

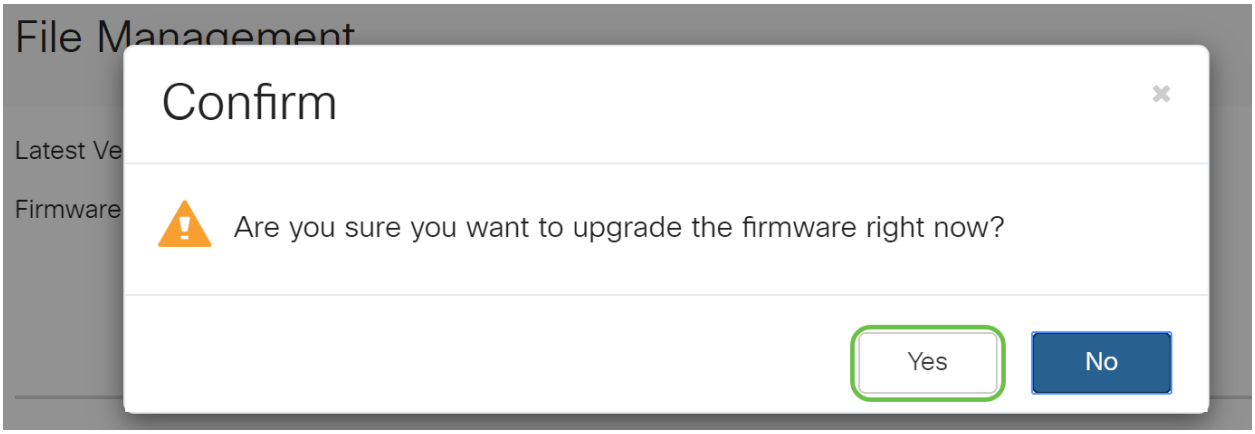


Schritt 4

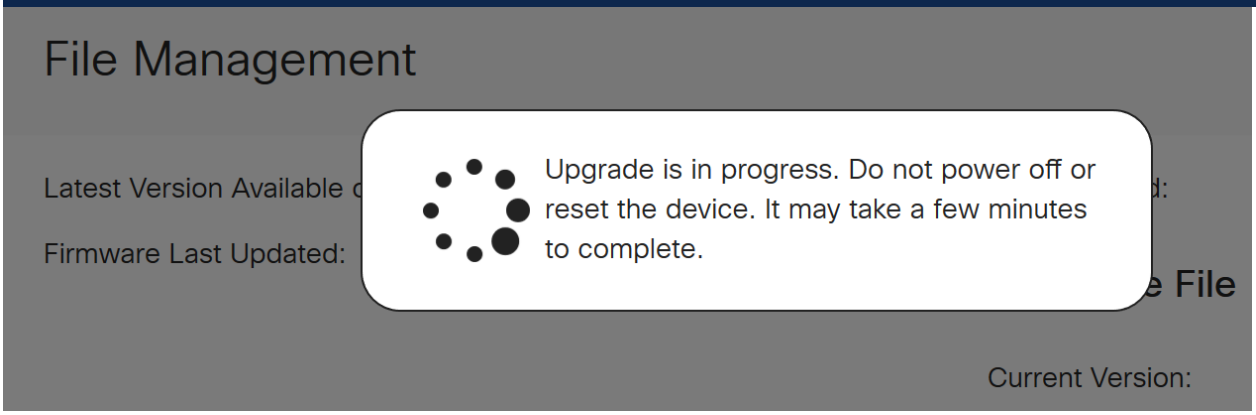
Klicken Sie auf **Upgrade**.

Schritt 5

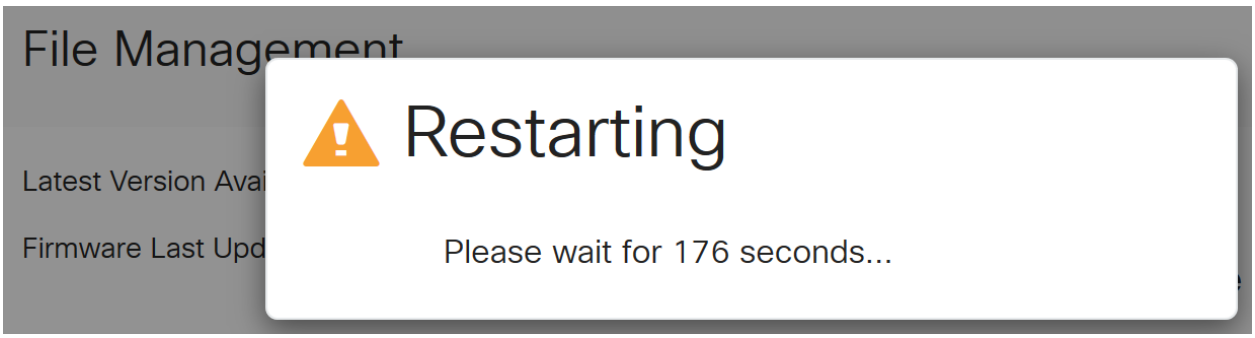
Klicken Sie im Bestätigungsfenster auf **Ja**, um fortzufahren.



Der Aktualisierungsvorgang muss unterbrechungsfrei ausgeführt werden. Während der Aktualisierung wird die folgende Meldung angezeigt.

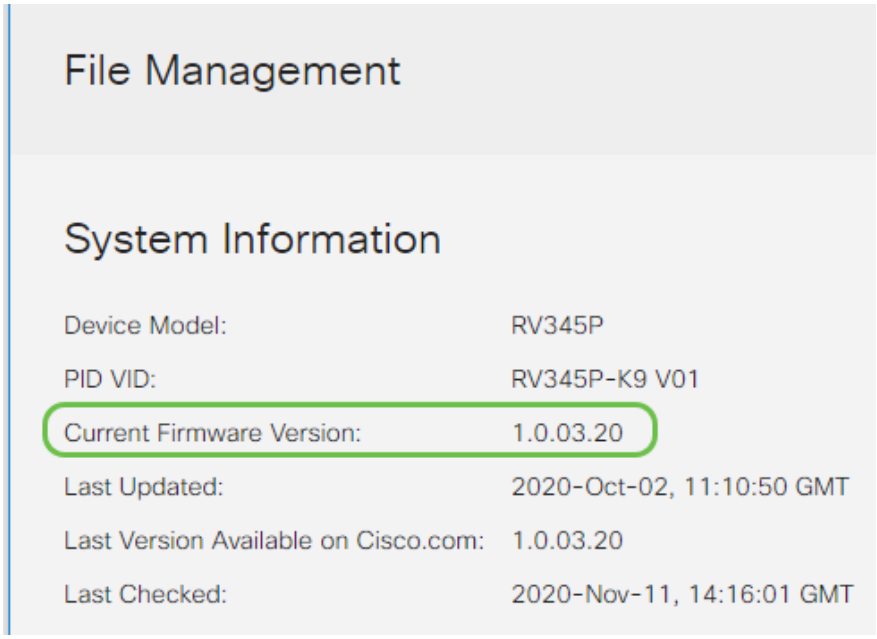


Nach Abschluss der Aktualisierung wird ein Benachrichtigungsfenster angezeigt, in dem Sie darüber informiert werden, dass der Router *neu gestartet* wird und eine Countdown für die geschätzte Zeit bis zum Abschluss des Vorgangs angezeigt wird. Danach werden Sie abgemeldet.



Schritt 6

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

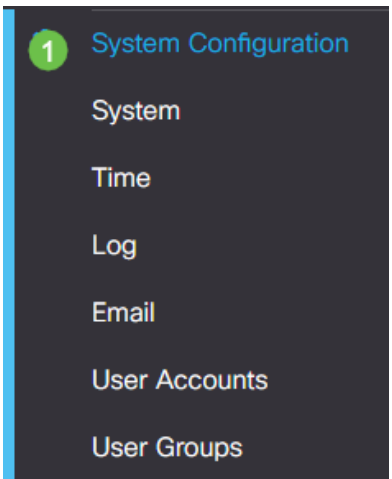


Konfigurieren automatischer Updates auf dem Router der Serie RV345P

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

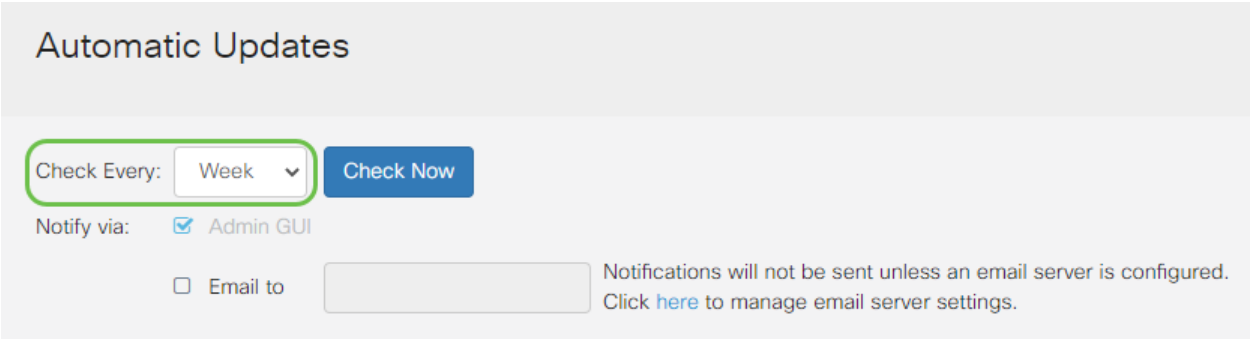
Schritt 1

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



Schritt 2

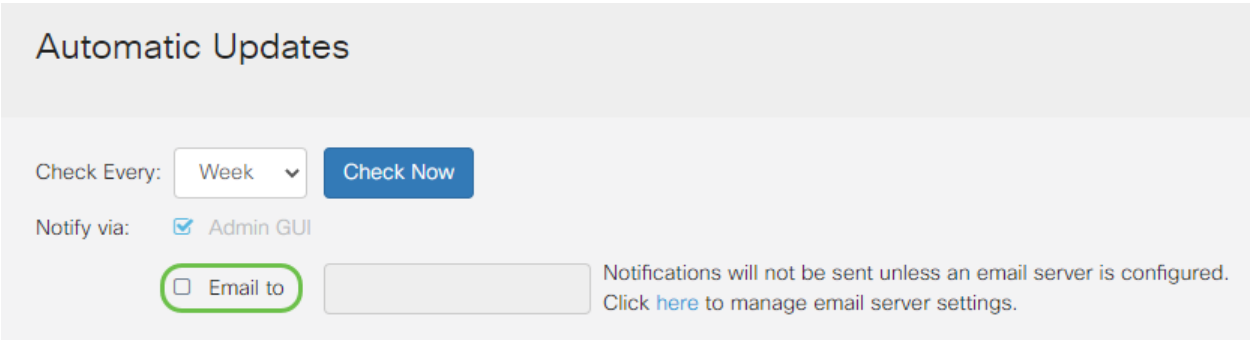
Wählen Sie aus der Dropdown-Liste *Check Every (Alle prüfen*) aus, wie oft der Router nach Updates suchen soll.



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.

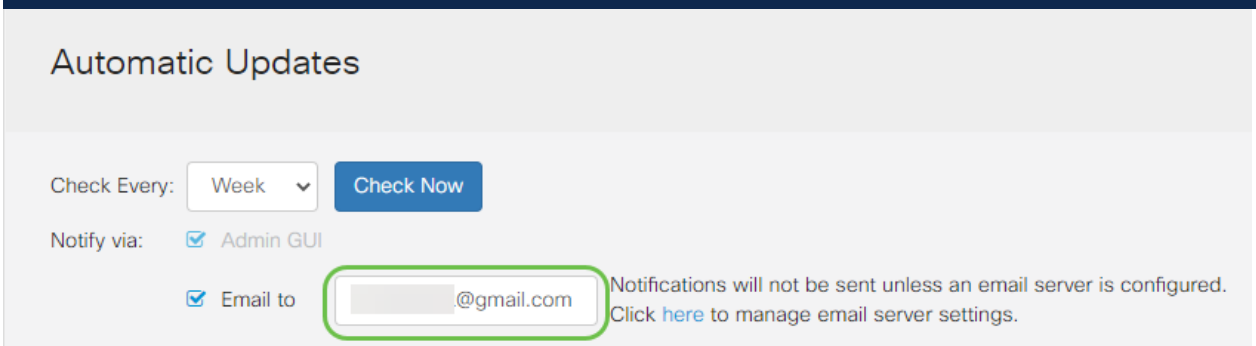
Wenn Sie E-Mail-Servereinstellungen einrichten möchten, klicken Sie hier, um mehr darüber zu erfahren.



Schritt 4

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

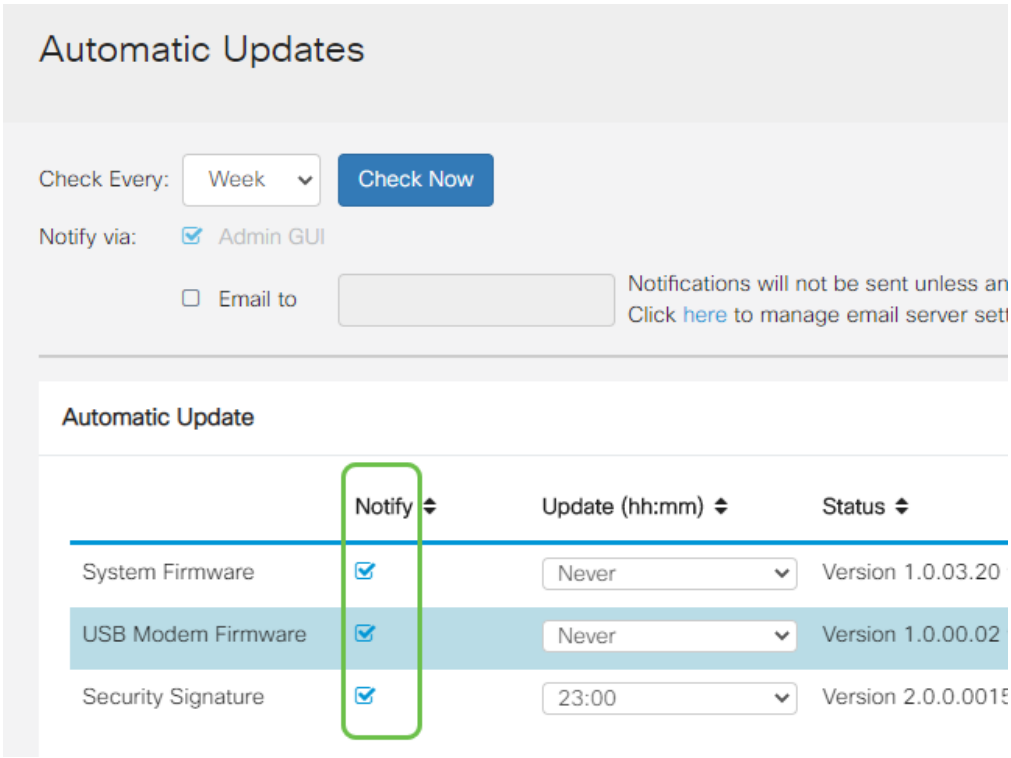
Es wird dringend empfohlen, ein separates E-Mail-Konto zu verwenden, anstatt Ihre persönliche E-Mail-Adresse zu verwenden, um die Privatsphäre zu wahren.



Schritt 5

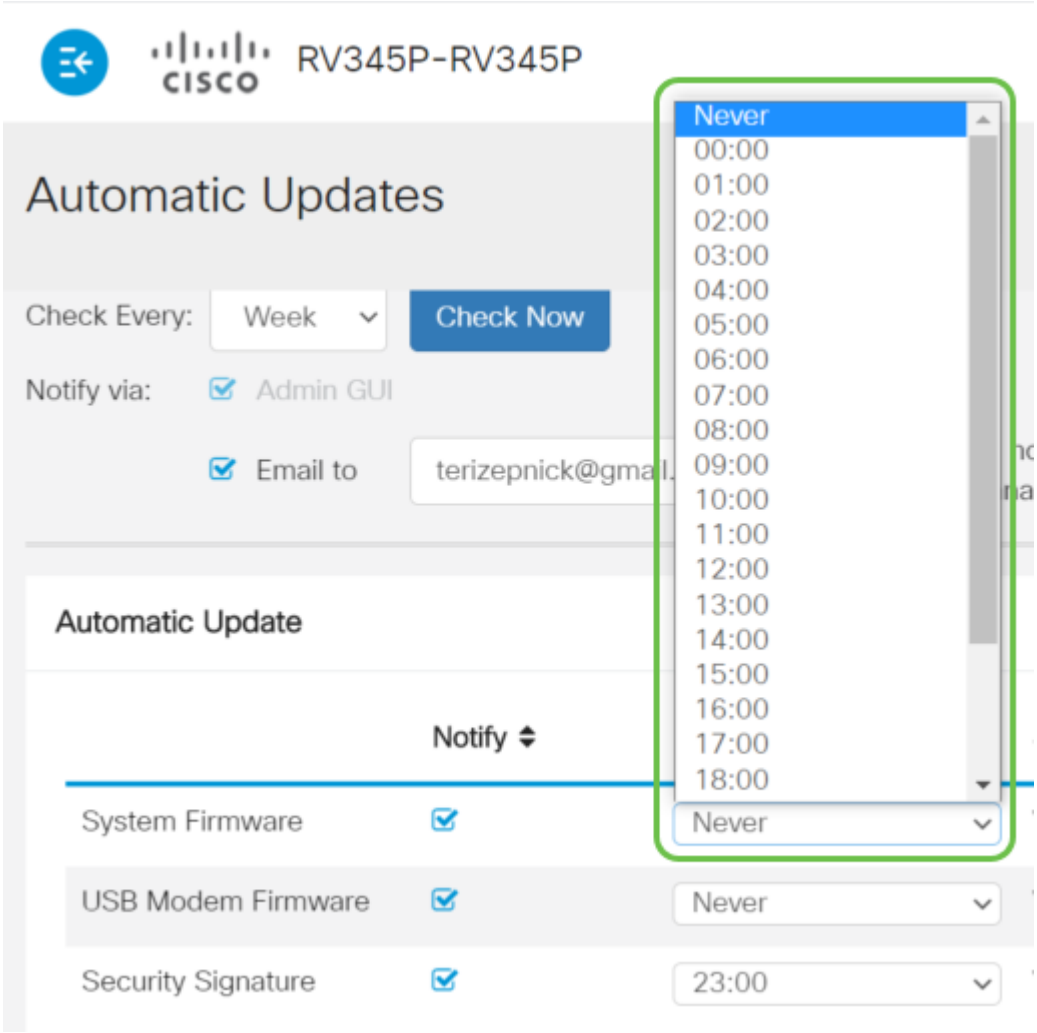
Aktivieren Sie im Bereich *Automatisch aktualisieren* die Kontrollkästchen **Benachrichtigen** für die Art von Aktualisierungen, über die Sie benachrichtigt werden möchten. Folgende Optionen sind verfügbar:

- 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.



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.



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 Problembehebung 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.

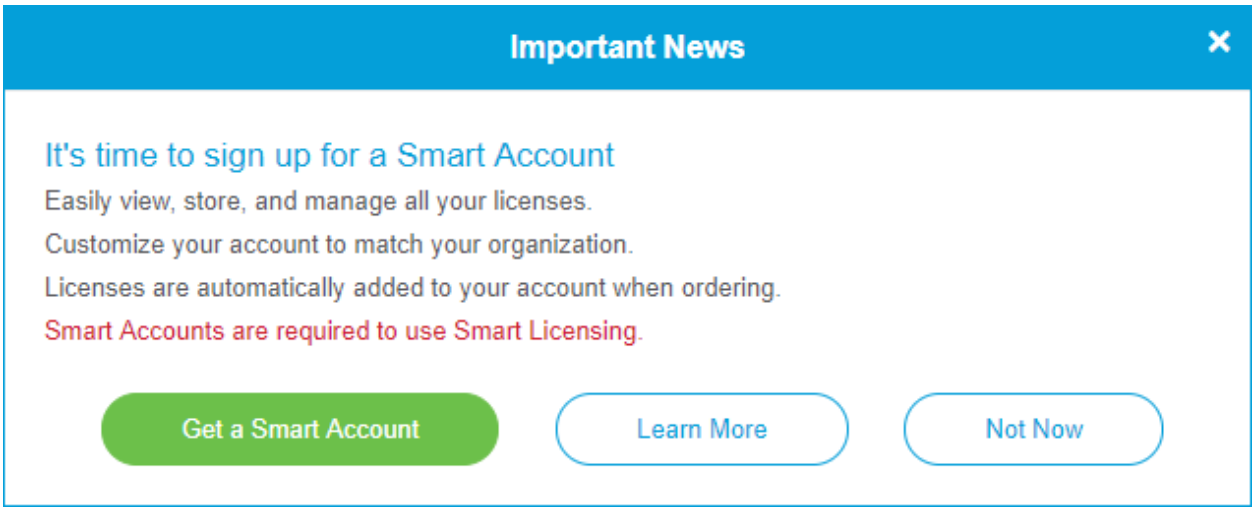
Indem Sie die Aktivierung dieses Smart Accounts genehmigen, stimmen Sie zu, dass

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.



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.

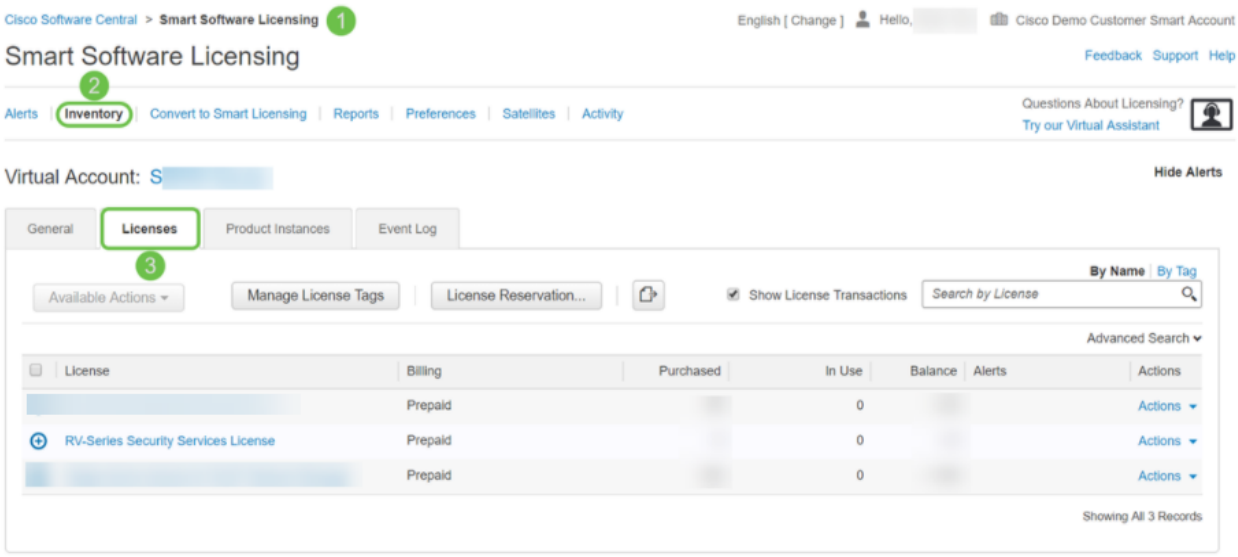
In der Tabelle unten wird die Teilenummer der Lizenz angezeigt.

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**.

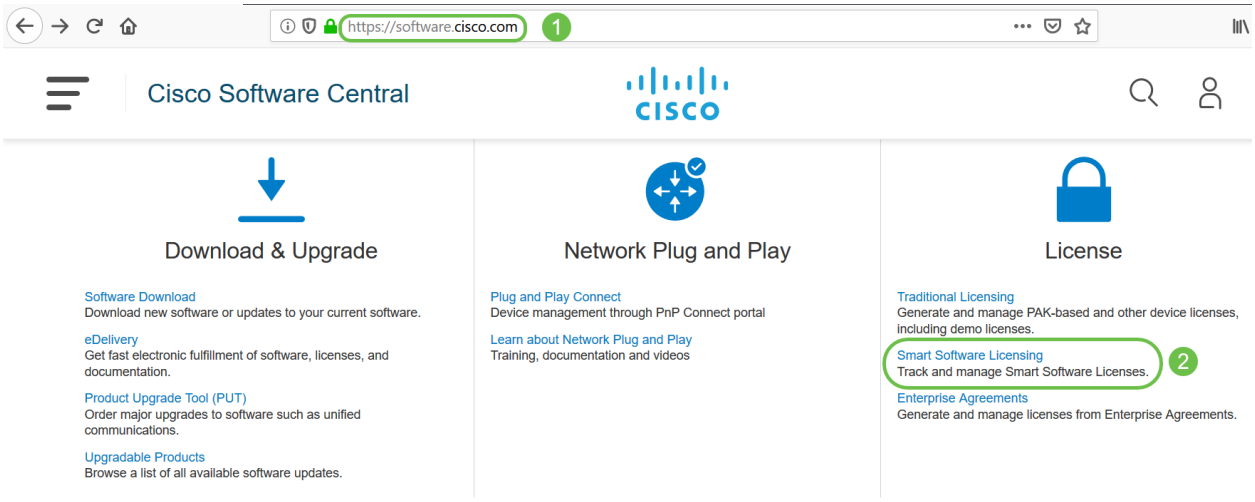


Wenn Ihre Lizenz nicht in Ihrem Smart Account angezeigt wird, wenden Sie sich an Ihren Cisco Partner.

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

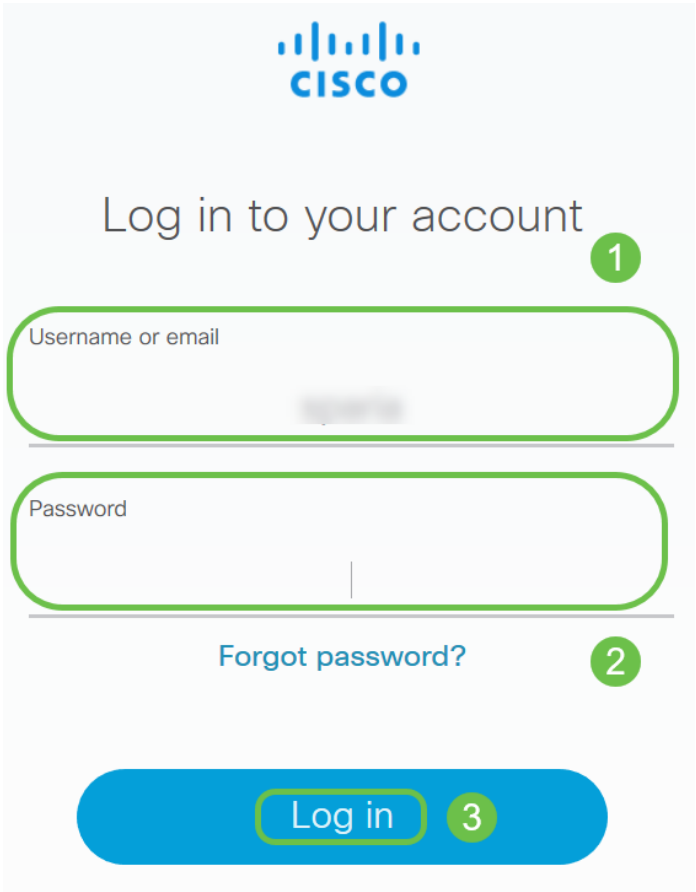
Schritt 1

Greifen Sie auf Cisco Software zu, und navigieren Sie zu **Smart Software Licensing**.



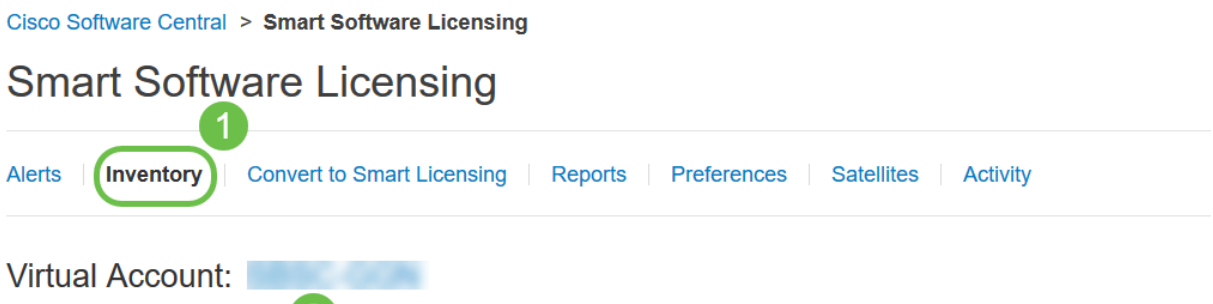
Schritt 2

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



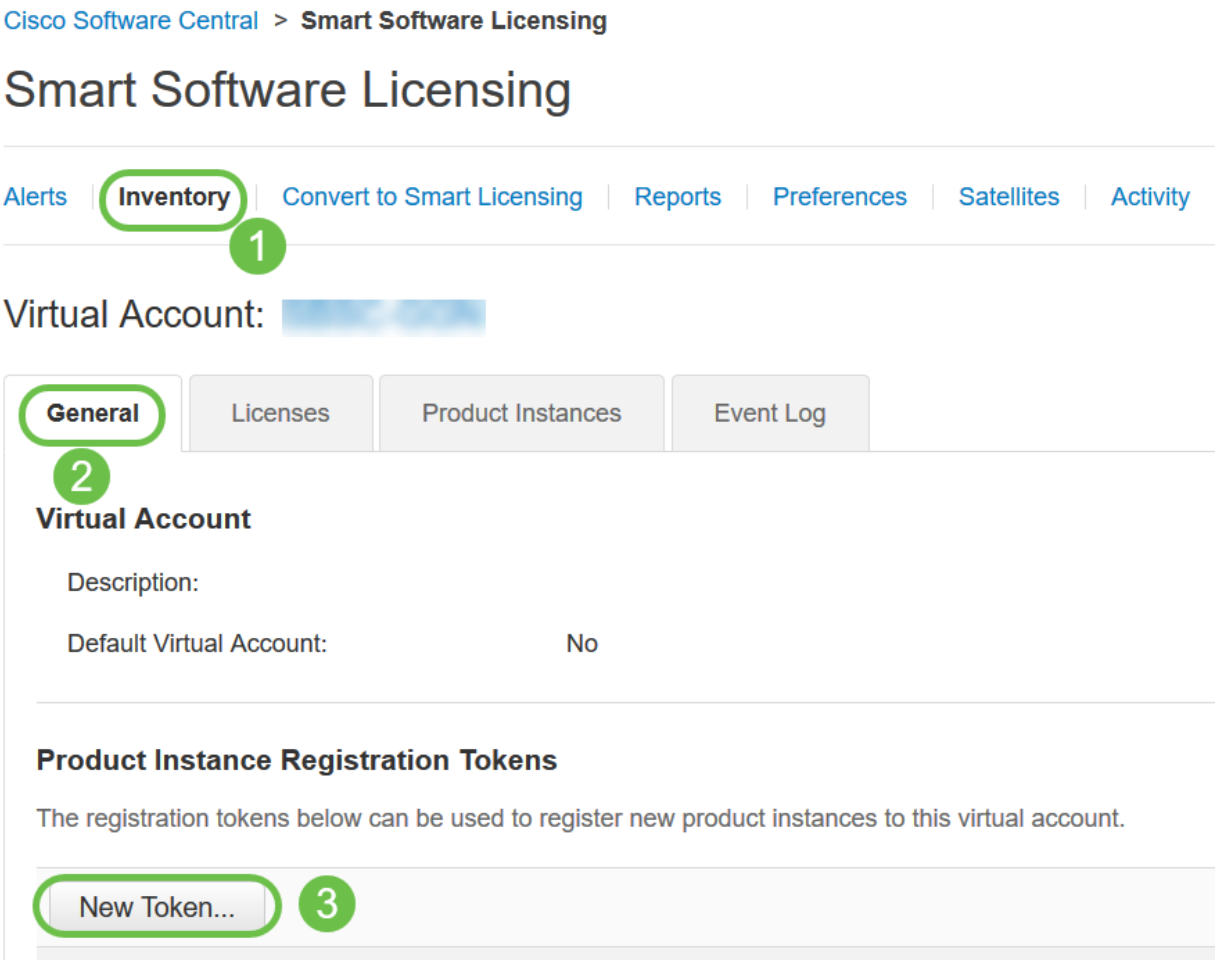
Schritt 3

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.



Schritt 4

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



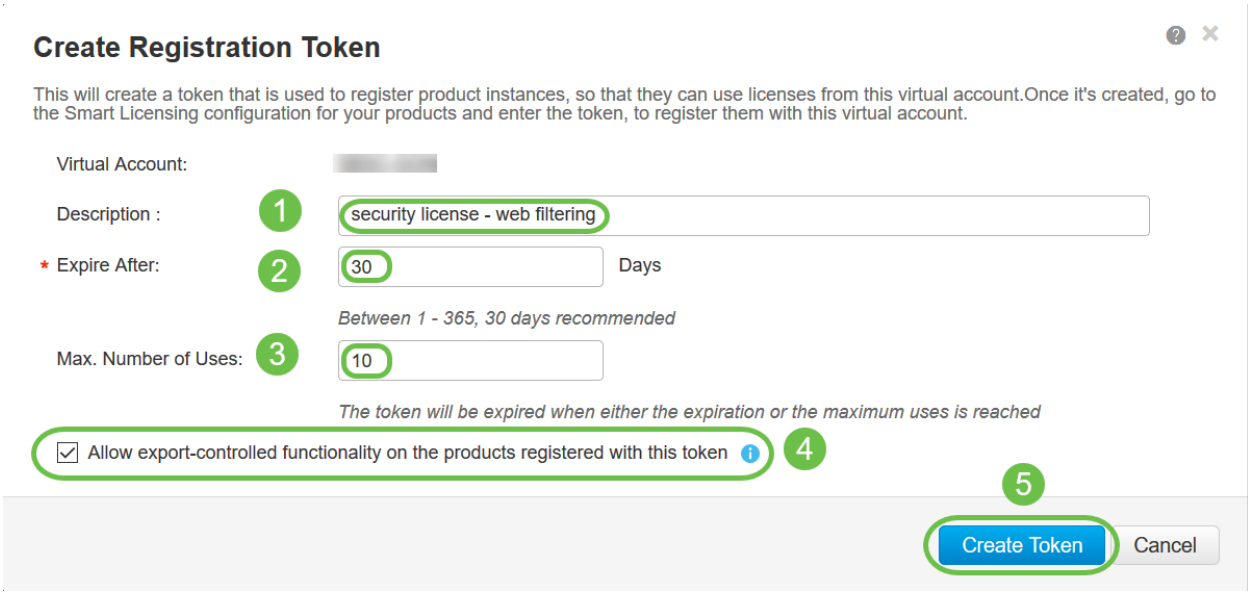
Schritt 5

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*:

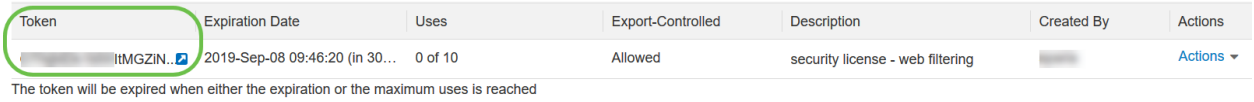
- Geben Sie im Feld Description (Beschreibung) eine eindeutige Beschreibung für das Token ein. In diesem Beispiel wird Security License - Web Filtering eingegeben.
- Geben Sie im Feld Ablaufdatum einen Wert zwischen 1 und 365 Tagen ein. Cisco empfiehlt für dieses Feld den Wert 30 Tage. Sie können den 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.

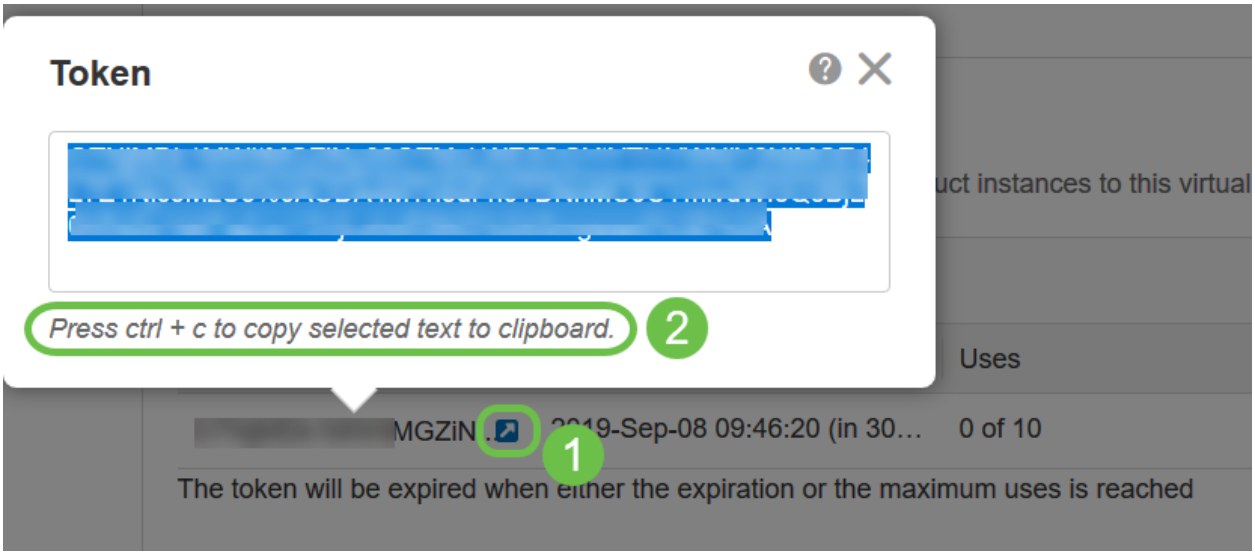


Sie haben nun erfolgreich ein Produktinstanzregistrierungstoken generiert.



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.



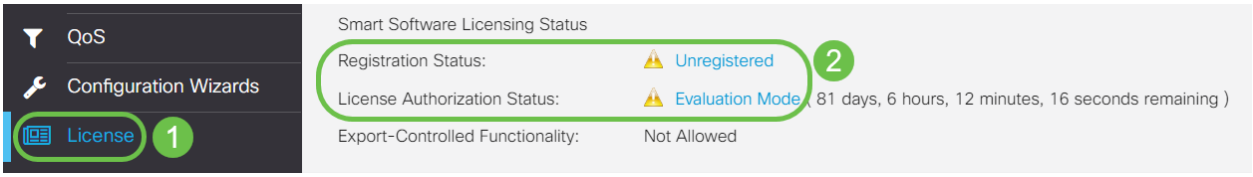
Schritt 7 (optional)

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.

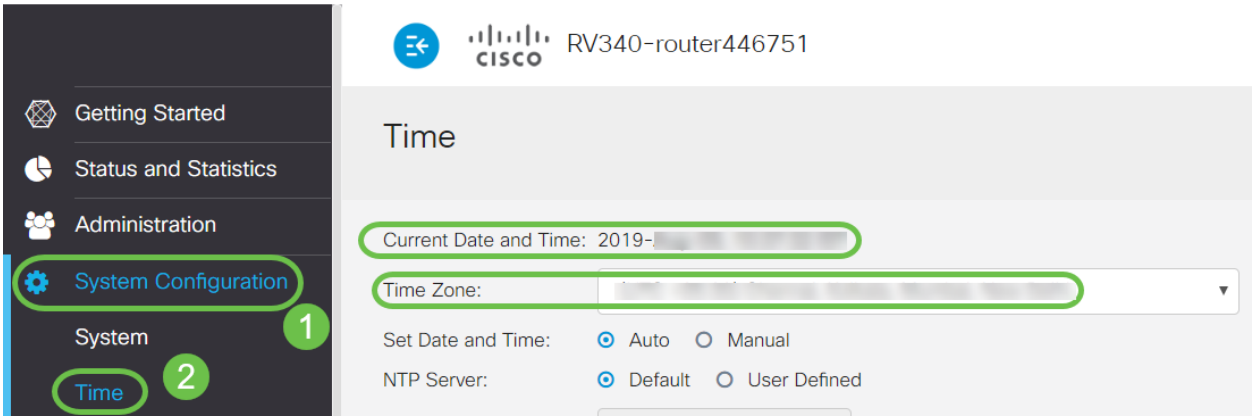
Schritt 8

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



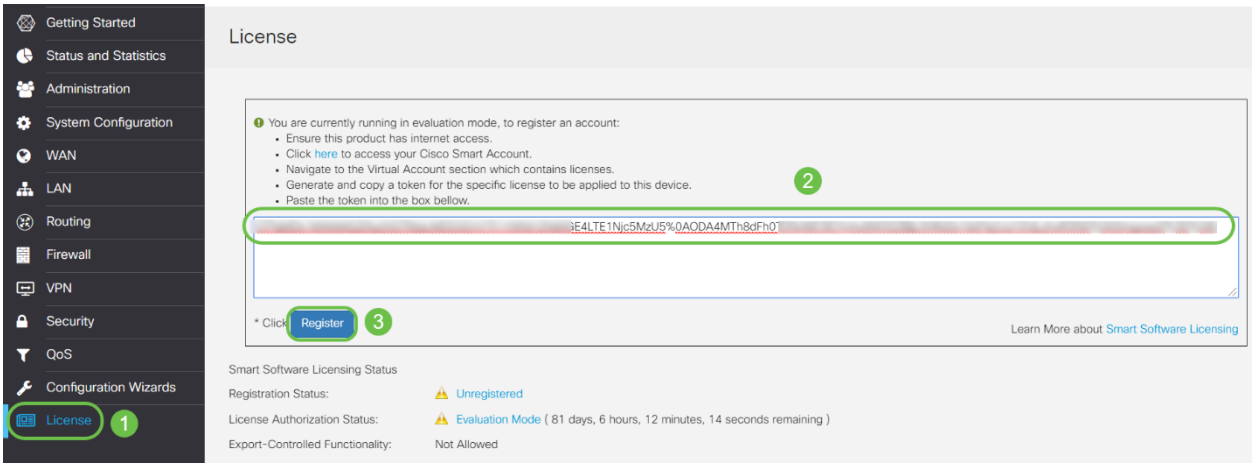
Schritt 9

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



Schritt 10

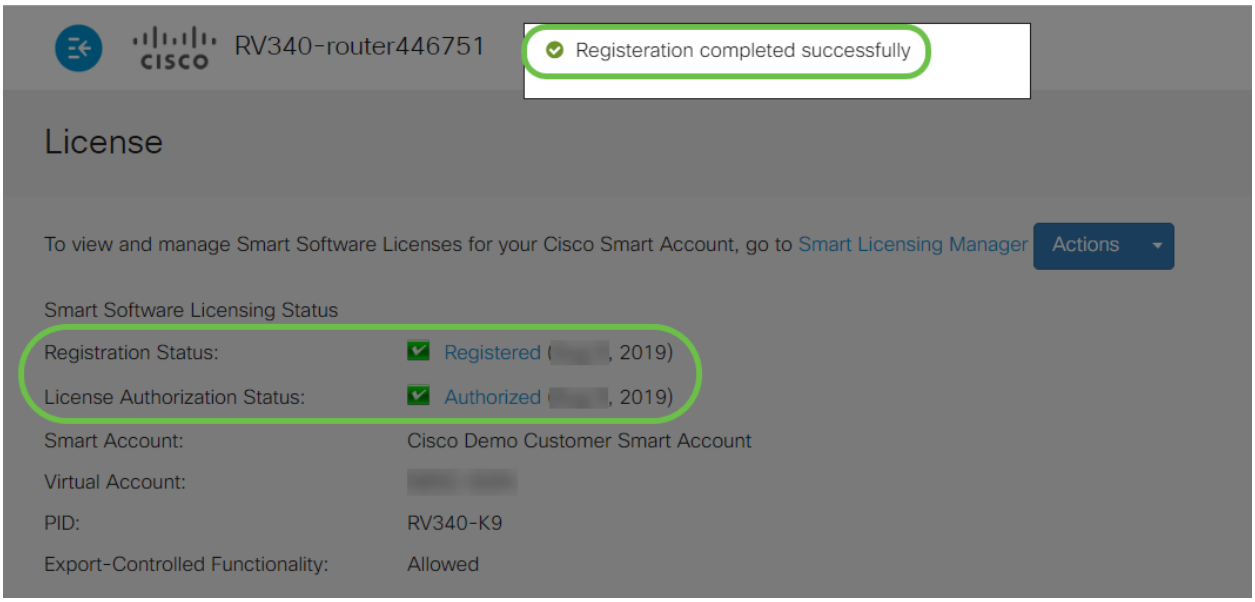
Navigieren Sie zu **Lizenz**. Fügen Sie das kopierte Token in Schritt 6 im Textfeld unter der Registerkarte *Lizenz ein*, indem Sie auf Ihrer Tastatur **Strg + v** auswählen. Klicken Sie auf **Registrieren**.



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

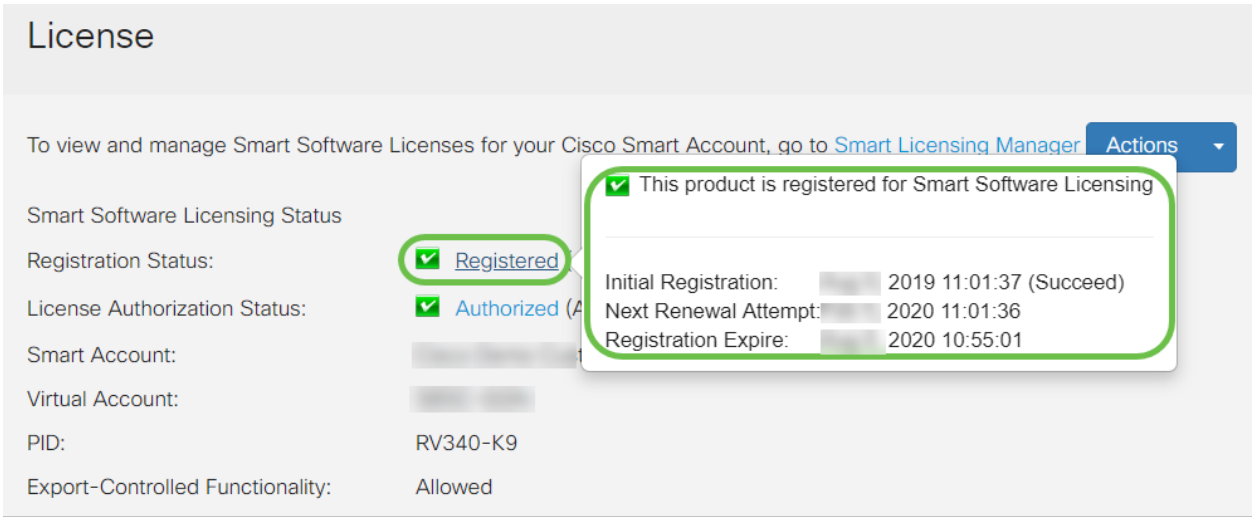
Schritt 11

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.



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:

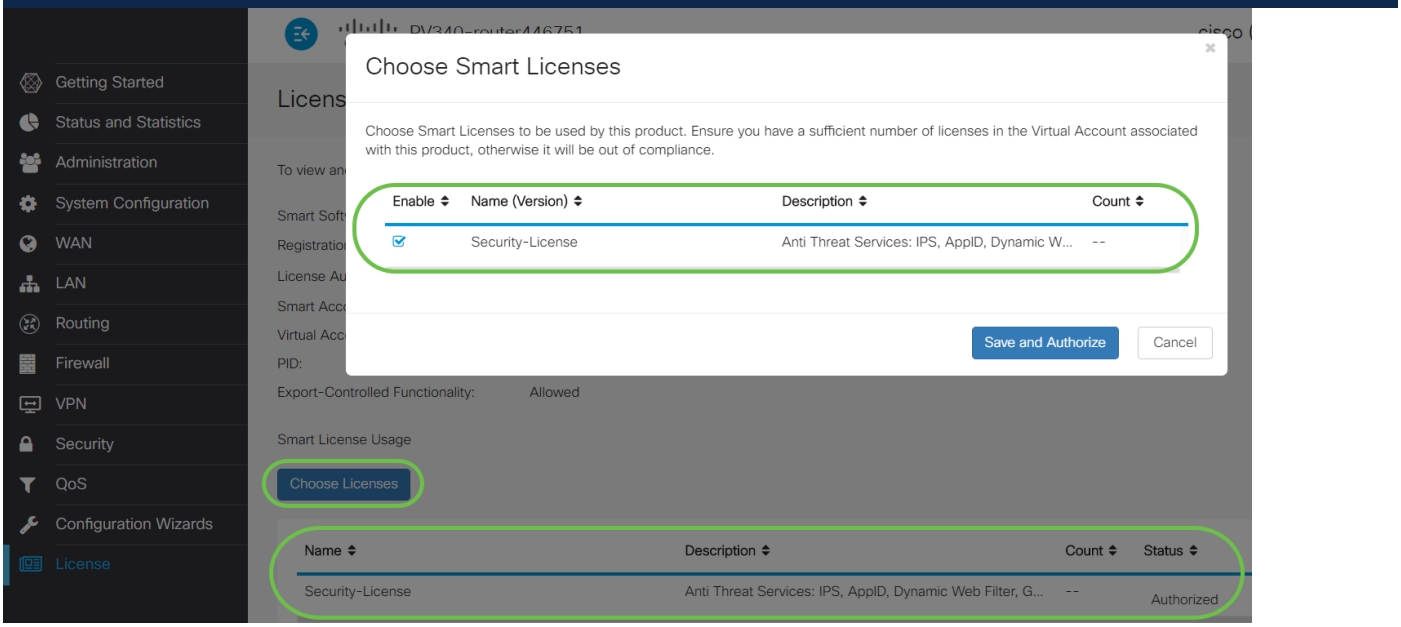


- Erstregistrierung: In diesem Bereich werden Datum und Uhrzeit der Lizenzregistrierung angezeigt.
- Nächster Verlängerungsversuch: In diesem Bereich werden das Datum und die Uhrzeit angezeigt, zu dem der Router versucht, die Lizenz zu verlängern.
- Registrierung abgelaufen - In diesem Bereich werden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

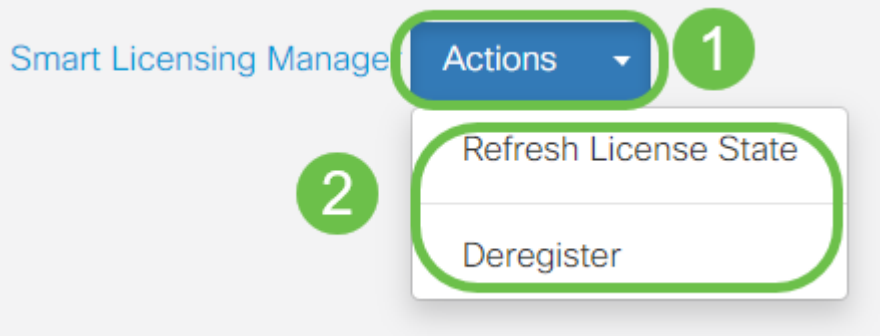
Wenn bei diesem Schritt Probleme auftreten, müssen Sie den Router möglicherweise neu starten.



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.



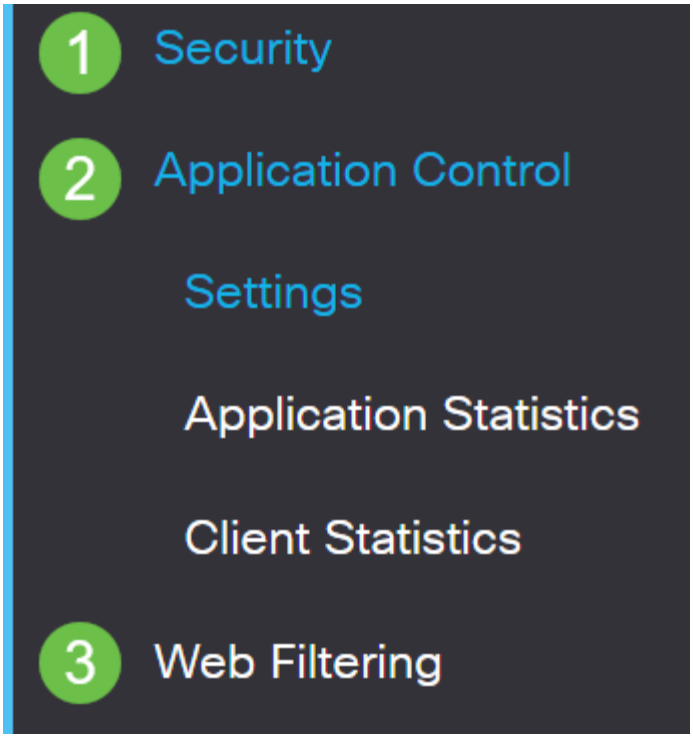
Nachdem Sie Ihre Lizenz auf dem Router installiert haben, müssen Sie die Schritte im nächsten Abschnitt ausführen.

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.

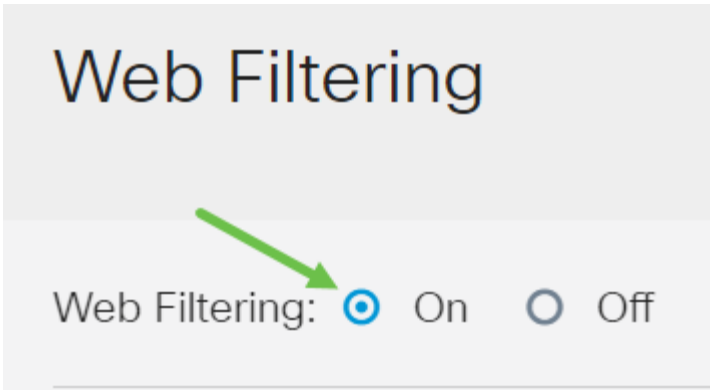
Schritt 1

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



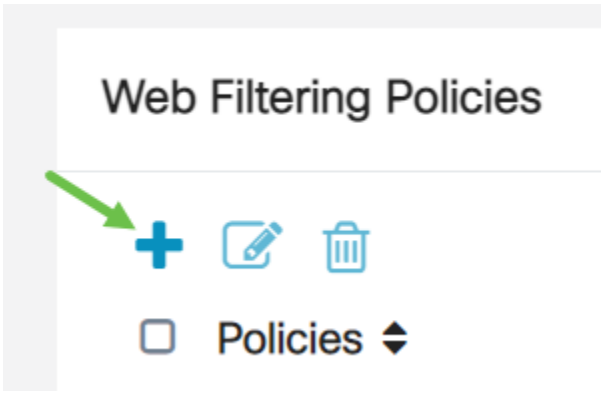
Schritt 2

Wählen Sie das Optionsfeld **Ein**.



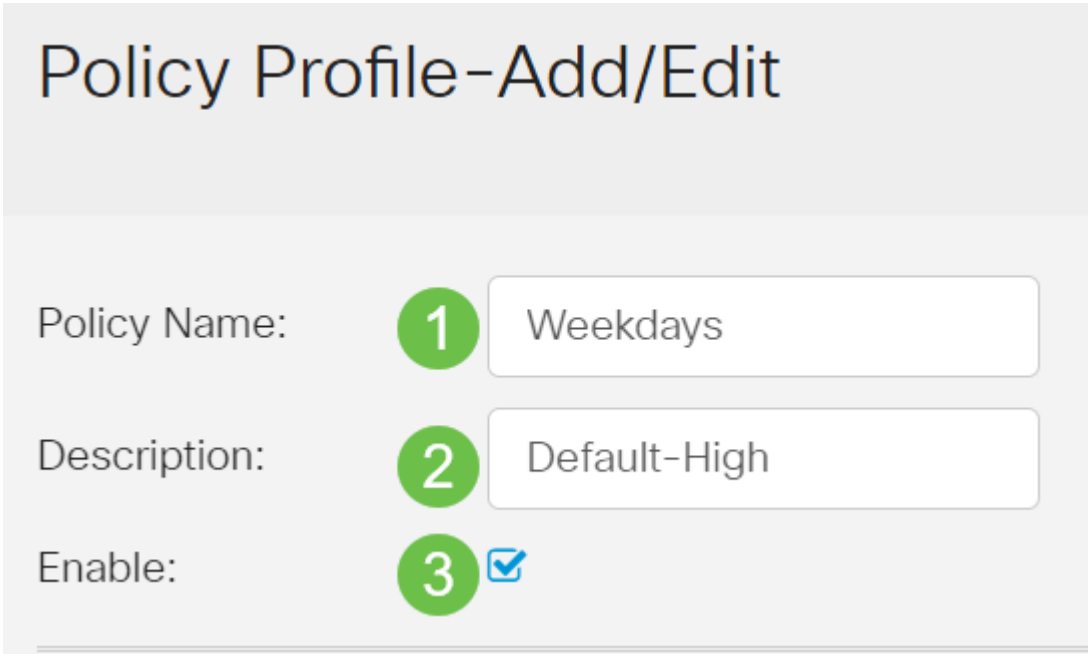
Schritt 3

Klicken Sie auf das **Symbol Hinzufügen**.



Schritt 4

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

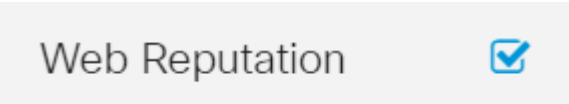


Wenn die Inhaltsfilterung auf Ihrem Router aktiviert ist, wird eine Benachrichtigung angezeigt, die Sie darüber informiert, dass die Inhaltsfilterung deaktiviert wurde und dass die beiden Funktionen nicht gleichzeitig aktiviert werden können. Klicken Sie auf **Apply**, um

mit der Konfiguration fortzufahren.

Schritt 5

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

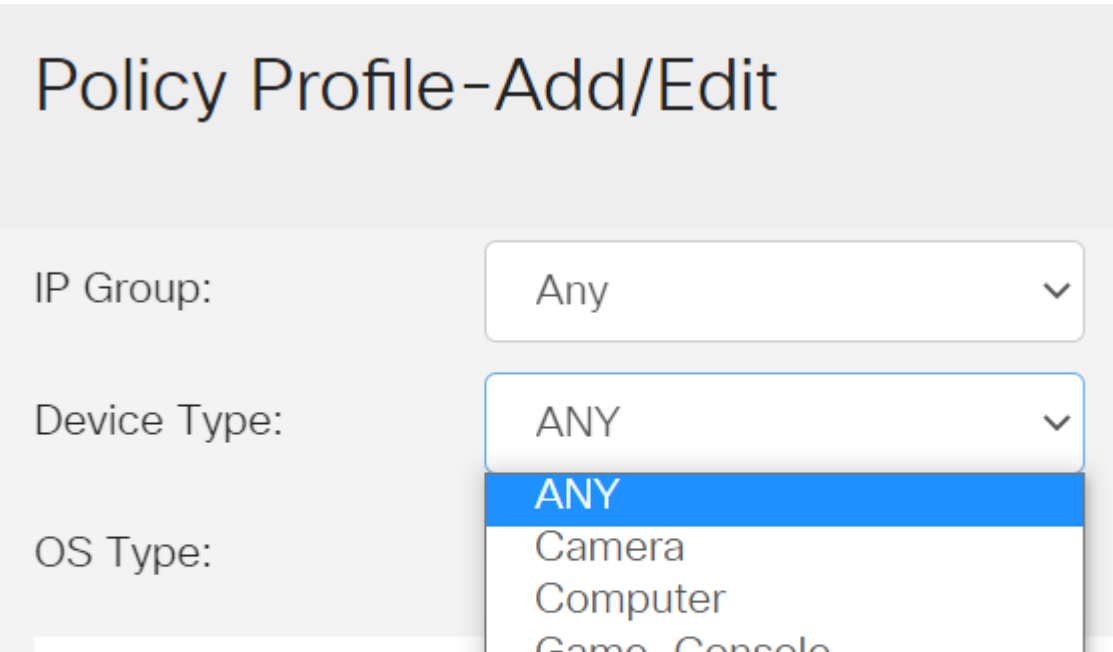


Die Filterung der Inhalte erfolgt nach dem Bekanntheitsgrad einer Website oder einer URL basierend auf einem Web-Reputationsindex. Wenn die Punktzahl unter 40 fällt, wird die Website blockiert. Weitere Informationen zur Web-Reputationstechnologie erhalten Sie hier.

Schritt 6

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

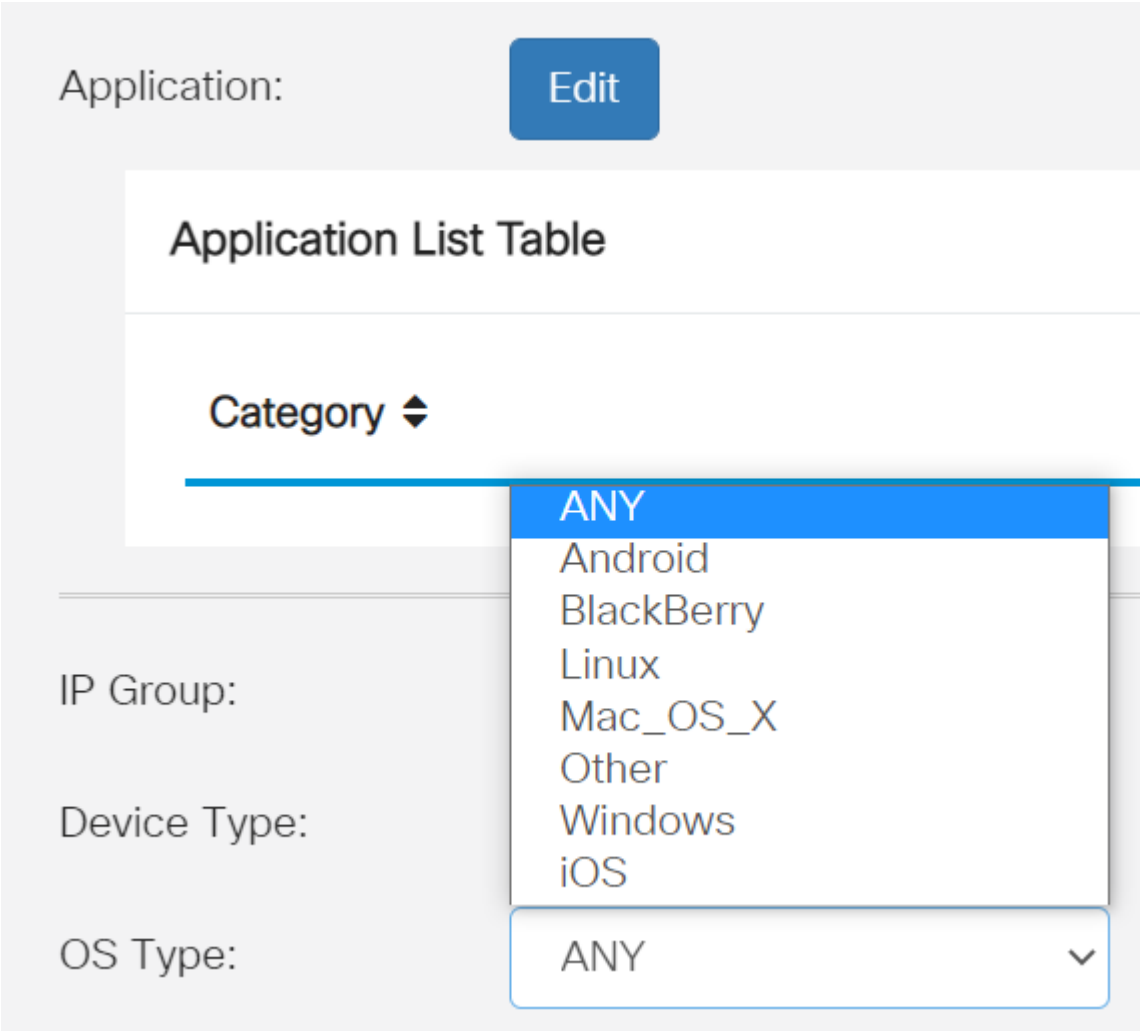
- BELIEBIG - Wählen Sie diese Option, um die Richtlinie auf jedes Gerät anzuwenden.
- Kamera: Wählen Sie diese Option aus, um die Richtlinie auf Kameras (z. B. IP-Sicherheitskameras) anzuwenden.
- Computer - Wählen Sie diese Option aus, um die Richtlinie auf Computer anzuwenden.
- Game_Console: Wählen 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.



Schritt 7

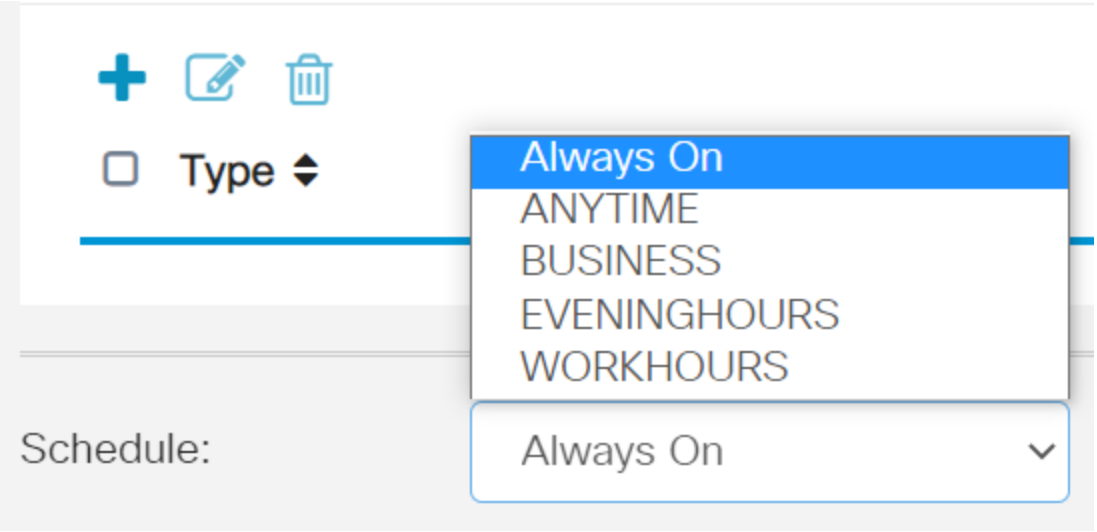
Wählen Sie aus der Dropdown-Liste *OS Type (Betriebssystemtyp*) ein Betriebssystem aus, für das die Richtlinie gelten soll. Es kann jeweils nur eine Option ausgewählt werden. Folgende Optionen sind verfügbar:

- 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.



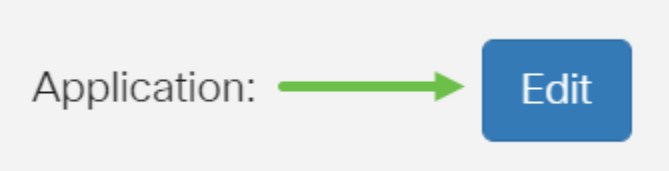
Schritt 8

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



Schritt 9

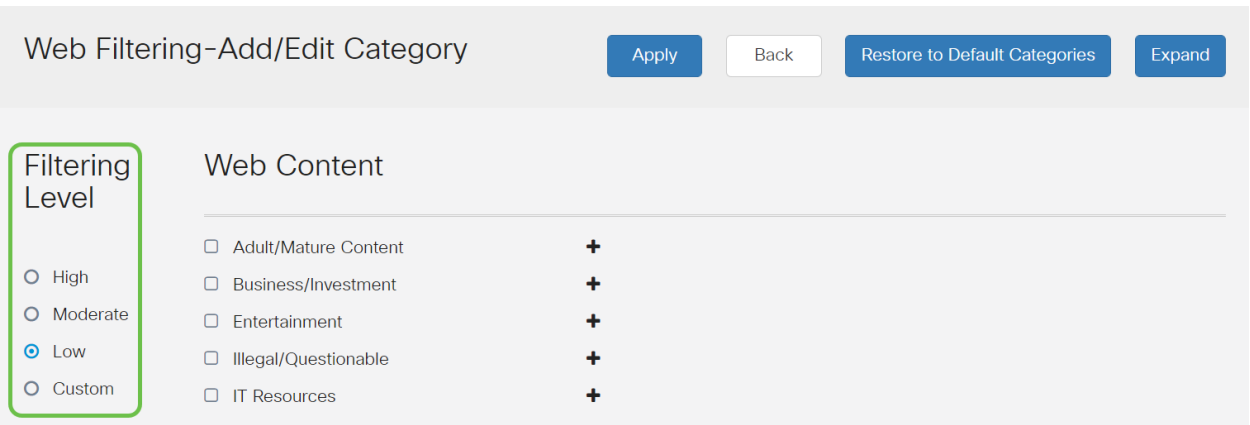
Klicken Sie auf das **Bearbeitungssymbol**.



Schritt 10

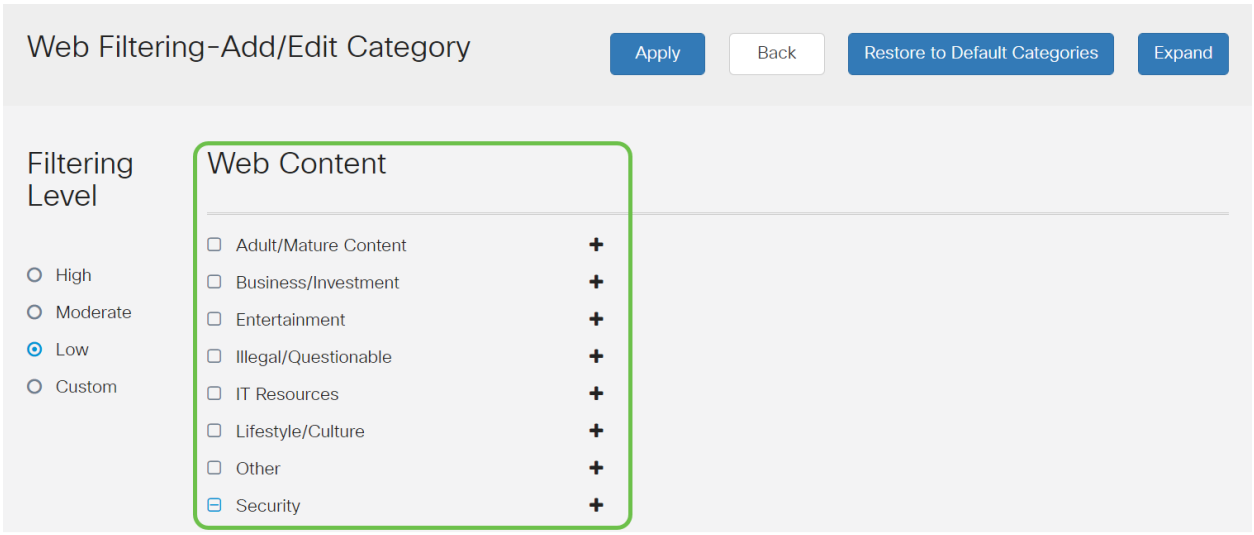
Klicken Sie in der Spalte Filterebene auf ein Optionsfeld, um schnell das Filtervolumen zu definieren, das den Netzwerkrichtlinien am besten entspricht. Die Optionen sind Hoch, Mittel, Niedrig und Benutzerdefiniert. Klicken Sie auf eine der unten stehenden Filterebenen, um die vordefinierten Unterkategorien 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.



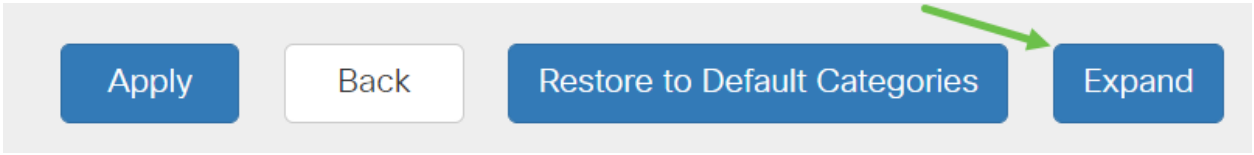
Schritt 11

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



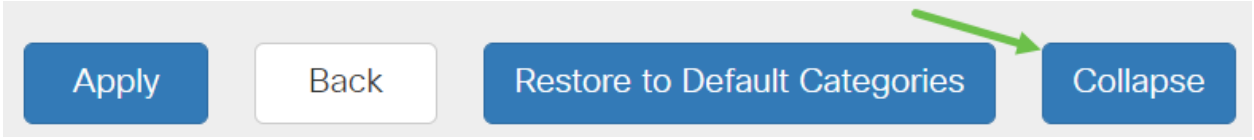
Schritt 12 (optional)

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



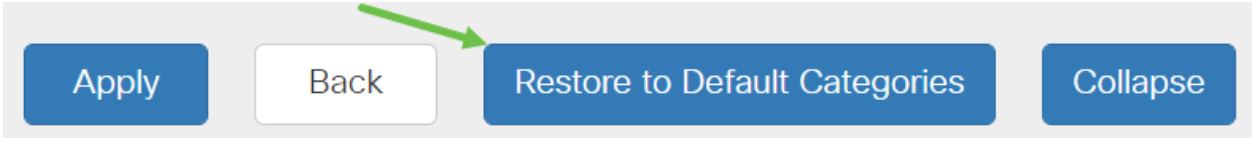
Schritt 13 (optional)

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



Schritt 14 (optional)

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



Schritt 15

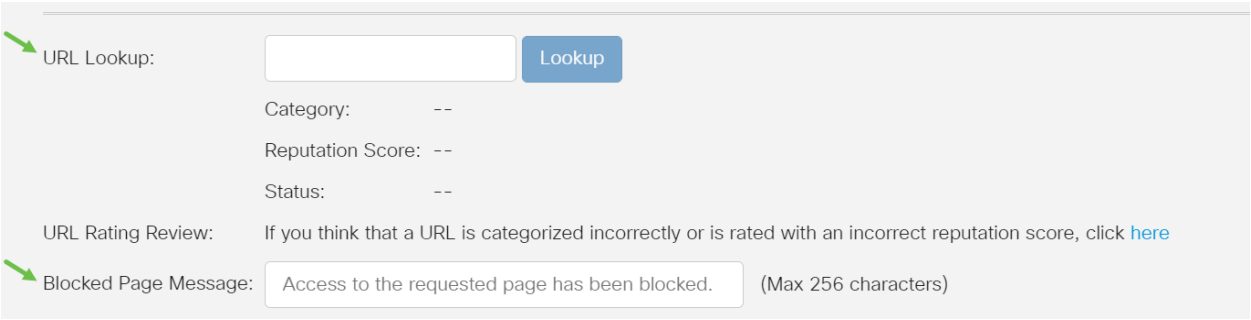
Klicken Sie auf **Apply**, um die Konfiguration zu speichern und zur Seite Filter zurückzukehren, um mit der Einrichtung fortzufahren.

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.



Schritt 17 (optional)

Klicken Sie auf Apply (Anwenden).

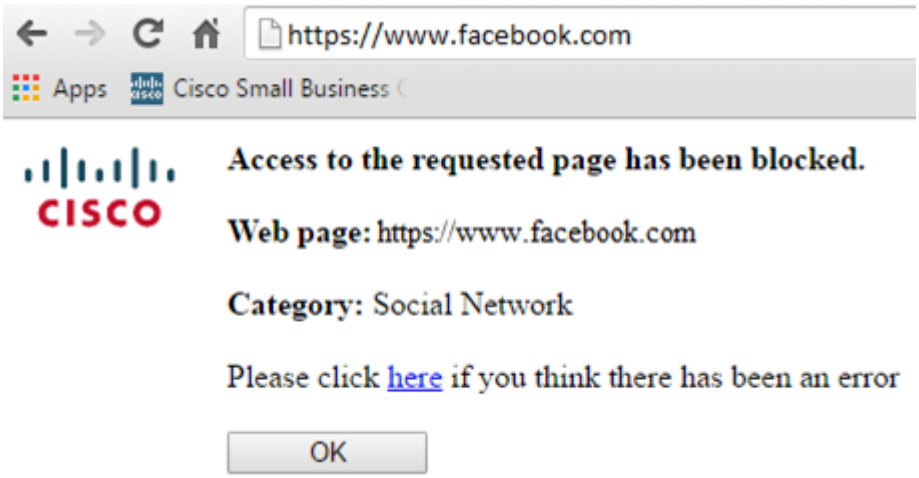
Schritt 18

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	Sie erhalten diese E-Mail nach Abschluss des Erwerbs der Lizenzen.
Cisco Verkaufsauftragsnummer	Um dies zu erhalten, müssen Sie möglicherweise zum Händler zurückkehren.
Screenshot Ihrer Smart Account-Lizenzseite	Mit einem Screenshot können Sie den Inhalt Ihres Bildschirms für unser Team freigeben. 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.

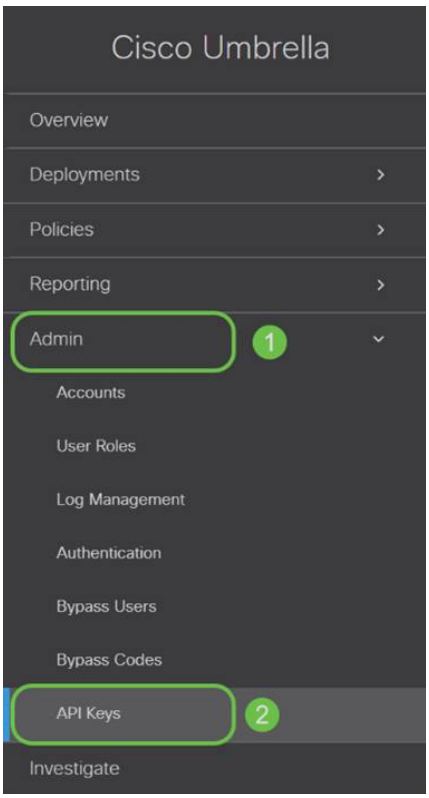
Umbrella ist in der Cloud tätig und führt zahlreiche sicherheitsrelevante Services durch. Von der Bedrohung bis zur Untersuchung nach einem Ereignis. Umbrella erkennt und verhindert Angriffe über alle Ports und Protokolle hinweg.

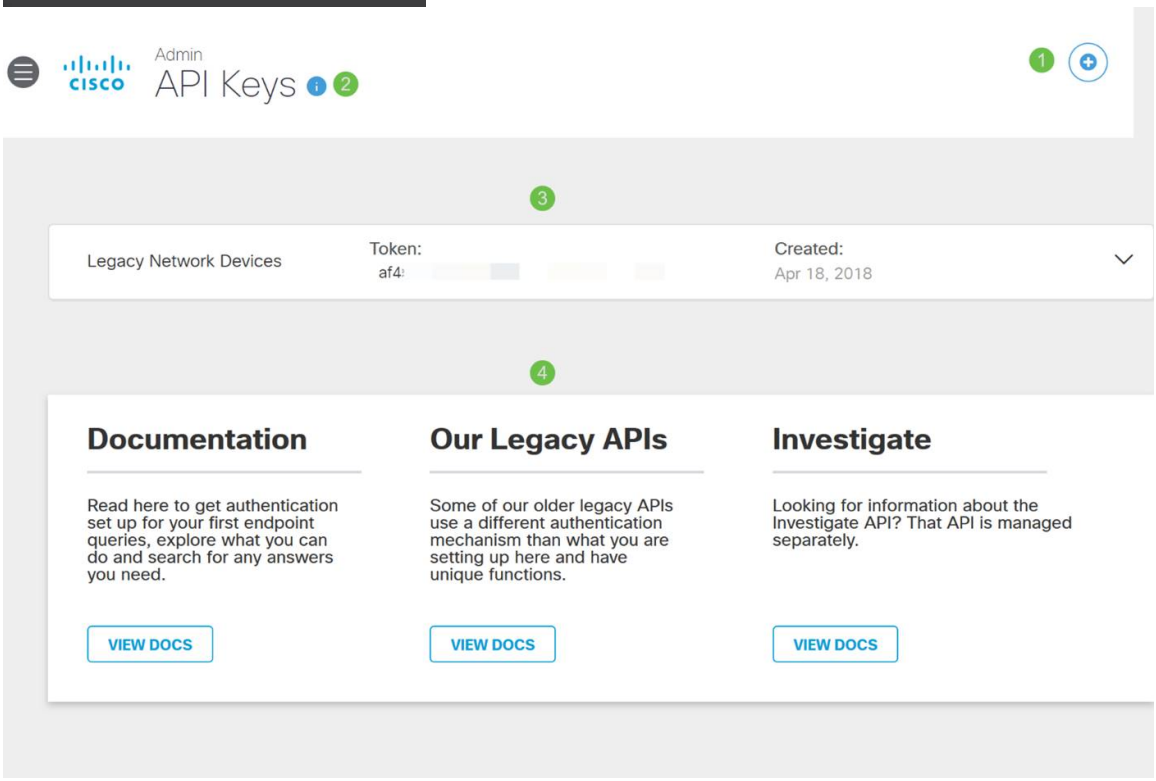
Umbrella verwendet DNS als Hauptvektor für die Verteidigung. Wenn Benutzer eine URL in ihre Browser-Leiste eingeben und auf *Enter* drücken, nimmt Umbrella an der Übertragung teil. Diese URL wird an den DNS-Resolver von Umbrella weitergeleitet. Wenn eine Sicherheitswarnung mit der Domäne verknüpft ist, 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)**.





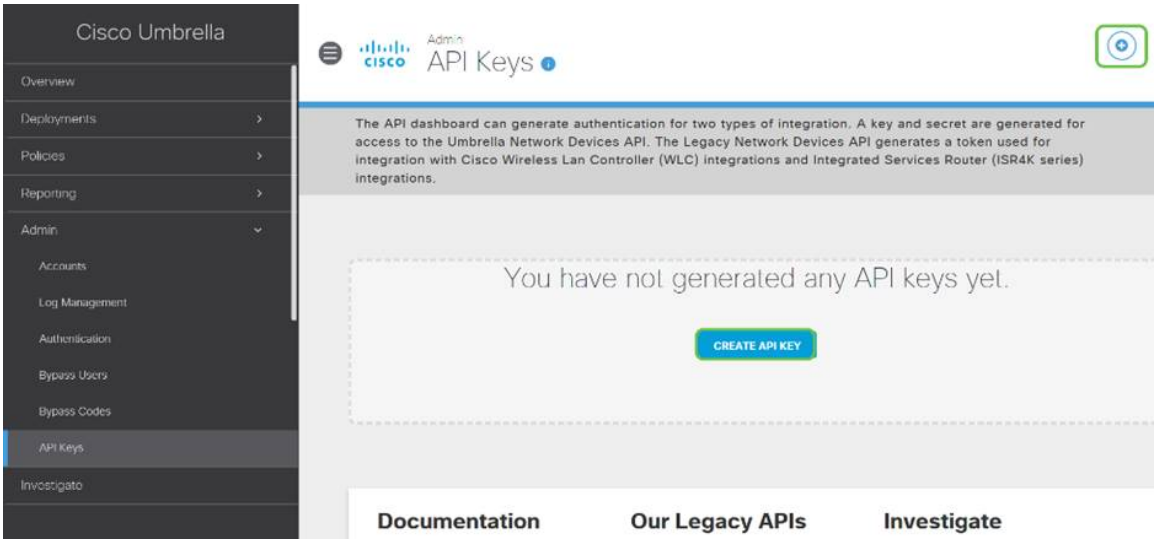
Anatomie des Bildschirms "API Keys" (API-Schlüssel) (mit bereits vorhandenem API-Schlüssel)

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

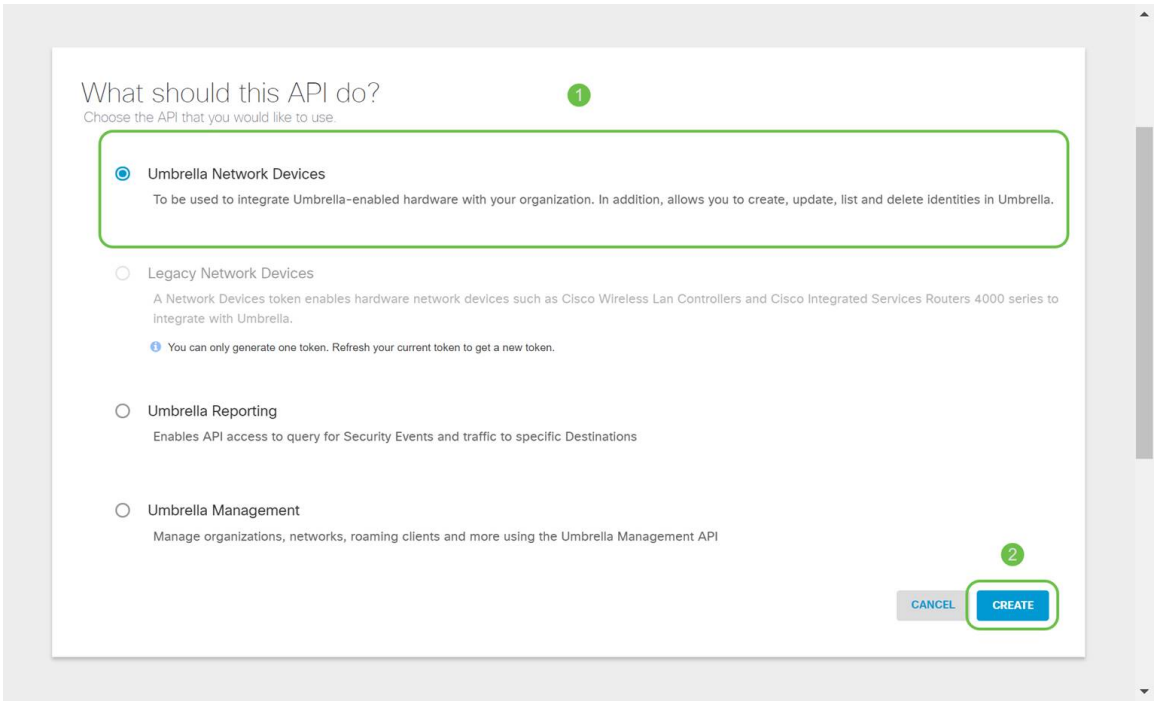
Klicken Sie in der rechten oberen Ecke auf die Schaltfläche **API-Schlüssel hinzufügen**, oder klicken Sie auf die Schaltfläche **API-Schlüssel erstellen**. Beide funktionieren gleich.



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

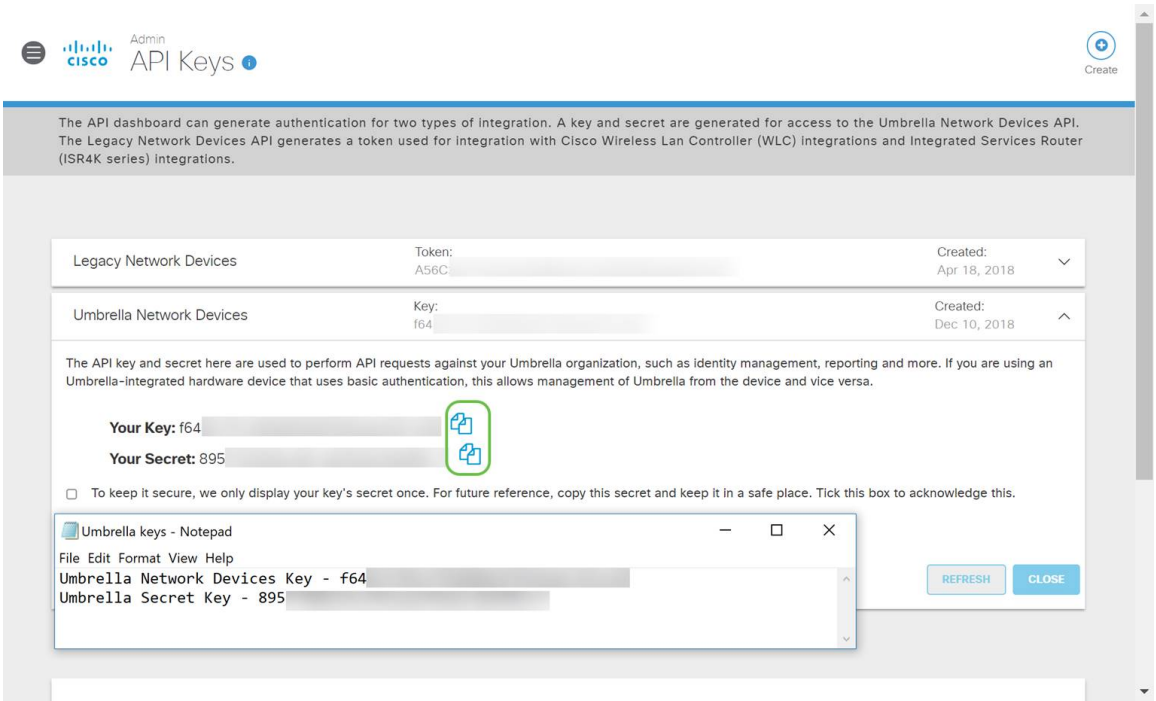
Schritt 3

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



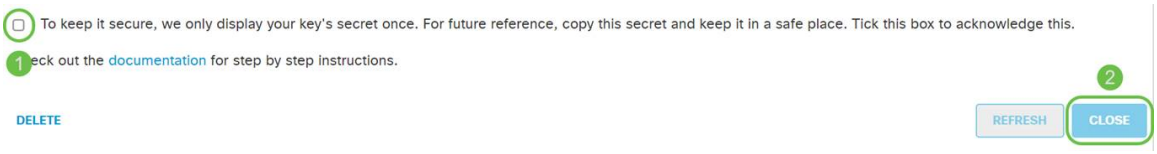
Schritt 4

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**.



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

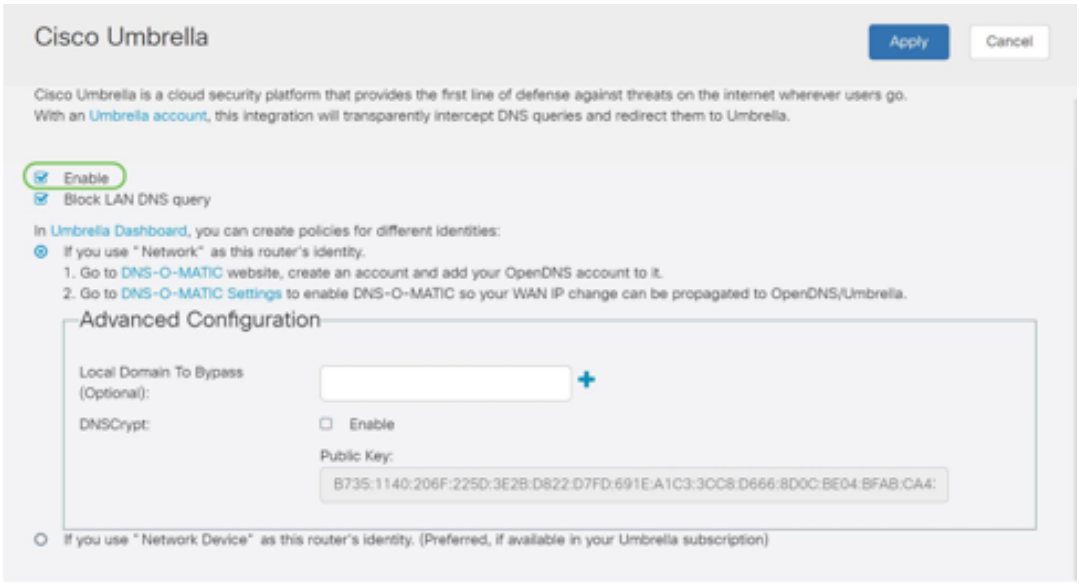
Nachdem wir API-Schlüssel in Umbrella erstellt haben, können Sie diese Schlüssel auf Ihrem RV345P installieren.

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.

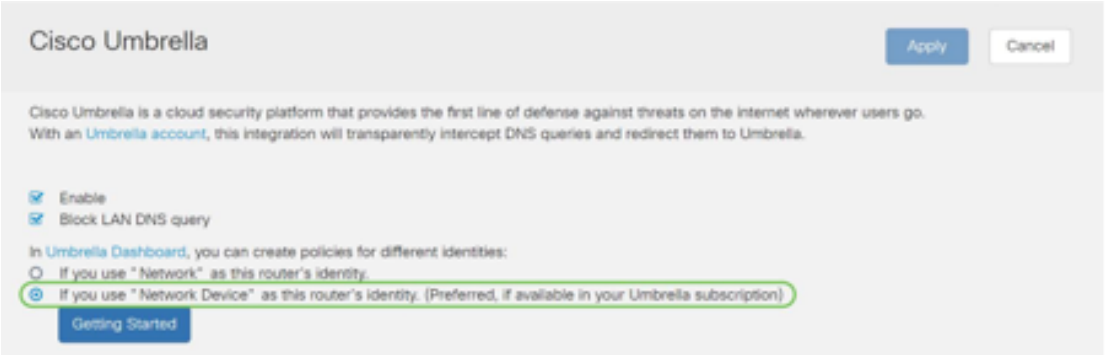


Schritt 3 (optional)

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.

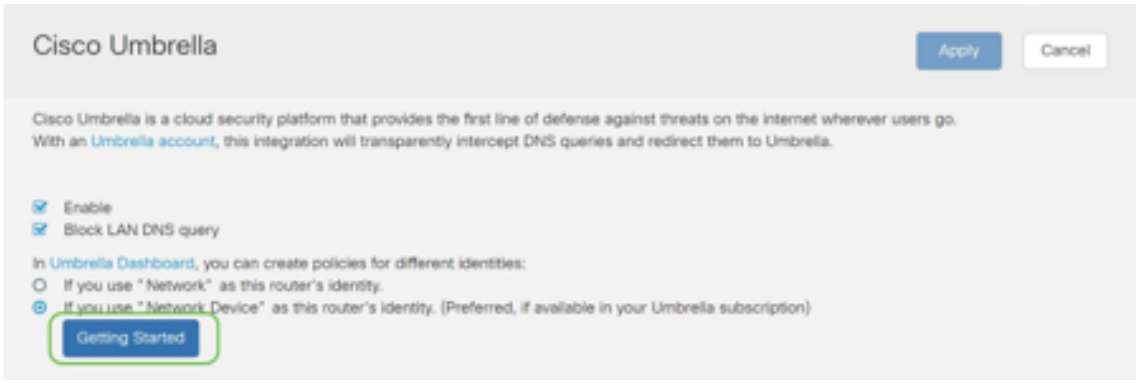
Schritt 4

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.



Schritt 5

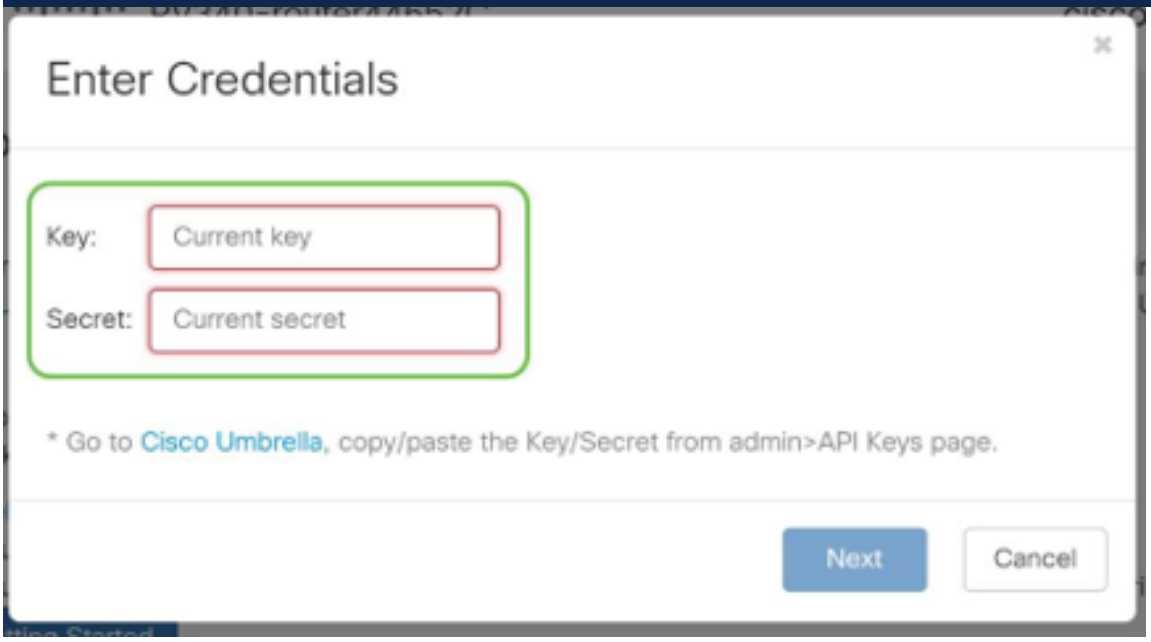
Klicken Sie auf **Erste Schritte**.



Schritt 6

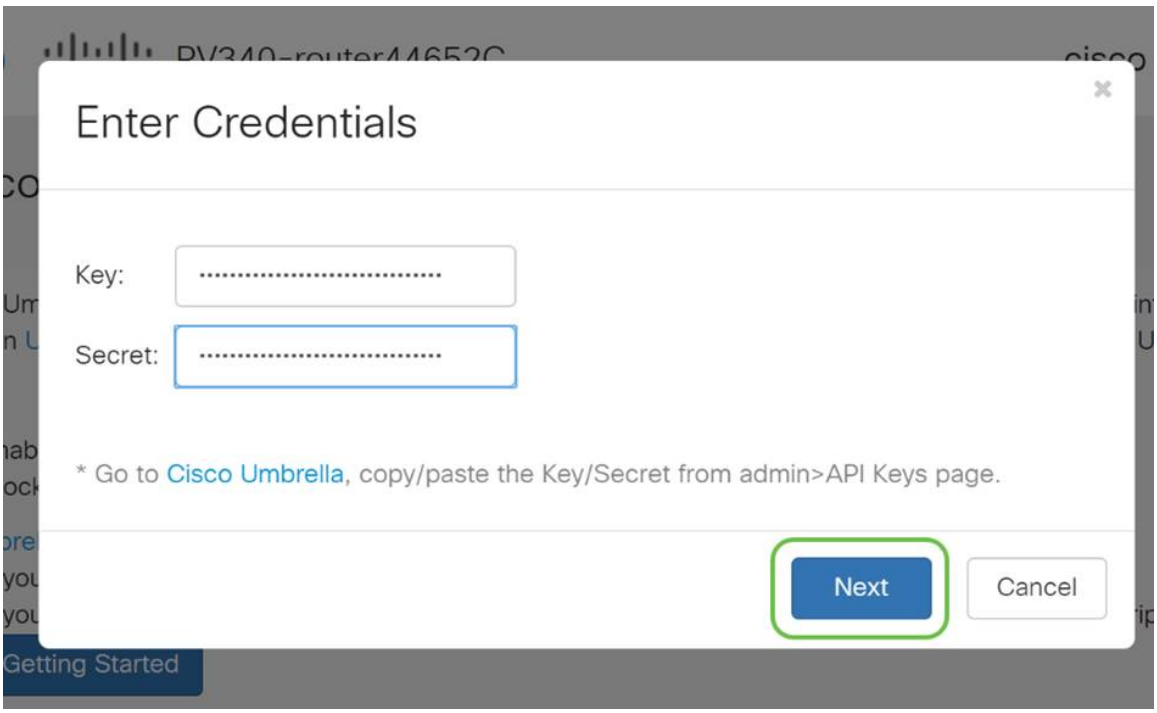
Geben Sie den **API-Schlüssel** und den **Geheimschlüssel** in die Textfelder ein.

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.



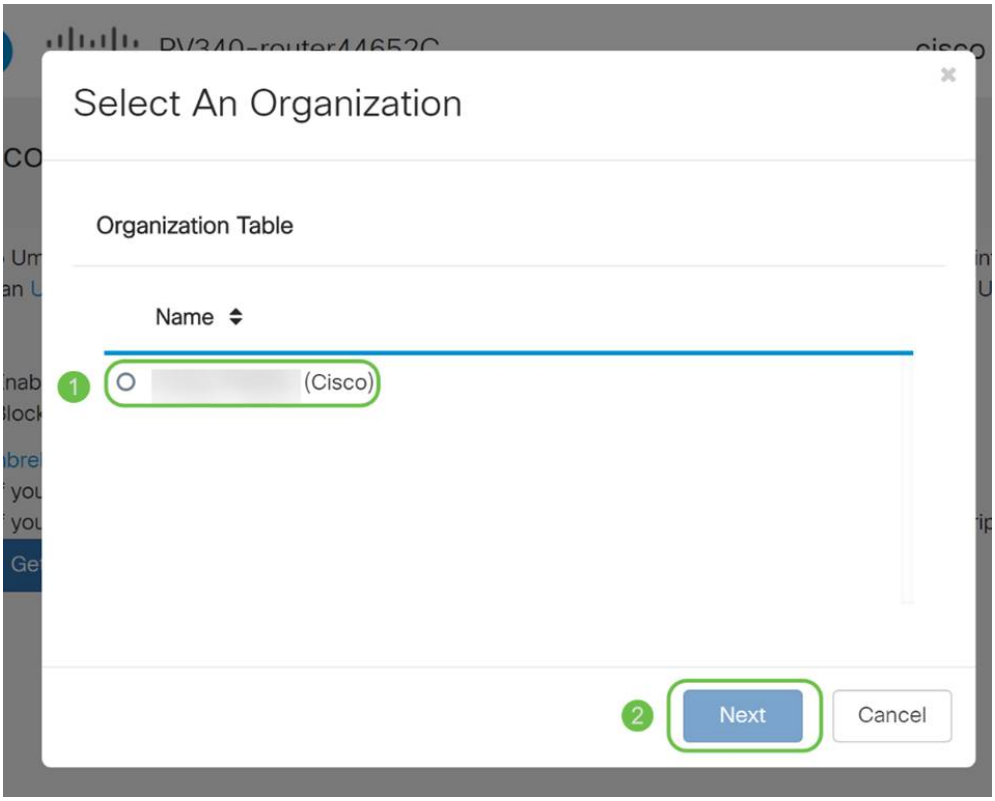
Schritt 7

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



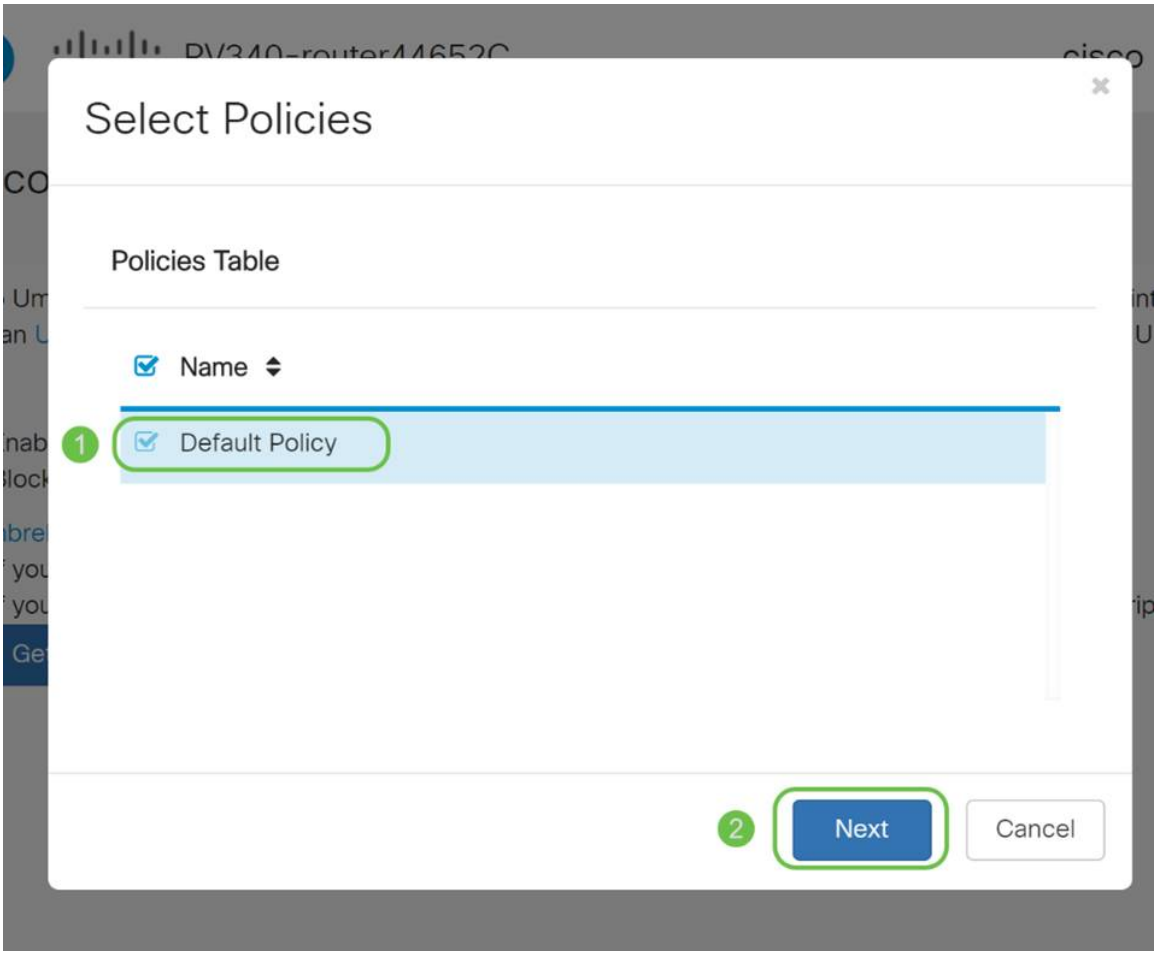
Schritt 8

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



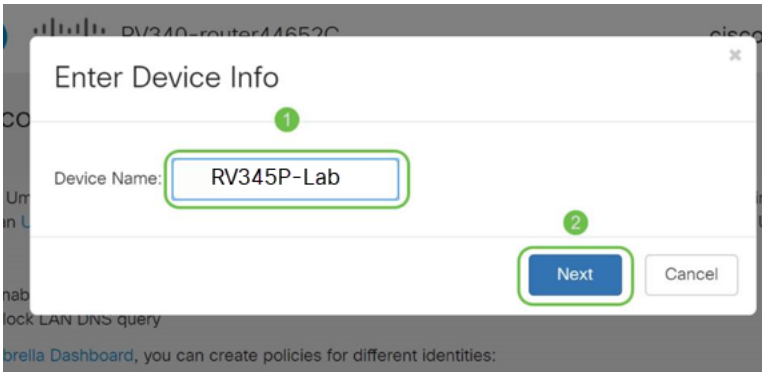
Schritt 9

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.



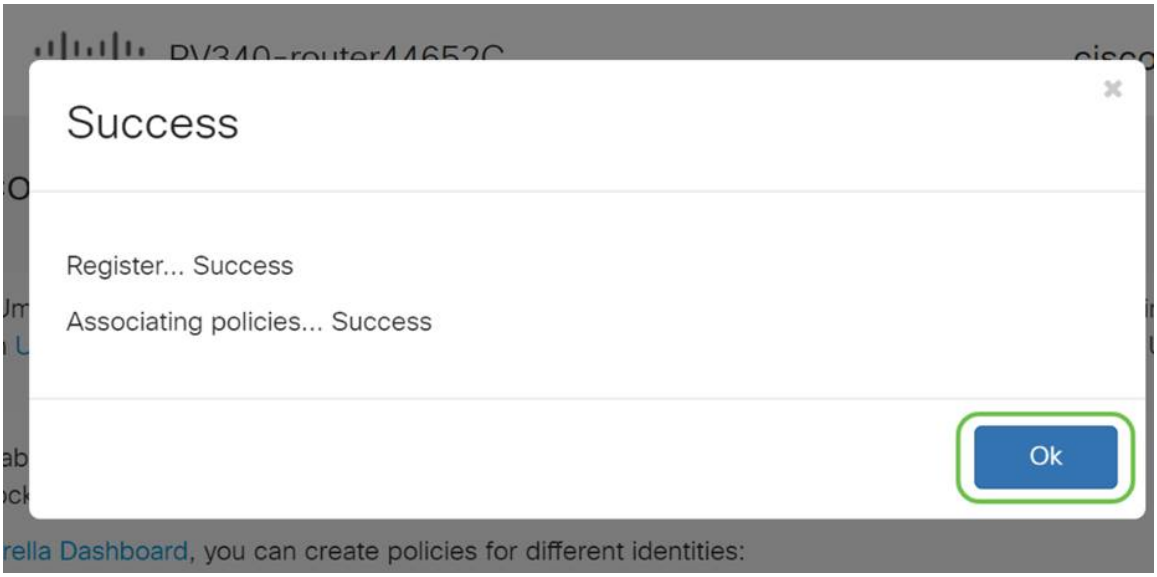
Schritt 10

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

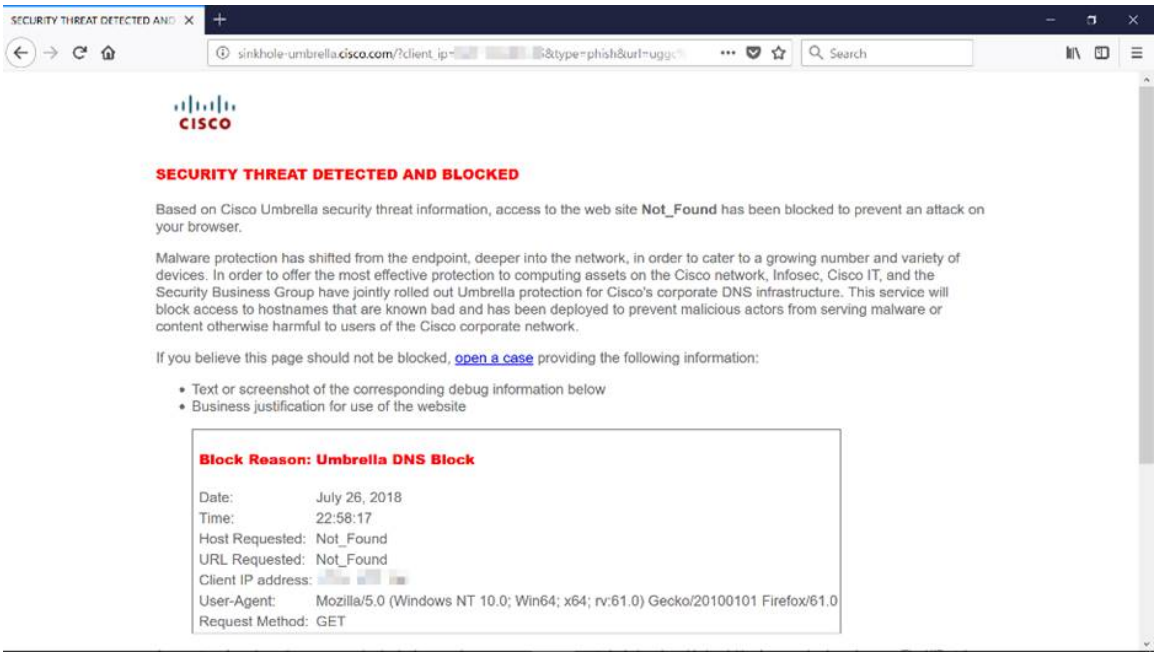
Im nächsten Bildschirm werden die von Ihnen ausgewählten Einstellungen validiert und eine Aktualisierung angezeigt, wenn diese erfolgreich zugeordnet wurde. Klicken Sie auf **OK**.



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 zu 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.

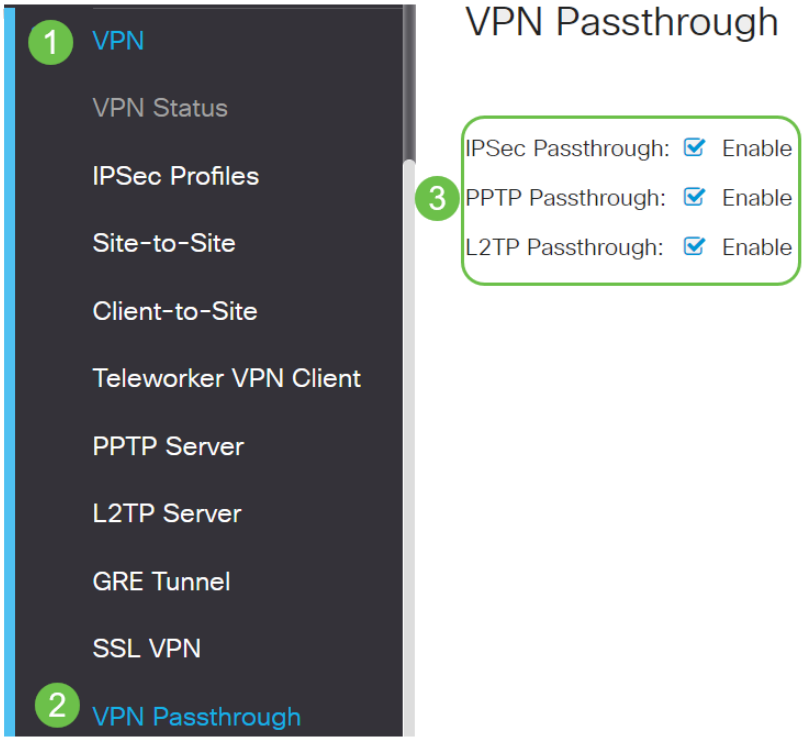
AnyConnect VPN ist das einzige von Cisco VPN unterstützte Produkt, das in diesem Konfigurationsleitfaden aufgeführt ist. Produkte von Drittanbietern, die nicht von Cisco stammen, einschließlich TheGreenBow und Shrew Soft, werden von Cisco nicht unterstützt. Sie werden ausschließlich zu Orientierungszwecken 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

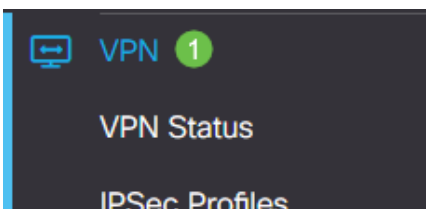
Die Verwendung von Cisco AnyConnect bietet mehrere Vorteile:

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

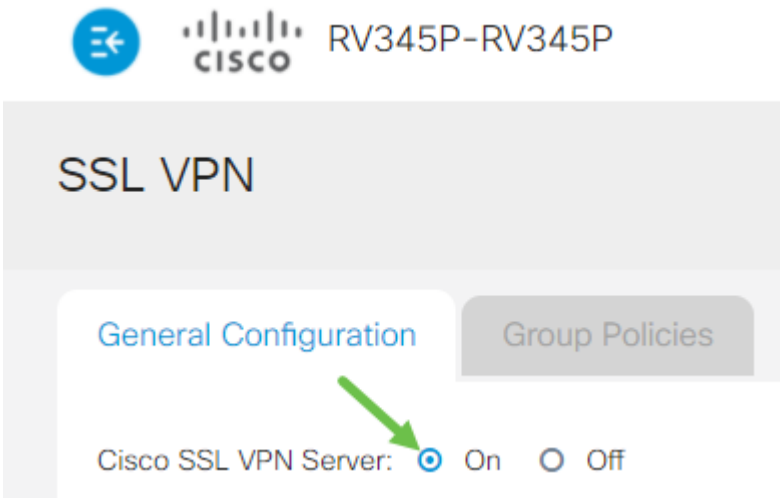
Schritt 1

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

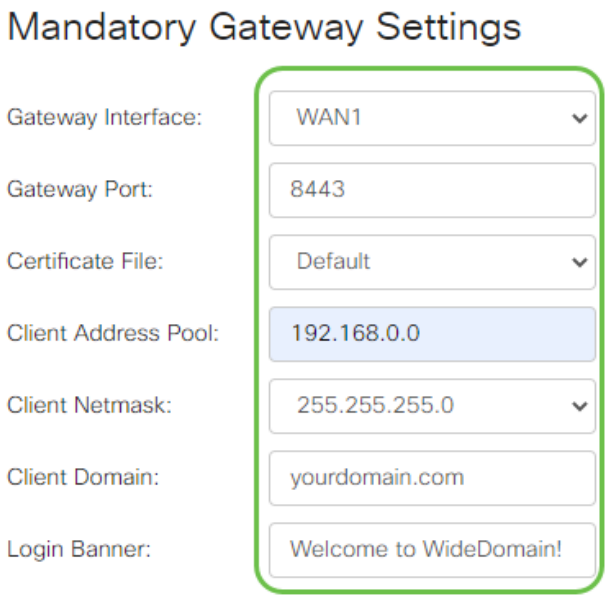
Die folgenden Konfigurationseinstellungen sind obligatorisch:

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-Domänennamen 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.



Schritt 2

Klicken Sie auf Apply (Anwenden).

Optionale Gateway-Einstellungen

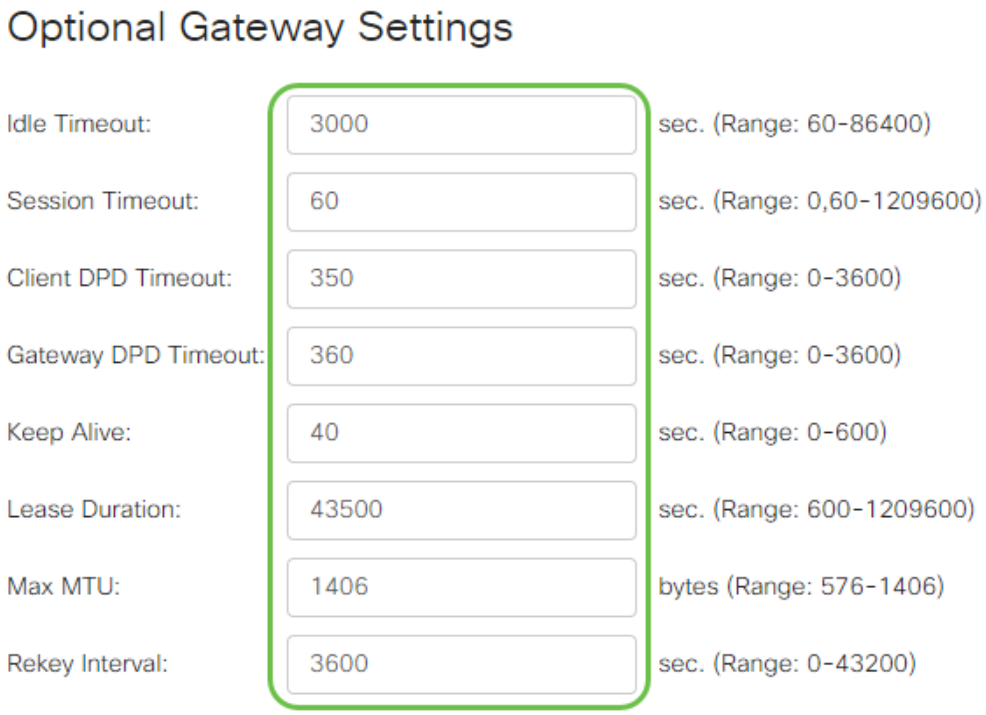
Schritt 1

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.



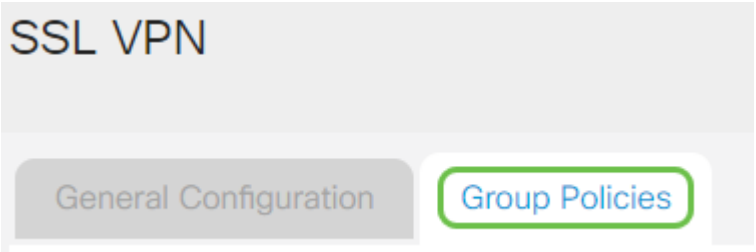
Schritt 2

Klicken Sie auf Apply (Anwenden).

Gruppenrichtlinien konfigurieren

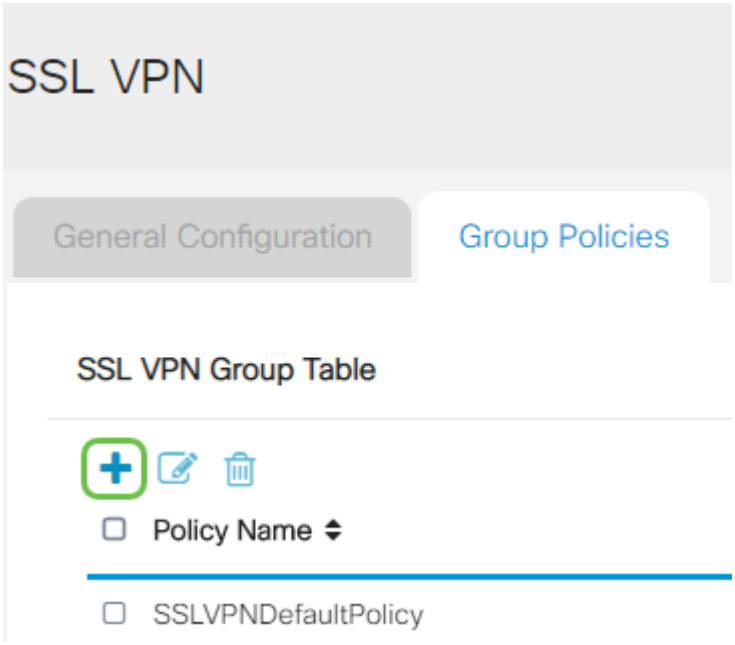
Schritt 1

Klicken Sie auf die Registerkarte **Gruppenrichtlinien**.



Schritt 2

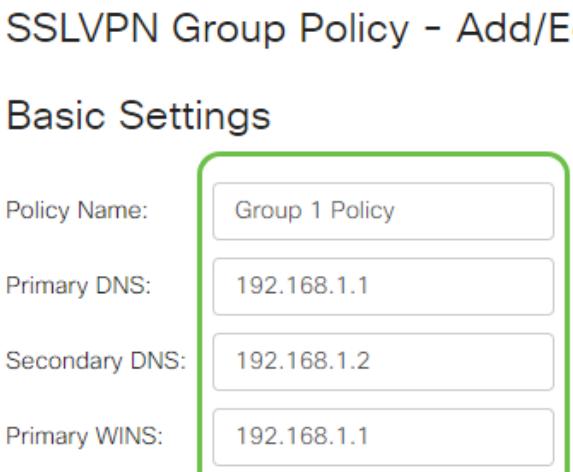
Klicken Sie unter der Tabelle für die SSL VPN-Gruppe auf das **Symbol Add** (Hinzufügen), um eine Gruppenrichtlinie hinzuzufügen.



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

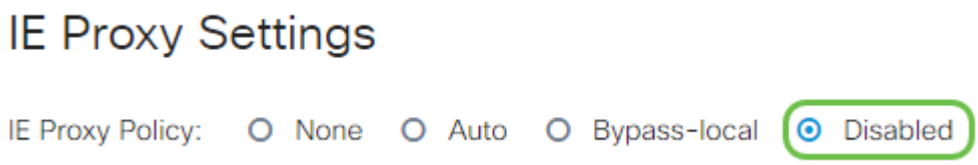
1. Geben Sie den bevorzugten Richtliniennamen in das Feld *Policy Name (Richtlinienname*) ein.
2. Geben Sie die IP-Adresse des primären DNS in das angegebene Feld ein. Standardmäßig wird diese IP-Adresse bereits angegeben.
3. *(Optional) Geben Sie die IP-Adresse des sekundären DNS in das angegebene Feld 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.



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.



Schritt 5 (optional)

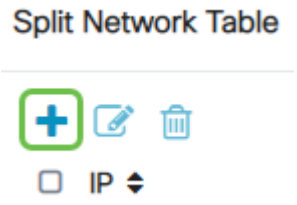
Aktivieren Sie im Bereich Getrennte Tunneling-Einstellungen das Kontrollkästchen **Enable Split Tunneling**, um das unverschlüsselte Senden von Internetdatenverkehr an das Internet zu ermöglichen. Full Tunneling sendet den gesamten Datenverkehr an das Endgerät, wo er dann an die Ziel-Ressourcen weitergeleitet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

Schritt 6 (optional)

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

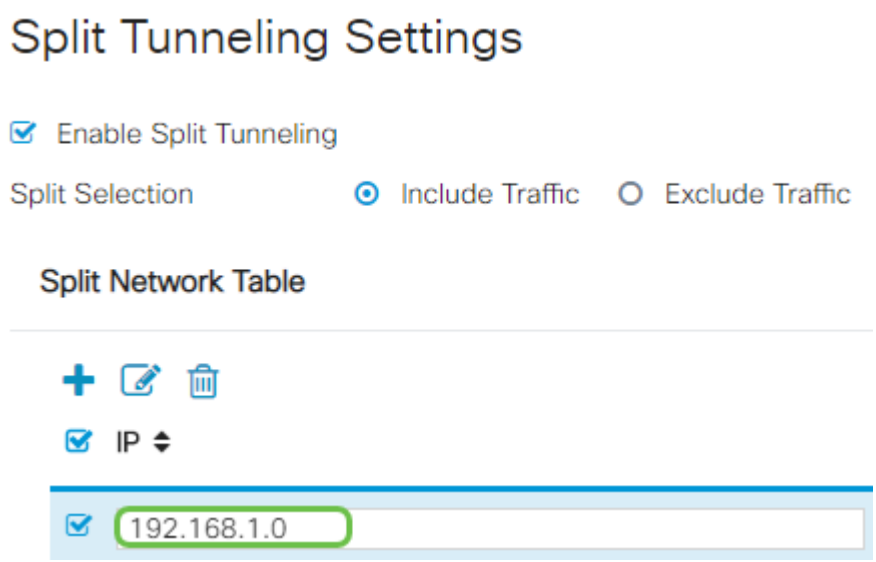
Schritt 7

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



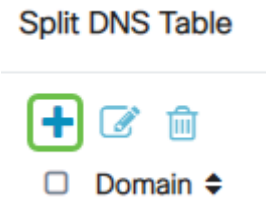
Schritt 8

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



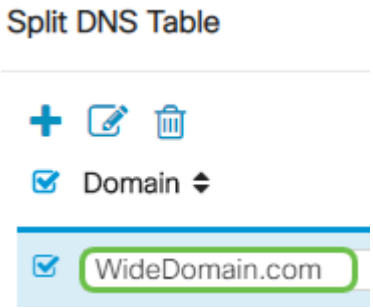
Schritt 9

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



Schritt 10

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



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

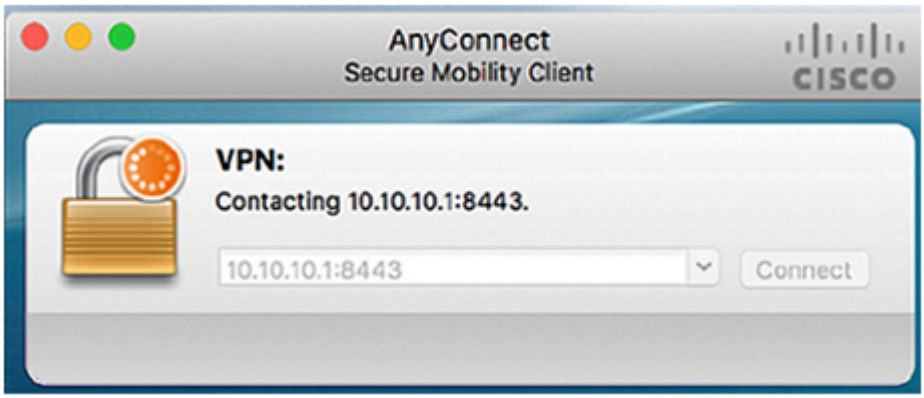
Schritt 1

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

Schritt 2

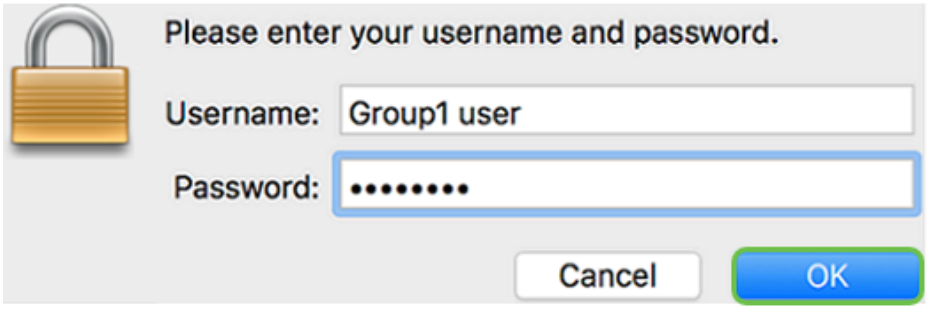
Geben Sie im Fenster des AnyConnect Secure Mobility Client die Gateway-IP-Adresse und die Gateway-Portnummer getrennt durch einen Doppelpunkt (:) ein, und klicken Sie dann auf **Verbinden**.

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



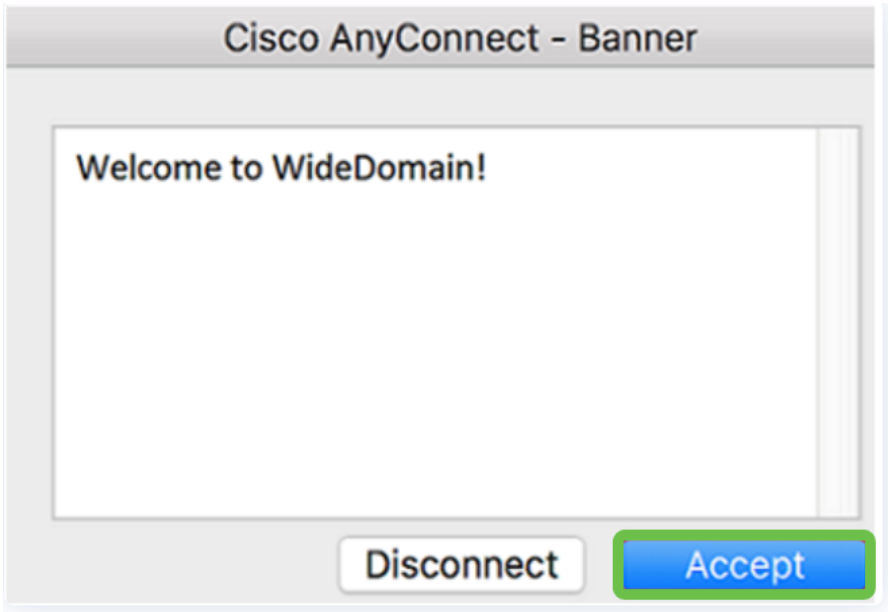
Schritt 3

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

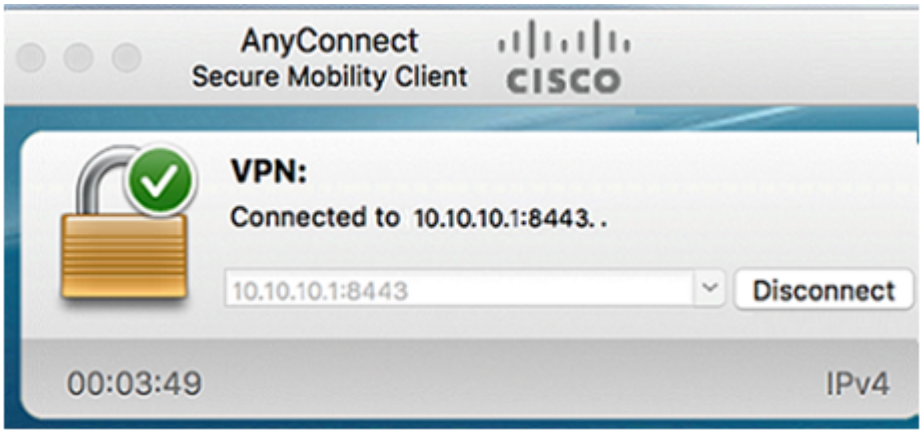


Schritt 4

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.

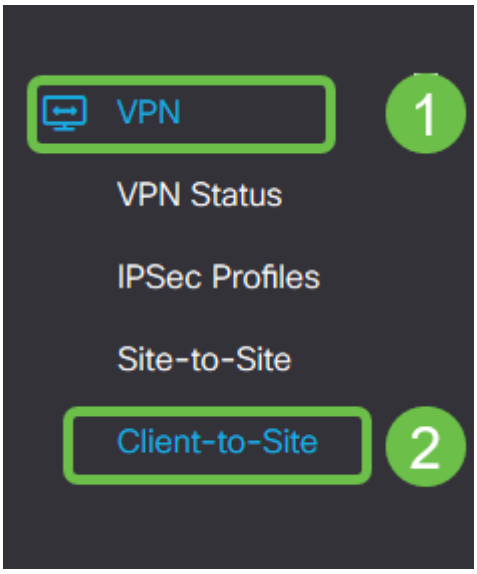
Sie können die neueste Version der Shrew Soft VPN-Clientsoftware hier herunterladen: https://www.shrew.net/download/vpn

Konfigurieren von Shrew Soft auf dem Router der Serie RV345P

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

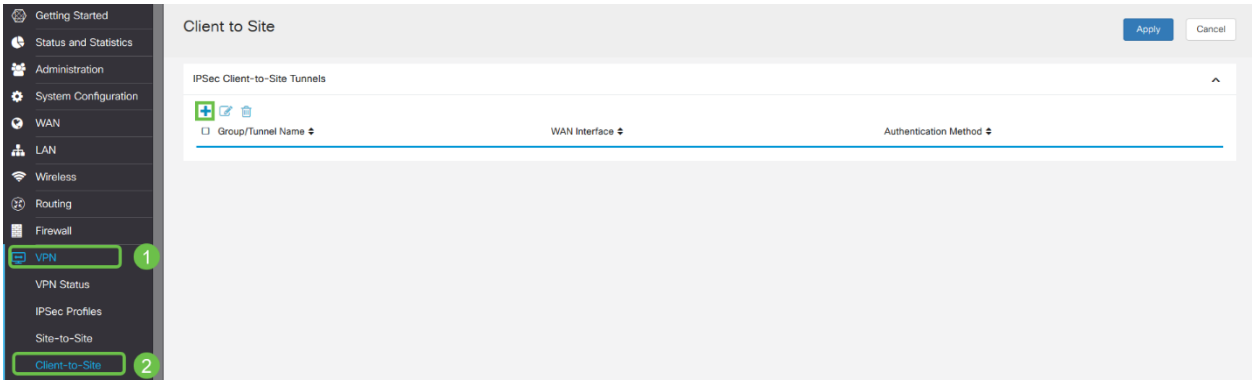
Schritt 1

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



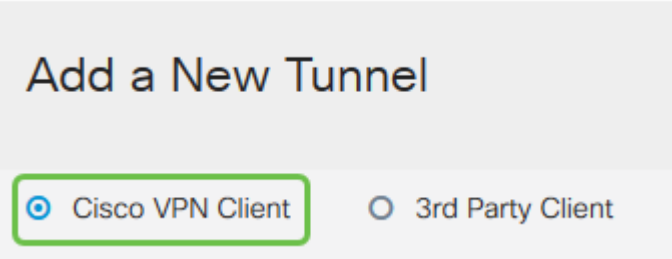
Schritt 2

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



Schritt 3

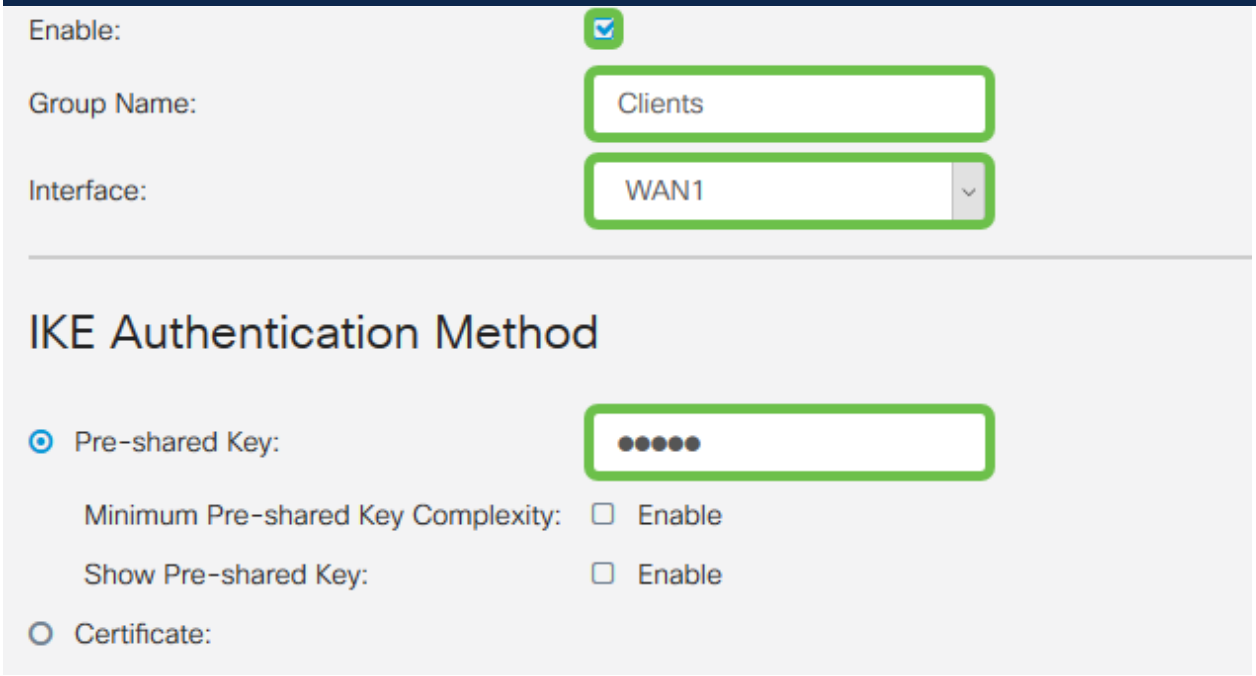
Wählen Sie die Option **Cisco VPN Client** aus.



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**.

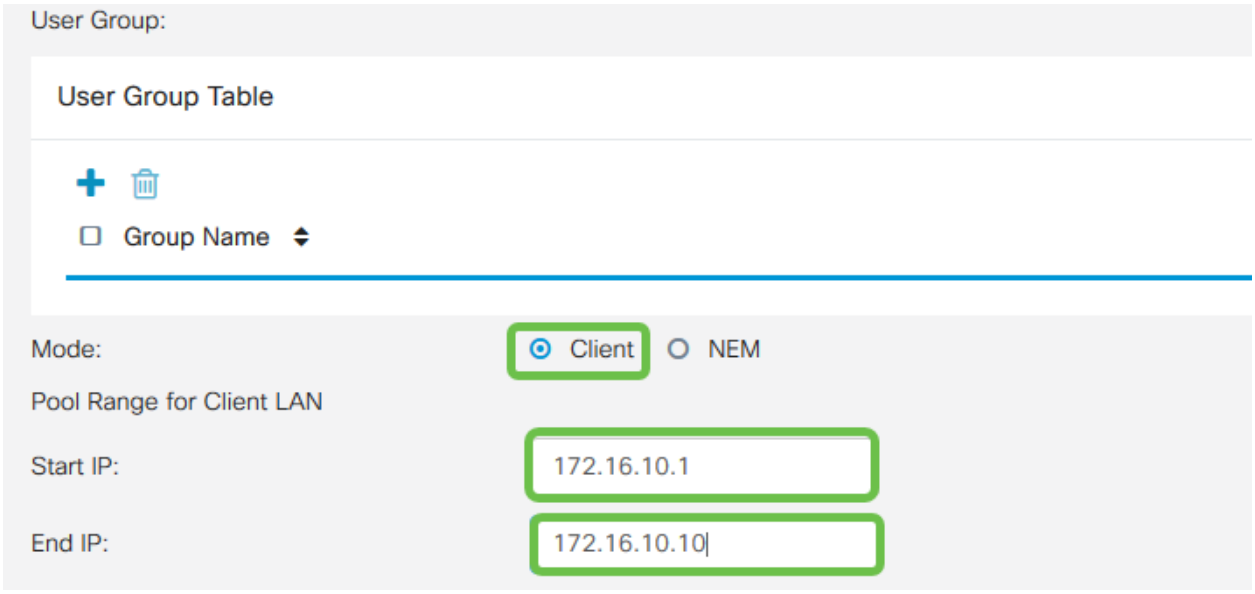
Bitte beachten Sie den *Gruppennamen* und den *Pre-shared Key*, wie sie später bei der Konfiguration des Clients verwendet werden.



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.

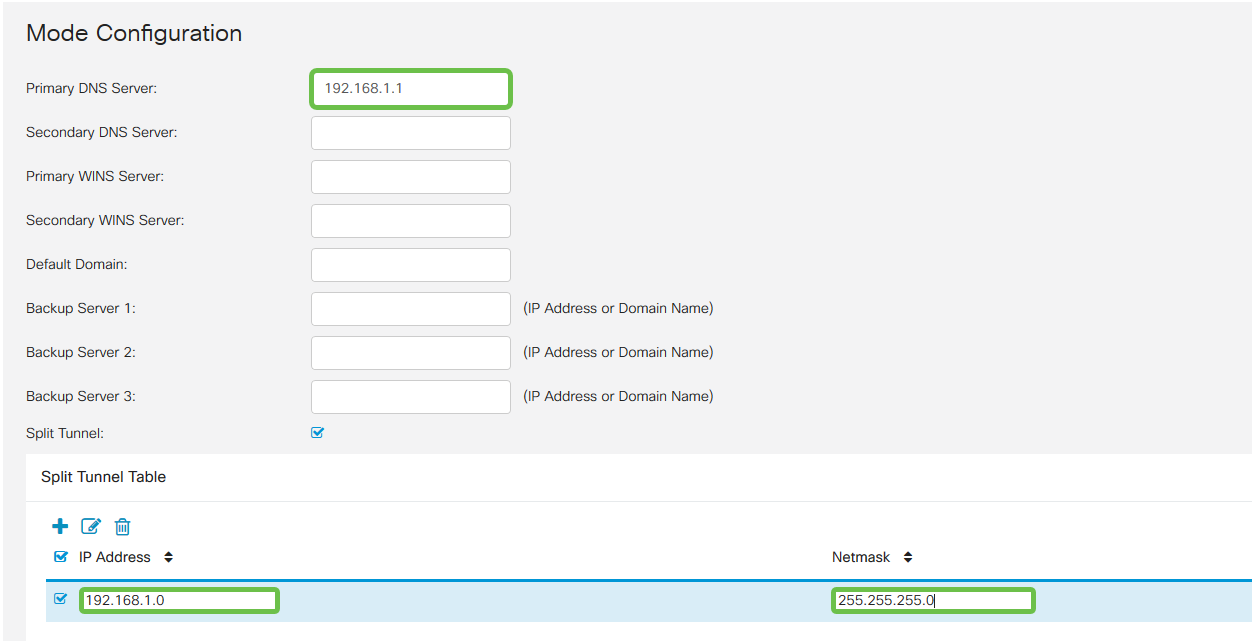
Der Pool-Bereich sollte ein eindeutiges Subnetz verwenden, das an keiner anderen Stelle im Netzwerk verwendet wird.



Schritt 6

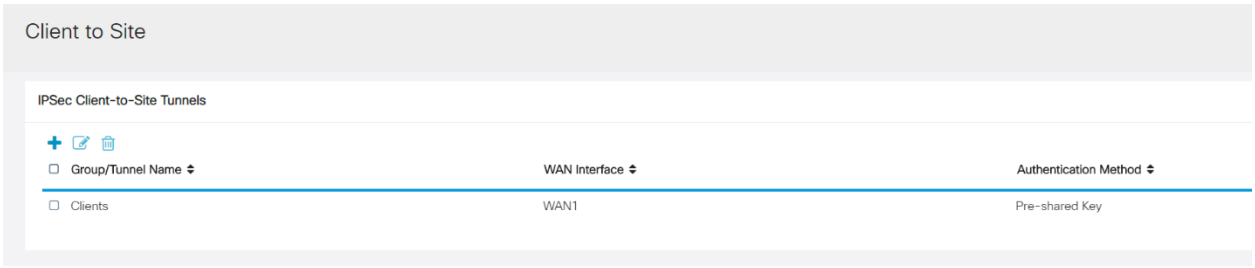
Hier konfigurieren Sie die Einstellungen für die **Moduskonfiguration**. Hier sind die Einstellungen, die wir verwenden werden:

- **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.



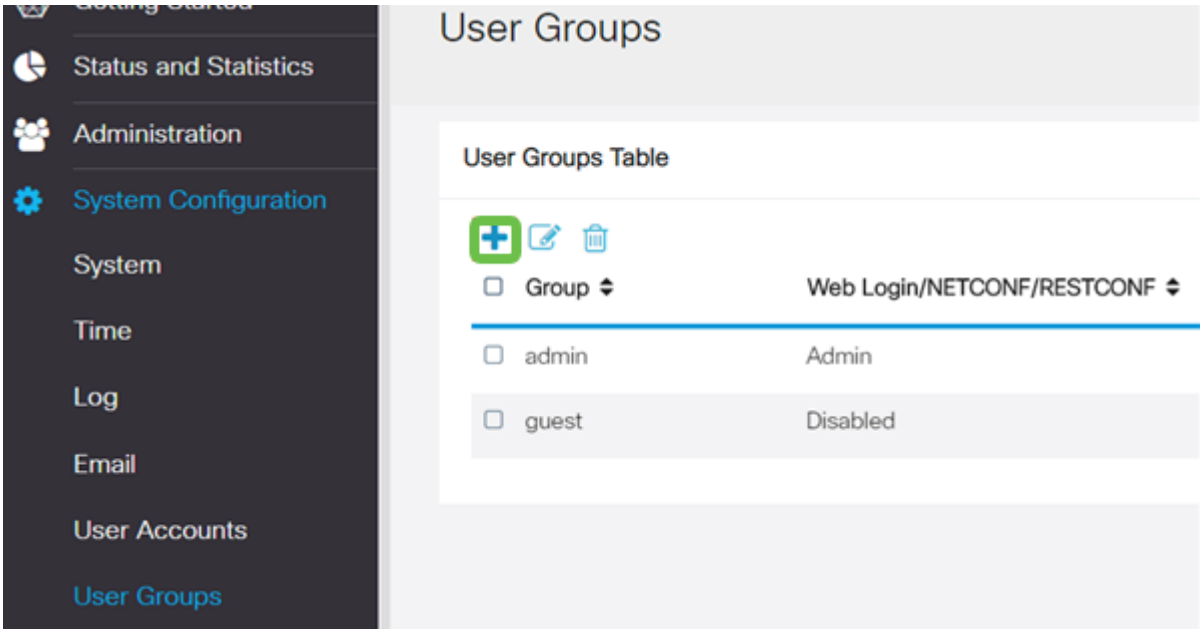
Schritt 7

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



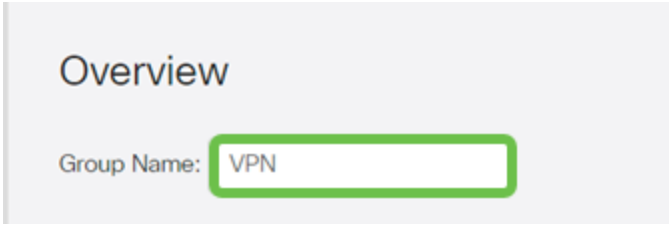
Schritt 8

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



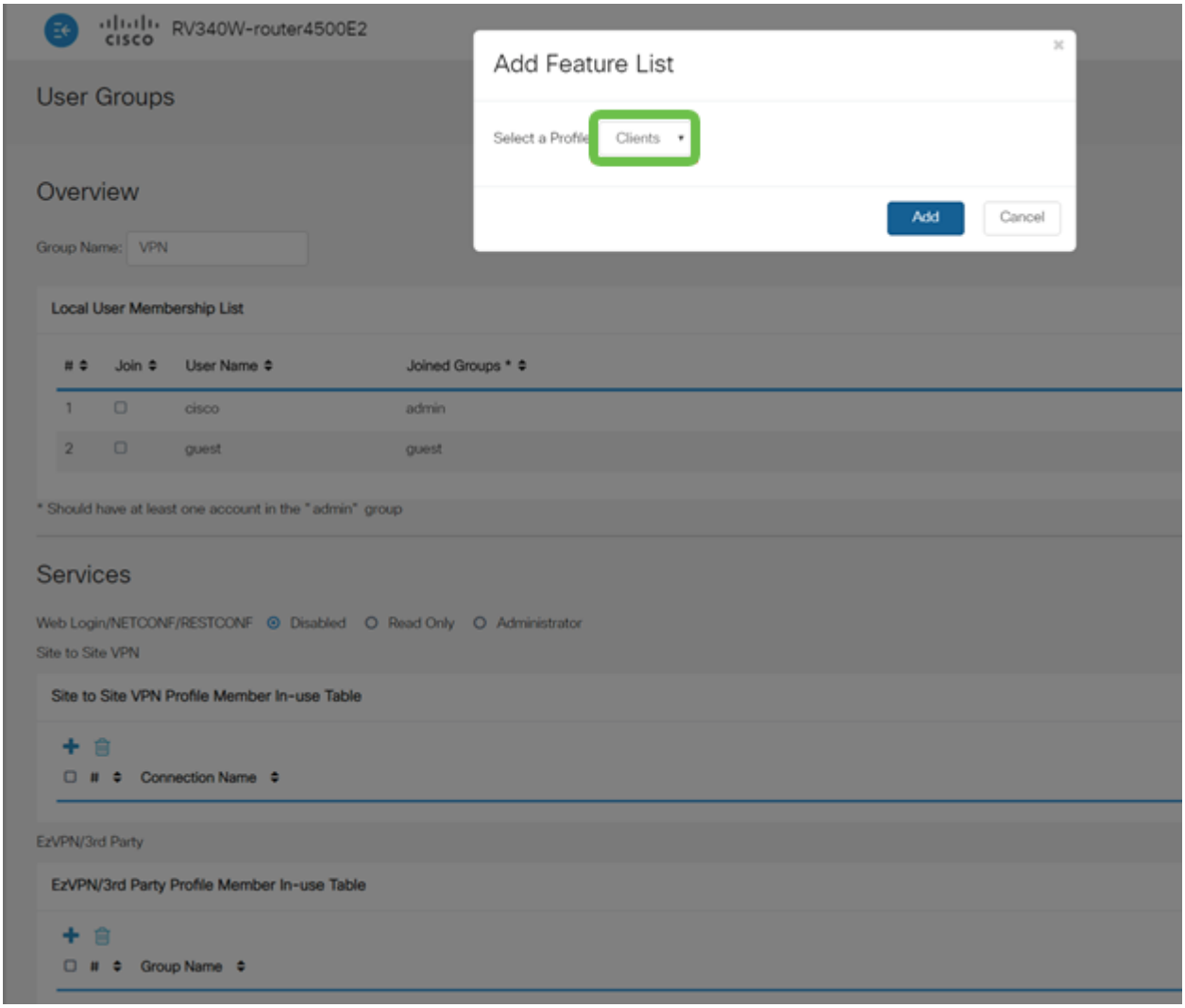
Schritt 9

Geben Sie einen **Gruppennamen ein**.



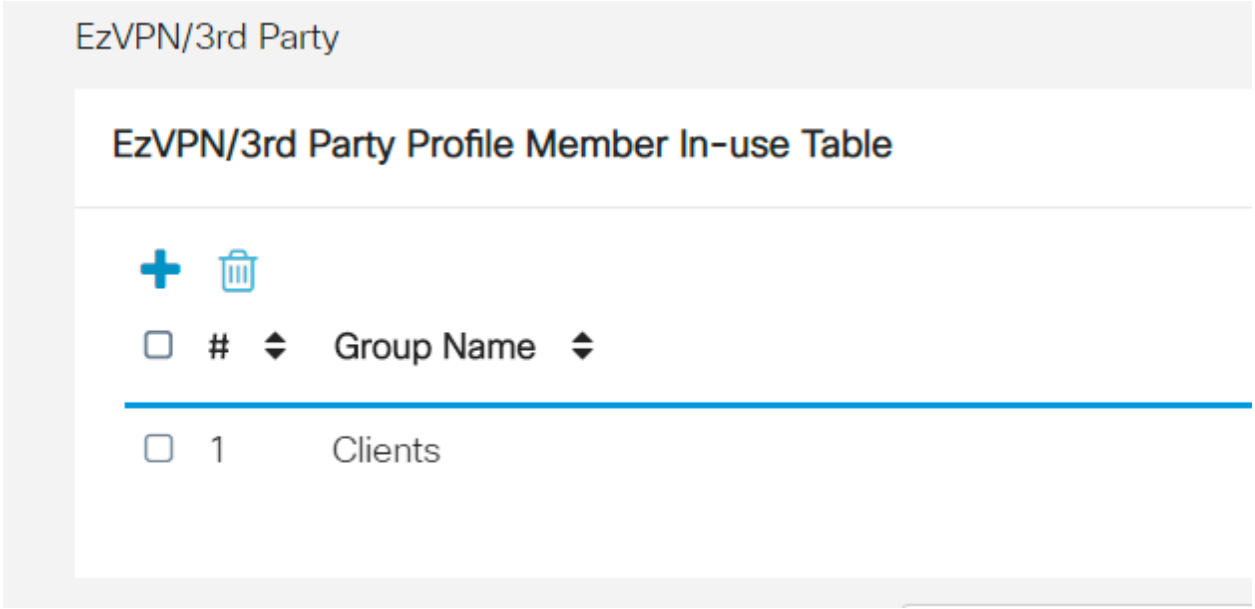
Schritt 10

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

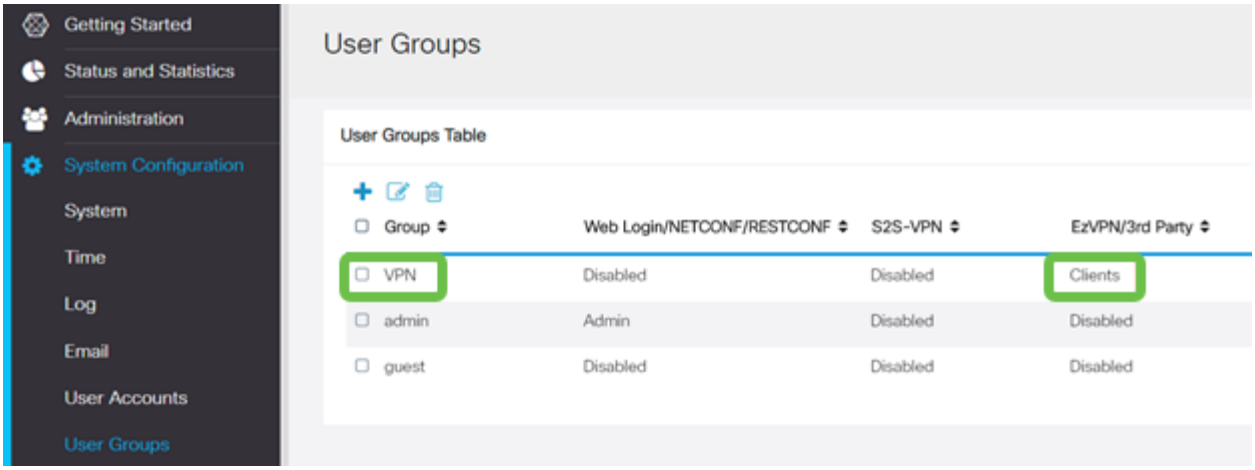
Sie sollten nun den **Client-to-Site**-Gruppennamen in der Liste für **EzVPN/Drittanbieter** sehen.



Schritt 12

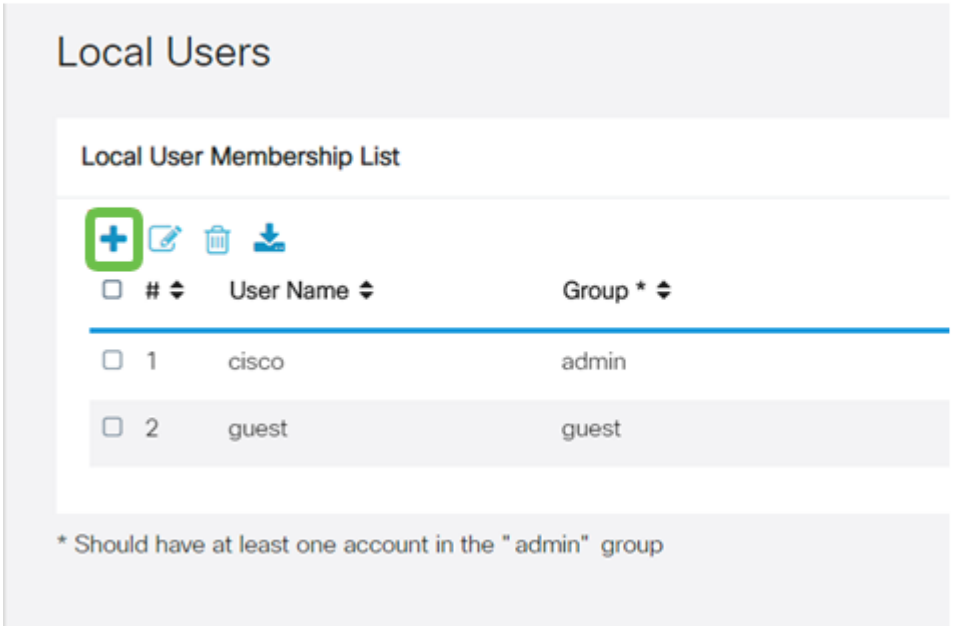
Nachdem Sie die Benutzergruppenkonfiguration **angewendet** haben, wird diese in der Liste der **Benutzergruppen** angezeigt und die neue Benutzergruppe wird mit dem zuvor

erstellten Client-to-Site-Profil verwendet.



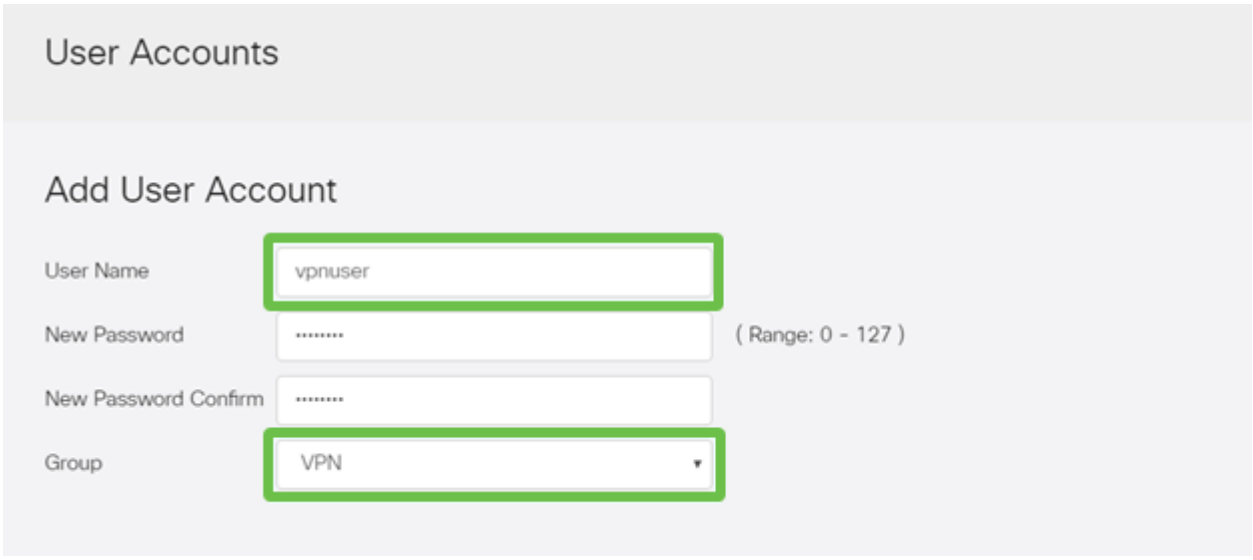
Schritt 13

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



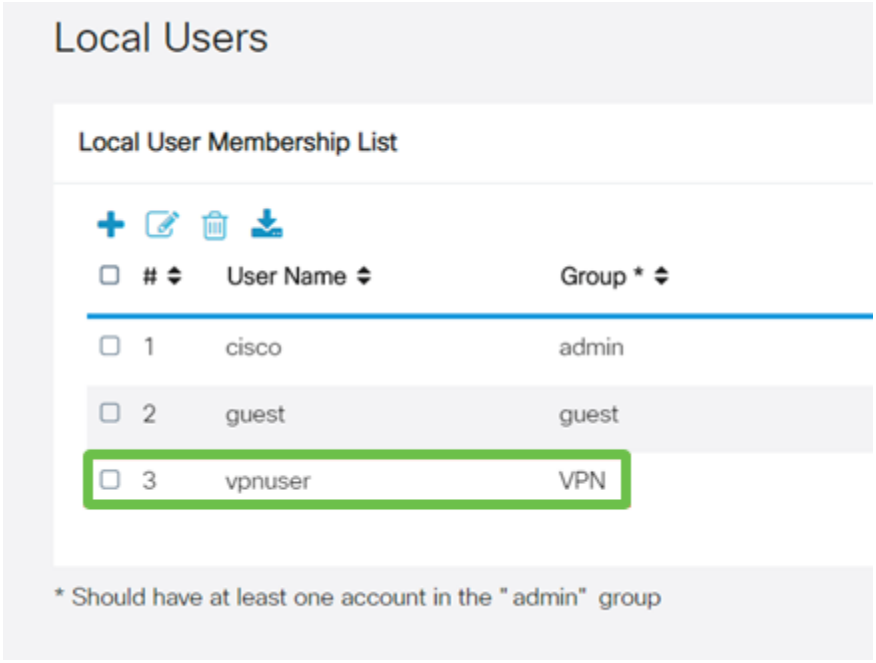
Schritt 14

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**.



Schritt 15

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



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

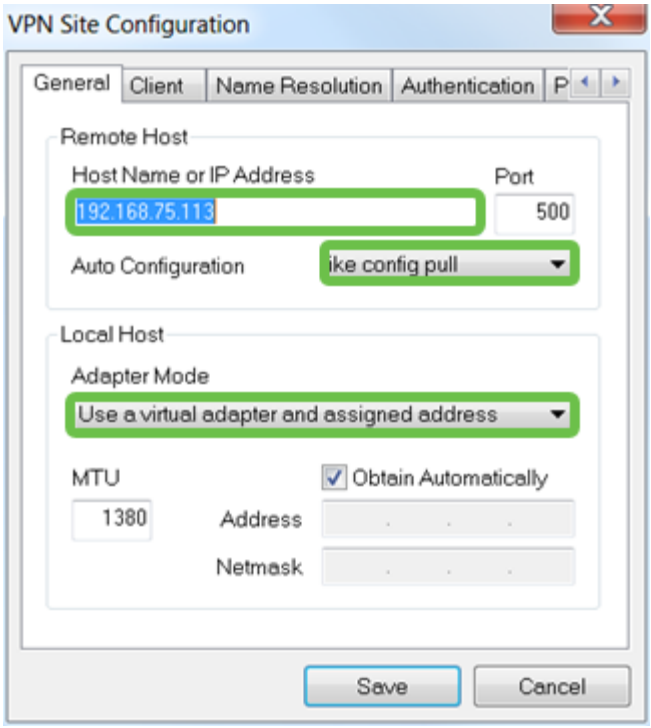
Führen Sie die folgenden Schritte aus.

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**:

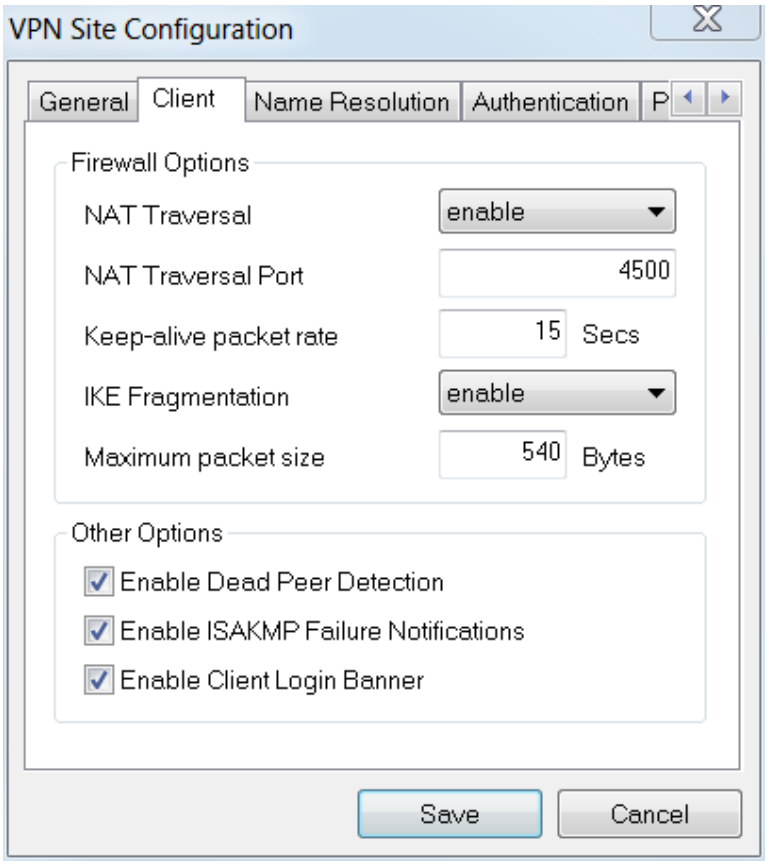
- **Hostname oder IP-Adresse**: Verwenden Sie die WAN-IP-Adresse (oder den Hostnamen des RV345P).

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



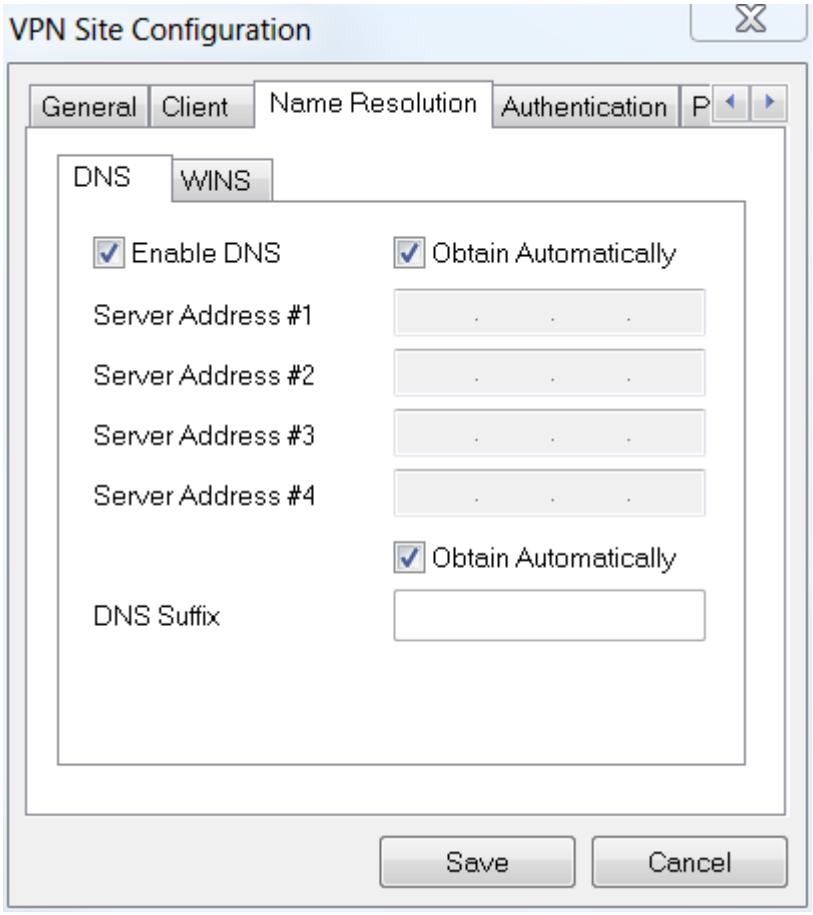
Schritt 2

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



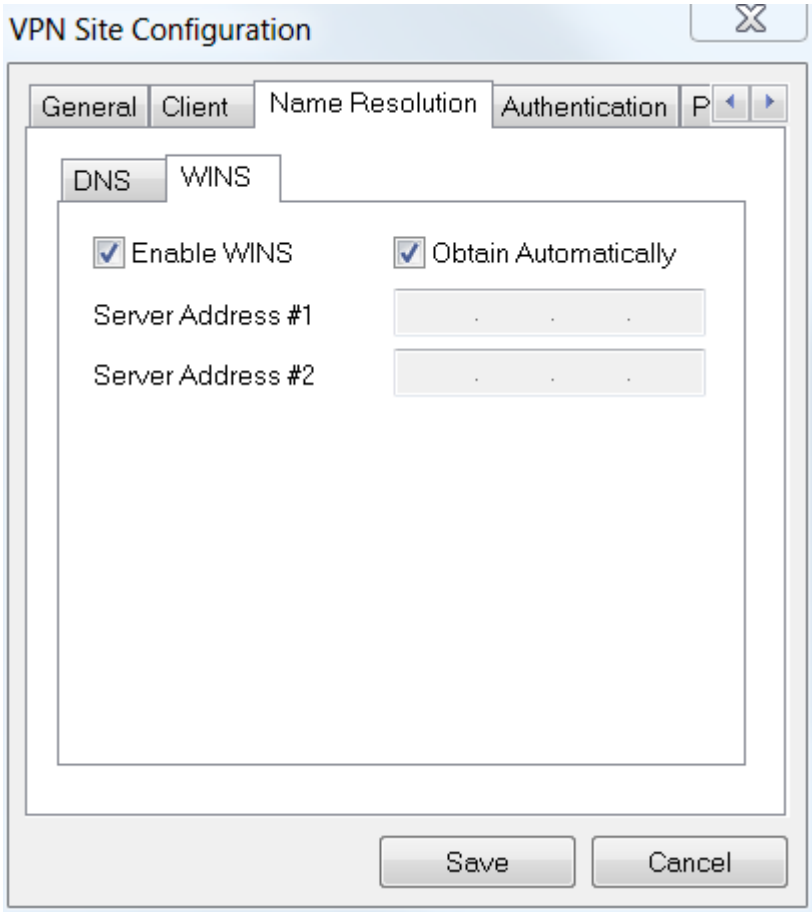
Schritt 3

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



Schritt 4

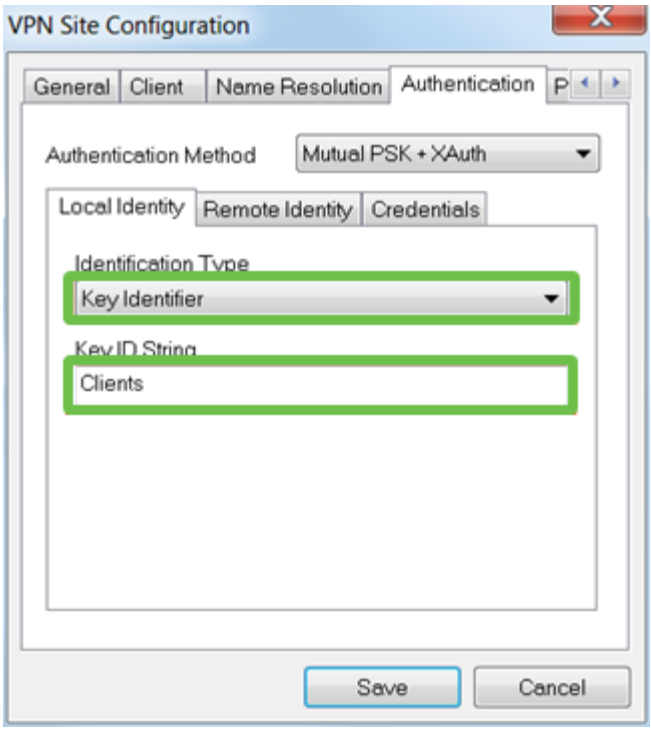
Aktivieren Sie unter **Namensauflösung > WINS**-Registerkarte das Kontrollkästchen **WINS aktivieren,** und lassen Sie das **Kontrollkästchen Automatisch beziehen** aktiviert.



Schritt 5

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

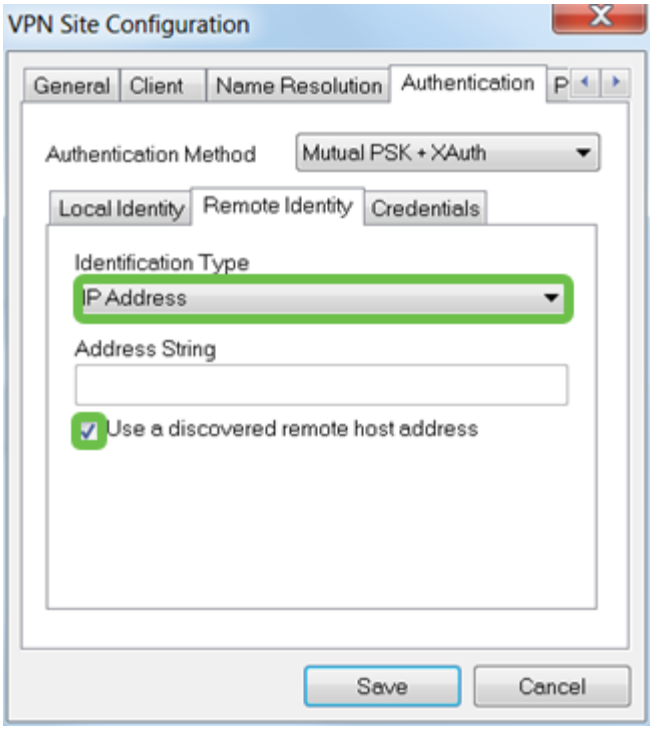
- **Identifizierungstyp**: **Schlüsselkennung** auswählen
- **Schlüssel-ID-Zeichenfolge**: Geben Sie den **Gruppennamen ein**, der auf dem RV345P konfiguriert wurde.



Schritt 6

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

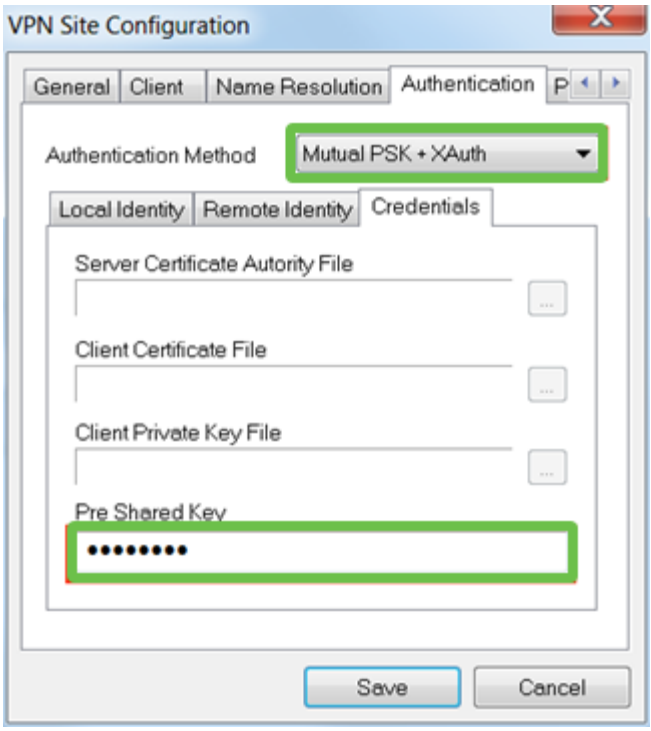
- **Identifizierungstyp**: IP-Adresse
- **Adresszeichenfolge**: <leer>
- **Verwenden Sie ein erkanntes** Adressfeld **des Remotehosts**: Aktiviert



Schritt 7

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

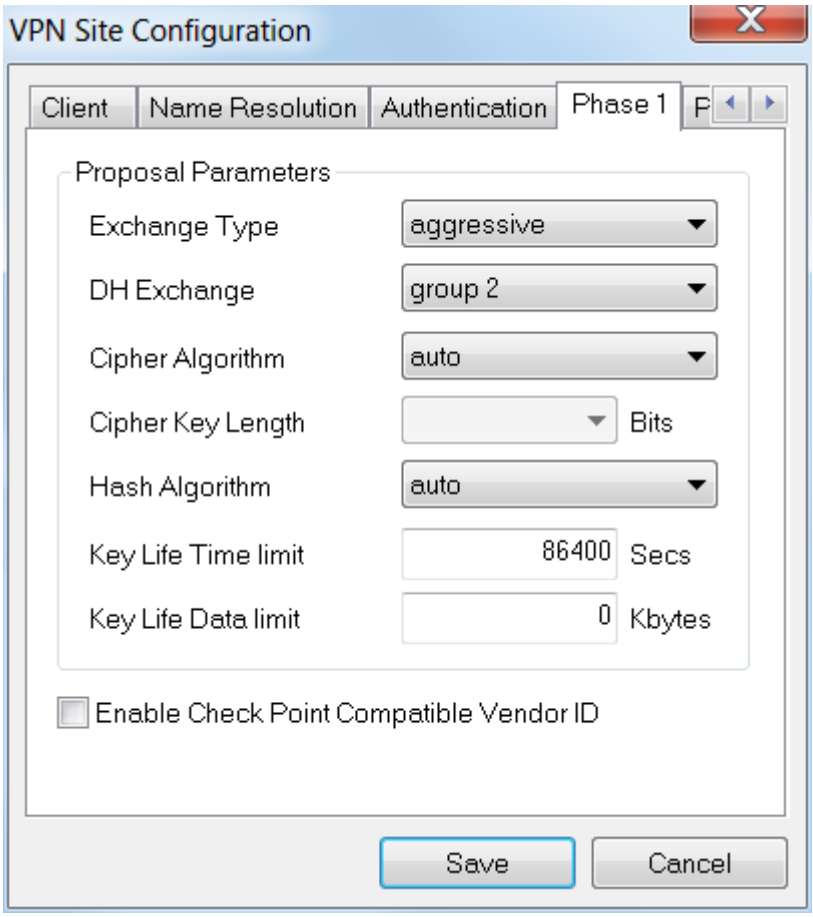
- **Authentifizierungsmethode**: Wählen Sie **Mutual PSK + XAuth aus**
- **Vorinstallierter Schlüssel**: Geben Sie den im RV345P-Clientprofil konfigurierten **Pre-shared Key ein.**



Schritt 8

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

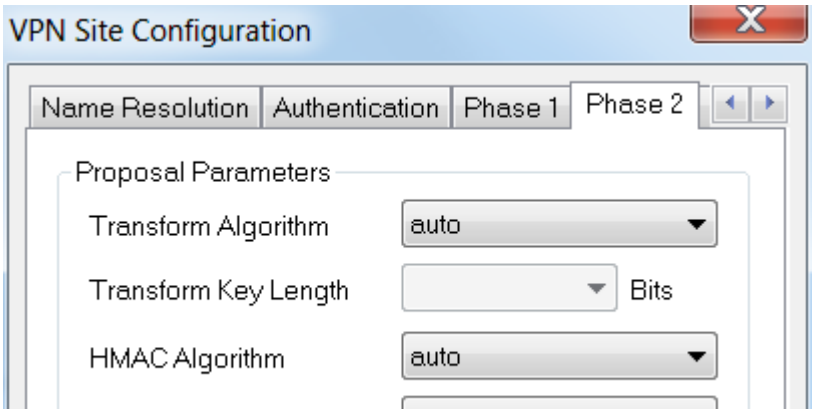
- **Exchange-Typ:** Aggressive
- **DH Exchange:** Gruppe 2
- **Cipher Algorithm:** Auto
- **Hash-Algorithmus:** Auto



Schritt 9

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

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

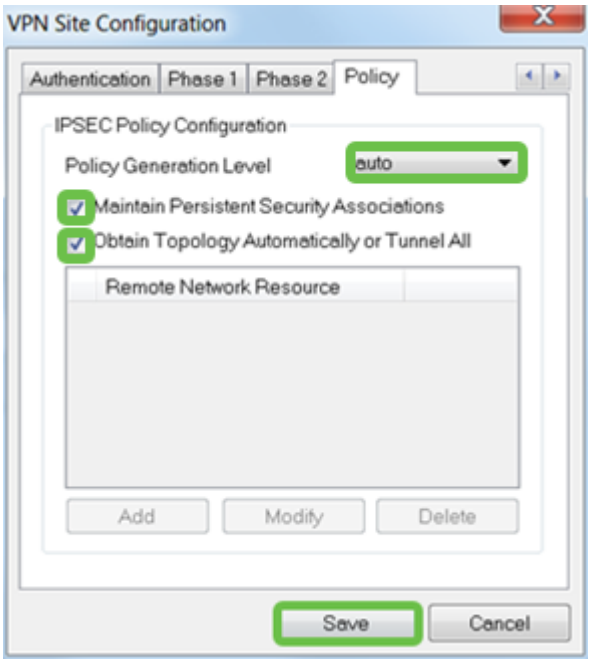


Schritt 10

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

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

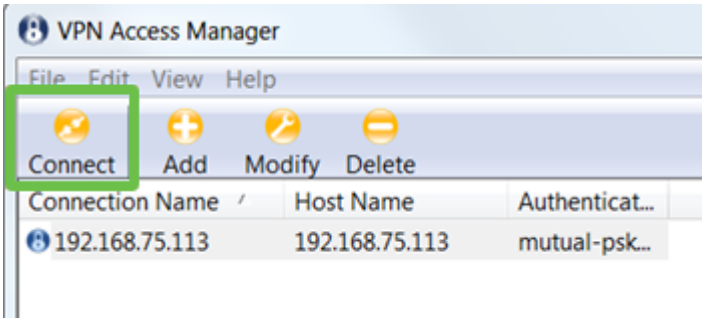
Da **Split-Tunneling** auf dem RV345P konfiguriert wurde, muss er hier nicht konfiguriert werden.



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**.

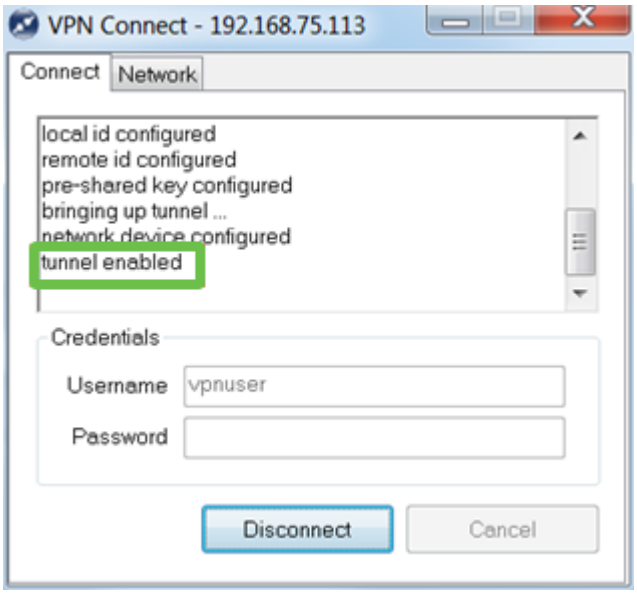


Schritt 12

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-Profils (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)

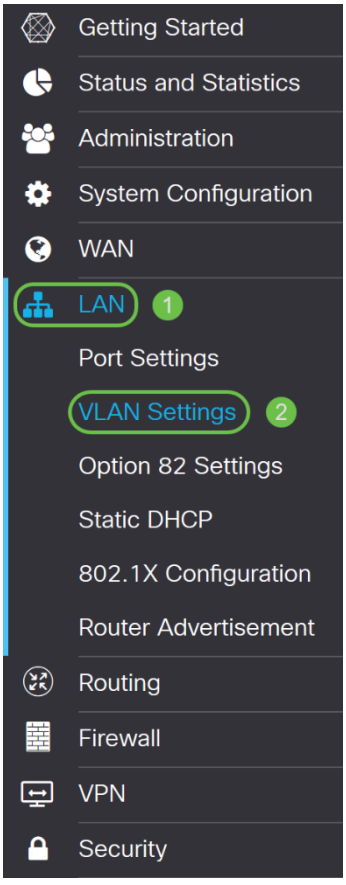
Mit einem Virtual Local Area Network (VLAN) können Sie ein Local Area Network (LAN) logisch in verschiedene Broadcast-Domänen segmentieren. In Umgebungen, in denen über das Netzwerk möglicherweise vertrauliche Daten übertragen werden, kann durch die Erstellung von VLANs die Sicherheit verbessert werden.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

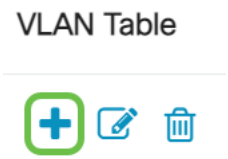
Schritt 1

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



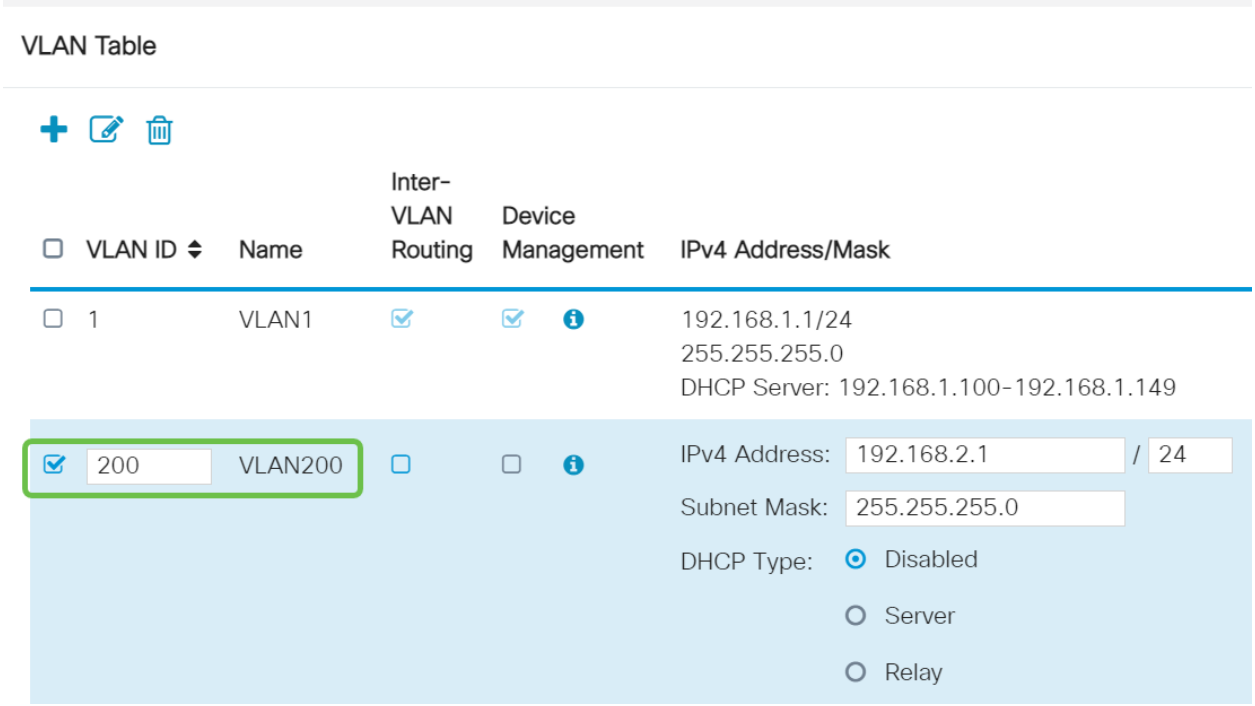
Schritt 2

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



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.



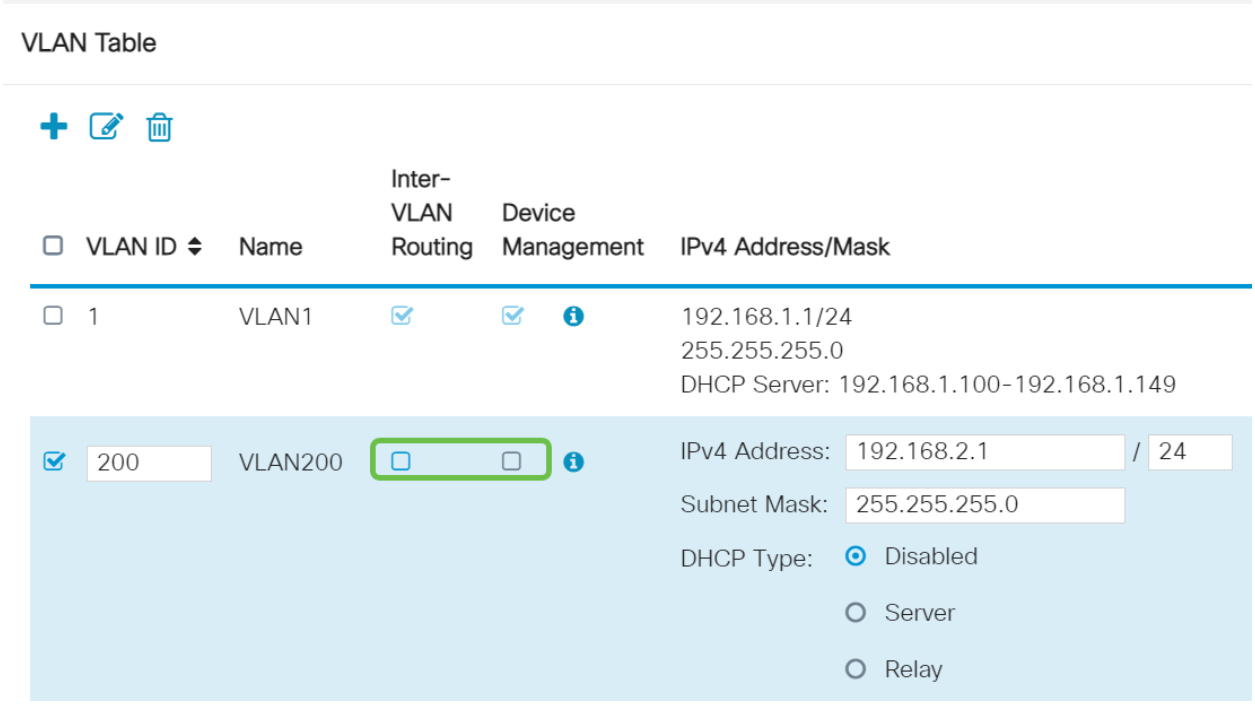
Schritt 4

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.

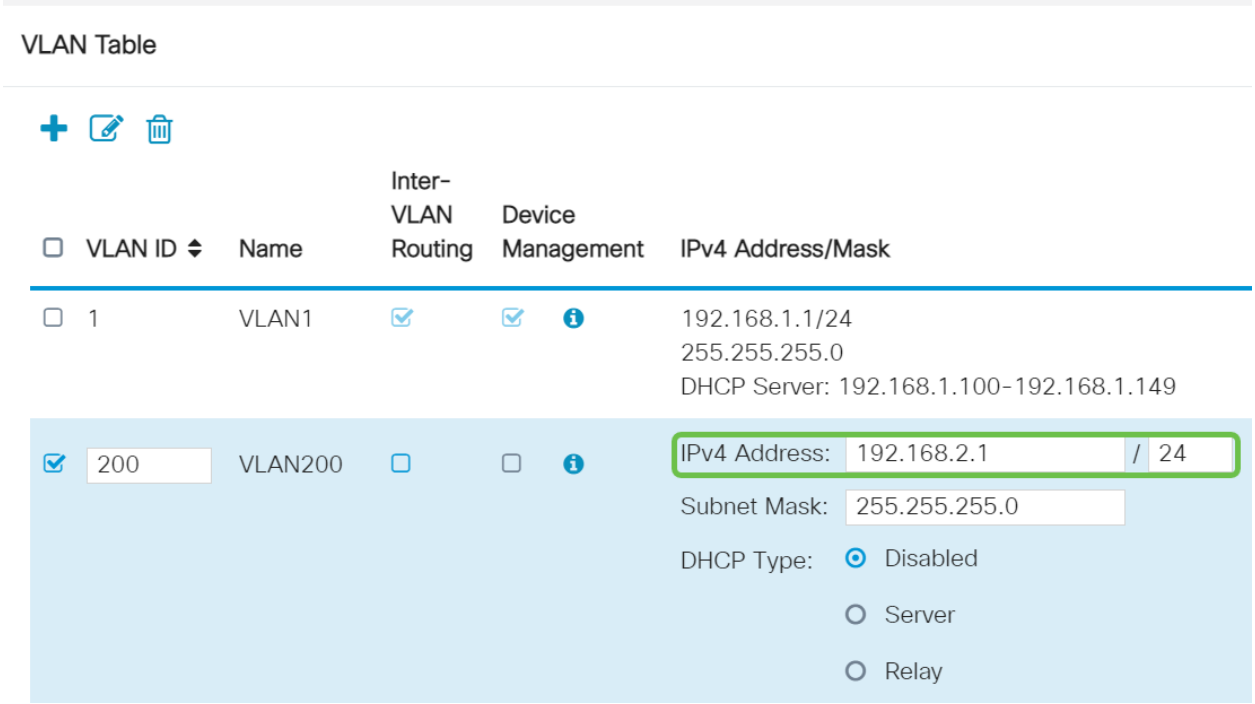
Die Geräteverwaltung ist die Software, mit der Sie sich über Ihren Browser über die Webbenutzeroberfläche des RV345P vom VLAN aus anmelden und den RV345P verwalten können. Dies sollte auch in Gastnetzwerken deaktiviert werden.

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



Schritt 5

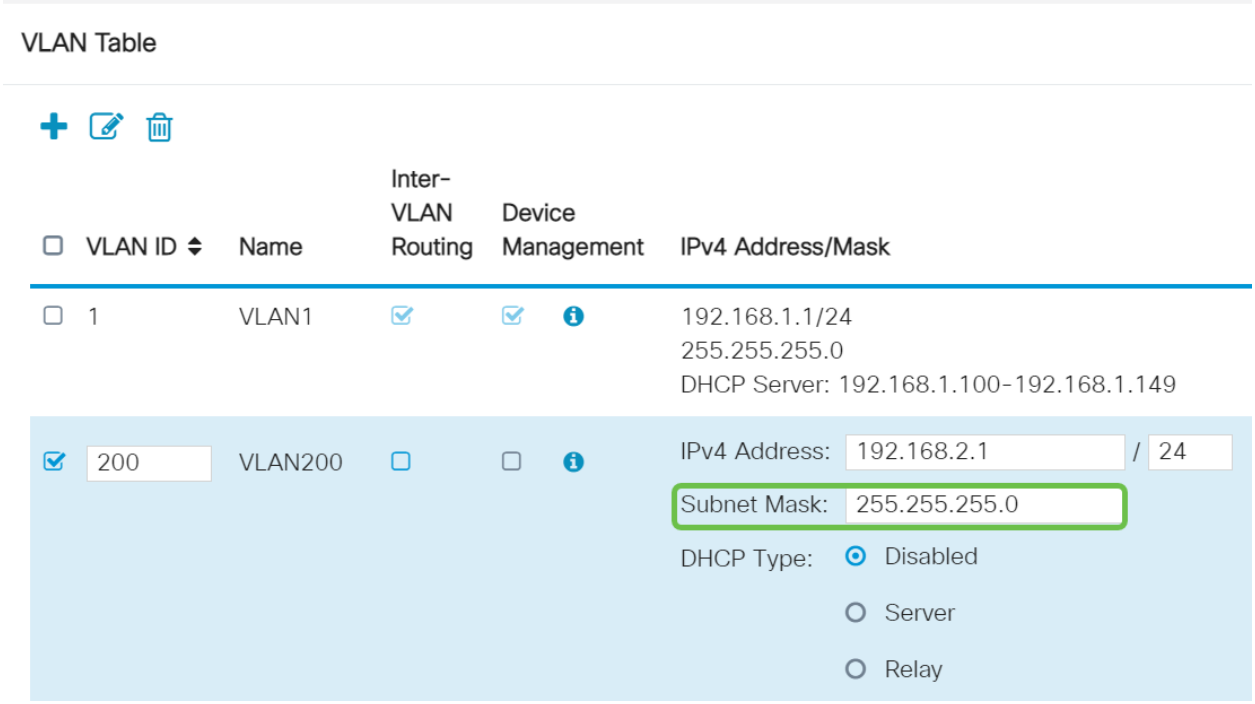
Die private IPv4-Adresse wird automatisch im Feld *IP-Adresse* eingetragen. Sie können dies auf Wunsch anpassen. In diesem Beispiel ist für das Subnetz 192.168.2.100-192.168.2.149 IP-Adressen für DHCP verfügbar. Für statische IP-Adressen sind die Werte 192.168.2.168.2.99 und 192.168.2.150-192.168.2.254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



Schritt 6

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

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



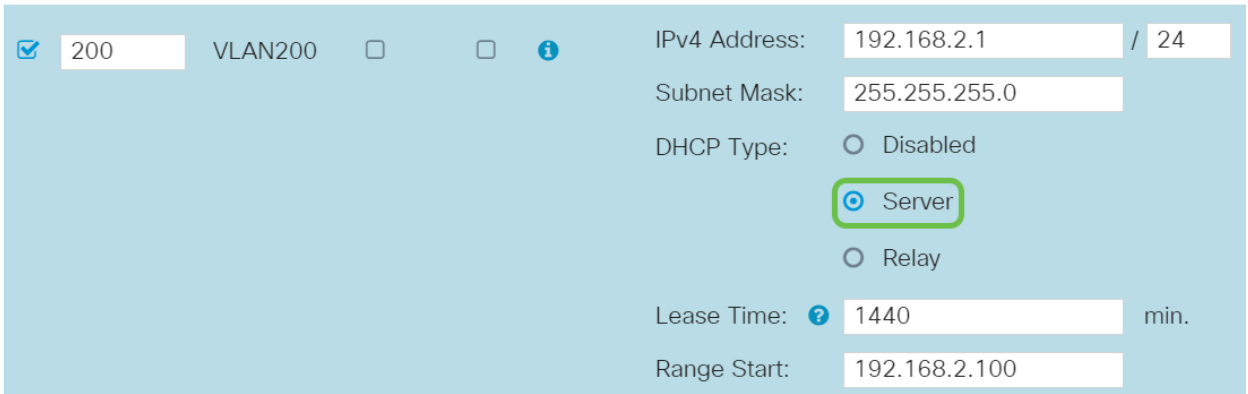
Schritt 7

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

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

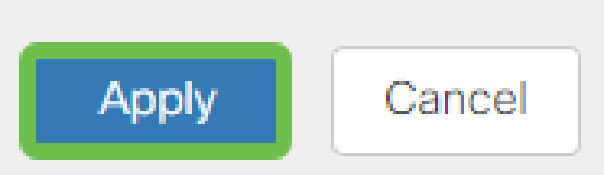
Server: Dies ist die am häufigsten verwendete Option.

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



Schritt 8

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



VLANs Ports zuweisen (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:

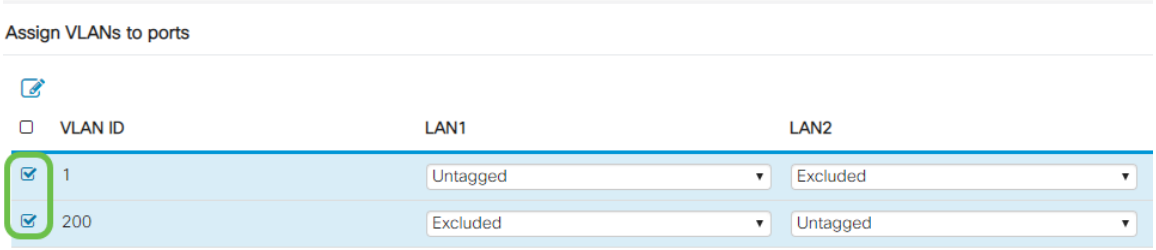
- Als Trunk-Port angesehen.
- Eines der VLANs kann als Untagged bezeichnet werden.
- Die übrigen VLANs, die Teil des Trunk-Ports sind, müssen mit Tagged gekennzeichnet werden.
- Die VLANs, die nicht Teil des Trunk-Ports sind, sollten für diesen Port mit Excluded (Ausgeschlossen) gekennzeichnet werden.

In diesem Beispiel gibt es keine Trunks.

Schritt 1

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

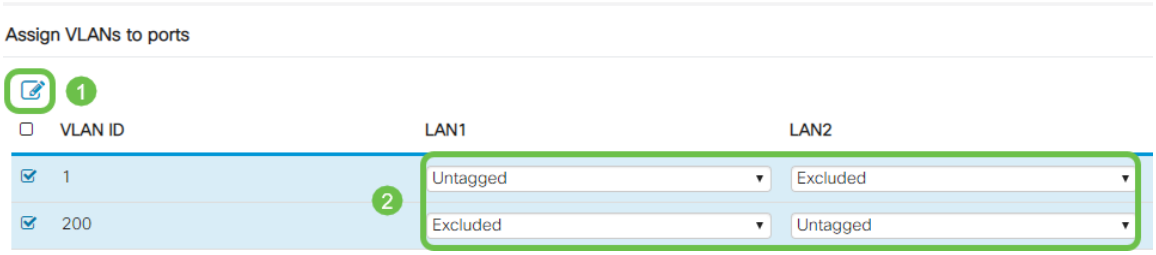
In diesem Beispiel haben wir *VLAN 1* und *VLAN 200* ausgewählt.



Schritt 2

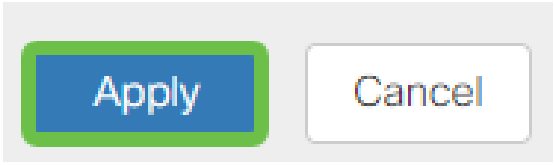
Klicken Sie auf **Bearbeiten**, um einem LAN-Port ein VLAN zuzuweisen, und geben Sie jede Einstellung als *Tagged*, *Untagged* oder *Excluded* an.

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.



Schritt 3

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



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.

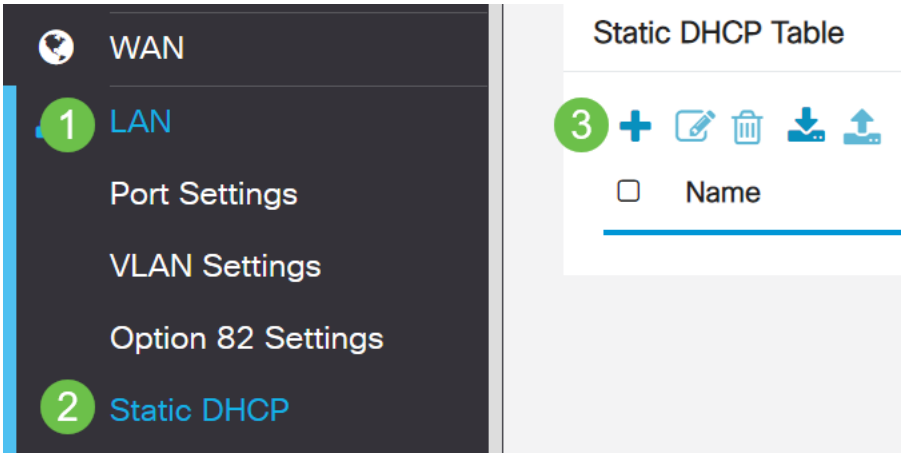
Hinzufügen einer statischen IP (optional)

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.

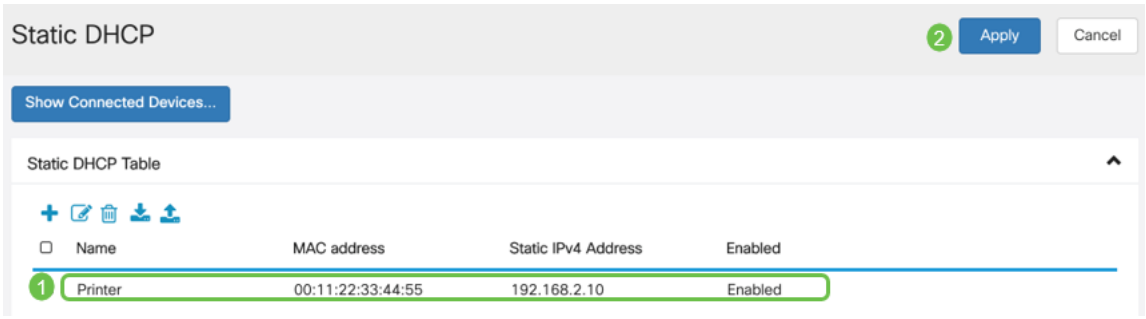
Schritt 1

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)

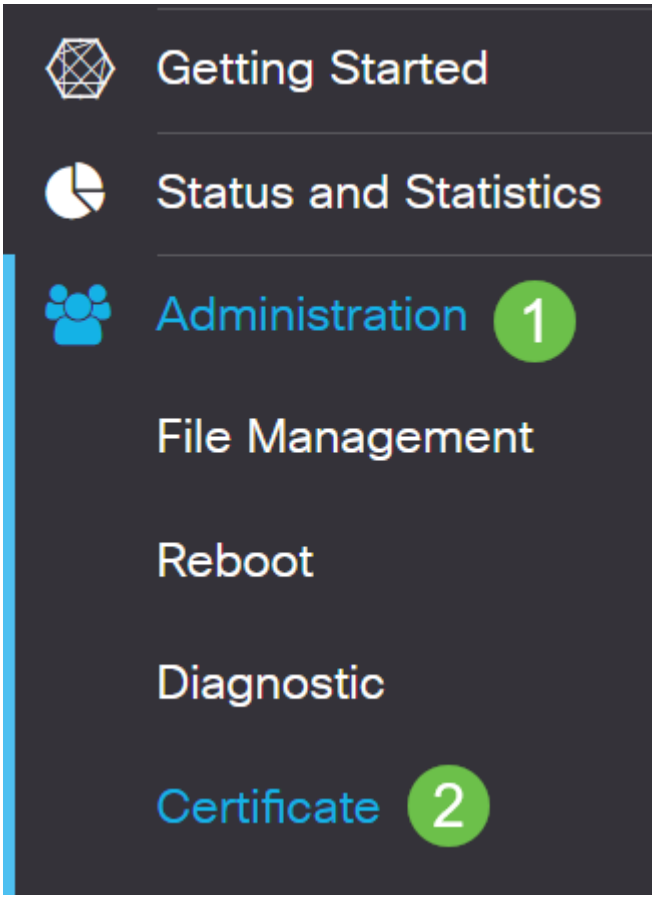
Ein digitales Zertifikat bescheinigt das Eigentum an einem öffentlichen Schlüssel durch den benannten Subjekt des Zertifikats. Dadurch können sich die Parteien auf Signaturen oder Behauptungen des privaten Schlüssels verlassen, der dem öffentlichen Schlüssel entspricht, der zertifiziert ist. Ein Router 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

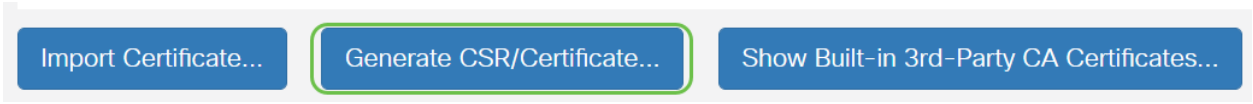
Schritt 1

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

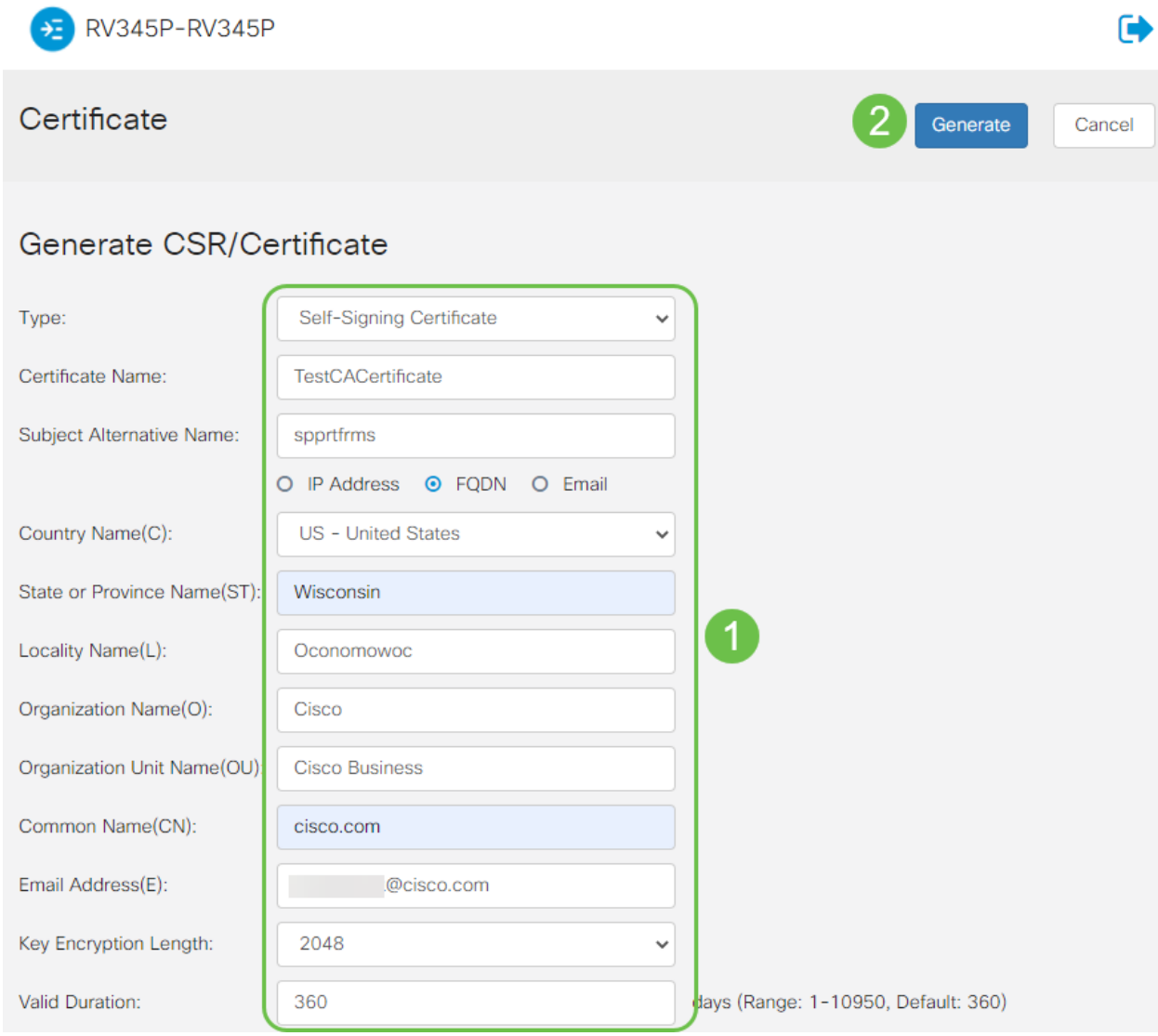
Füllen Sie die Felder mit folgenden Angaben aus:

- 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

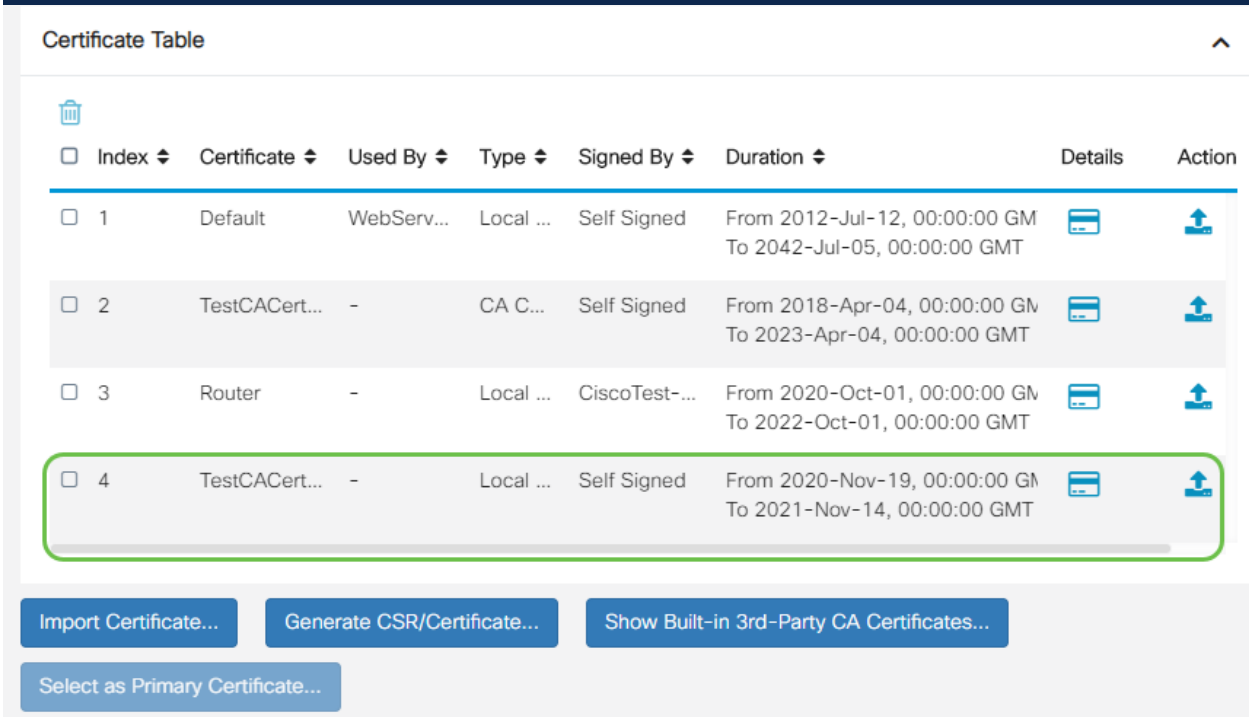
Schlüssel geheim gehalten wird.

- 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 Domänennamen (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 Domänenname 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**.



Das generierte Zertifikat sollte nun in der Zertifikatstabelle angezeigt werden.

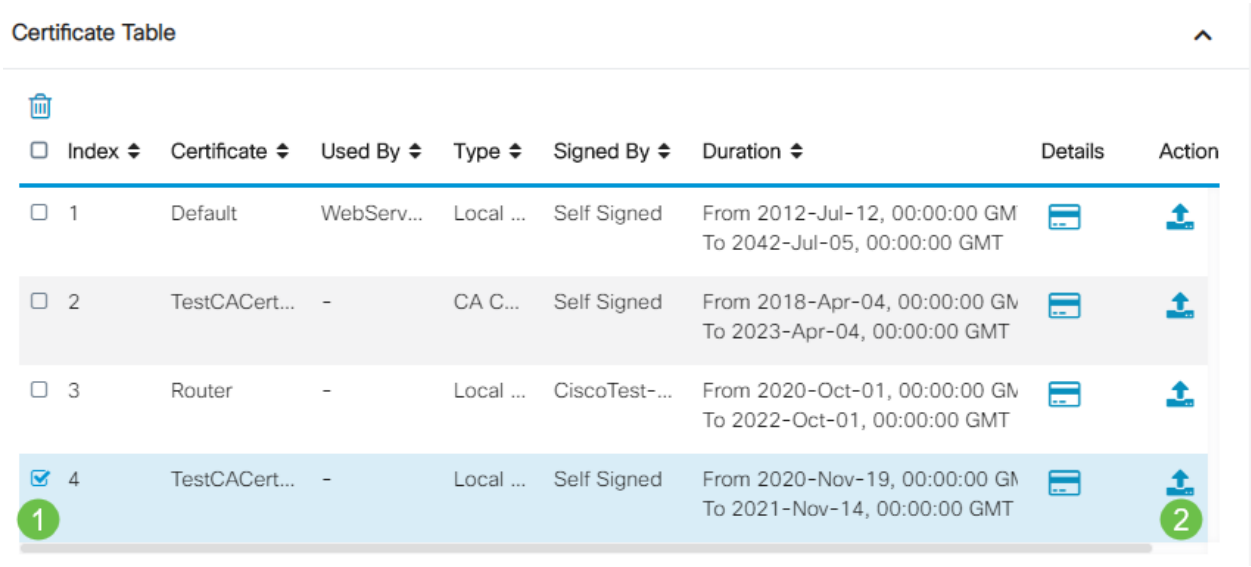


Sie sollten jetzt erfolgreich ein Zertifikat auf dem RV345P-Router erstellt haben.

Zertifikat exportieren

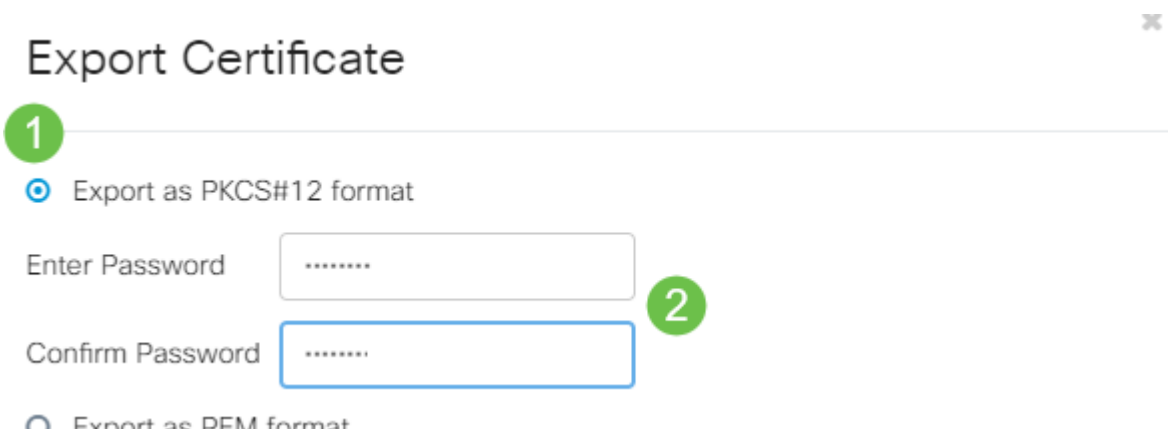
Schritt 1

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



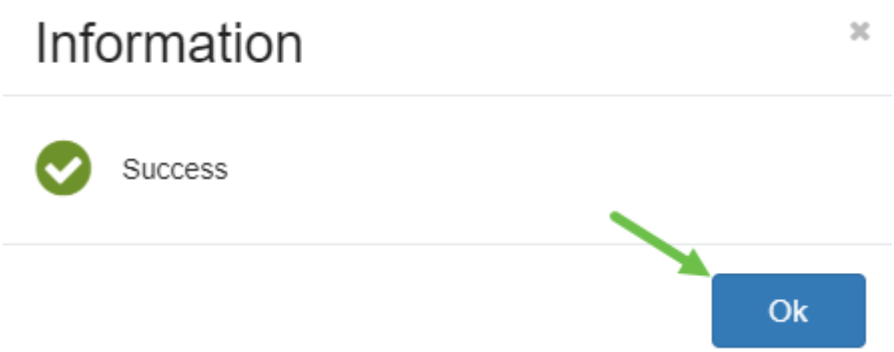
Schritt 2

- 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, wird ein Kennwort benötigt, 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**.



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**.

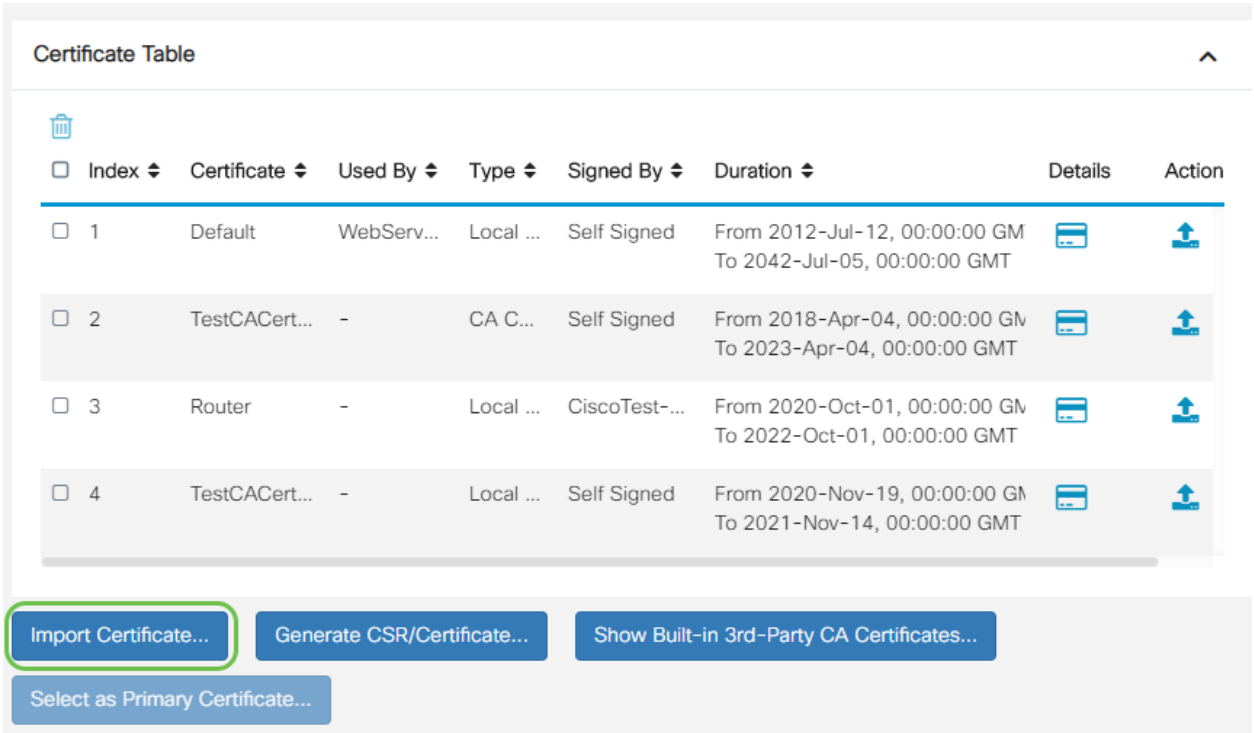


Sie sollten jetzt erfolgreich ein Zertifikat für den Router der Serie RV345P exportiert haben.

Importieren eines Zertifikats

Schritt 1

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



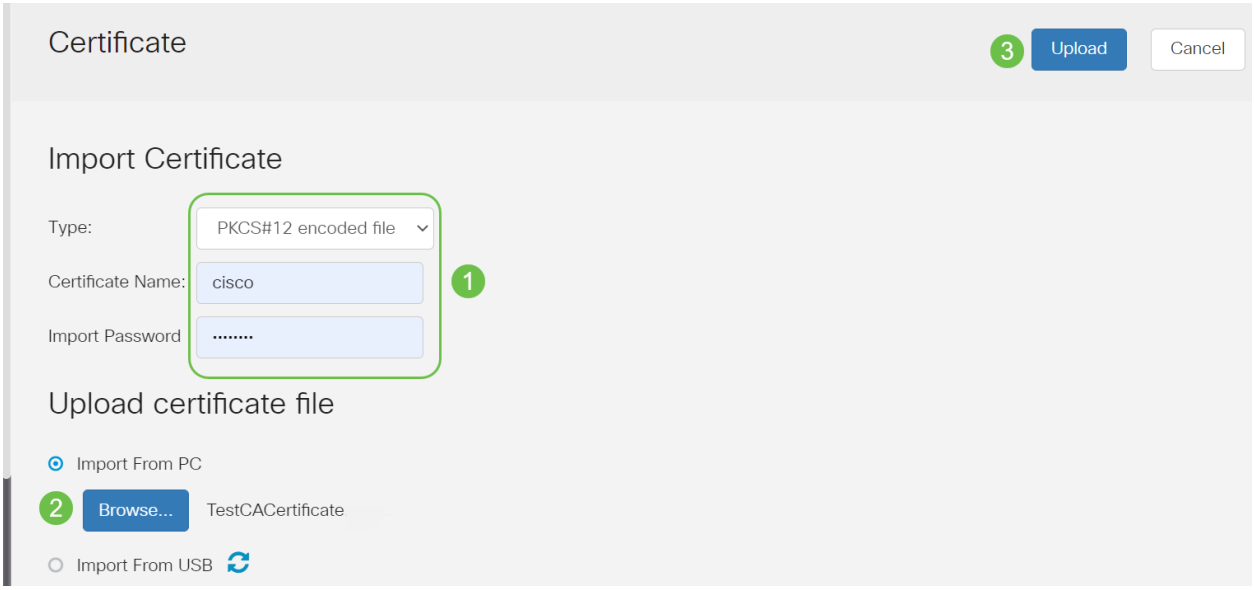
Schritt 2

- 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

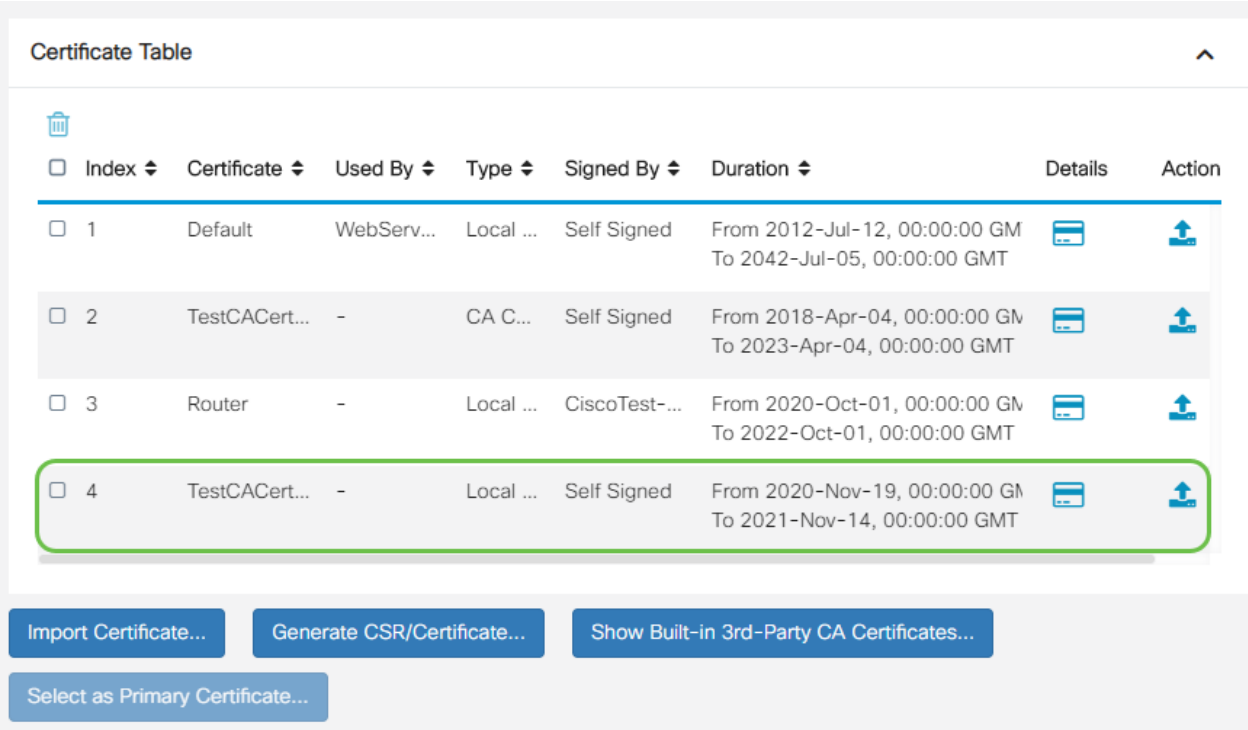
im Zertifikat enthaltenen Informationen korrekt sind.
    - PKCS #12 Encoded file — Public Key Cryptography Standards (PKCS) #12 ist ein Format zum Speichern eines Serverzertifikats.

- 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**.



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



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 CBW140AC

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

Wenn Ihr Access Point nicht neu ist, stellen Sie sicher, dass er sofort auf die Werkseinstellungen zurückgesetzt ist, damit der *CiscoBusiness-Setup* SSID in Ihren Wi-Fi-Optionen angezeigt wird. Weitere Informationen hierzu finden Sie unter Neustarten und Zurücksetzen auf die werkseitigen Standardeinstellungen auf RV345x-Routern.

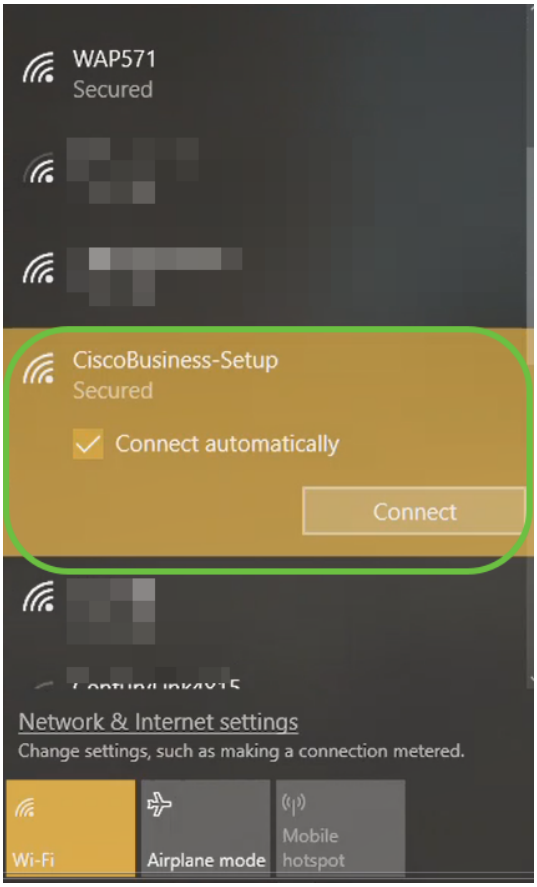
Richten Sie den primären 140AC Wireless Access Point auf der Webbenutzeroberfläche ein.

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

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

Schritt 1

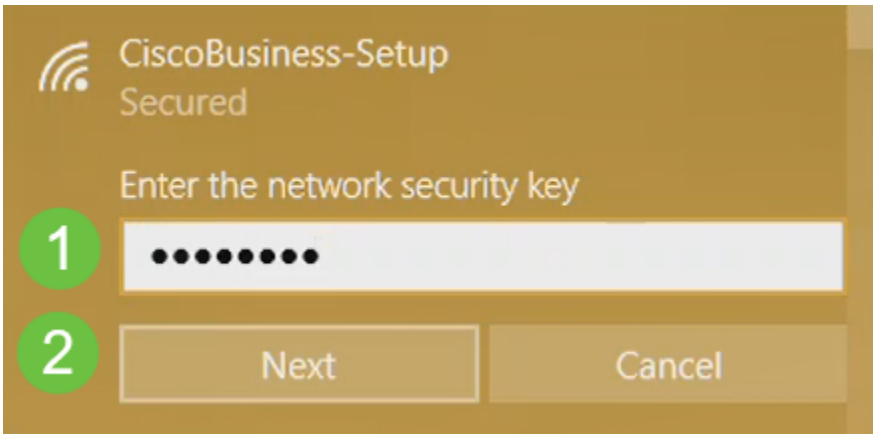
Klicken Sie auf Ihrem PC auf das **Wi-Fi-Symbol** und wählen Sie *CiscoBusiness-Setup* Wireless Network. Klicken Sie auf Verbinden.



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

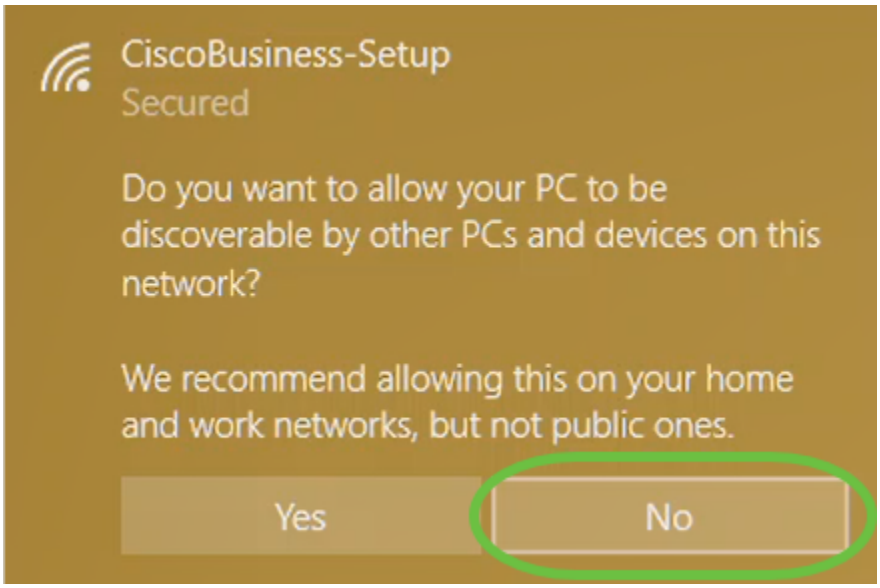
Schritt 2

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



Schritt 3

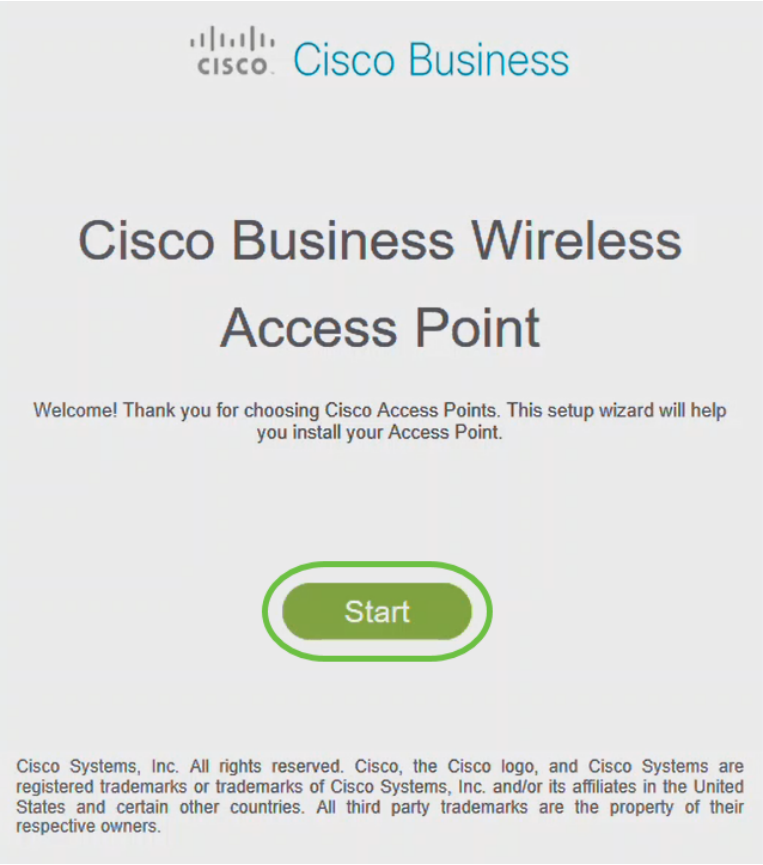
Sie erhalten den folgenden Bildschirm. Da immer nur ein Gerät konfiguriert werden kann, klicken Sie auf **Nein**.



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

Schritt 4

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



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

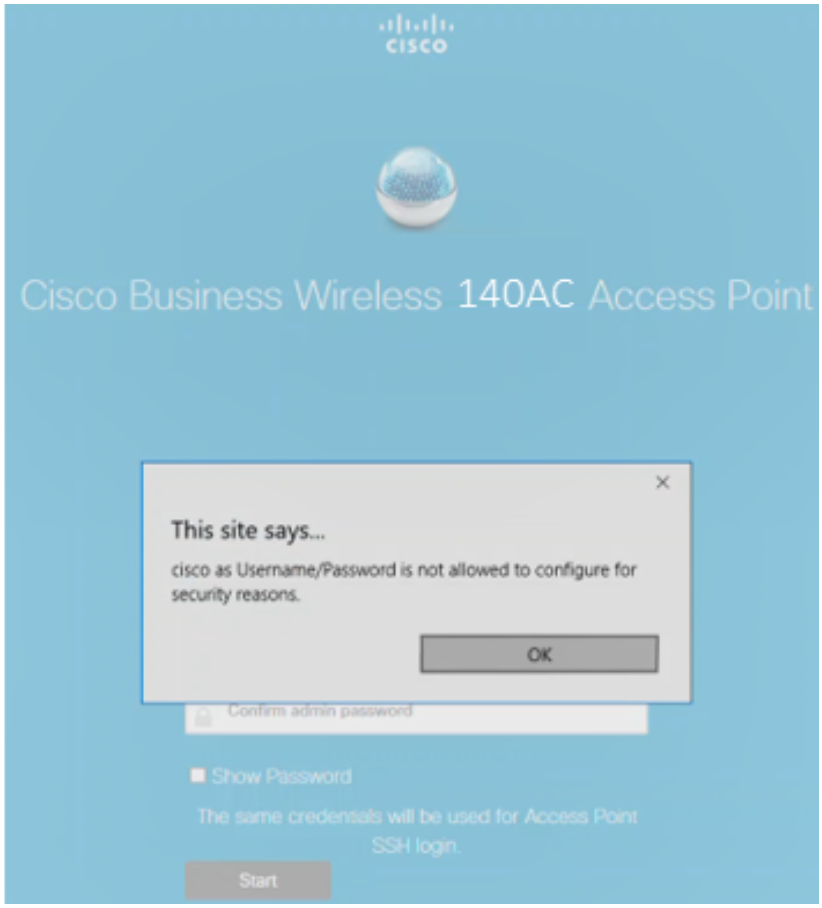
Schritt 5

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

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

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

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

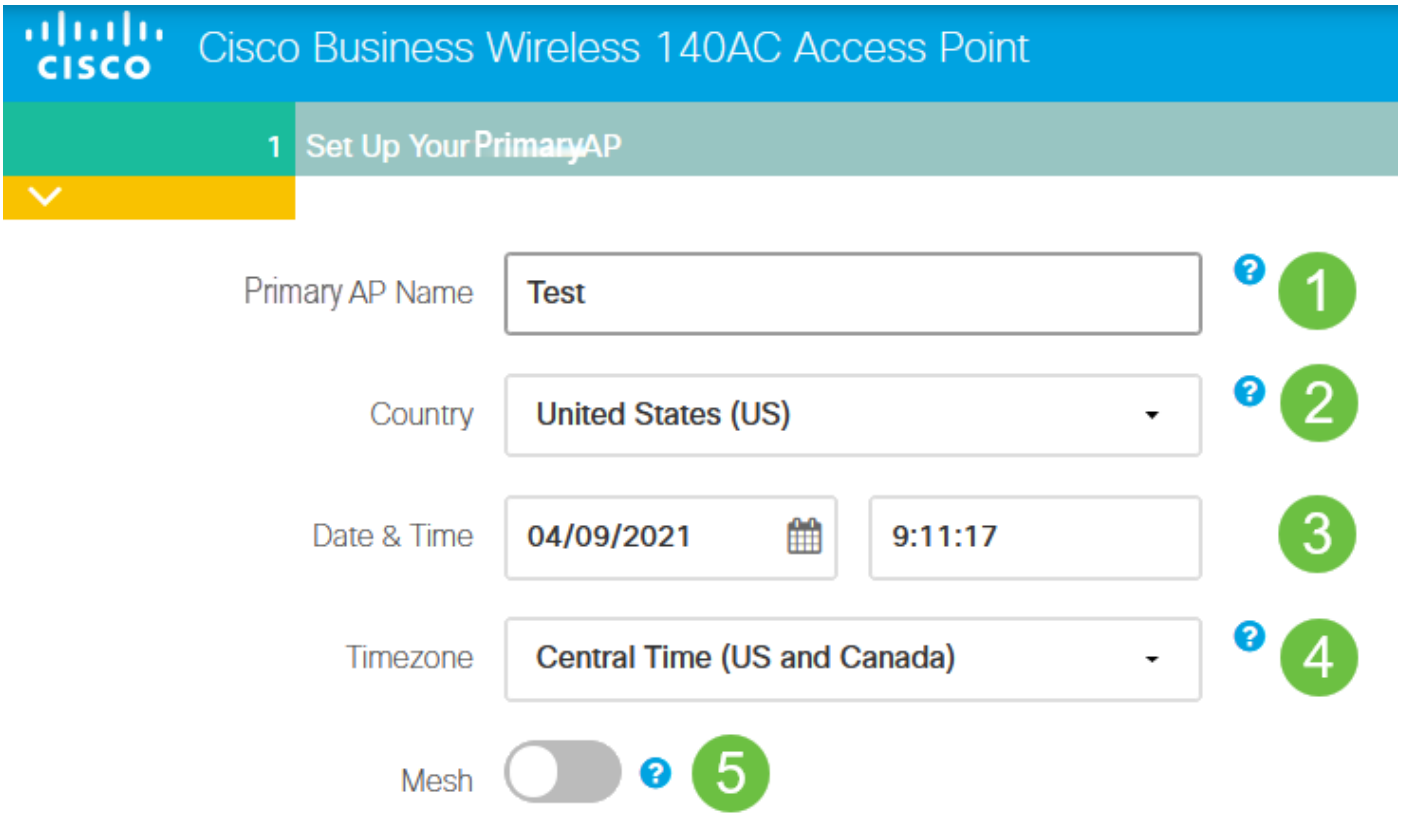


Schritt 6

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

- Primärer AP-Name

- Land
- Datum und Uhrzeit
- Zeitzone
- Mesh



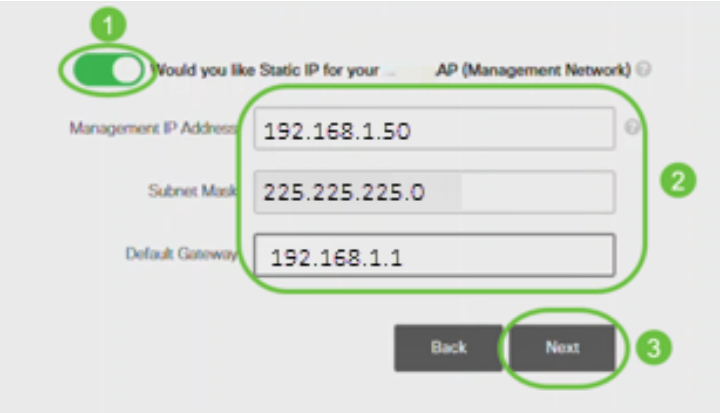
Mesh sollte nur aktiviert werden, wenn Sie ein Mesh-Netzwerk erstellen möchten. Standardmäßig ist sie deaktiviert.

Schritt 7

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

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

Klicken Sie auf **Weiter**.



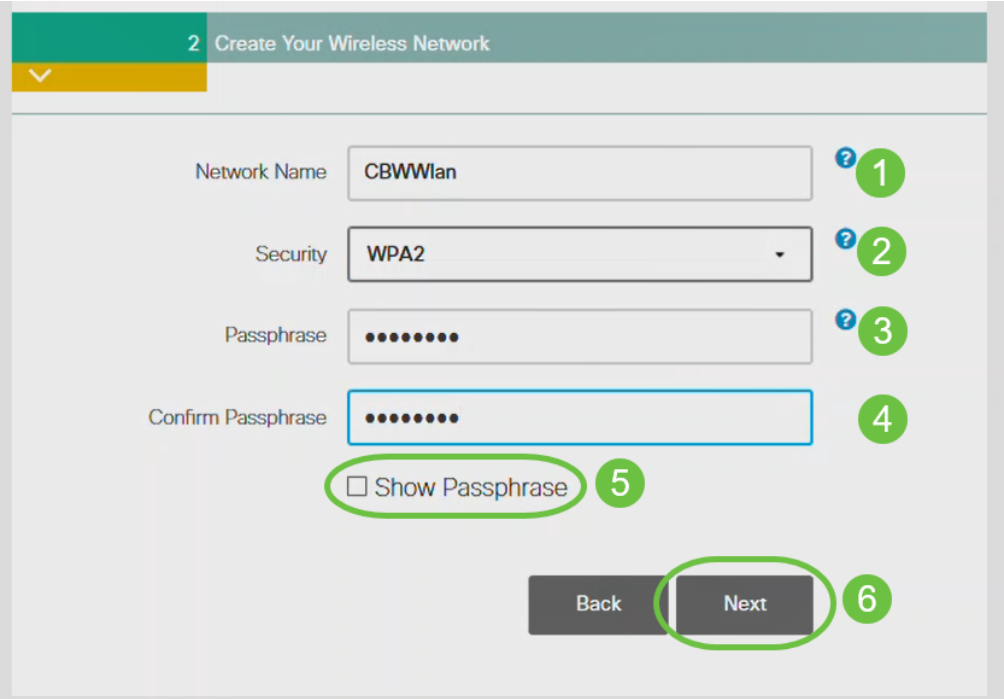
Diese Option ist standardmäßig deaktiviert.

Schritt 8

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

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

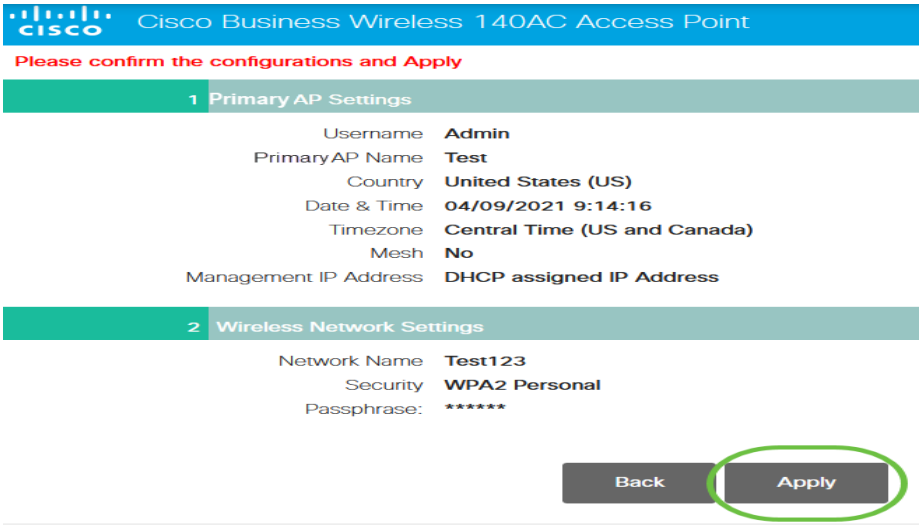
Klicken Sie auf **Weiter**.



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

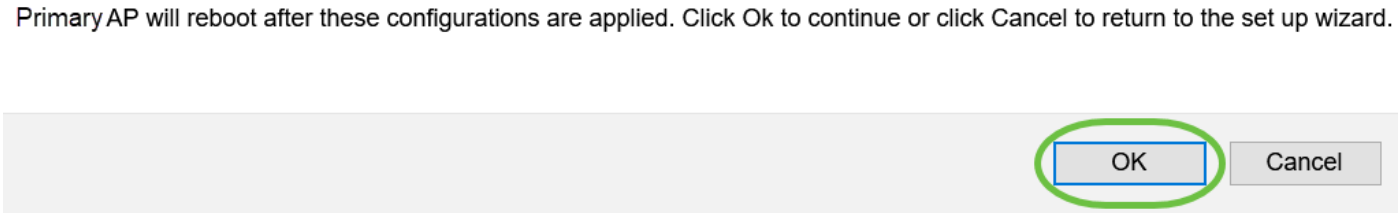
Schritt 9

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

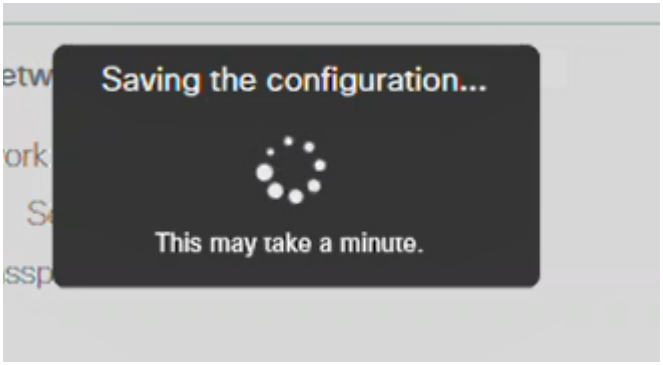


Schritt 10

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



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

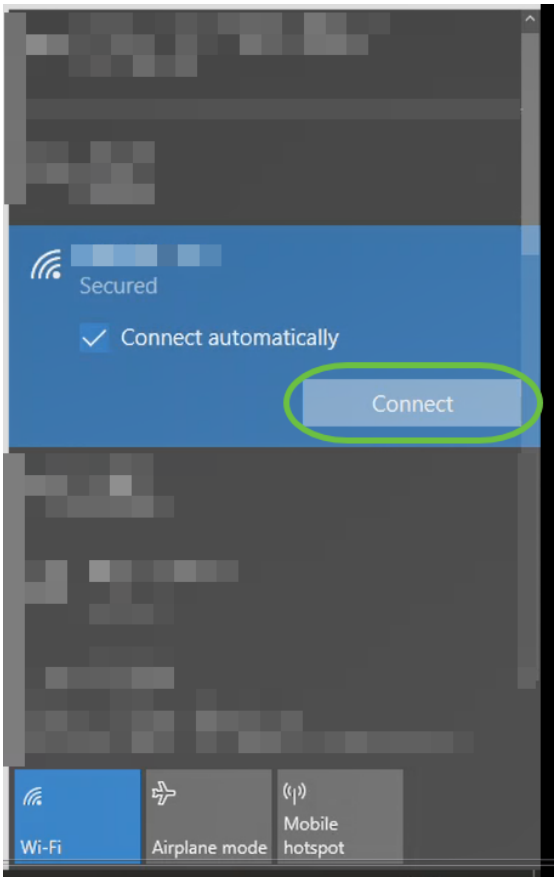


Während des Neustarts durchläuft die LED im Access Point mehrere Farbmuster. Wenn die LED grün blinkt, fahren Sie mit dem nächsten Schritt fort. Wenn die LED das rote Blinkmuster nicht überschreitet, weist dies darauf hin, dass kein DHCP-Server in Ihrem Netzwerk vorhanden ist. Stellen Sie sicher, dass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

Schritt 11

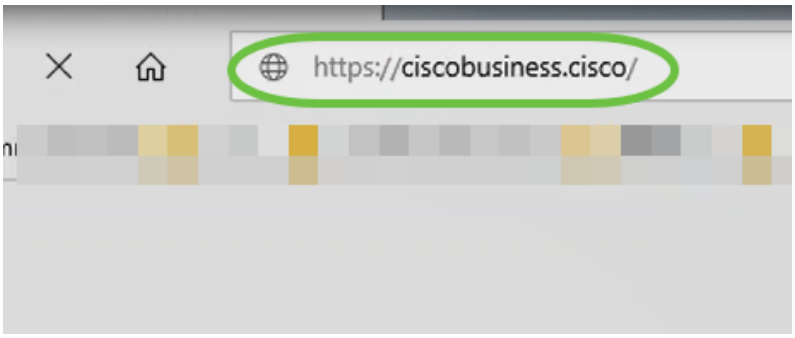
Gehen Sie zu den Wireless-Optionen auf Ihrem PC, und wählen Sie das Netzwerk aus, das Sie konfiguriert haben. Klicken Sie auf **Verbinden**.

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



Schritt 12

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



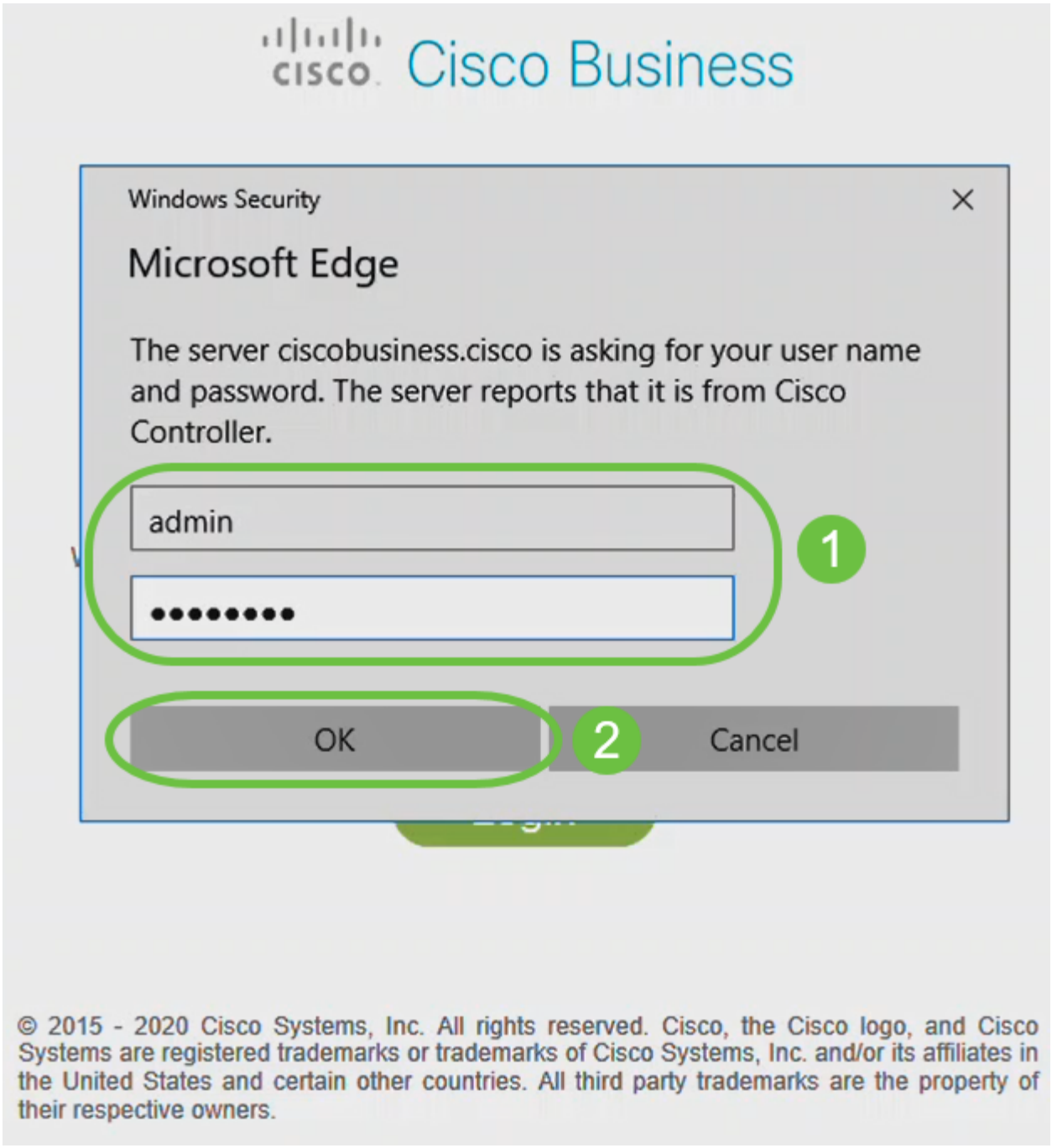
Stellen Sie sicher, dass Sie in diesem Schritt *https* und nicht *http* eingeben.

Schritt 13

Klicken Sie auf **Anmelden**.

Schritt 14

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



Schritt 15

Sie können auf die Webbenutzeroberflächenseite des Access Points zugreifen.

Tipps zur Wireless-Fehlerbehebung

Wenn Sie Probleme haben, lesen Sie die folgenden Tipps:

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

Konfigurieren der CBW142ACM-Mesh-Extender mithilfe der Webbenutzeroberfläche

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

Schritt 1

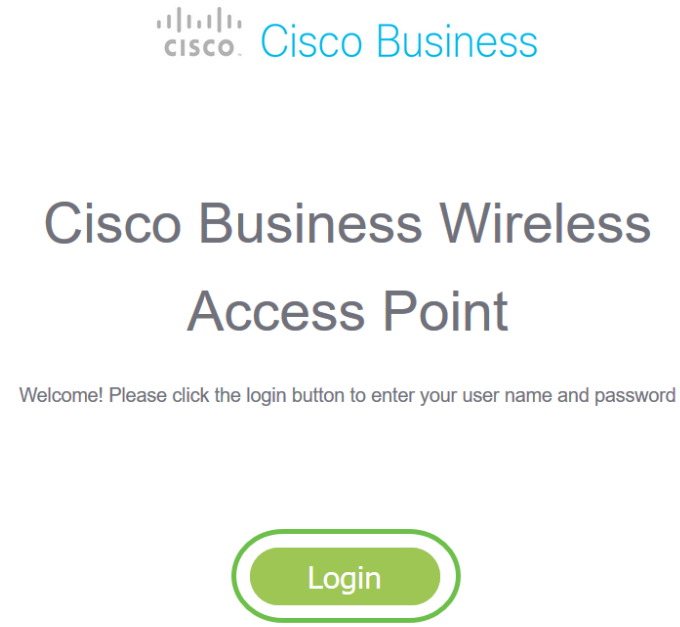
Schließen Sie die beiden Mesh-Extender an die Wand an den ausgewählten Standorten an. Notieren Sie die MAC-Adresse jedes Mesh-Extenders.

Schritt 2

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

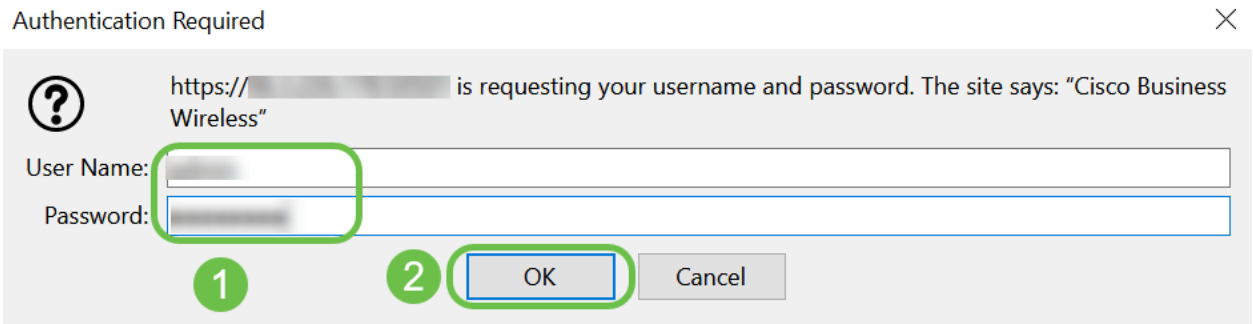
Schritt 3

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



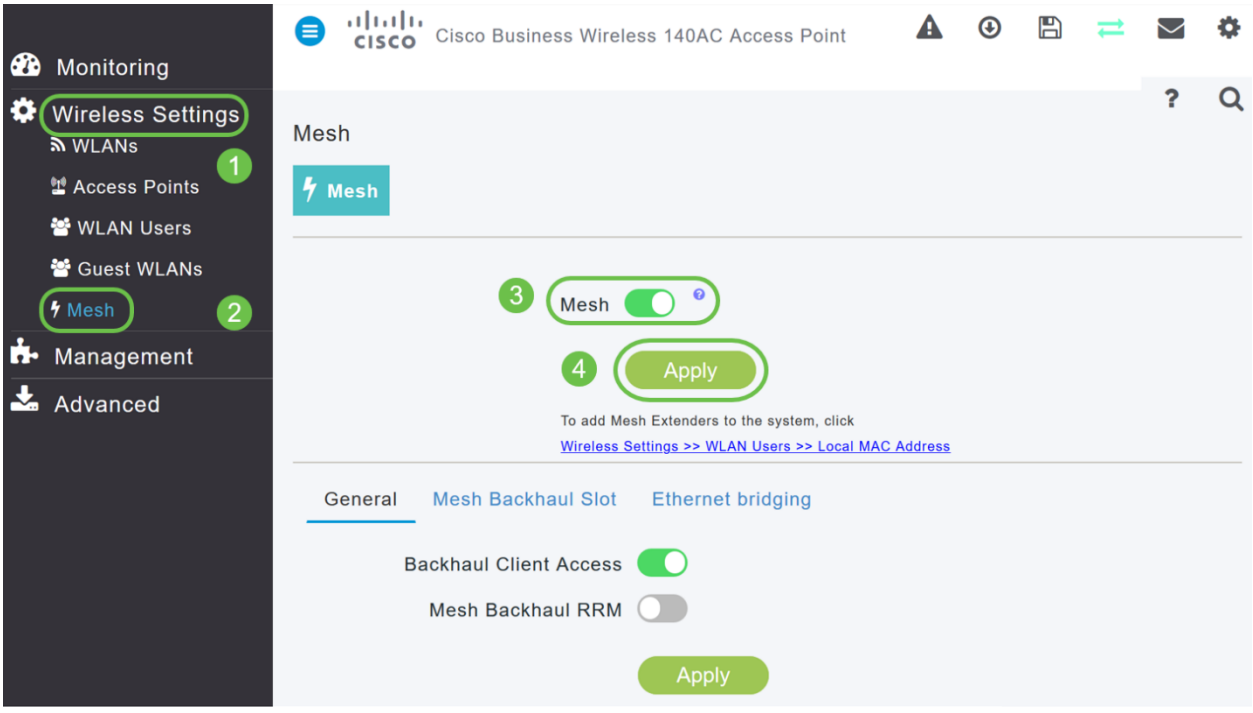
Schritt 4

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



Schritt 5

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

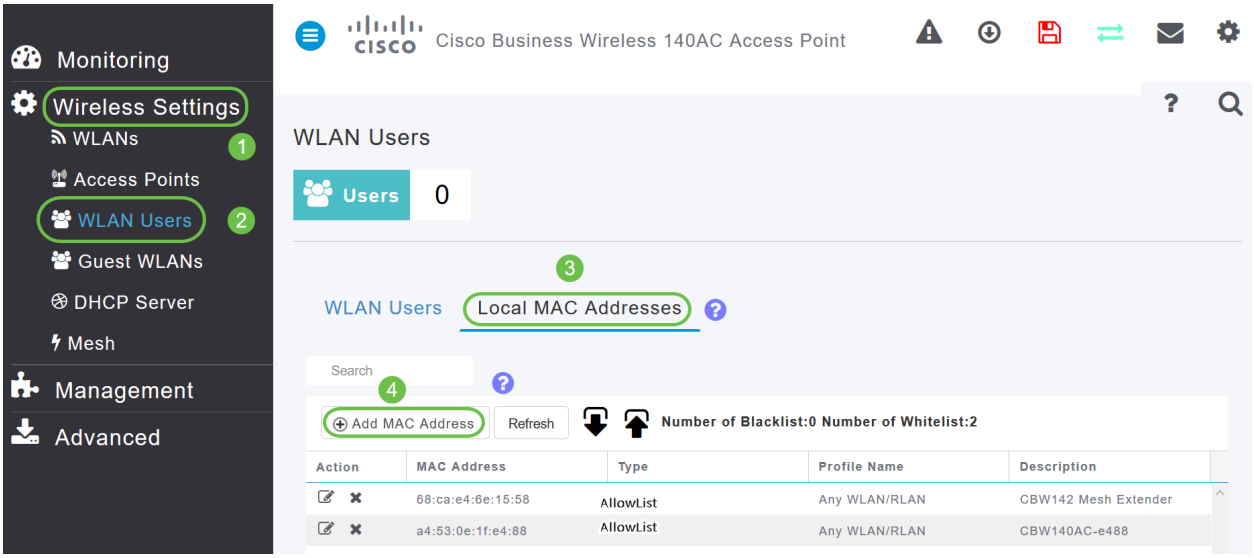


Schritt 6

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

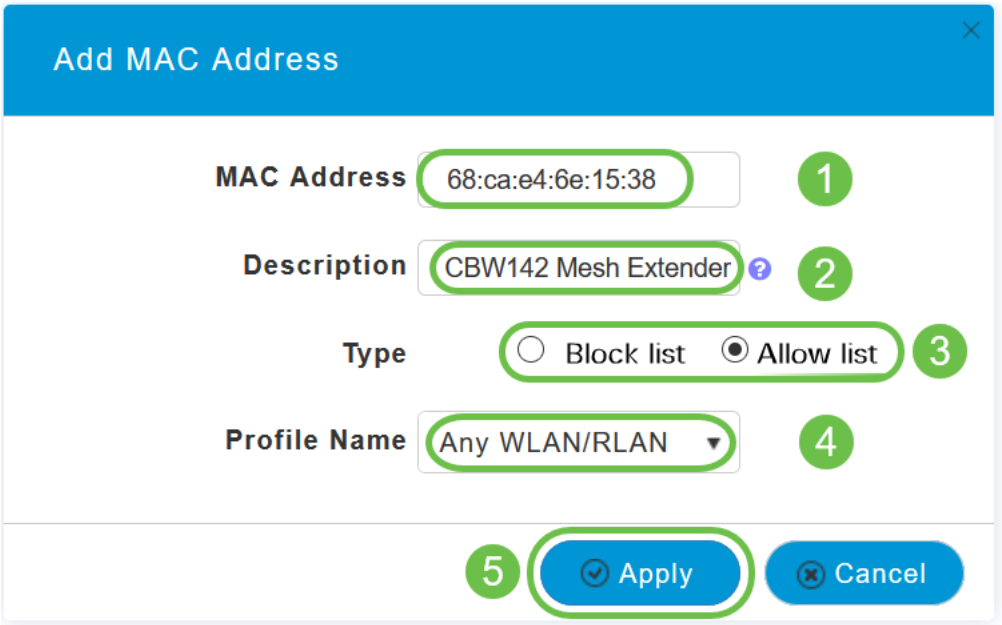
Schritt 7

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



Schritt 8

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



Schritt 9

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

Wiederholen Sie diese Schritte für jeden Mesh-Extender.

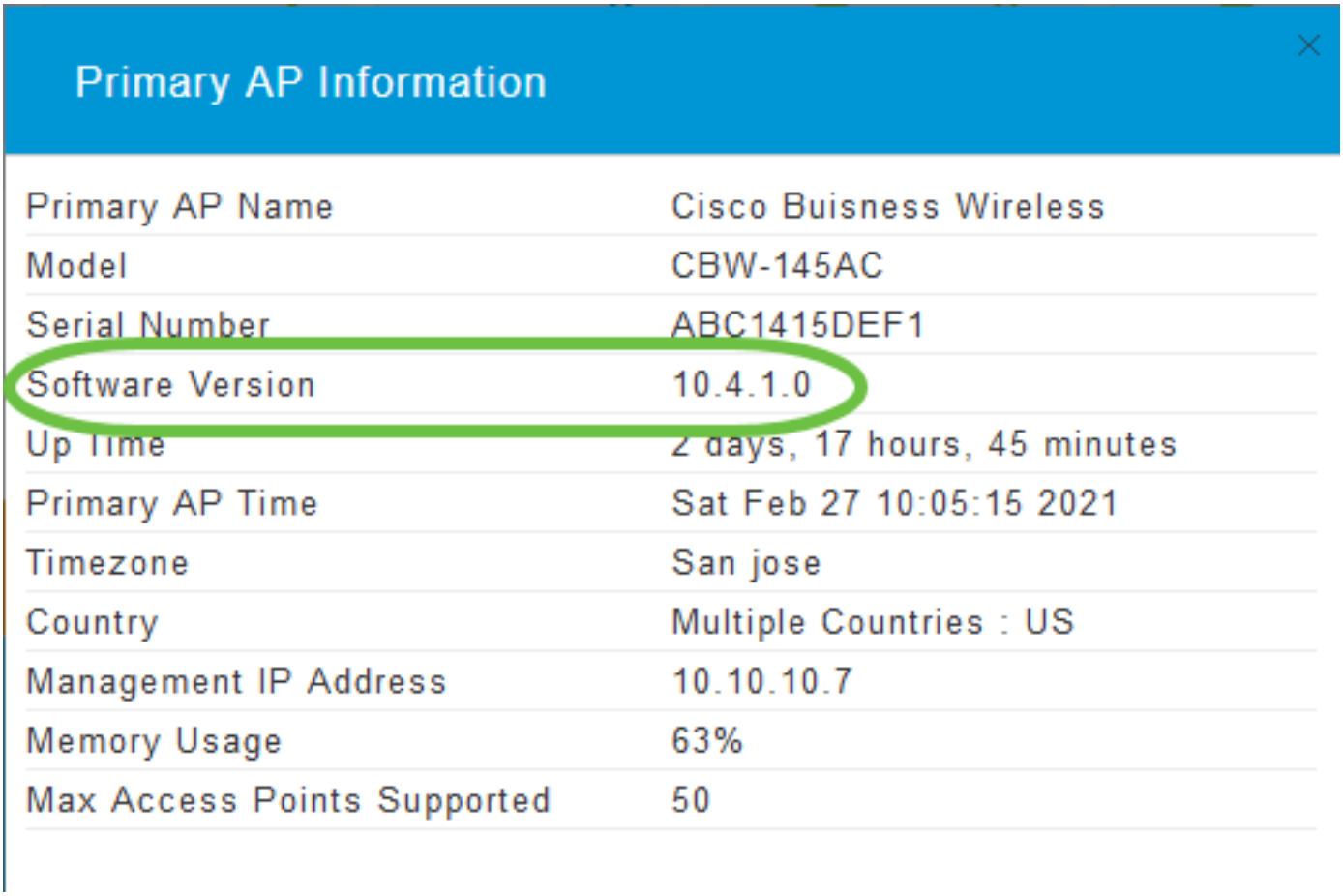
Überprüfen und Aktualisieren der Software mithilfe der Webbenutzeroberfläche

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

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

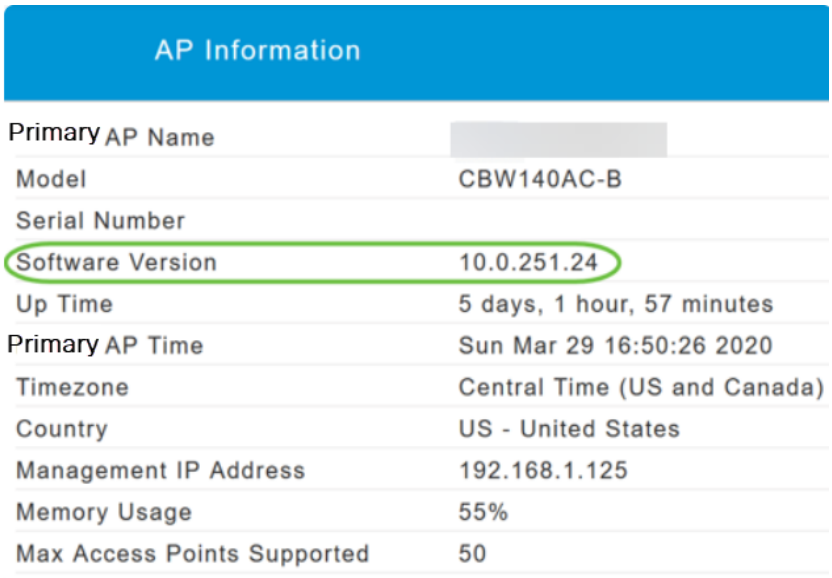
Schritt 1

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



Schritt 2

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



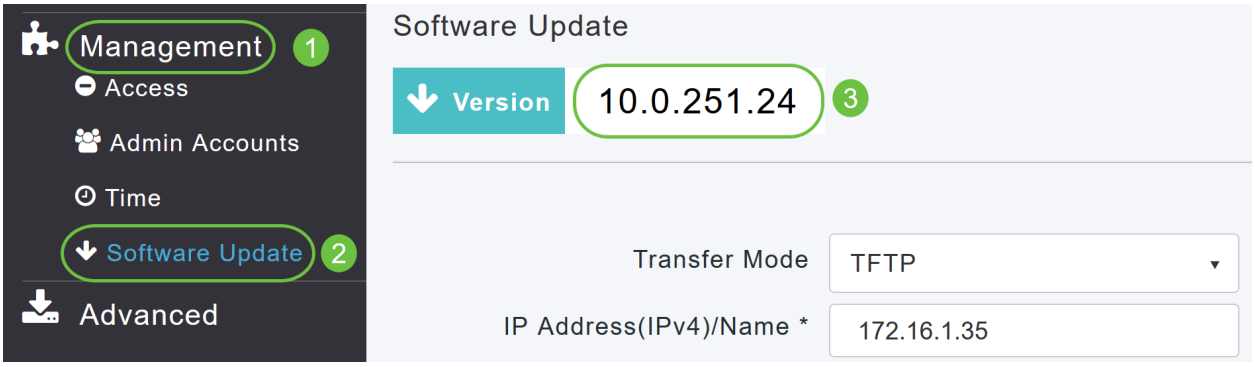
Wenn Sie die neueste Version der Software ausführen, können Sie zum Abschnitt Create WLANs (WLANs erstellen) springen.

Schritt 3

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

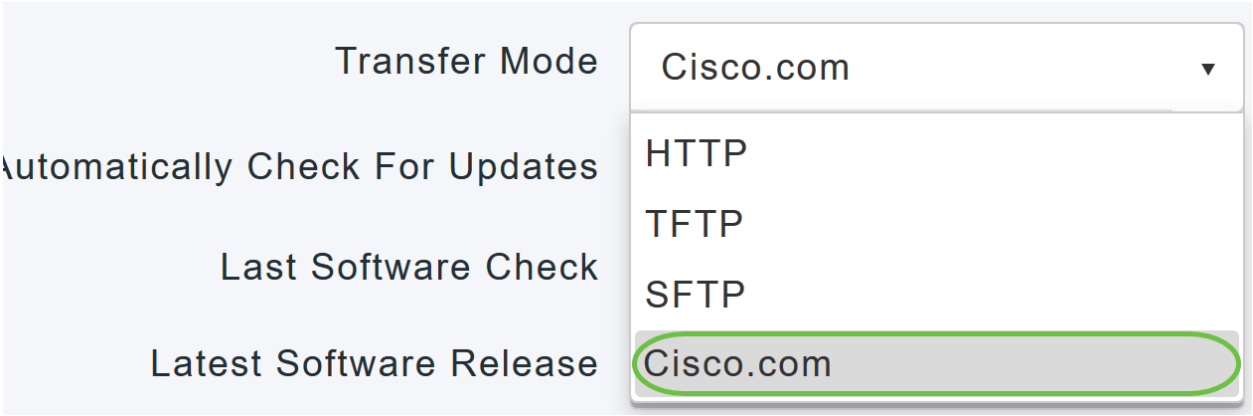
Das Fenster *Software Update* wird mit der aktuellen Softwareversionsnummer oben

angezeigt.



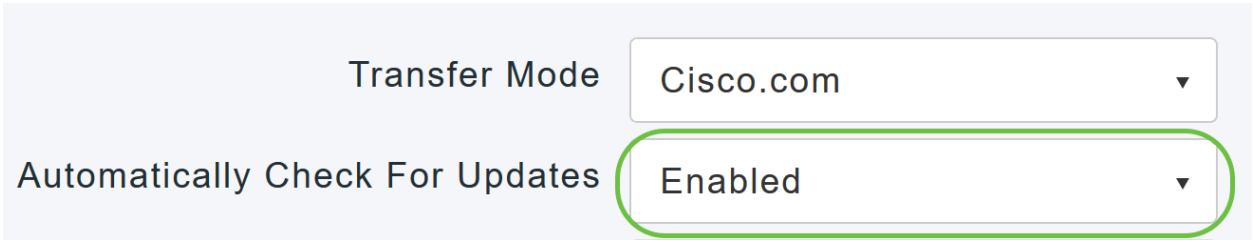
Sie können die CBW AP-Software aktualisieren, und die aktuellen Konfigurationen auf dem primären Access Point werden nicht gelöscht.

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



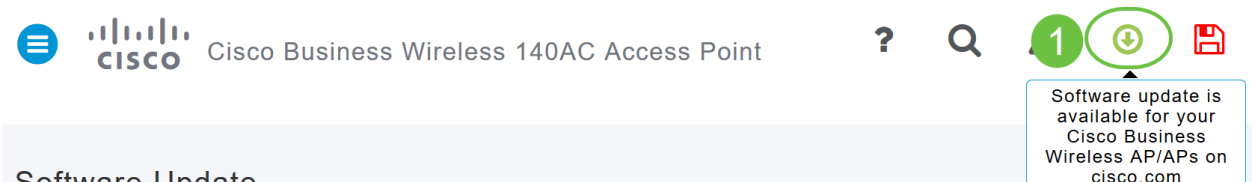
Schritt 4

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



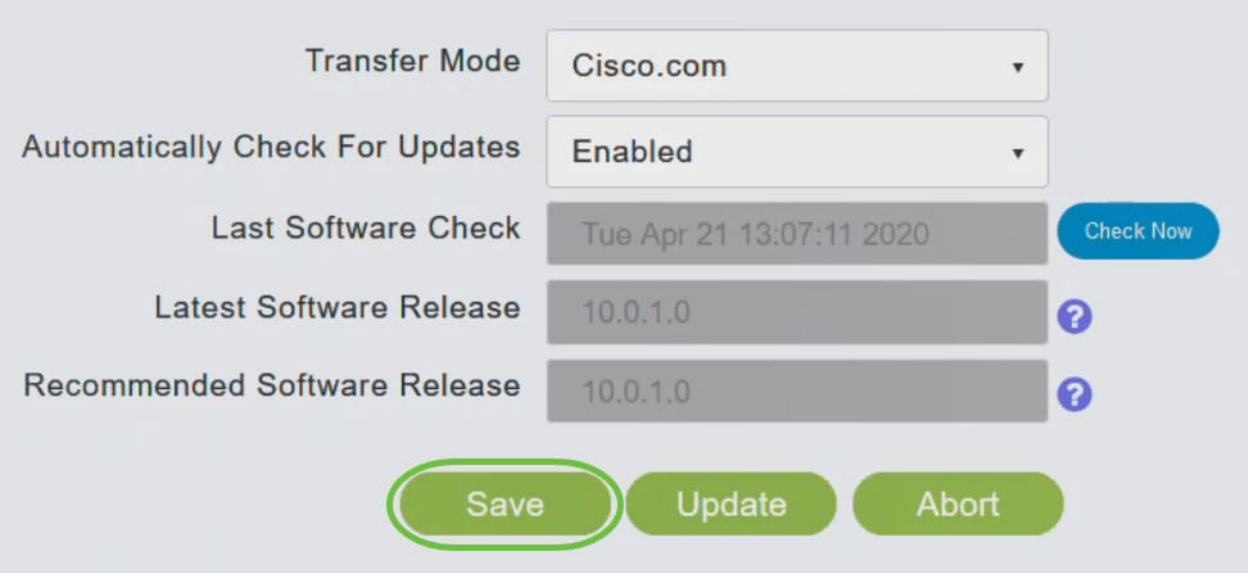
Wenn eine Softwareprüfung durchgeführt wird und eine neuere Aktualisierung der neuesten oder empfohlenen Software auf Cisco.com verfügbar ist, dann:

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

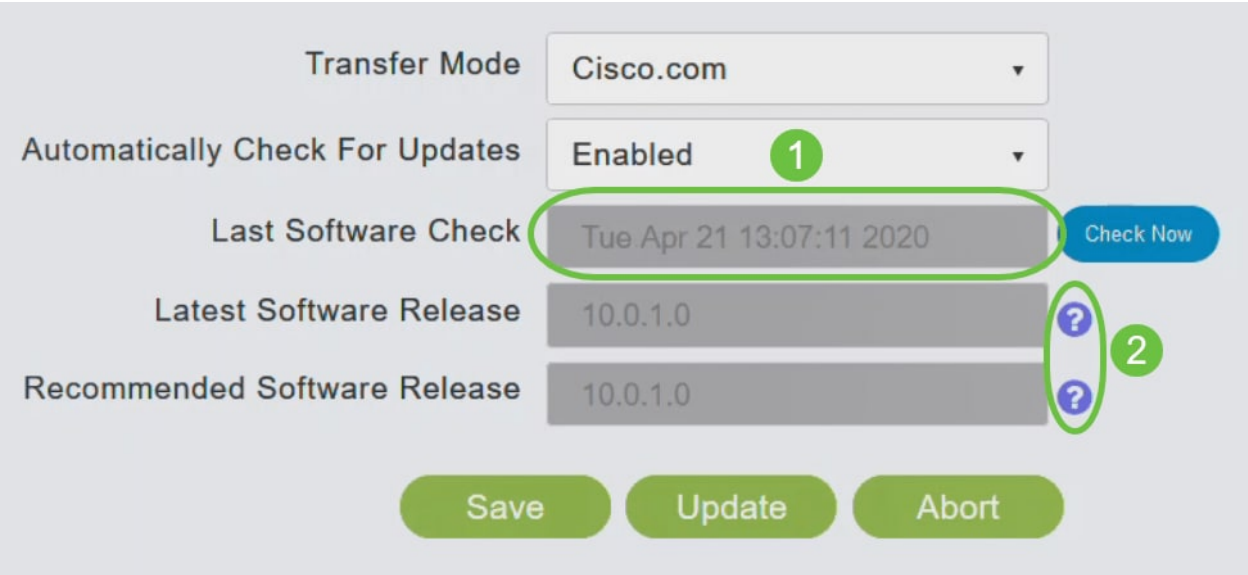


Schritt 5

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

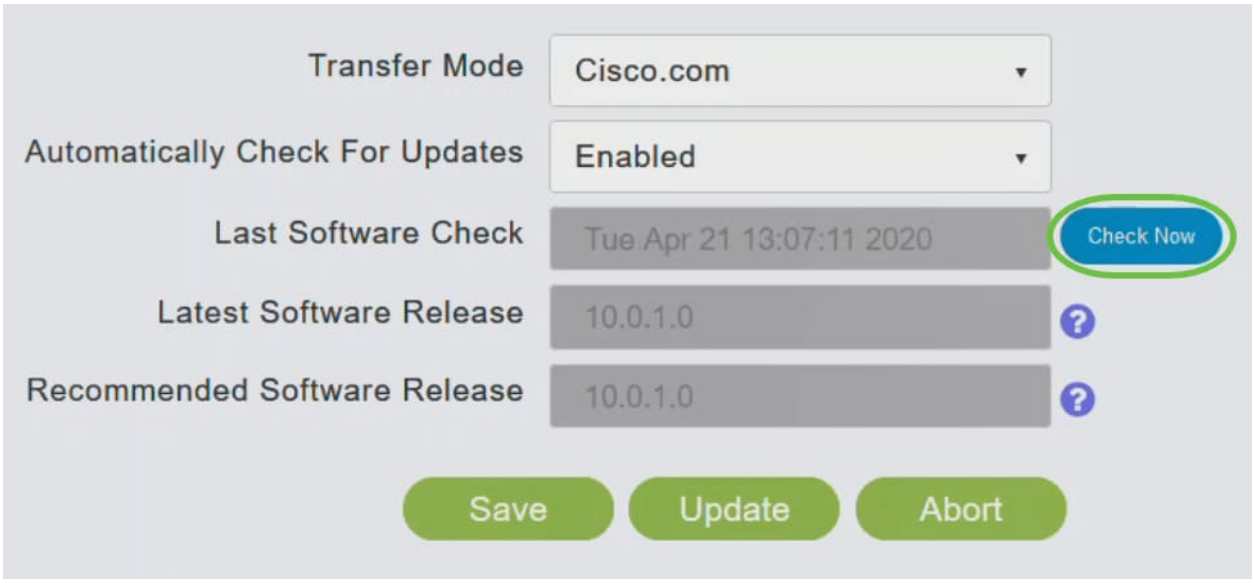


Im Feld *Letzte Softwareprüfung* wird der Zeitstempel der letzten automatischen oder manuellen Softwareprüfung angezeigt. Sie können die Notizen der angezeigten Versionen anzeigen, indem Sie auf das **Fragezeichen-Symbol** neben dem Symbol klicken.



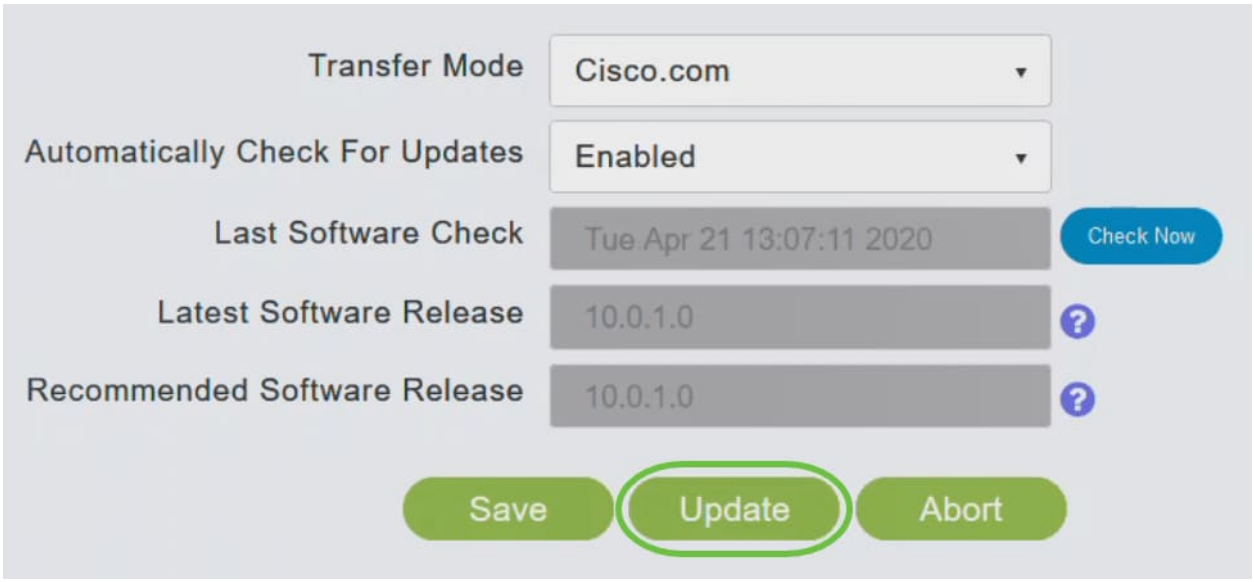
Schritt 6

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



Schritt 7

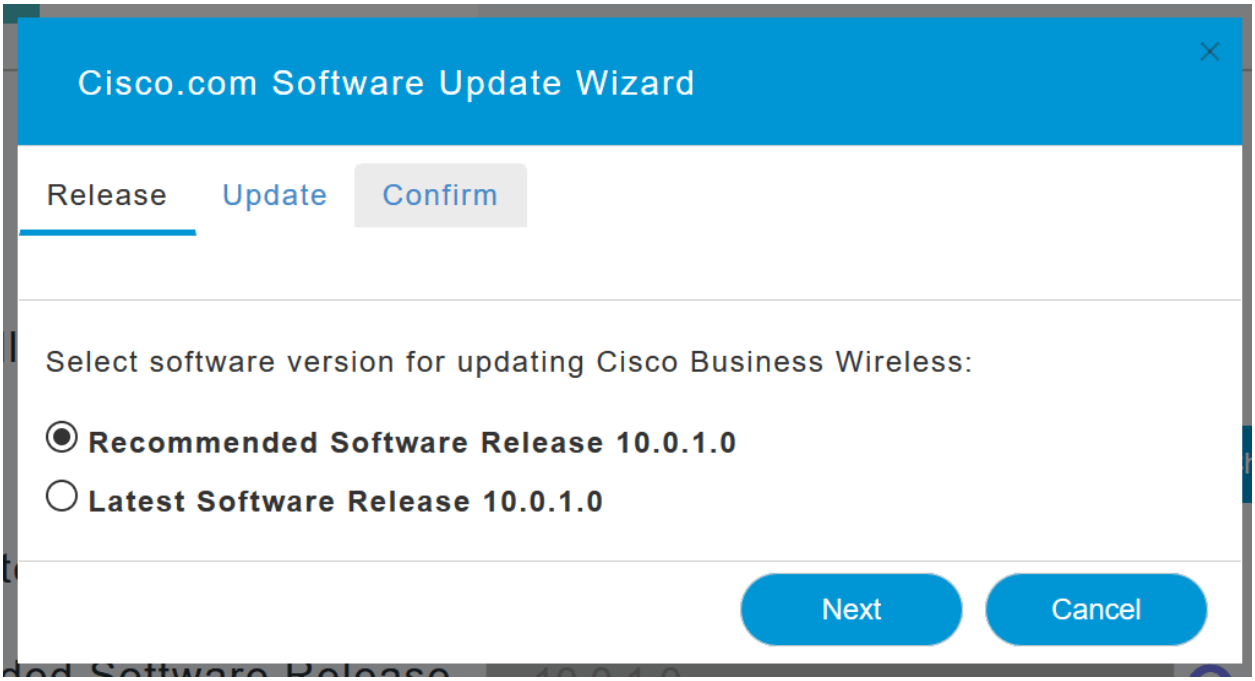
Um mit der Softwareaktualisierung fortzufahren, klicken Sie auf **Aktualisieren**.



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

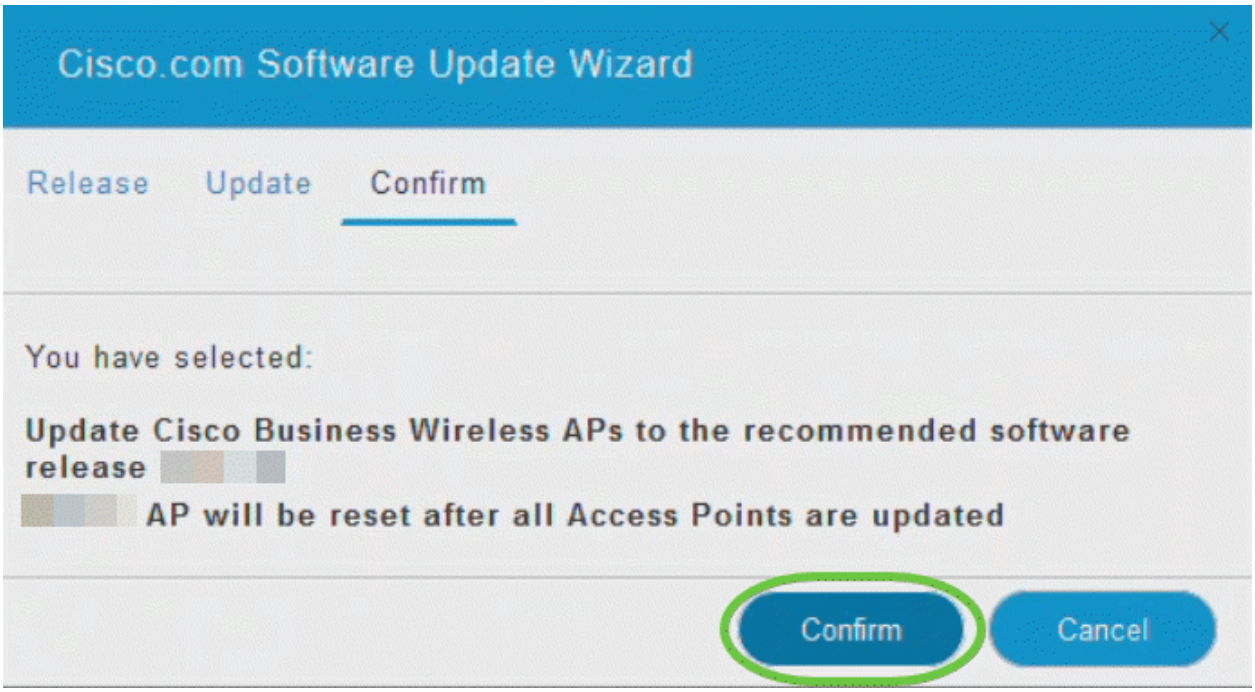
- Registerkarte "Version": Geben Sie an, ob Sie auf die empfohlene Softwareversion oder die neueste Softwareversion aktualisieren möchten.
- Registerkarte "Aktualisieren": Geben Sie an, wann die Access Points zurückgesetzt werden sollen. Sie können entweder sofort entscheiden, ob Sie den Vorgang abschließen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

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



Schritt 8

Klicken Sie auf **Bestätigen**.

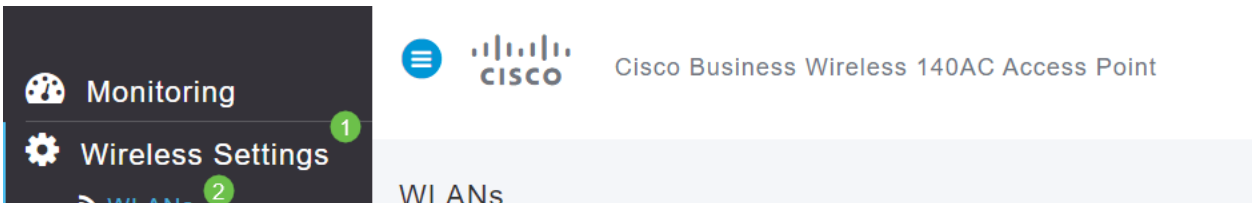


Erstellen von WLANs auf der Webbenutzeroberfläche

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

Schritt 1

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



Schritt 2

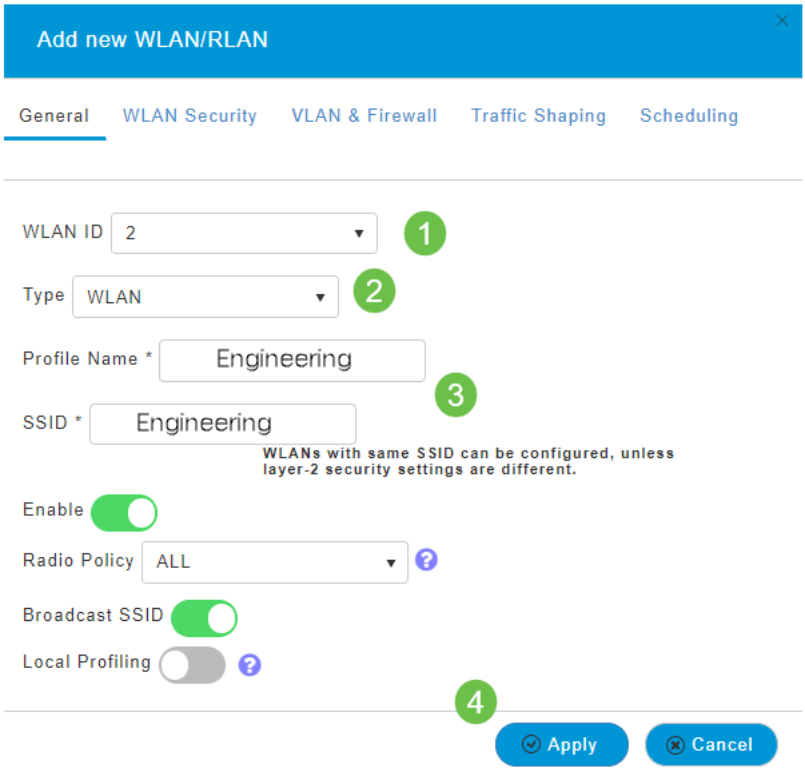
Geben Sie auf der Registerkarte *Allgemein* die folgenden Informationen ein:

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

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

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

Klicken Sie auf Apply (Anwenden).



Schritt 3

Sie gelangen zur Registerkarte *WLAN-Sicherheit*.

In diesem Beispiel wurden die folgenden Optionen als Standard beibehalten:

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

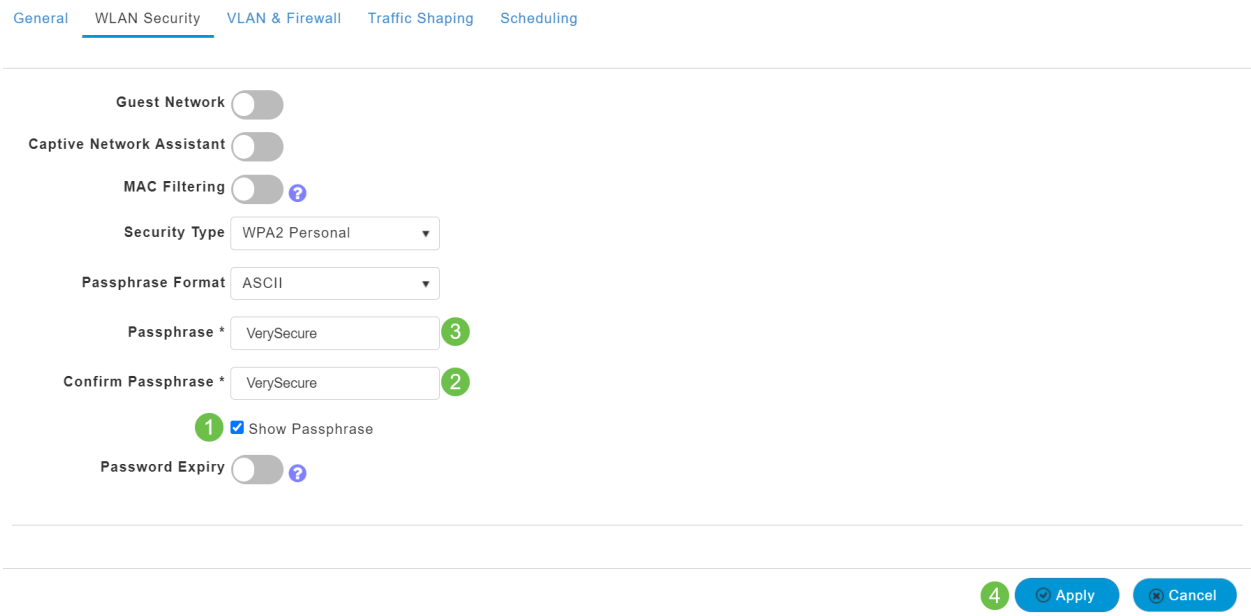
WPA2 Personal ist eine Methode zur Sicherung Ihres Netzwerks mithilfe einer PSK-Authentifizierung. Der PSK wird sowohl auf dem primären Access Point, unter der WLAN-Sicherheitsrichtlinie als auch auf dem Client separat konfiguriert. WPA2 Personal verlässt sich nicht auf einen Authentifizierungsserver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

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

In diesem Szenario wurden die folgenden Felder eingegeben:

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

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

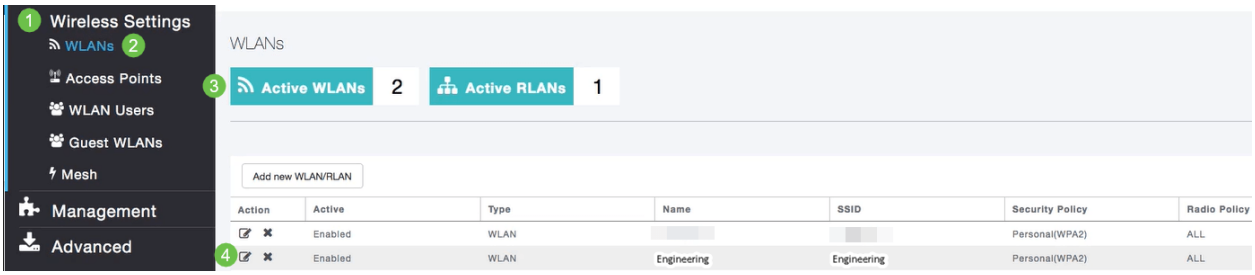


Schritt 4

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

Schritt 5

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



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

Optionale Wireless-Konfigurationen

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

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

Erstellen eines Gast-WLAN mithilfe der Webbenutzeroberfläche (optional)

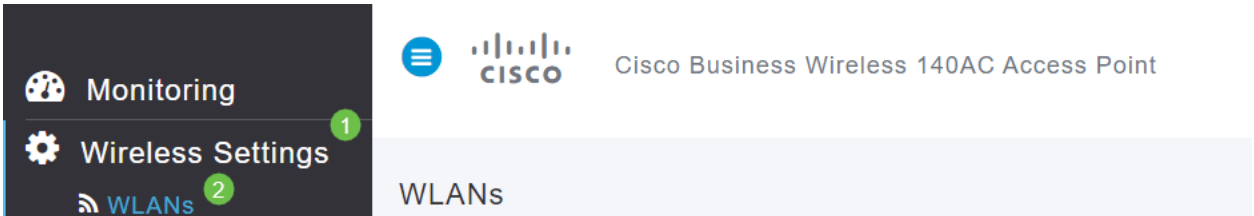
Ein Gast-WLAN bietet Gastzugriff auf Ihr Cisco Business Wireless-Netzwerk.

Schritt 1

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

Schritt 2

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



Schritt 3

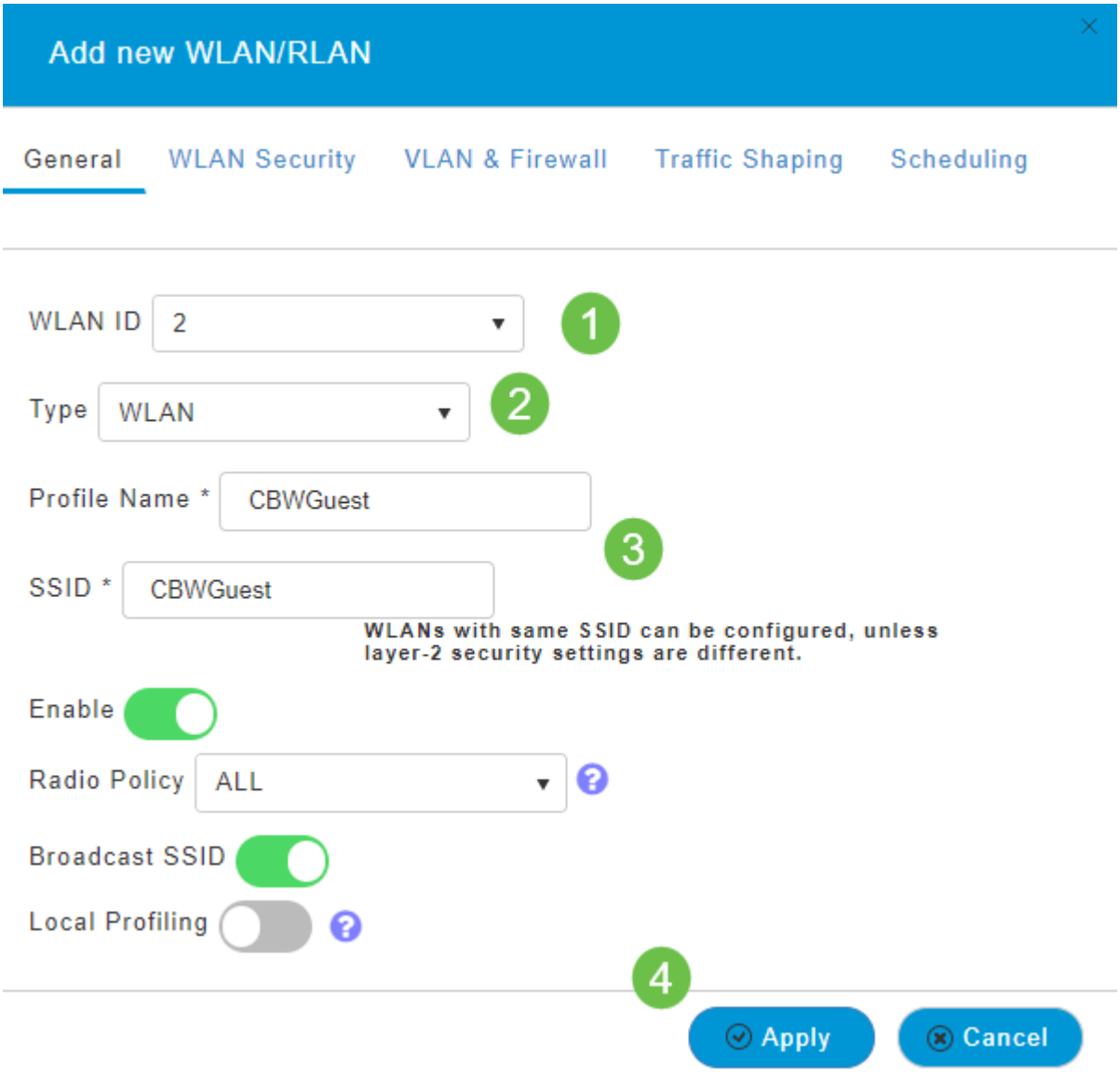
Geben Sie auf der Registerkarte *Allgemein* die folgenden Informationen ein:

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

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

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

Klicken Sie auf Apply (Anwenden).

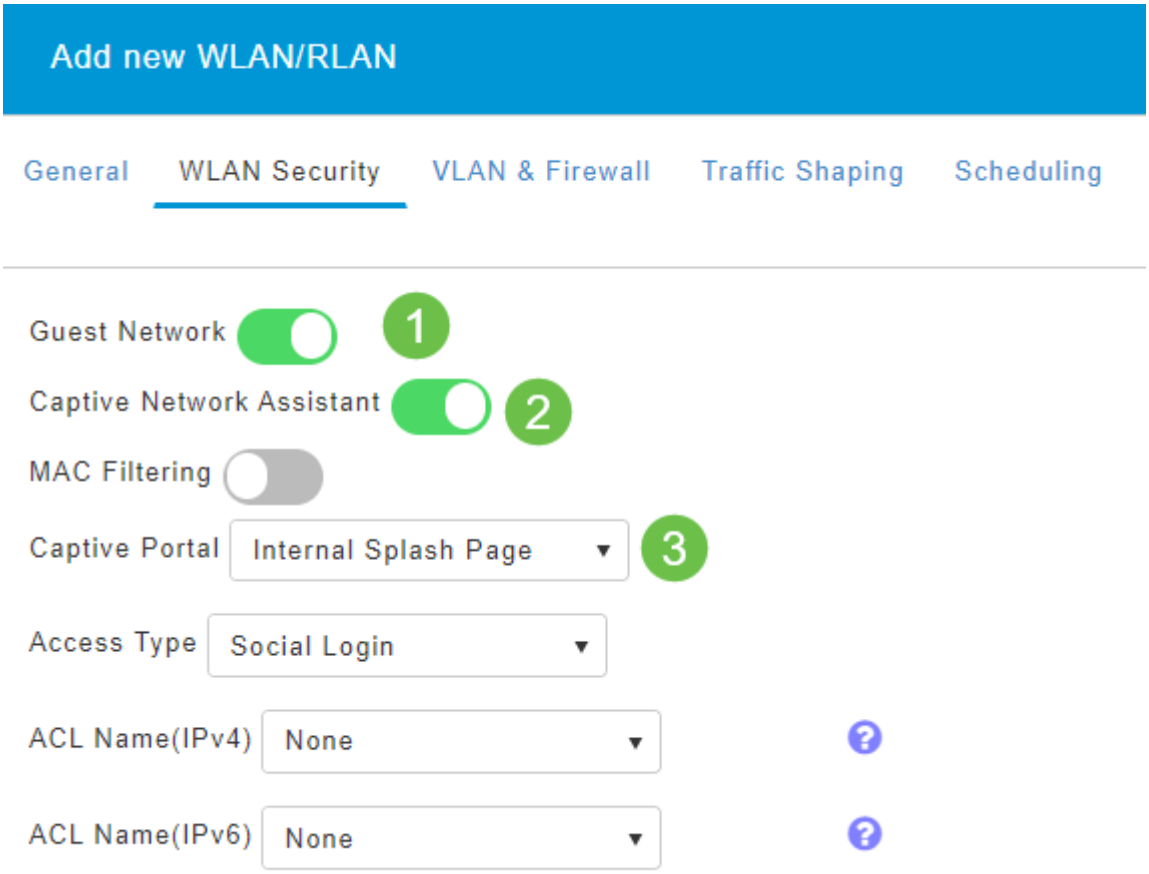


Schritt 4

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

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

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



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

Schritt 5

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

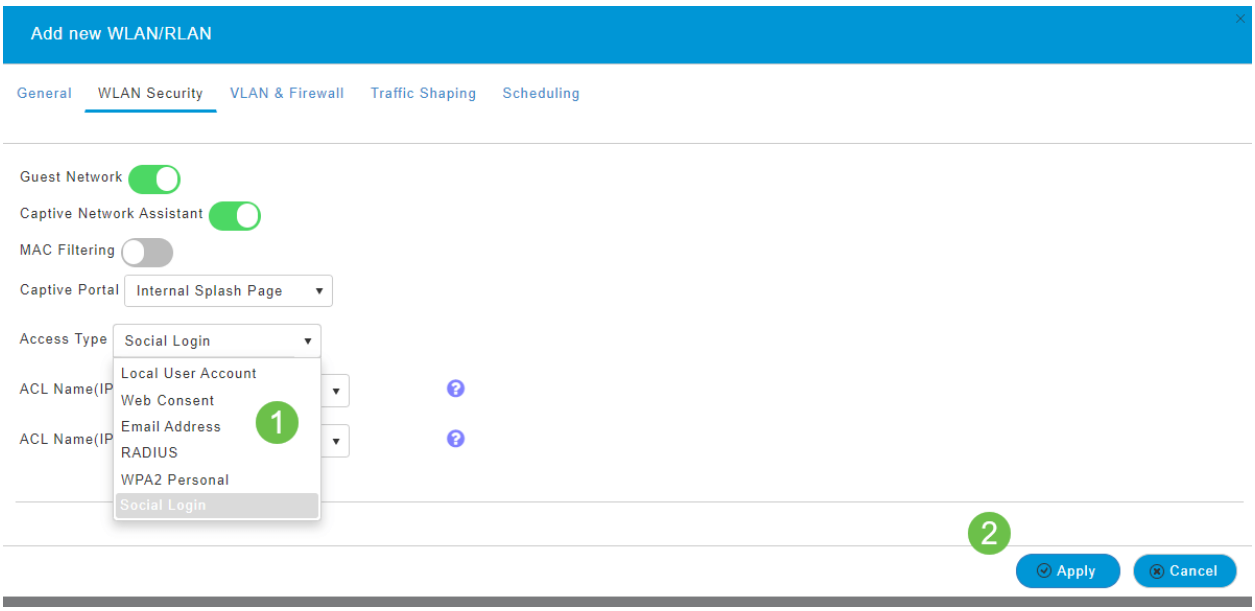
Weitere Optionen für den *Zugriffstyp* sind:

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

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

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

Klicken Sie auf Apply (Anwenden).



Schritt 6

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

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

Erstellen von Anwendungsprofilen mithilfe der Webbenutzeroberfläche (optional)

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

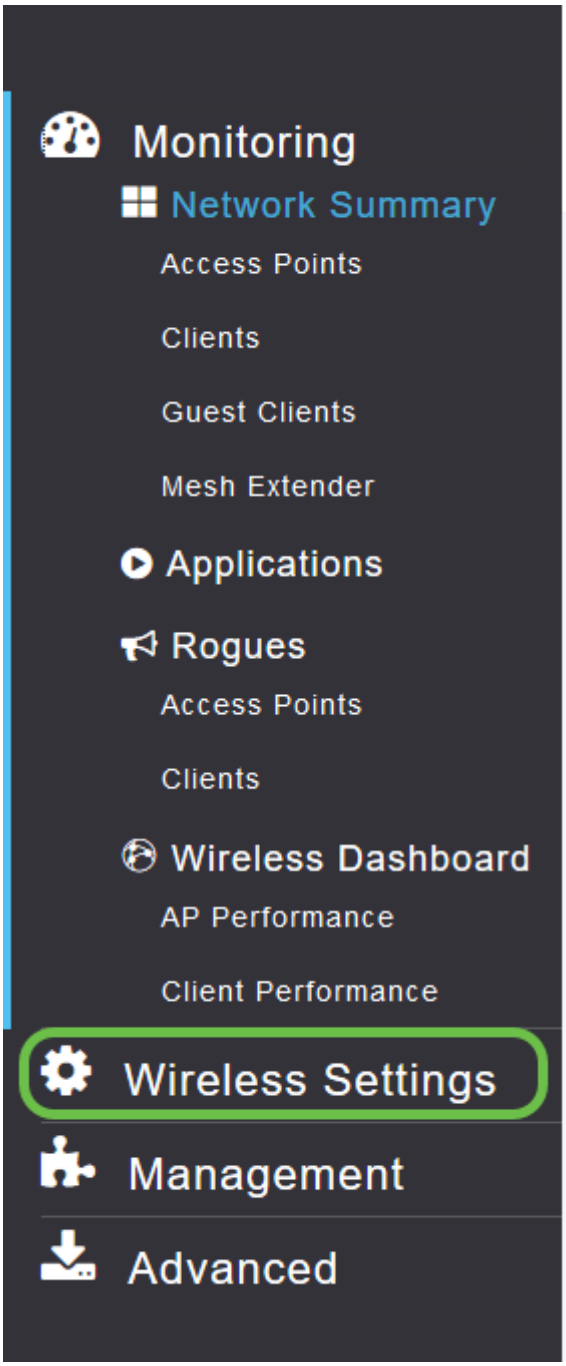
leiten, ähnlich wie ein Flussdiagramm. Weitere Richtlinienfunktionen sind Gastzugriff, Zugriffskontrolllisten und QoS.

Schritt 1

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

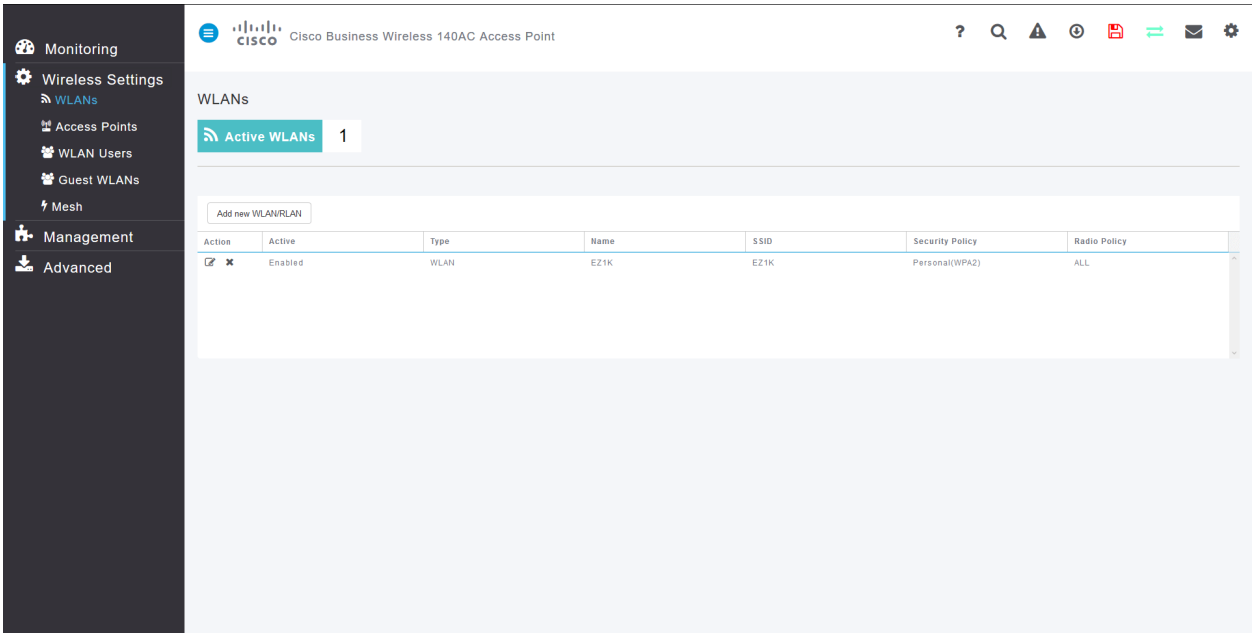
Schritt 2

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



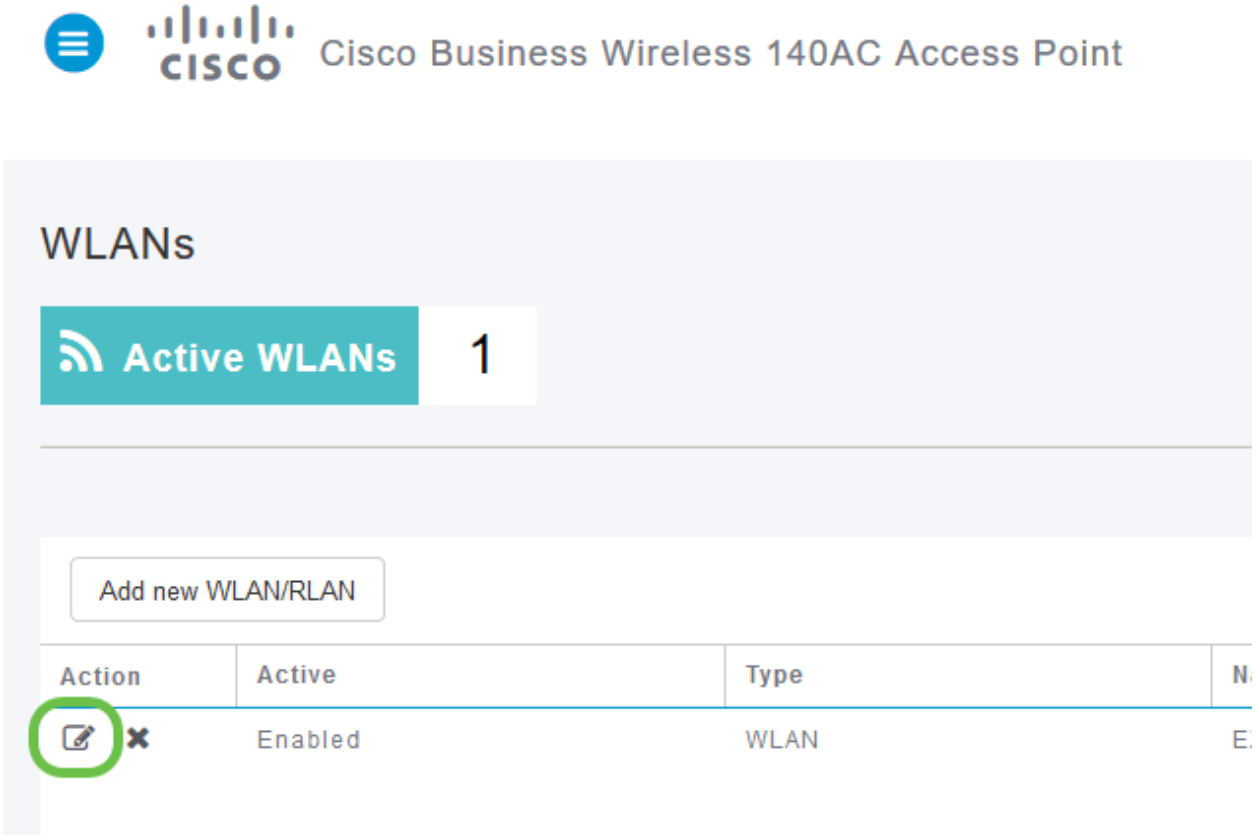
Das Bild unten ähnelt dem Bild, das Sie sehen, wenn Sie auf den Link Wireless

Settings (Wireless-Einstellungen) klicken.

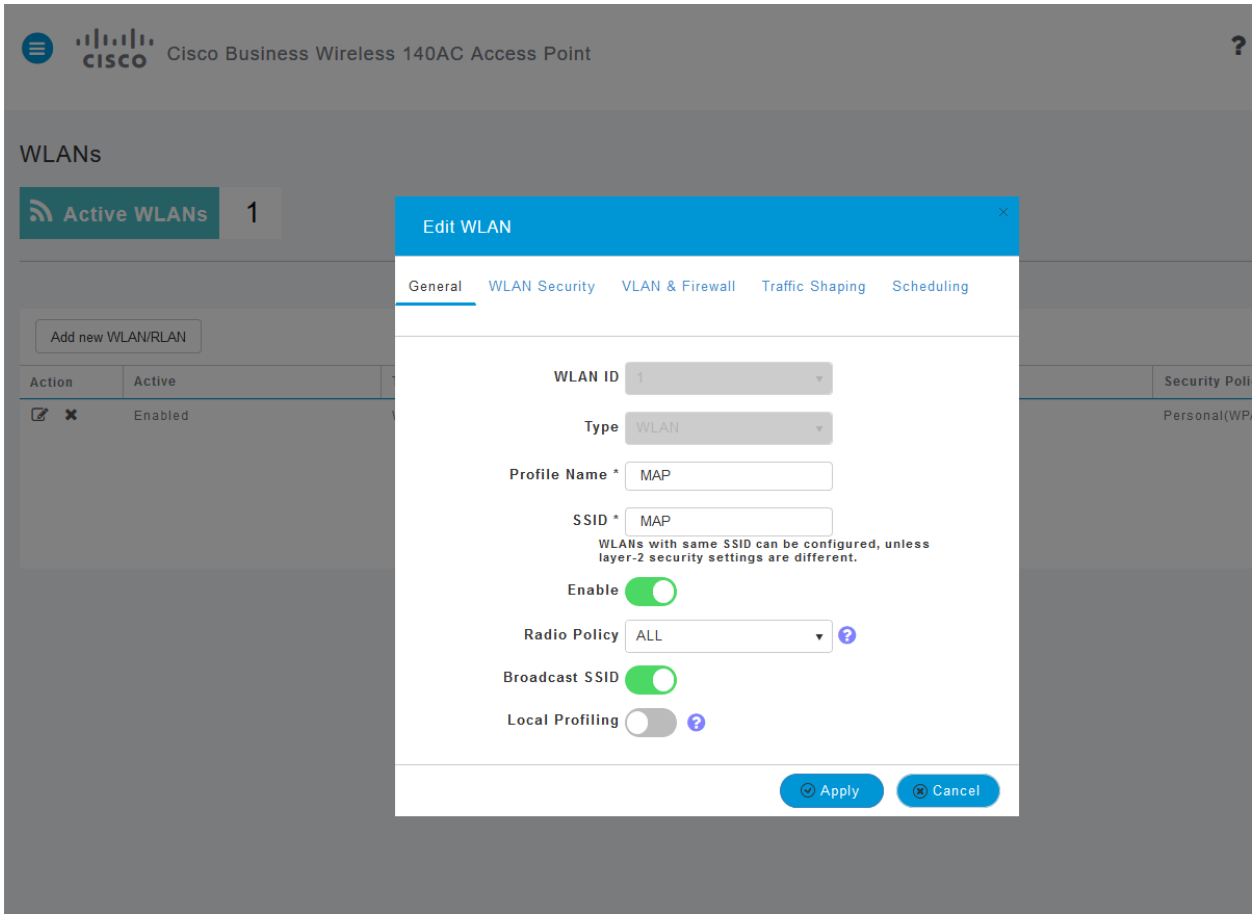


Schritt 3

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

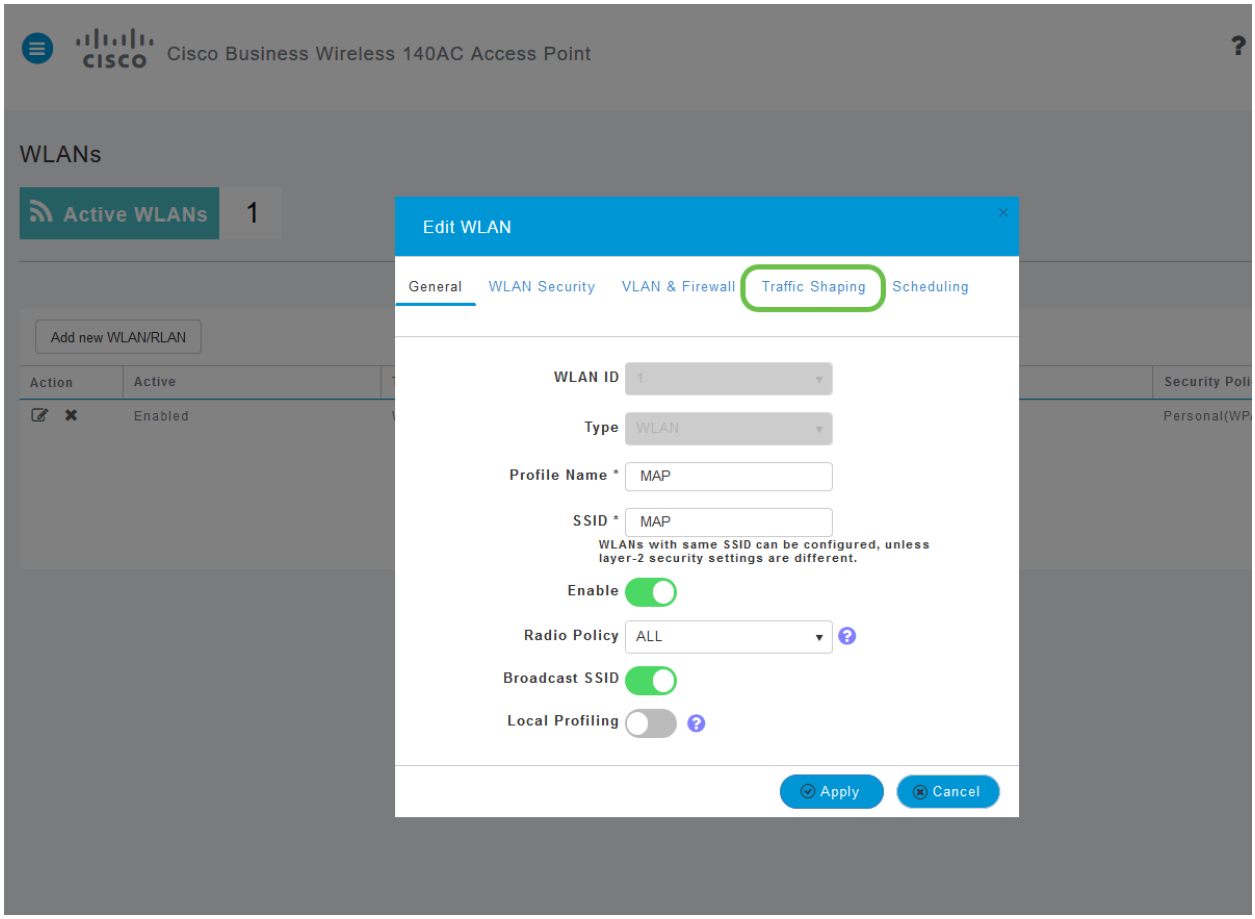


Da Sie vor kurzem das WLAN hinzugefügt haben, wird Ihre Seite *Edit WLAN* wie folgt angezeigt:

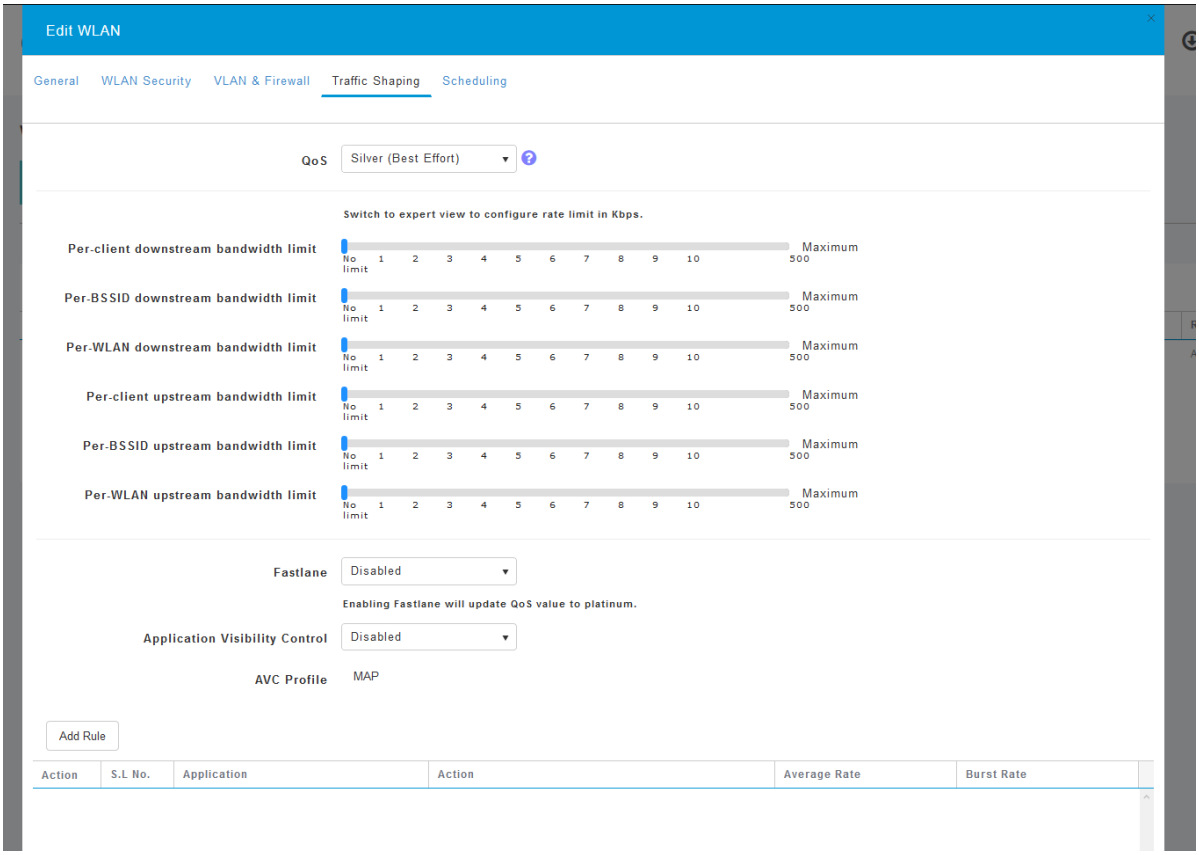


Schritt 4

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

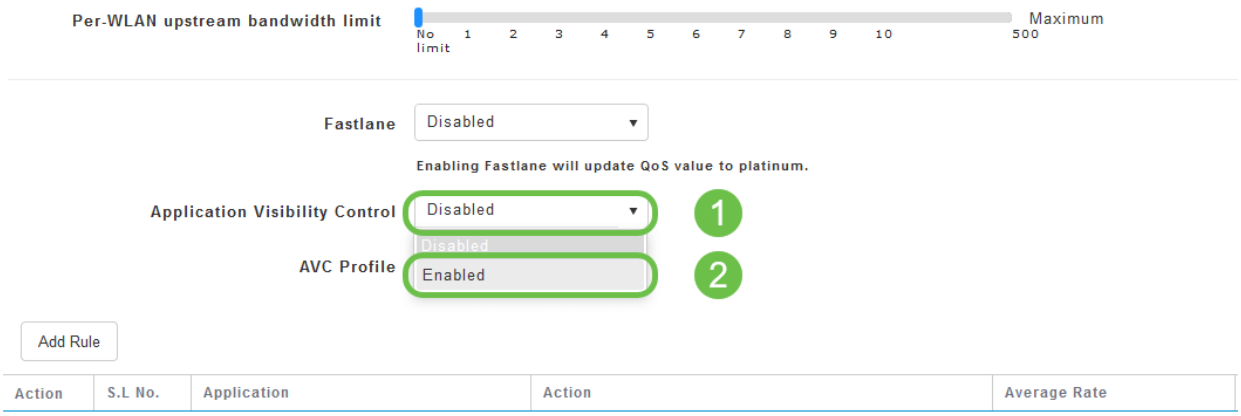


Ihr Bildschirm wird möglicherweise wie folgt angezeigt:



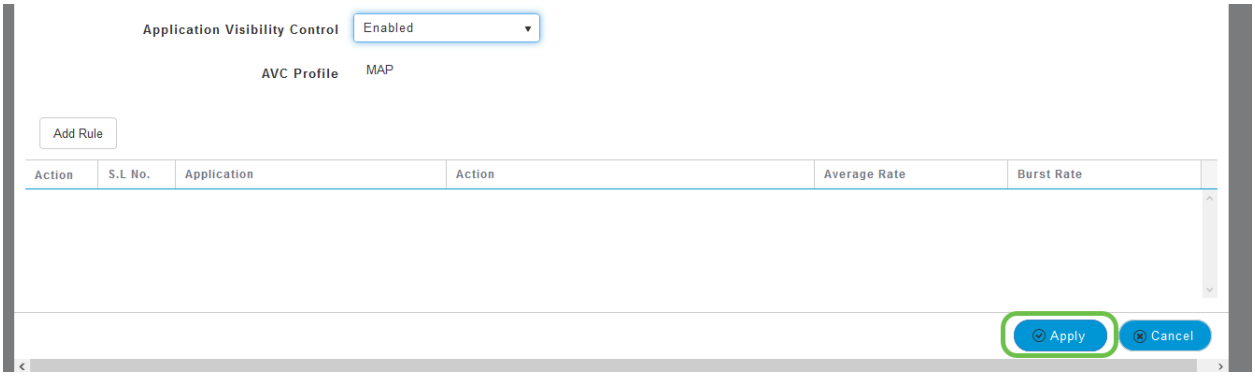
Schritt 5

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



Schritt 6

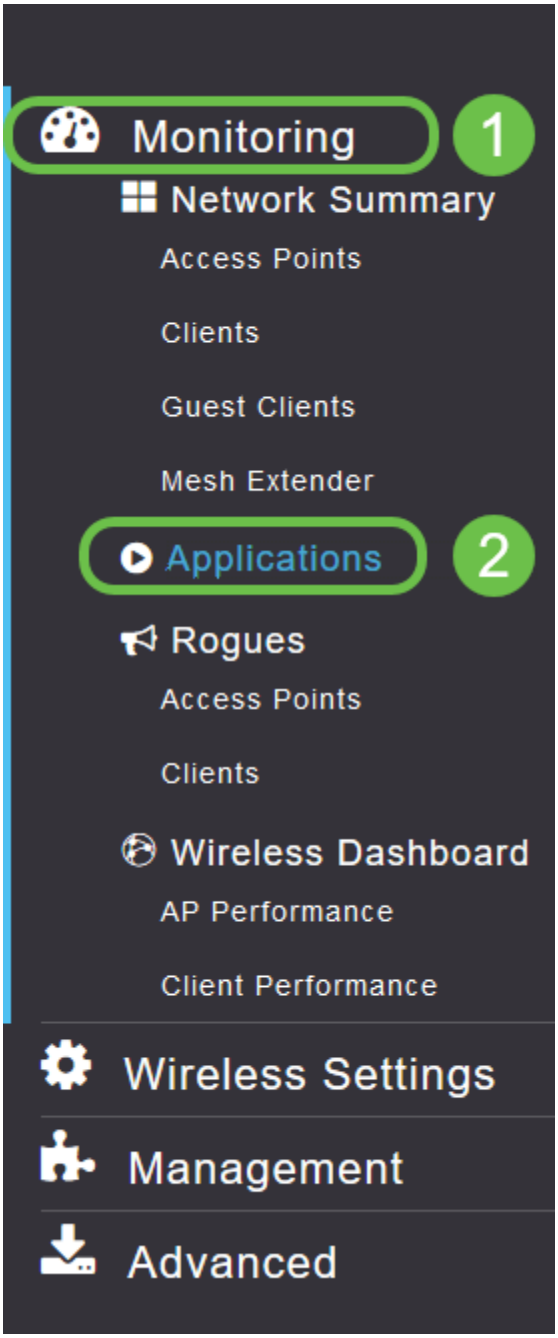
Klicken Sie auf die Schaltfläche **Übernehmen**.



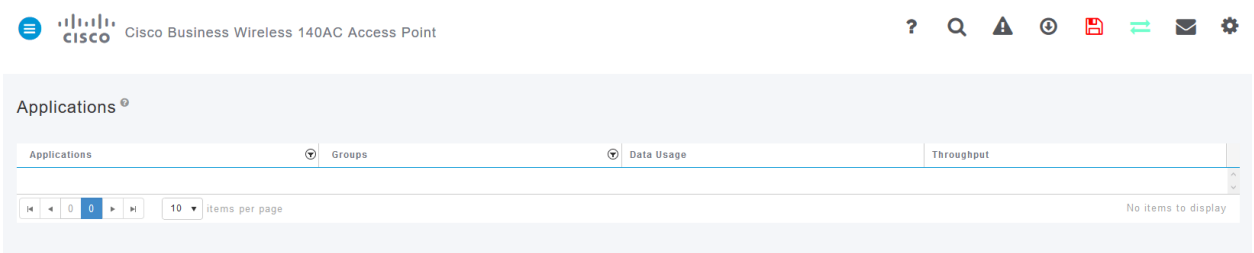
Diese Einstellung muss aktiviert werden, da die Funktion sonst nicht funktioniert.

Schritt 7

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



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



Auf dieser Seite werden folgende Informationen angezeigt:

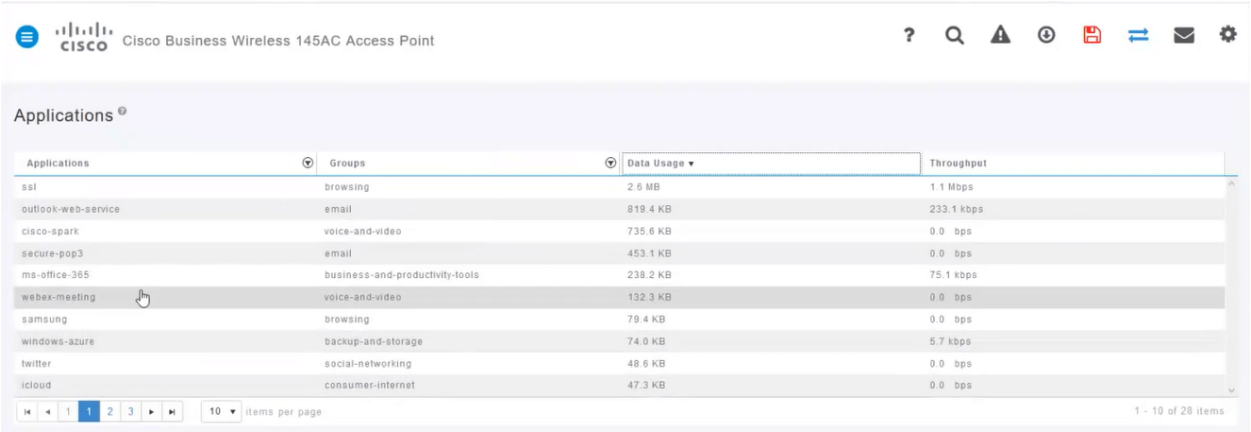
- Anwendung - umfasst viele verschiedene Typen
- Gruppen: Gibt den Typ der Anwendungsgruppe an, um das Sortieren zu vereinfachen.
- Datennutzung - Die von diesem Service insgesamt verwendete Datenmenge
- Durchsatz - Die von der Anwendung genutzte Bandbreite

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

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

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

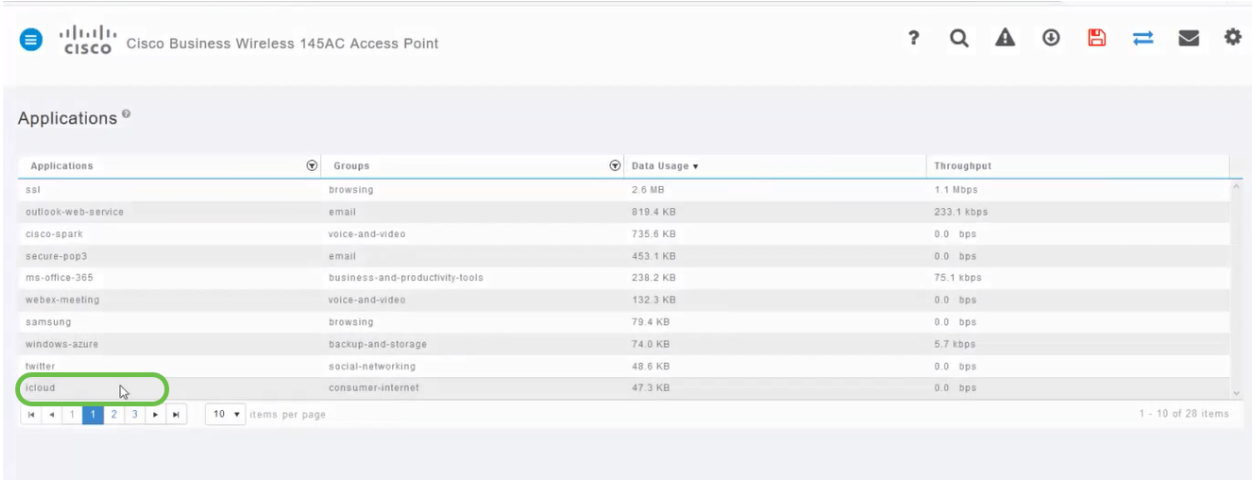
Hier sehen Sie ein Beispiel dafür, wie die Seite aussieht, wenn sie ausgefüllt wird.



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

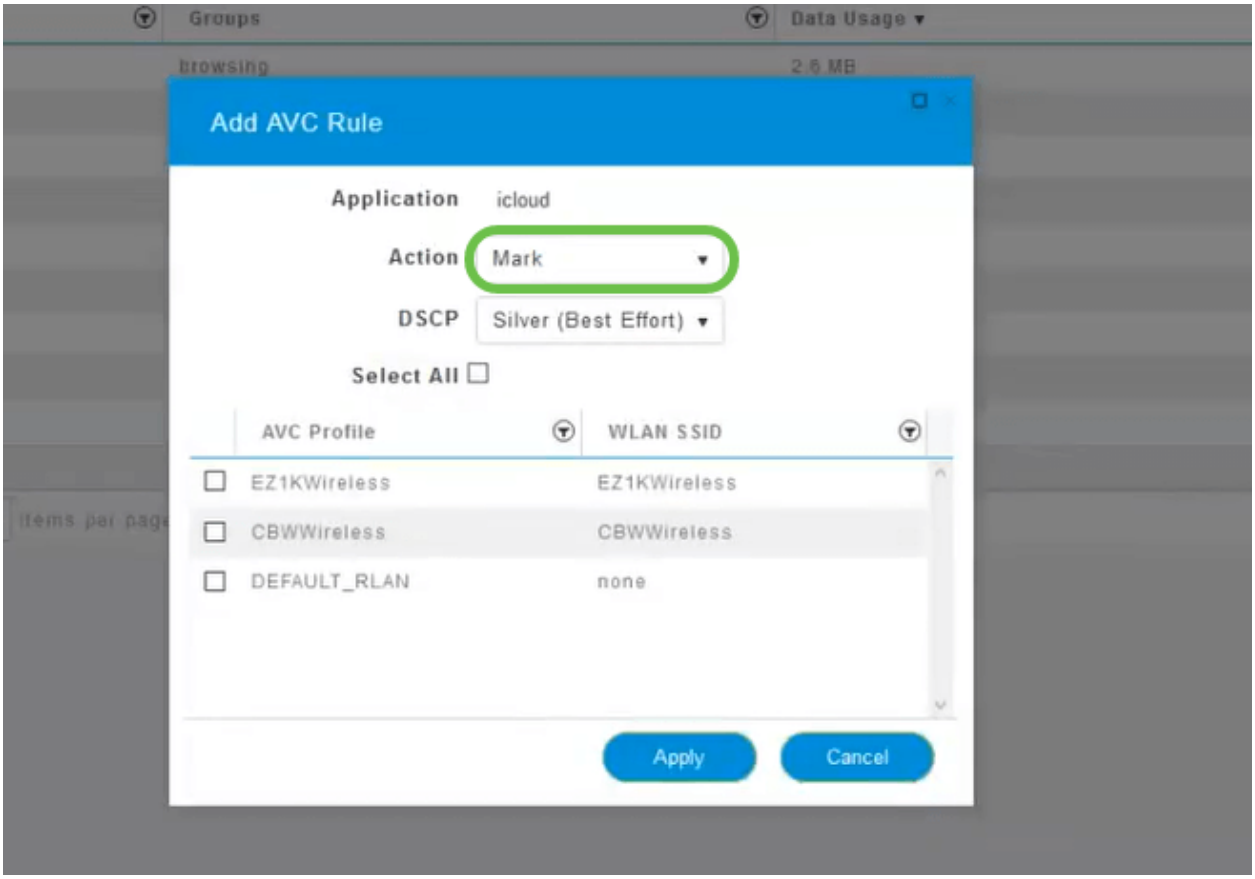
Schritt 8

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



Schritt 9

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



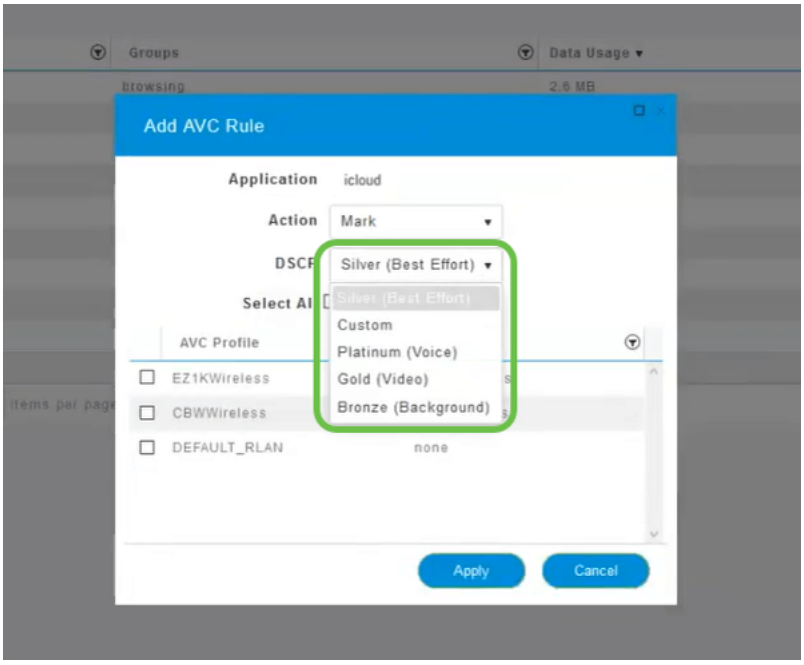
Bei diesem Beispiel überlassen wir diese Option *Mark*.

Maßnahmen zur Aufnahme des Datenverkehrs

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

Schritt 10

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



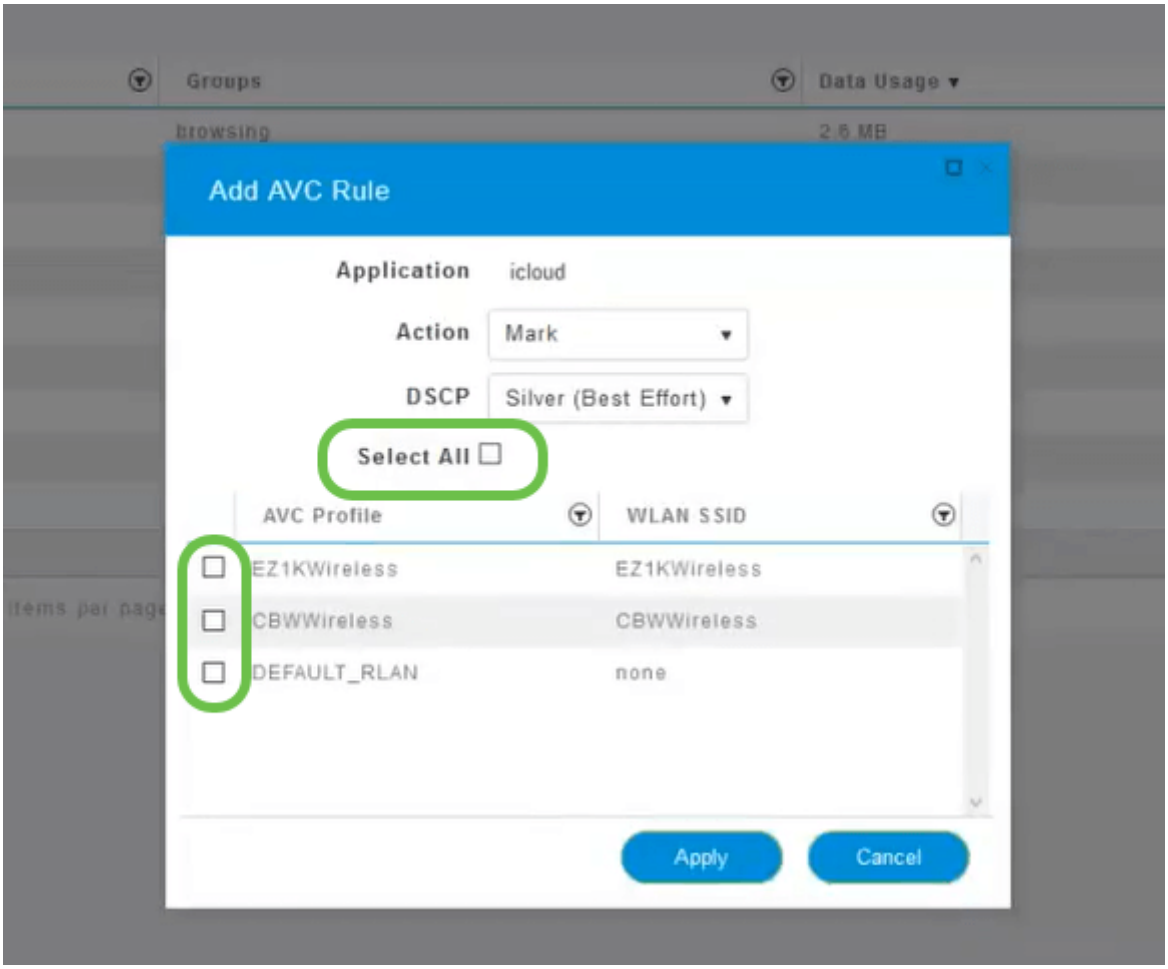
Nachfolgend sind die DSCP-Optionen für den zu markierenden Datenverkehr aufgeführt. Diese Optionen gehen von weniger Ressourcen zu mehr Ressourcen über, die für den zu bearbeitenden Datenverkehrstyp verfügbar sind.

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

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

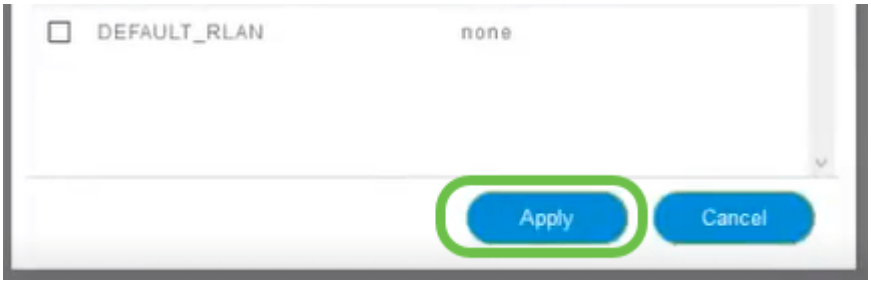
Schritt 11

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



Schritt 12

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



In zwei Fällen könnte dies gelten:

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

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

Client-Profiling mithilfe der Webbenutzeroberfläche (optional)

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

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

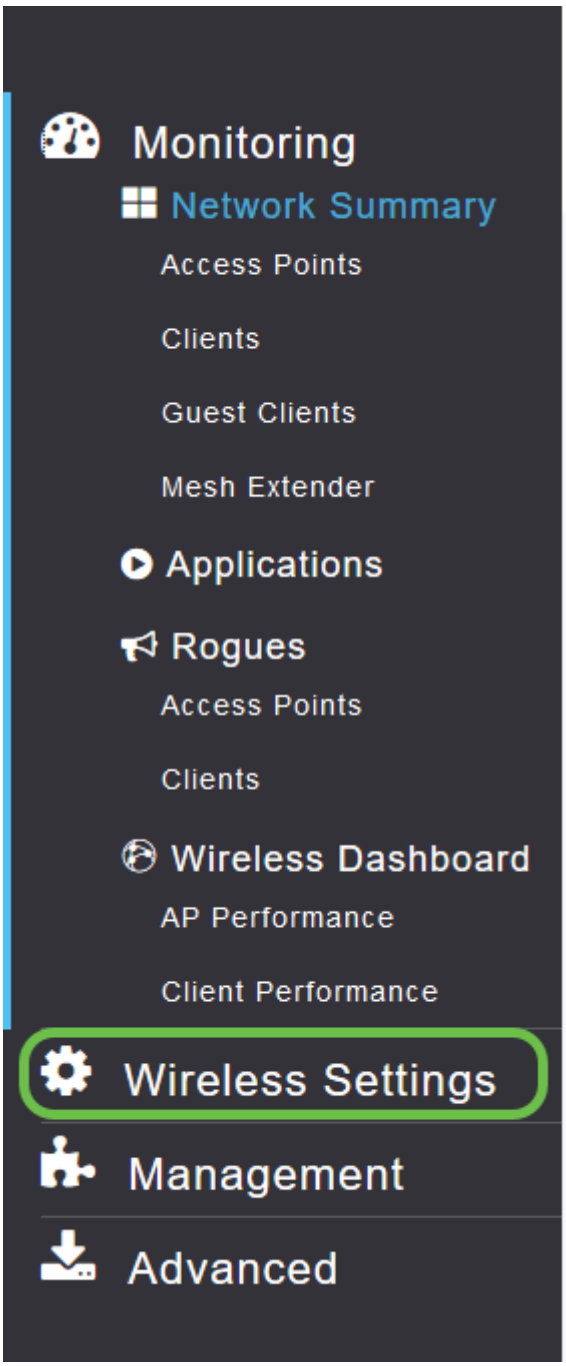
Statistiken über diese Clients enthalten die Menge der verwendeten Daten und den Durchsatz.

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

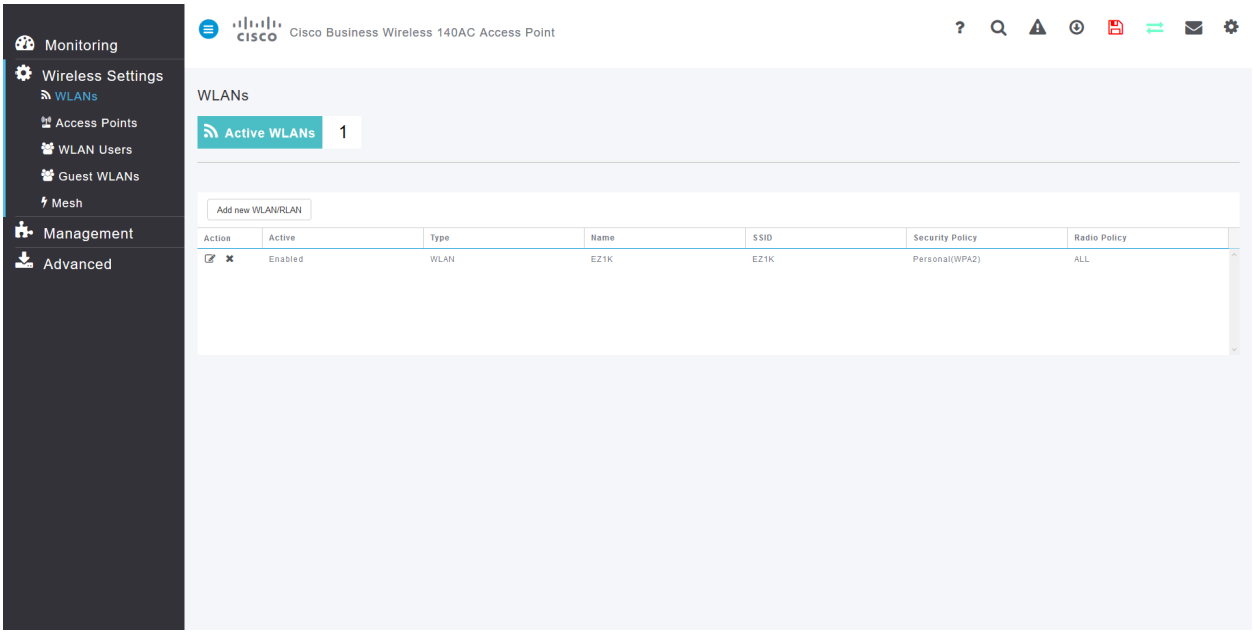
Nach der Aktivierung finden Sie die Clientdetails für Ihr Netzwerk im Abschnitt Überwachung der Webbenutzeroberfläche.

Schritt 1

Klicken Sie auf **Wireless Settings**.

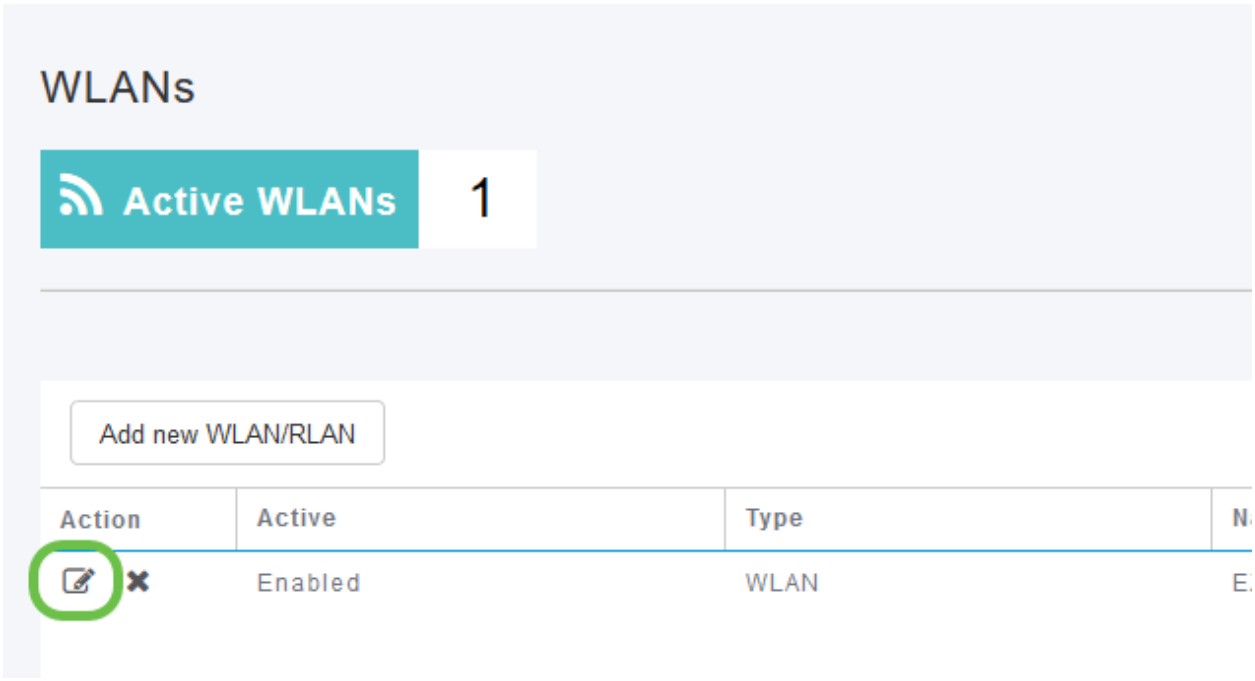


Die folgende Abbildung ähnelt der Anzeige, wenn Sie auf den Link Wireless Settings (Wireless-Einstellungen) klicken:



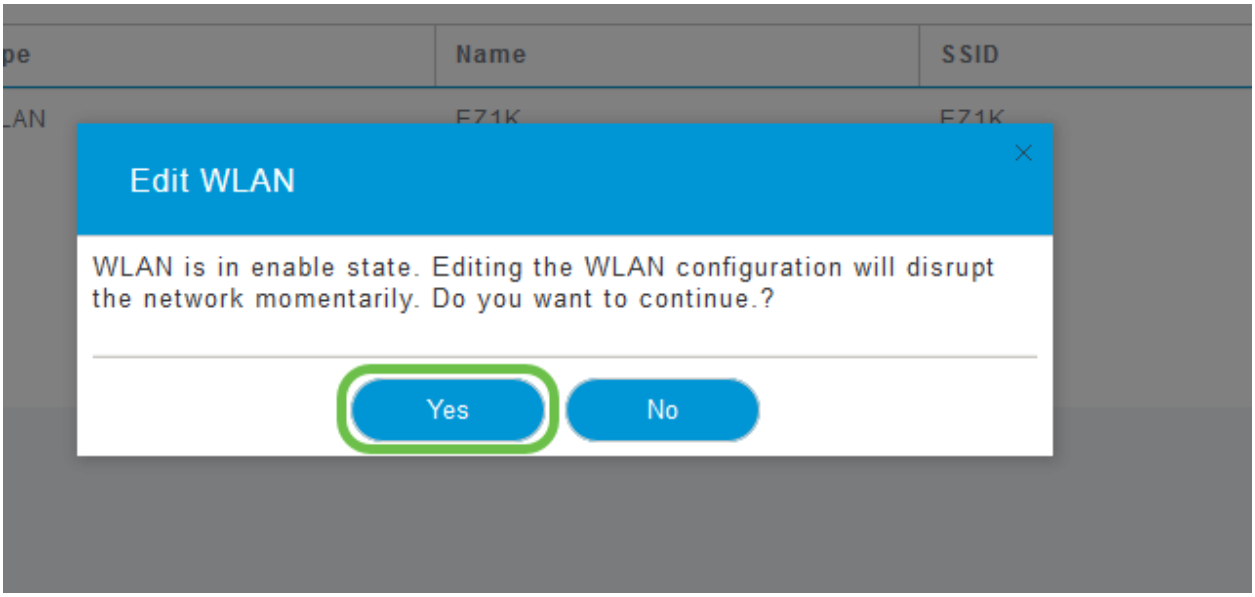
Schritt 2

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



Schritt 3

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

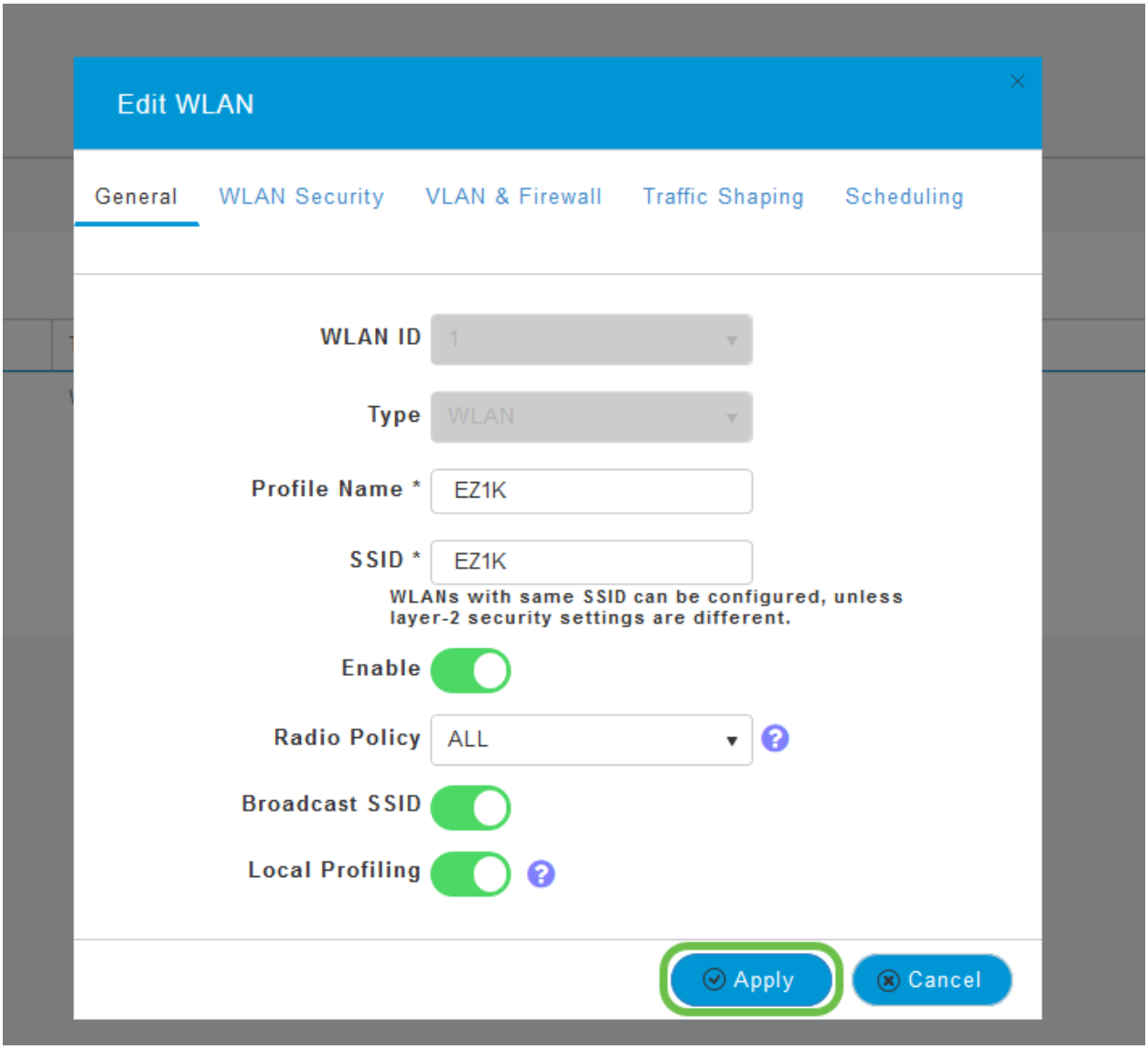


Schritt 4

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

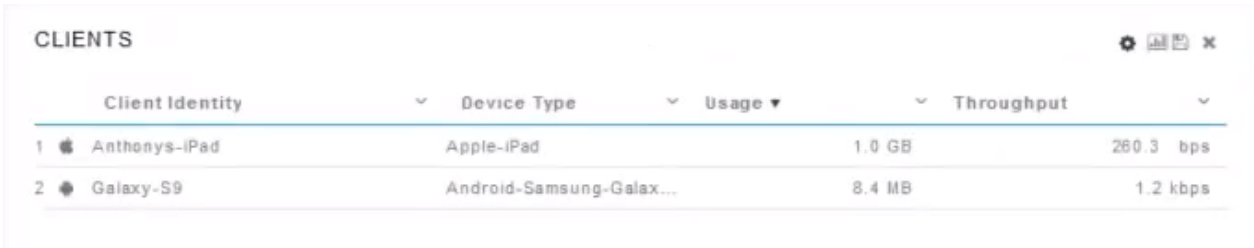
Schritt 5

Klicken Sie auf Apply (Anwenden).



Schritt 6

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



Schlussfolgerung

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

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

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

Hardware:

- Cisco RV345P VPN-Router mit PoE
- Cisco Business Access Point der Serie 140AC
- Cisco Business 142ACM Mesh Extender