

Konfigurieren eines IPSEC-VPN mithilfe des integrierten MAC-Clients für den Router der Serie RV32x

Konfigurieren eines IPSEC-VPN mithilfe des integrierten MAC-Clients für den Router der Serie RV32x

Ziel

In diesem Dokument wird erläutert, wie der integrierte MAC-Client für die Verbindung mit einem RV32x-Router verwendet wird.

Unterstützte Geräte | Software-Version

- RV320 | 1.3.2.02
- RV325 | 1.4.2.22

Einleitung

Ein Internet Protocol Security Virtual Private Network (IPSEC VPN) ermöglicht die sichere Bereitstellung von Remote-Ressourcen durch die Einrichtung eines verschlüsselten Tunnels über das Internet. Der integrierte MAC-Client ist ein integrierter Client, der auf allen MACs verfügbar ist und mit dem Sie sich über IPSEC mit dem VPN verbinden können. Die RV32x-Router fungieren als IPSEC VPN-Server und unterstützen den integrierten MAC-Client.

Dieses Dokument besteht aus zwei Teilen:

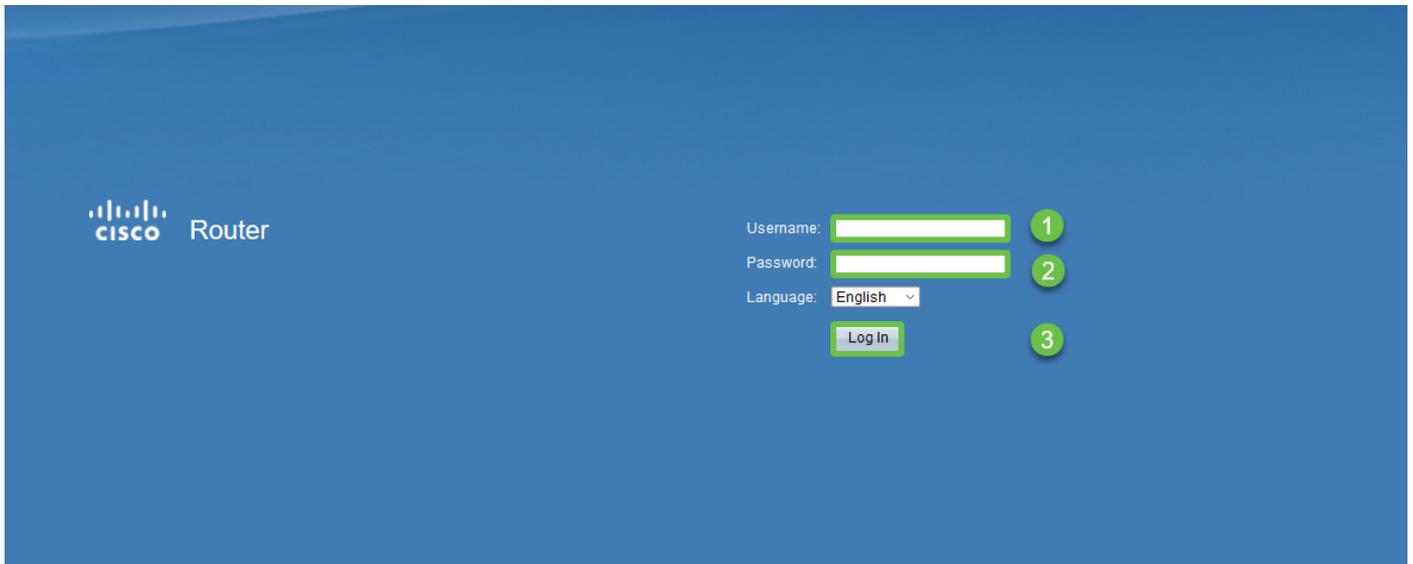
- Konfigurieren des Routers der Serie RV32x
- Konfigurieren des integrierten MAC-Clients

Konfigurieren Sie den Router der Serie RV32x:

Zunächst wird das Client-to-Site-VPN auf dem Router der Serie RV32x konfiguriert.

Schritt 1

Melden Sie sich mit gültigen Anmeldeinformationen beim Router an.



Schritt 2

Navigieren Sie zu VPN > VPN Passthrough. Bestätigen Sie, dass IPSEC-Passthrough aktiviert ist, und klicken Sie auf Speichern.

Getting Started

Setup Wizard

System Summary

▶ Setup

▶ DHCP

▶ System Management

▶ Port Management

▶ Firewall

▼ **VPN** **1**

- Summary
- Gateway to Gateway
- Client to Gateway
- FlexVPN (Spoke)
- VPN Passthrough** **2**
- PPTP Server

▶ OpenVPN

▶ Certificate Management

▶ Log

User Management

VPN Passthrough

IPSec Passthrough: Enable **3**

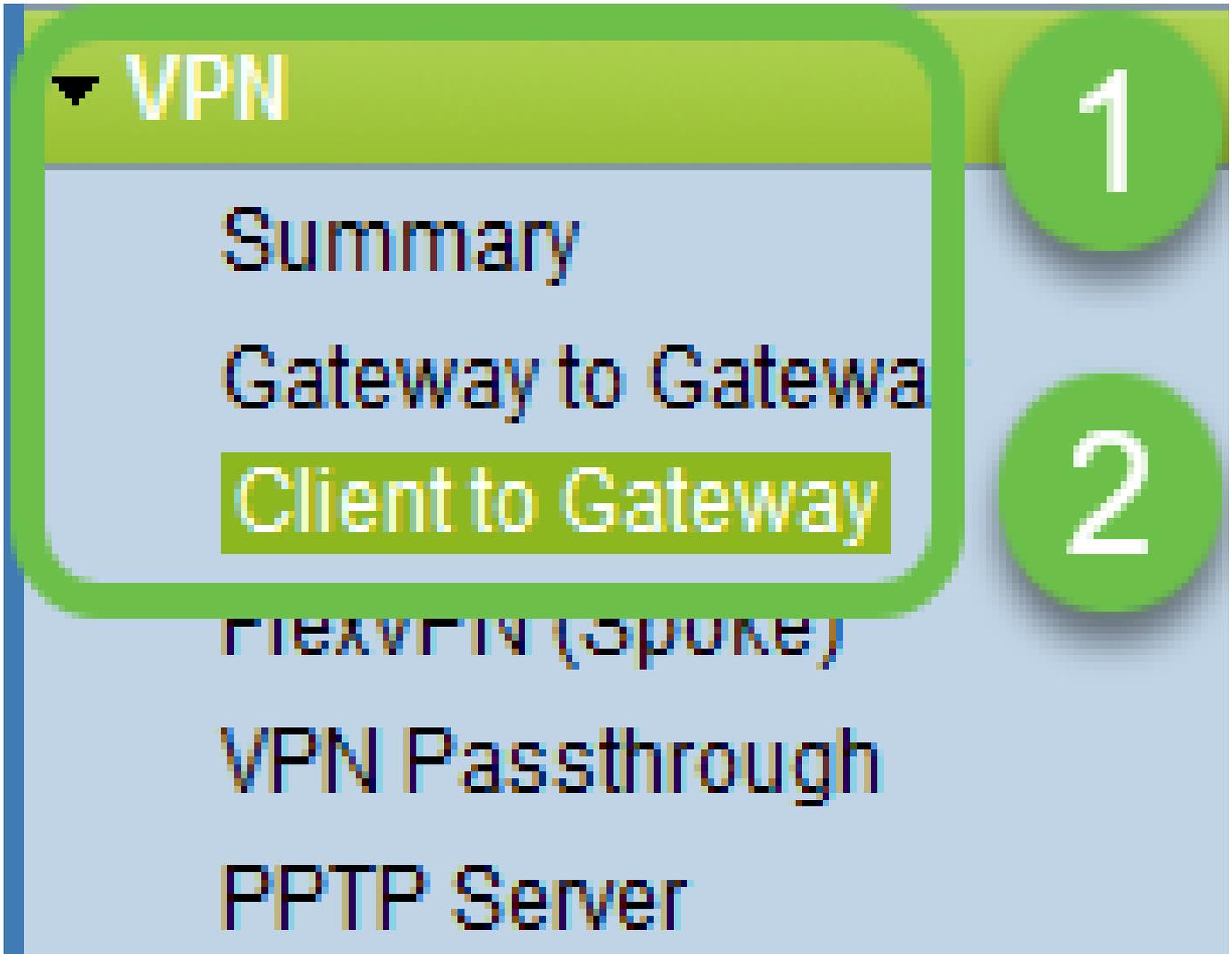
PPTP Passthrough: Enable

L2TP Passthrough: Enable

Save Cancel

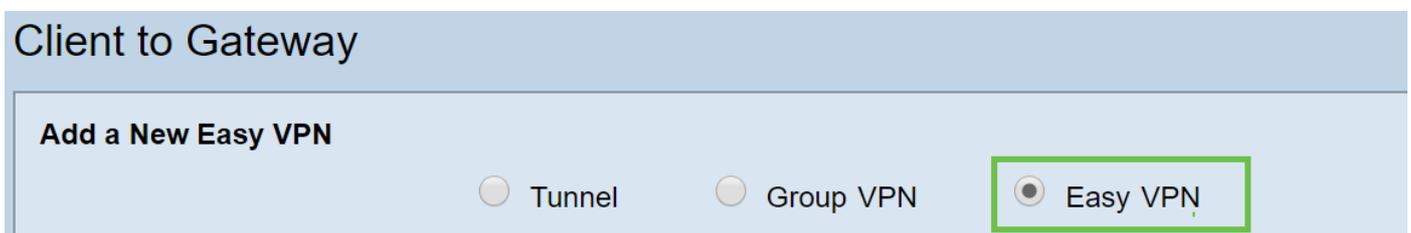
Schritt 3

Navigieren Sie zu VPN > Client to Gateway.



Schritt 4

Wählen Sie die Easy VPN-Option aus.



Schritt 5

Konfigurieren Sie den Tunnelnamen, geben Sie ein Kennwort ein, wählen Sie die WAN-Schnittstelle aus, aktivieren Sie den Tunnel, und wählen Sie den Eintrag "Tunnel Mode" aus. Klicken Sie auf Speichern, um die Konfigurationen zu speichern.

Vollständiger Tunnelmodus ausgewählt, Kennwortkomplexität deaktiviert.

Client to Gateway

Add a New Easy VPN

Tunnel Group VPN Easy VPN

Group No. 1

Tunnel Name: CiscoVPN

Minimum Password Complexity: Enable

Password: Cisco123

Interface: WAN1

Enable:

Tunnel Mode: Full Tunnel

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Extended Authentication: Default - Local Database

Schritt 6

Navigieren Sie zu VPN > Summary, und bestätigen Sie, dass der VPN-Tunnel konfiguriert wurde.

▶ Firewall

▼ VPN

1

Summary

2

Gateway to Gateway

Client to Gateway

FlexVPN (Spoke)

VPN Passthrough

PPTP Server

▶ OpenVPN

▶ Certificate Management

▶ Log

Schritt 7

Bestätigen Sie, dass der VPN-Tunnel konfiguriert wurde.

Group VPN Status

Connection Table								
Type	Group Name	Tunnels	Phase2 Enc/Auth/Grp	Local Group	Remote Client	Details	Action	
<input type="radio"/> Easy VPN	CiscoVPN	0	AES/MD5	192.168.1.0 255.255.255.0	CiscoVPN		N/A	

Add Edit Delete

Schritt 8

Navigieren Sie zu Benutzerverwaltung, und wählen Sie die Schaltfläche Hinzufügen unter Benutzerverwaltung aus.

Getting Started
Setup Wizard
System Summary
Setup
DHCP
System Management
Port Management
Firewall
VPN
OpenVPN
Certificate Management
Log
User Management 1

User Management

Domain Management Table

Domain Name	Authentication Type	Authentication Server IP
<input type="radio"/> Default	Local Database	N/A

Add... Edit... Delete

User Management Table

<input type="checkbox"/> Username	Password	Group	Domain
<input type="checkbox"/> cisco	*****	Administrator	Default
<input type="text" value="User"/>	<input type="password" value="*****"/>	All Users	Default

2 Add Edit Delete

Save Cancel

Schritt 9

Geben Sie Benutzernamen und Kennwort ein, wählen Sie Gruppe und Domäne aus, und klicken Sie auf Speichern.

User Management Table

<input type="checkbox"/> Username	Password	Group	Domain
<input type="checkbox"/> cisco	*****	Administrator	Default
<input type="text" value="User"/>	<input type="password" value="*****"/>	All Users	Default

Add Edit Delete

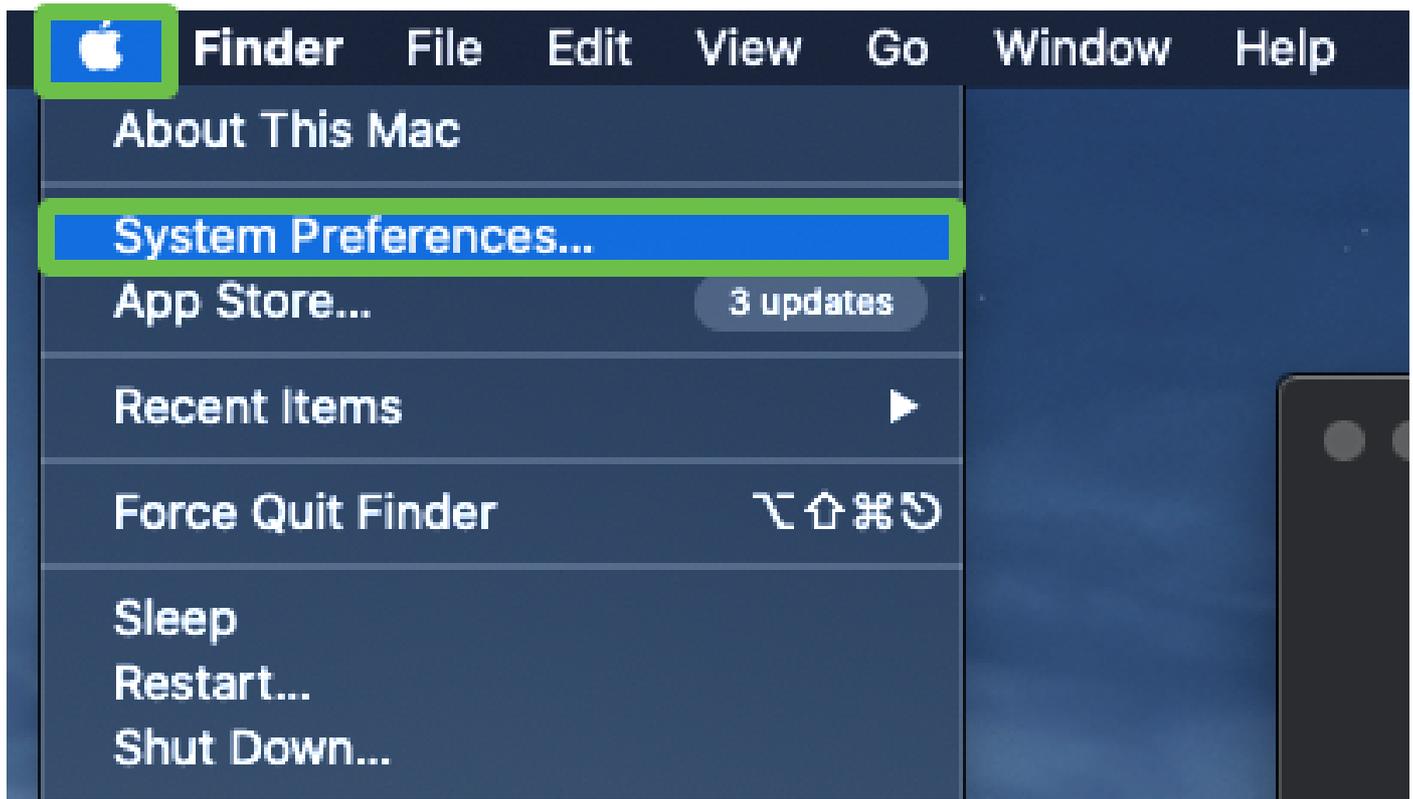
Save Cancel

Integrierte MAC-Adresse konfigurieren Kunde

Nun konfigurieren Sie den integrierten MAC-Client.

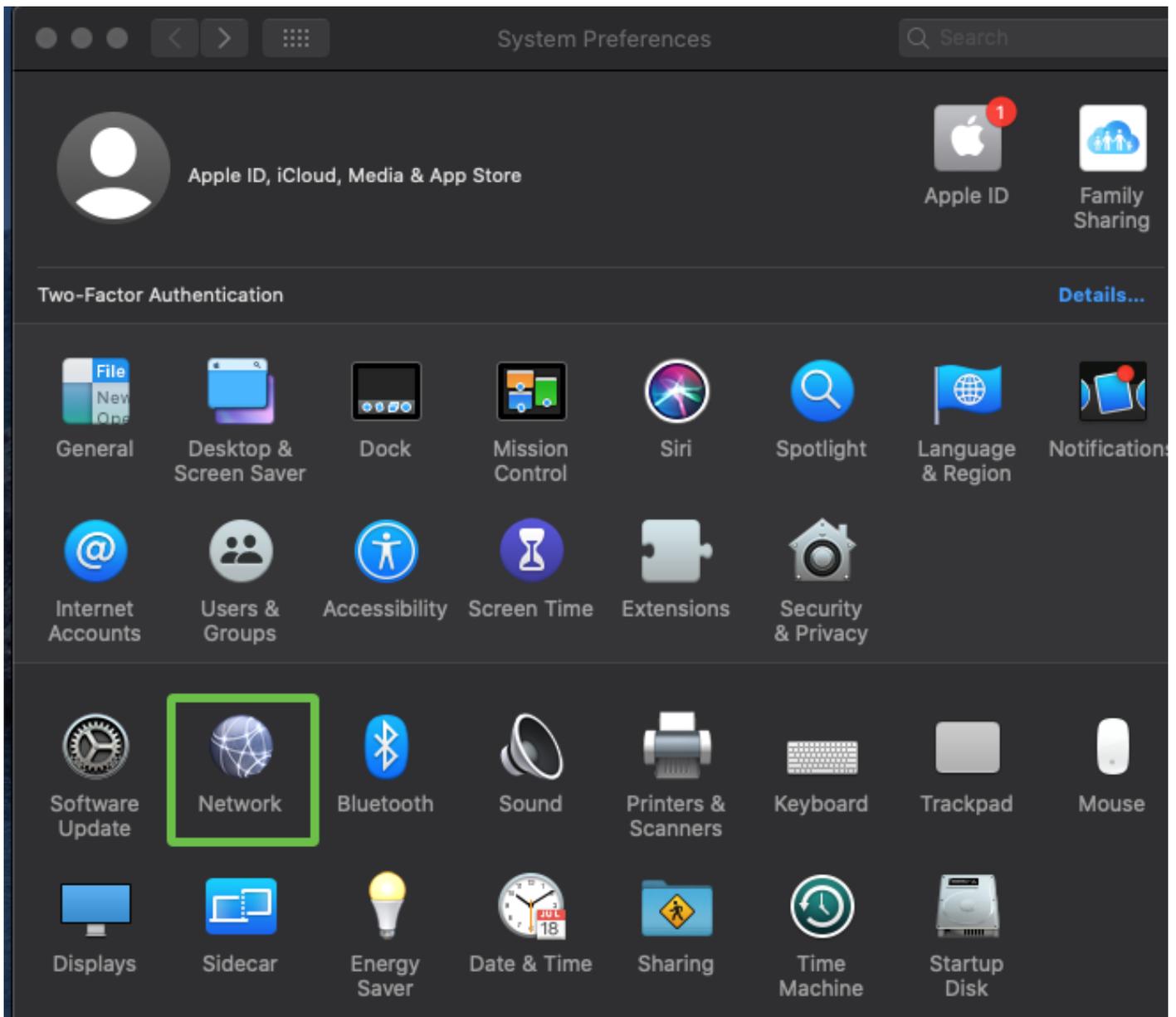
Schritt 1

Navigieren Sie zum Apple-Symbol in der Symbolleiste. Wählen Sie Systemvoreinstellungen aus.



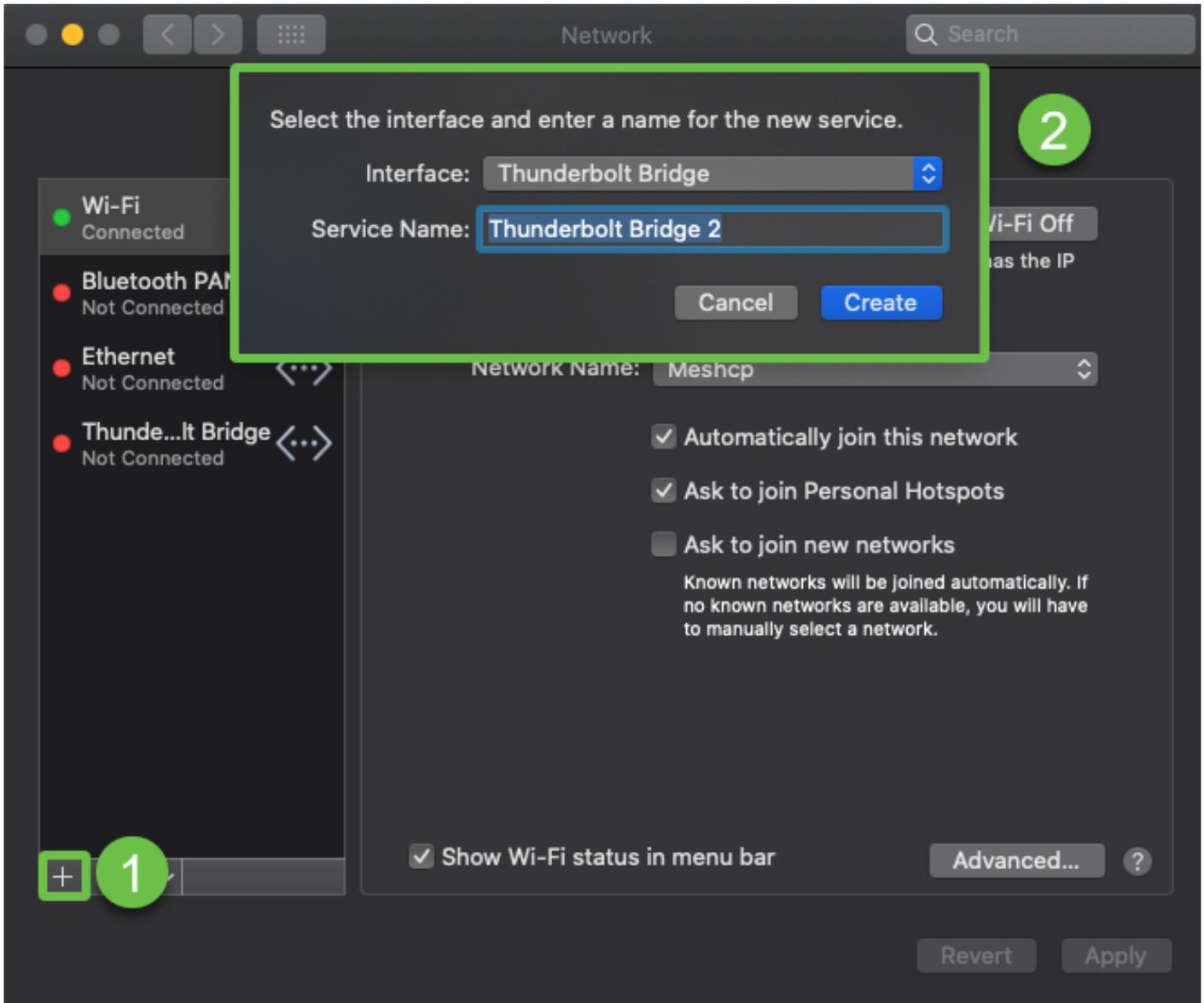
Schritt 2

Navigieren zum Netzwerk



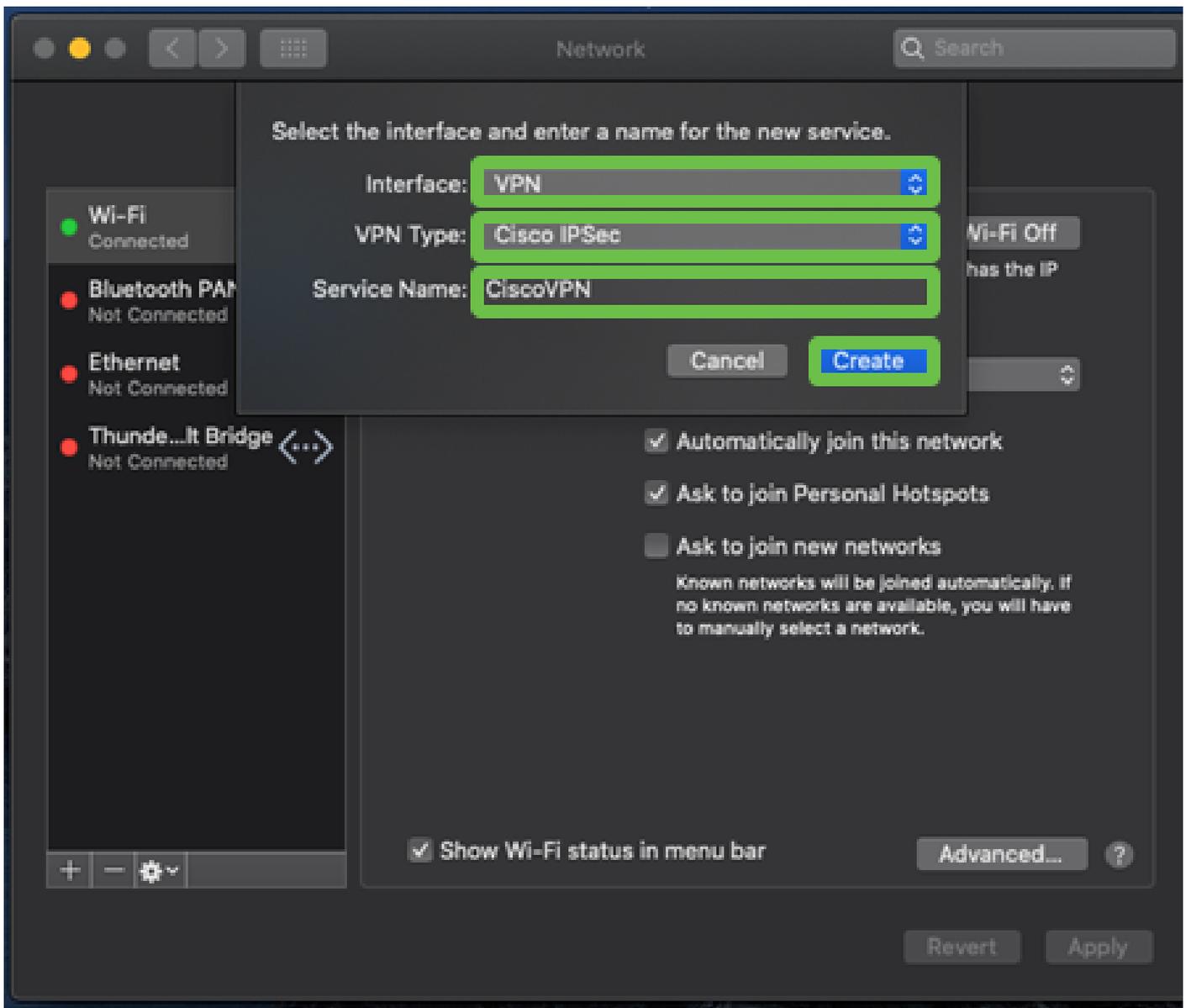
Schritt 3

Wechseln Sie zur Schaltfläche Hinzufügen, und wählen Sie dann die Registerkarte Interface (Schnittstelle) aus.



Schritt 4

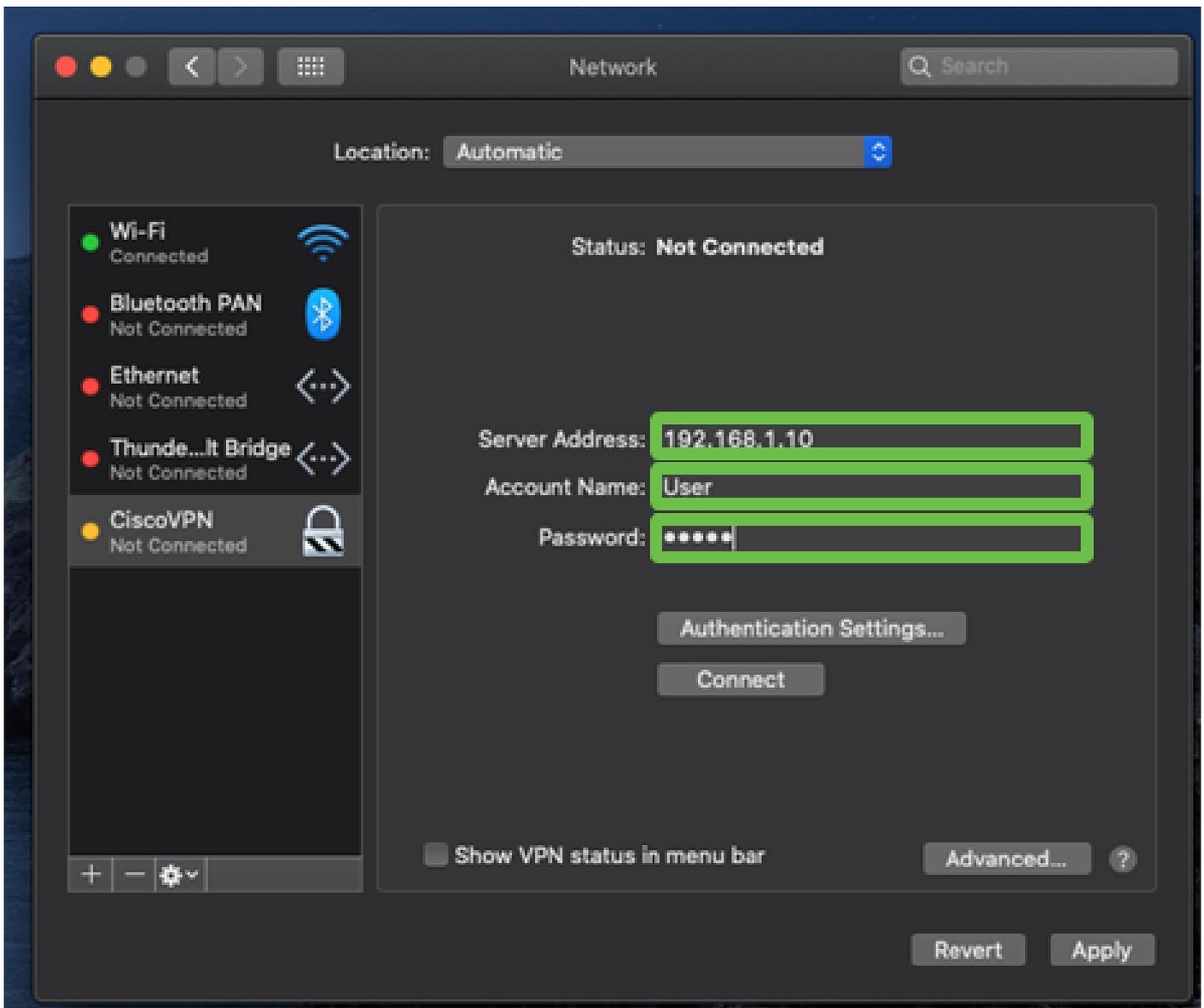
Wählen Sie Interface als VPN, VPN Type als Cisco IPSec aus, und geben Sie den Dienstnamen ein, der mit dem im Router konfigurierten Tunnelnamen übereinstimmt. Klicken Sie auf Erstellen.



Schritt 5

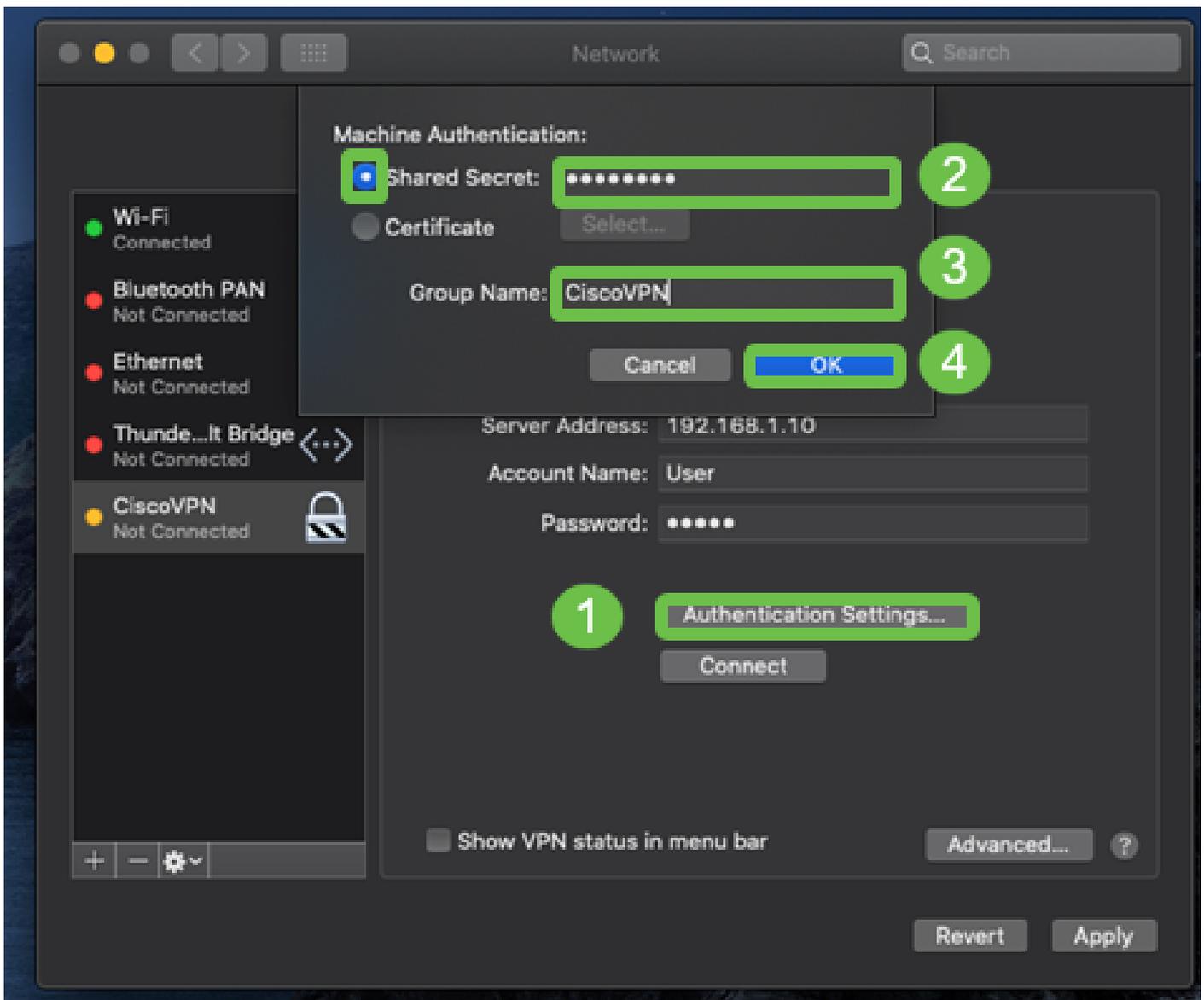
Navigieren Sie zum VPN, und geben Sie Serveradresse, Kontoname und Kennwort ein.

Der Kontoname und das Kennwort sind in den Benutzerkonten konfiguriert.



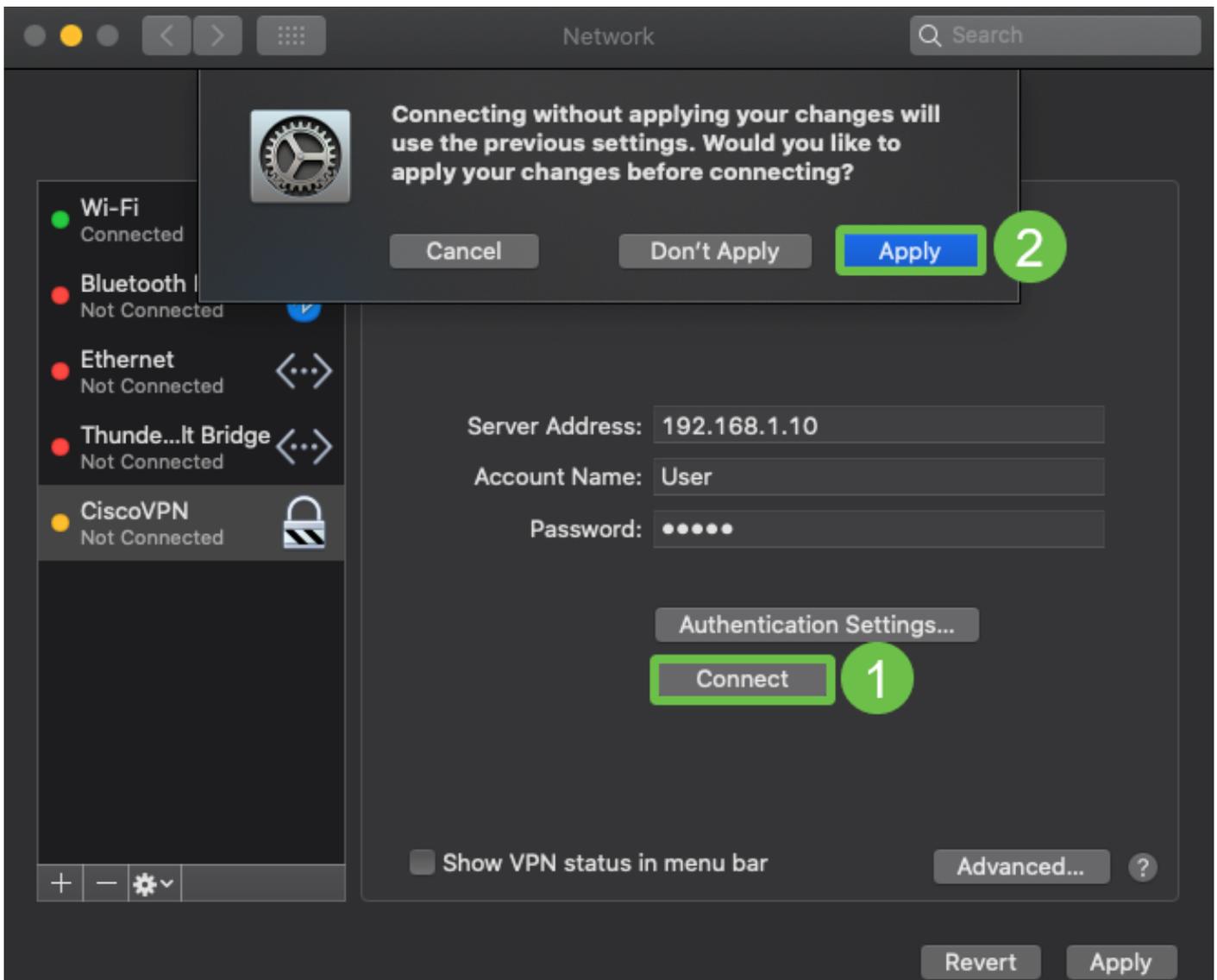
Schritt 6

Wählen Sie die Schaltfläche Authentifizierungseinstellungen. Die Registerkarte Computerauthentifizierung wird angezeigt. Geben Sie unter "Shared Secret" das Tunnelkennwort und unter "Group Name" den Tunnelnamen ein, und drücken Sie OK.



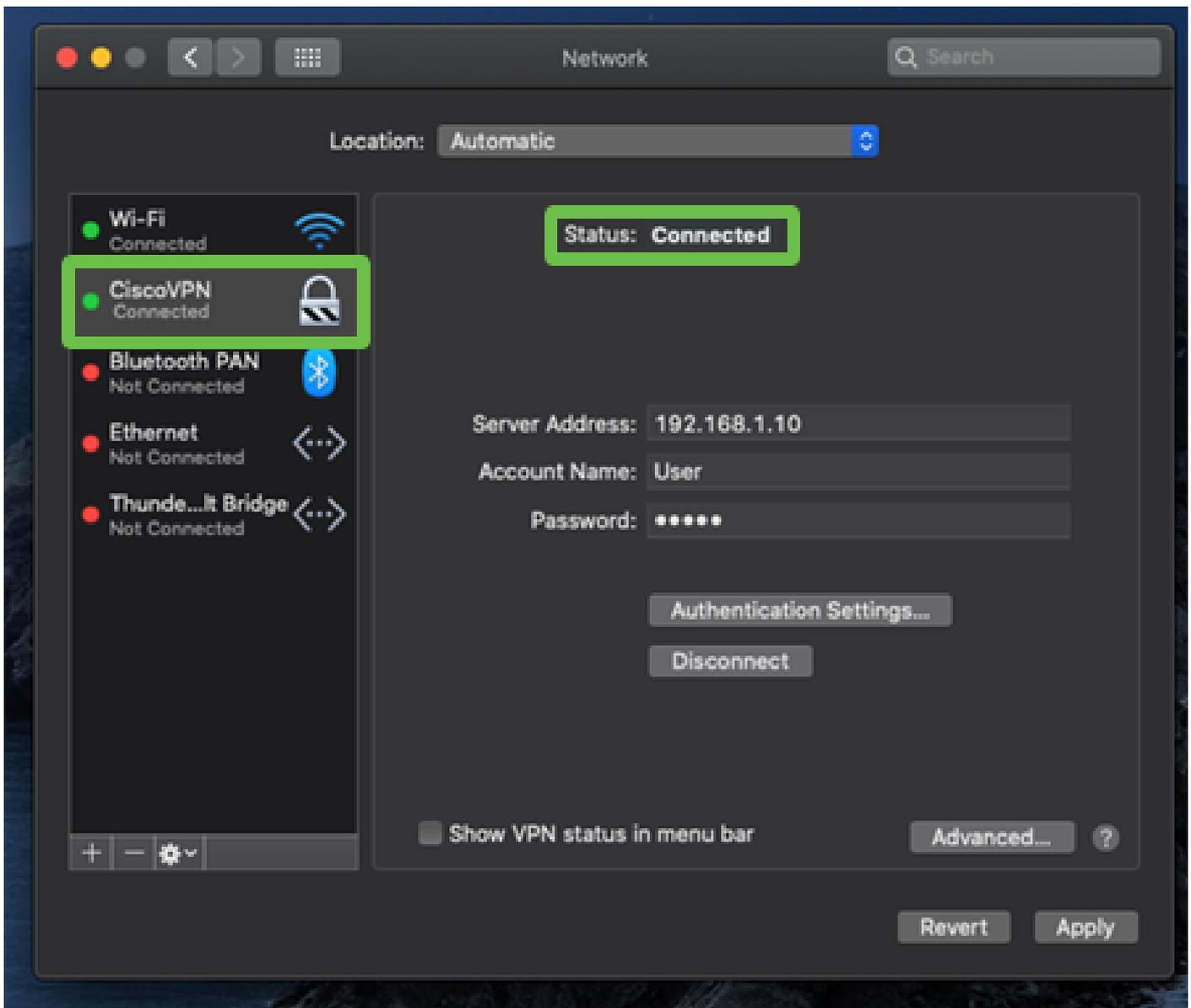
Schritt 7

Drücken Sie Verbinden. Eine Warnmeldung wird angezeigt, und drücken Sie Übernehmen.



Schritt 8

Der Verbindungsstatus sollte als Verbunden angezeigt werden.



Schlussfolgerung

Wir haben den Easy VPN-Tunnel mithilfe von IPSEC IKEV1 zwischen dem Router der Serie RV32X und einem MAC-Computer mithilfe des integrierten MAC-Clients konfiguriert. Stellen Sie sicher, dass der Tunnel auf dem Router mit Easy VPN für diese Verbindung konfiguriert ist, und geben Sie auf der Client-Seite die gleichen Informationen ein, um die Verbindung sicherzustellen. Jetzt können Sie sich mit Ihrem VPN verbinden und auf die Informationen zugreifen, die Sie möglicherweise benötigen.

Informationen zu dieser Übersetzung

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