Konfigurieren des Simple Network Management Protocol in Cisco Business Wireless Access Point

Ziel

In diesem Dokument wird erläutert, wie Sie die SNMP-Einstellungen (Simple Network Management Protocol) für Ihren Cisco Business Wireless Access Point (CBW) konfigurieren.

Anwendbare Geräte | Softwareversion

- 140AC (Datenblatt) | 10.0.1.0 (Laden Sie die aktuelle Version herunter)
- 145AC (Datenblatt) | 10.0.1.0 (Laden Sie die aktuelle Version herunter)
- 240AC (Datenblatt) | 10.0.1.0 (Laden Sie die aktuelle Version herunter)

Einführung

Die CBW APs unterstützen den neuesten 802.11ac Wave 2-Standard für höhere Leistung, besseren Zugriff und Netzwerke mit höherer Dichte. Sie bieten branchenführende Leistung mit hochsicheren und zuverlässigen Wireless-Verbindungen für eine robuste mobile Endbenutzerumgebung.

SNMP ist ein beliebtes Netzwerkverwaltungsprotokoll, das zum Erfassen von Informationen aller Geräte im Netzwerk sowie zum Konfigurieren und Verwalten dieser Geräte verwendet wird. Sie können sowohl den SNMP v2c- als auch den SNMP v3-Zugriffsmodus über die Master-AP-Webschnittstelle konfigurieren. SNMPv2c ist das Community String-basierte Administrations-Framework für SNMPv2. Community String ist ein Passworttyp, der im Klartext übertragen wird. Die SNMP v3-Funktion bietet sicheren Zugriff auf Geräte, indem Datenpakete über das Netzwerk authentifiziert und verschlüsselt werden.

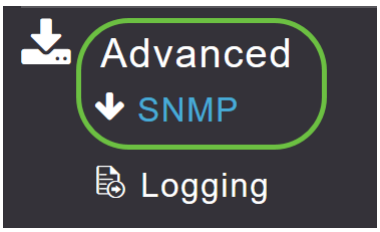
Sie können die folgenden SNMP-Zugriffsmodi für den Master-AP konfigurieren:

- Nur SNMP v2c
- Nur SNMP v3
- SNMP v2c und SNMP v3
- Weder SNMP v2c noch SNMP v3

SNMP konfigurieren

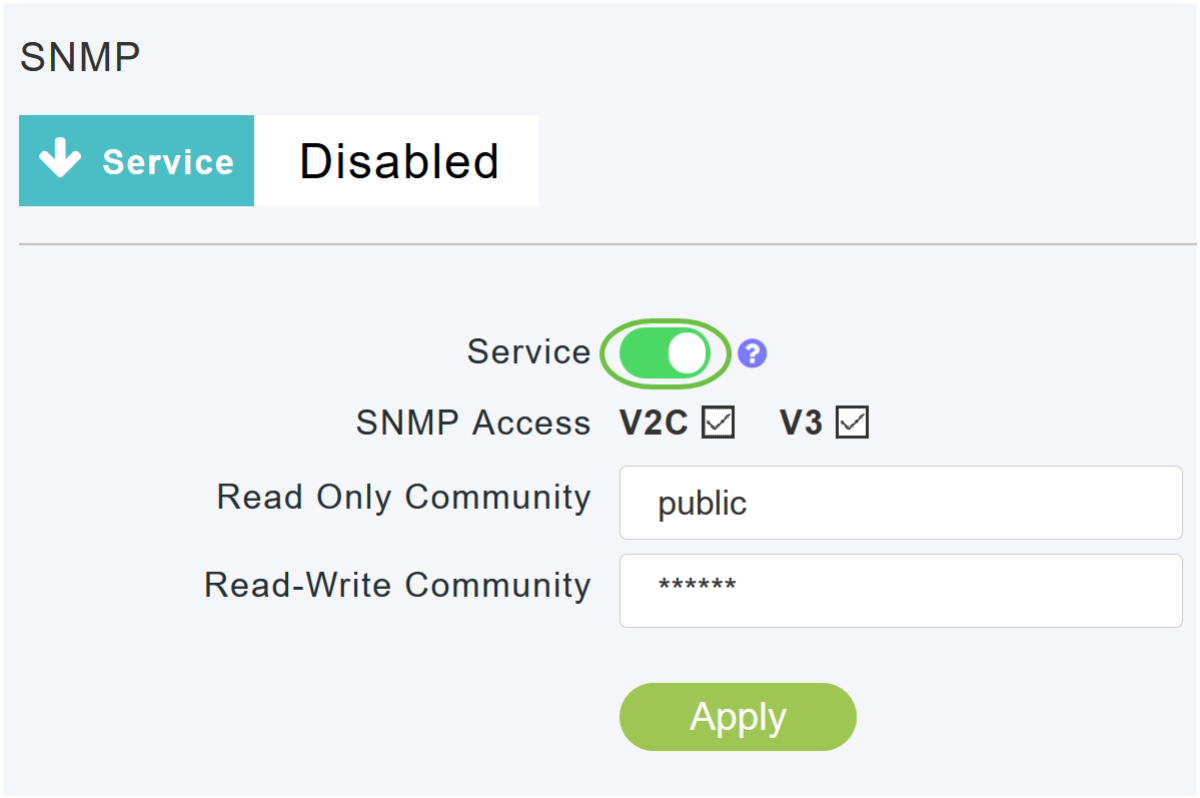
Schritt 1

Wählen Sie **Erweitert > SNMP aus**.



Schritt 2

Aktivieren Sie die SNMP-Dienstoption für die Abfrage der Konfiguration mithilfe des MIB-Browsers.

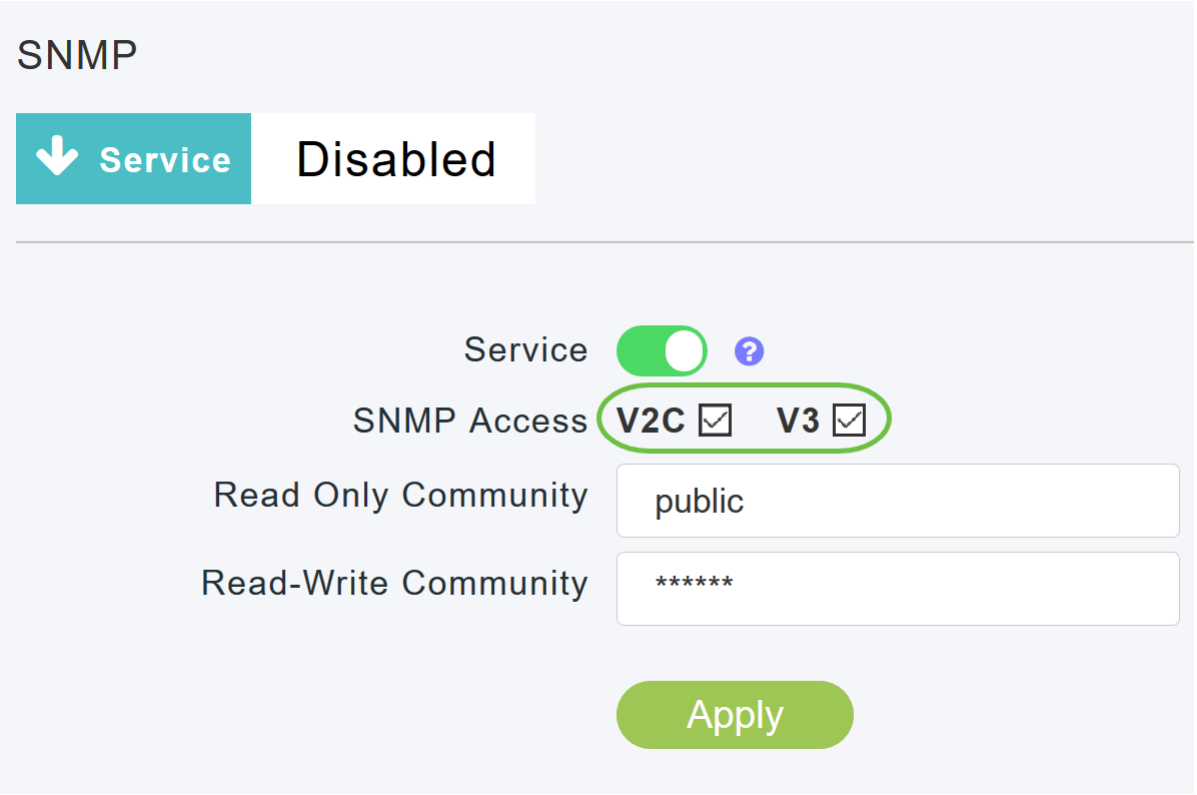


Schritt 3

Aktivieren Sie im SNMP-Setup-Fenster das entsprechende Kontrollkästchen neben dem *SNMP-Zugriff,* um den gewünschten SNMP-Modus zu aktivieren.

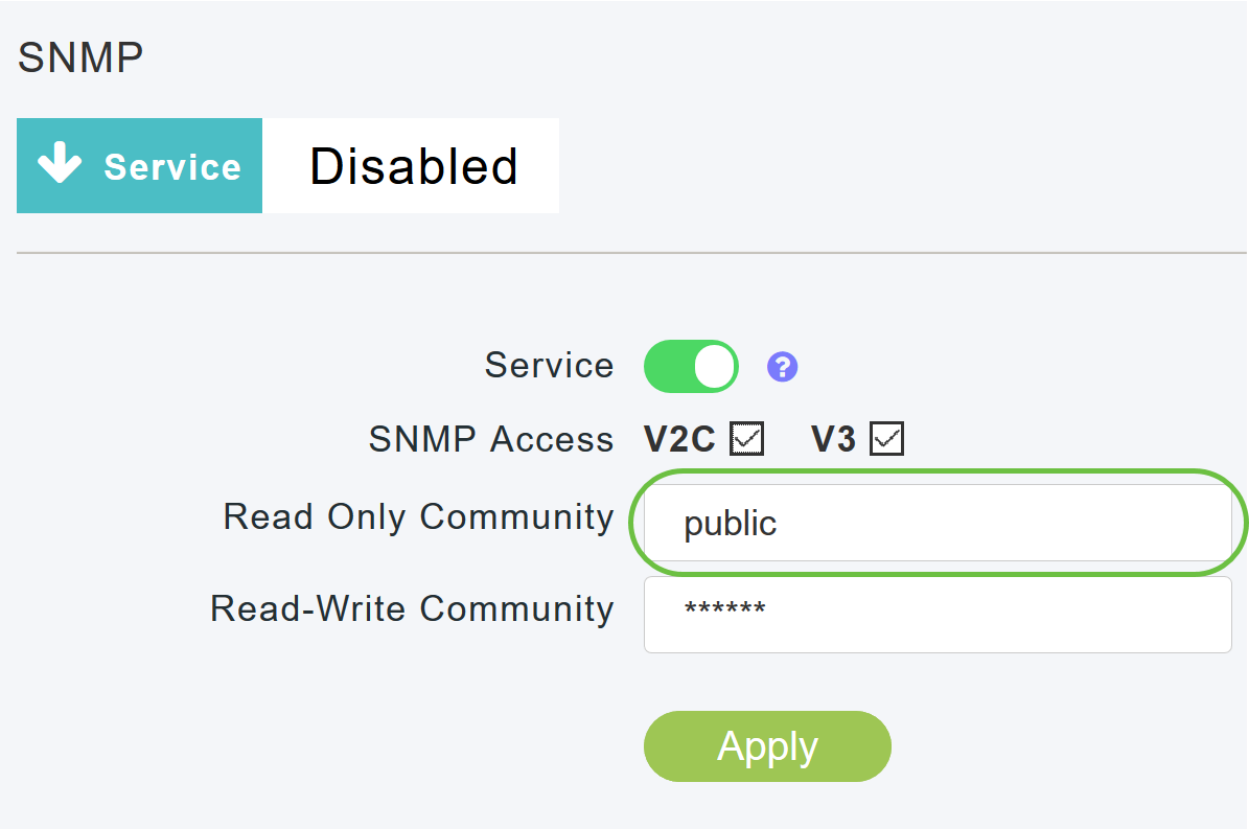
Der Standardmodus ist v2c (oder standardmäßig ist entweder der SNMP-Zugriffsmodus oder einer der beiden ausgewählt).

Der ausgewählte SNMP-Zugriffsmodus ist aktiviert.



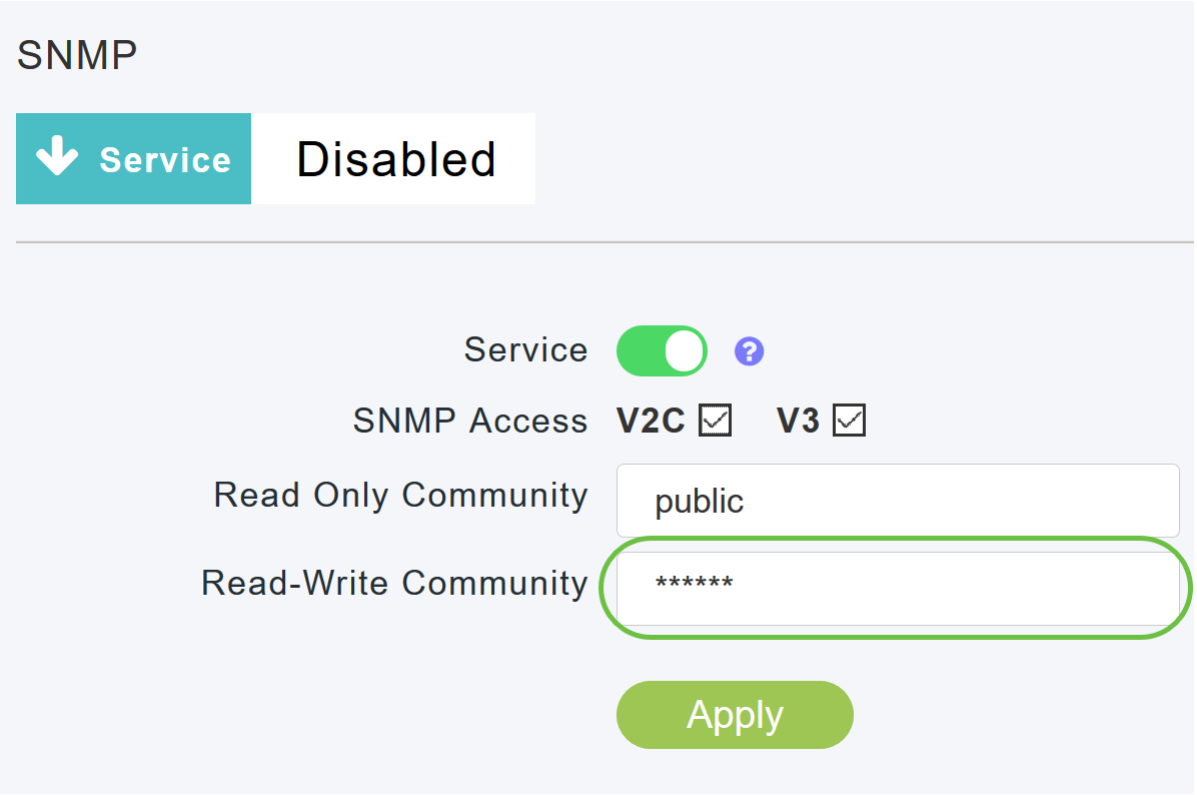
Schritt 4

Geben Sie im *Feld Nur-Lesen-Community* den gewünschten Community-Namen ein. Der Standardname ist **public**.



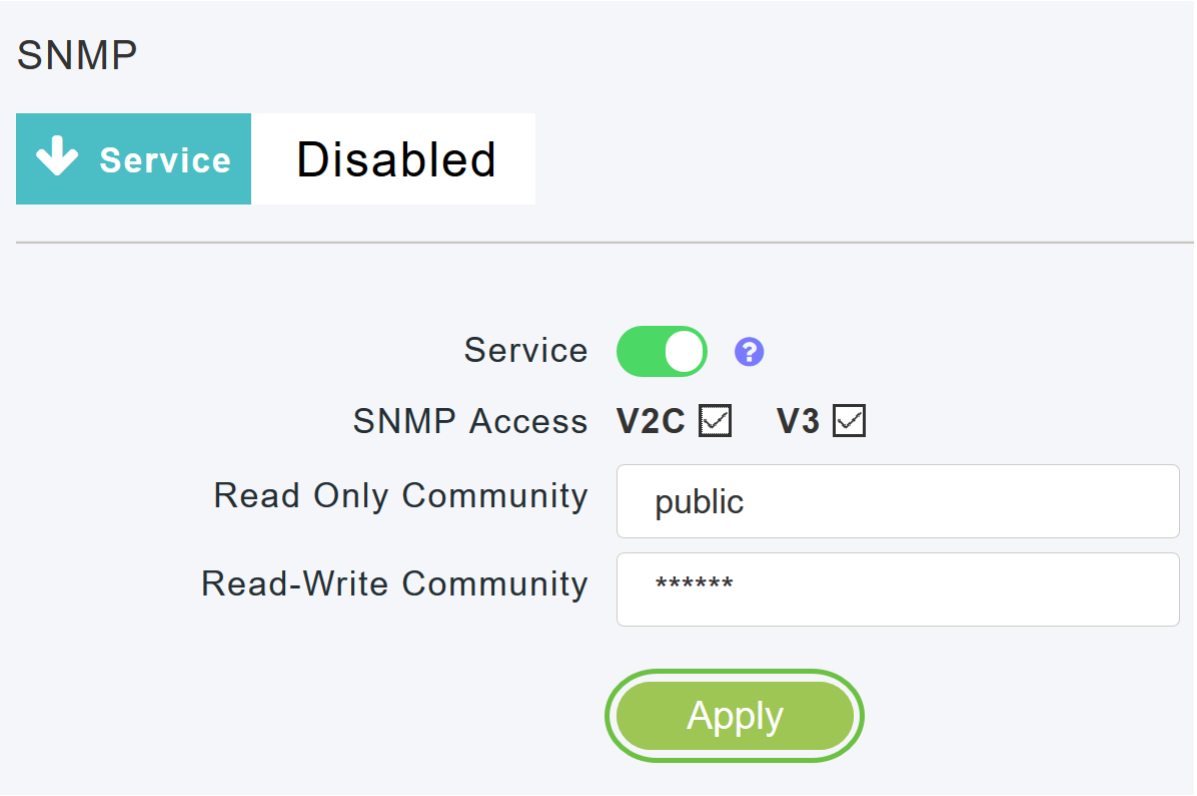
Schritt 5

Geben Sie im Feld *Read-Write Community* den gewünschten Community-Namen ein. Der Standardname ist **private**.



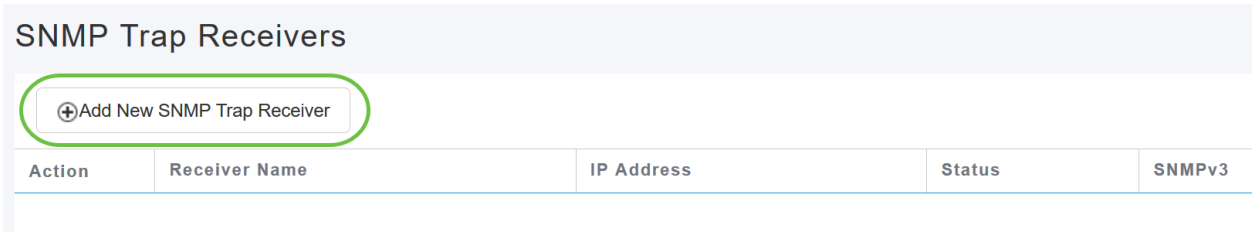
Schritt 6

Klicken Sie auf **Übernehmen**.



Schritt 7

Um den SNMP-Trap-Empfänger zu konfigurieren, klicken Sie auf **Neuen SNMP-Trap-Empfänger hinzufügen**. Dieses Tool empfängt, protokolliert und zeigt SNMP-Traps an, die von Netzwerkgeräten gesendet werden. Die Standardeinstellung ist Disabled (Deaktiviert).

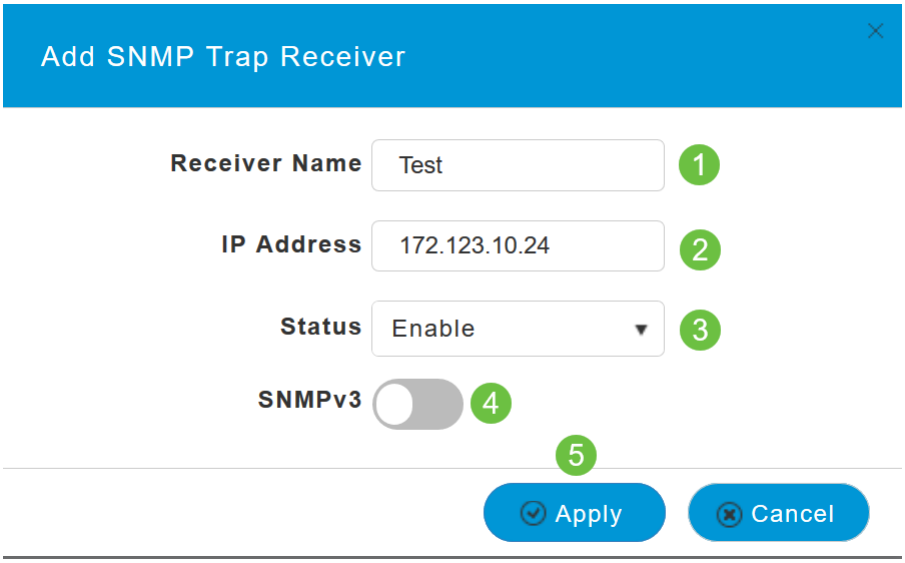


Schritt 8

Konfigurieren Sie im Fenster *SNMP Trap Receiver hinzufügen* Folgendes:

- Empfängername
- IP-Adresse des Servers, zu dem Sie eine Verbindung herstellen möchten
- Status
- Option zum Aktivieren von SNMPv3

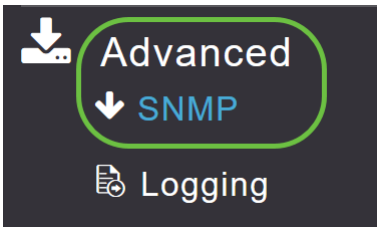
Klicken Sie auf **Übernehmen**.



SNMPv3-Benutzer hinzufügen

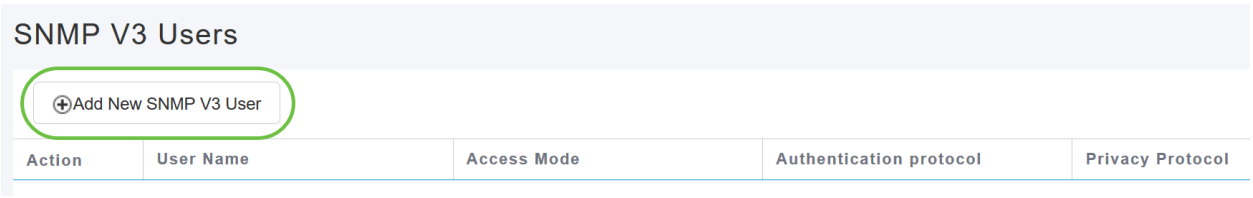
Schritt 1

Wählen Sie **Erweitert > SNMP aus**.



Schritt 2

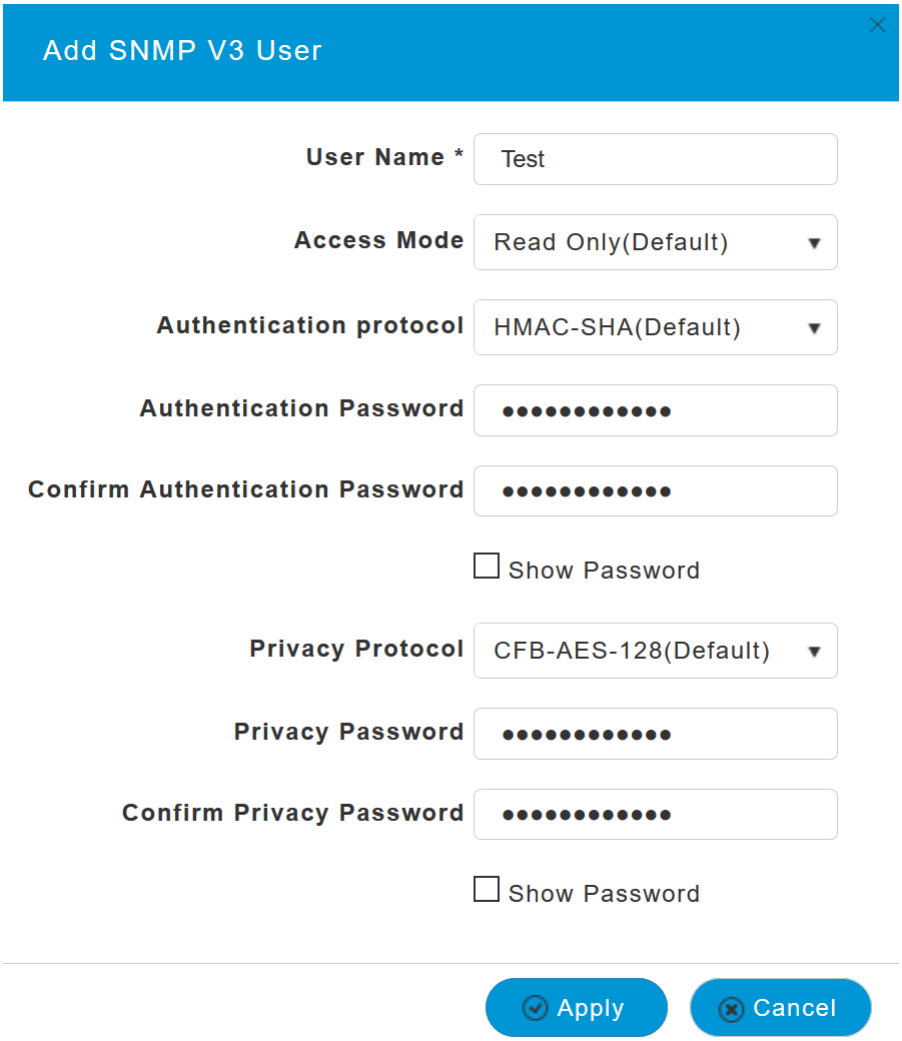
Klicken Sie im Fenster SNMP Setup unter dem Abschnitt *SNMPv3-Benutzer* auf die Schaltfläche **Neues SNMPv3-Benutzer hinzufügen**.



Schritt 3

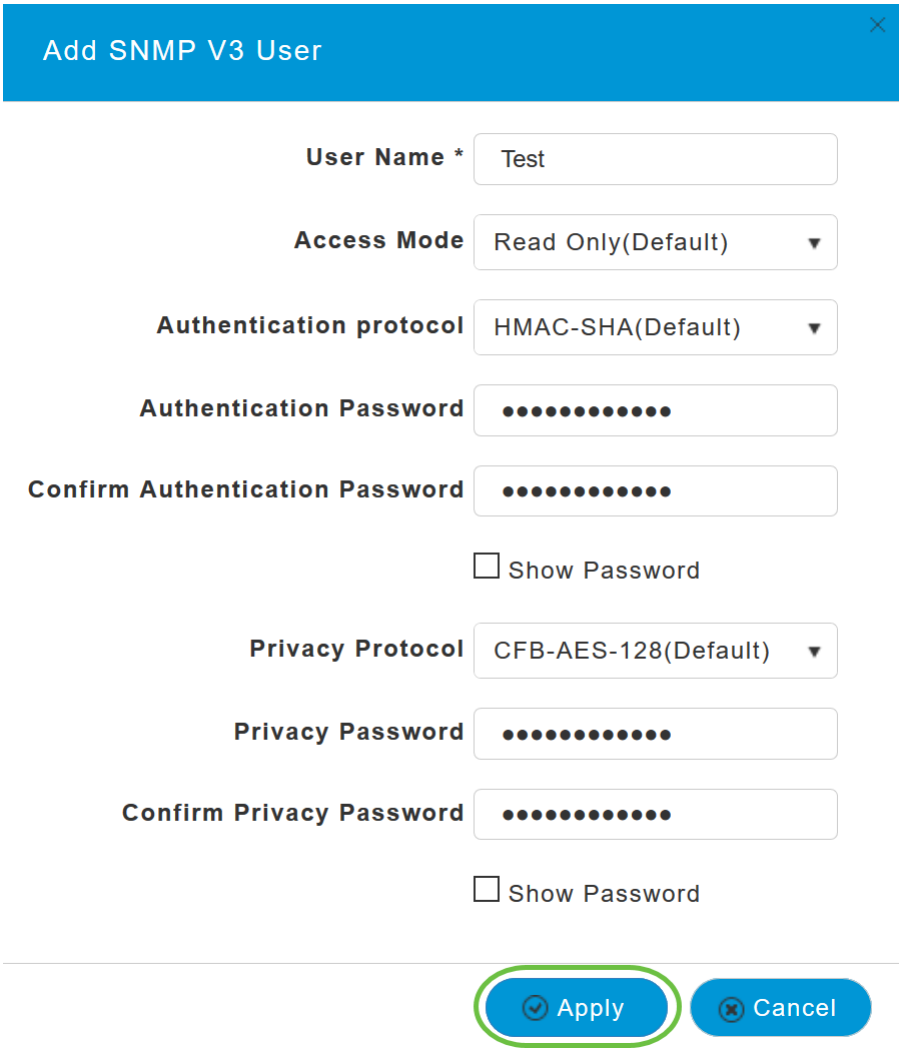
Geben Sie im Fenster *SNMP v3-Benutzer hinzufügen* die folgenden Details ein:

- *Benutzername*: Geben Sie den gewünschten Benutzernamen für den neuen SNMPv3-Benutzer ein.
- *Zugriffsmodus*: Wählen Sie aus der Dropdown-Liste einen der gewünschten Modi aus: *Schreibgeschützt* oder *Lese-/Schreibzugriff.* Der Standardwert ist "**Read *Only"***.
- *Authentifizierungsprotokoll* - Wählen Sie in der Dropdown-Liste *Authentication Protocol* (Authentifizierungsprotokoll) eine der folgenden Optionen aus: HMAC-MD5, HMAC-SHA oder None. Das Standardauthentifizierungsprotokoll ist **HMAC-SHA**.
- *Authentifizierungskennwort* - Geben Sie das gewünschte Authentifizierungskennwort ein. Verwenden Sie eine Kennwortlänge von mindestens 12 bis 31 Zeichen.
- *Authentifizierungskennwort bestätigen* - Bestätigen Sie das oben angegebene Authentifizierungskennwort. Sie können das Kontrollkästchen Show Password (Kennwort anzeigen) aktivieren, um die Einträge in den Feldern Authentication Password (Authentifizierungskennwort) und Confirm Authentication Password (Authentifizierungskennwort bestätigen) anzuzeigen und zu überprüfen, ob die Zeichen übereinstimmen.
- *Datenschutzprotokoll* - Wählen Sie aus der Dropdown-Liste eine der folgenden Optionen aus: CBC-DES, CFB-AES-128 oder None. Das Standard-Datenschutzprotokoll ist **CFB-AES-128**.
- *Datenschutzkennwort* - Geben Sie das gewünschte Datenschutzkennwort ein. Verwenden Sie eine Kennwortlänge von mindestens 12 bis 31 Zeichen.
- *Datenschutzkennwort bestätigen* - Bestätigen Sie das oben angegebene Datenschutzkennwort. Sie können das Kontrollkästchen Show Password (Kennwort anzeigen) aktivieren, um die Einträge in den Feldern Privacy Password (Datenschutzkennwort) und Confirm Privacy Password (Datenschutzkennwort bestätigen) anzuzeigen und zu überprüfen, ob die Zeichen übereinstimmen.

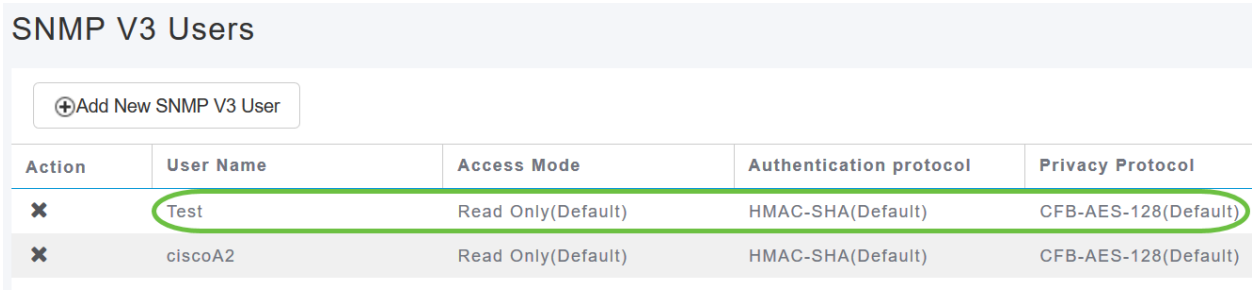


Schritt 4

Klicken Sie auf **Apply**, um einen neuen SNMPv3-Benutzer zu erstellen.



Der neu hinzugefügte SNMPv3-Benutzer wird in der Tabelle *SNMP V3-Benutzer* im Fenster SNMP Setup (SNMP-Einrichtung) angezeigt.

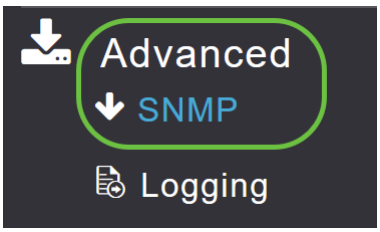


Sie können maximal 7 SNMPv3-Benutzer hinzufügen.

SNMPv3-Benutzer löschen

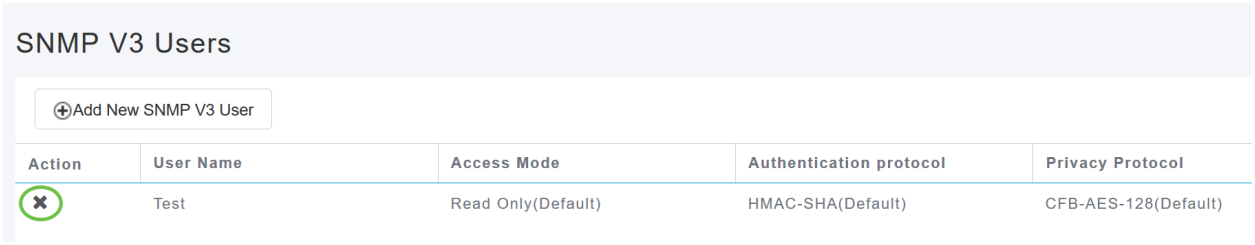
Schritt 1

Wählen Sie **Erweitert > SNMP aus**.



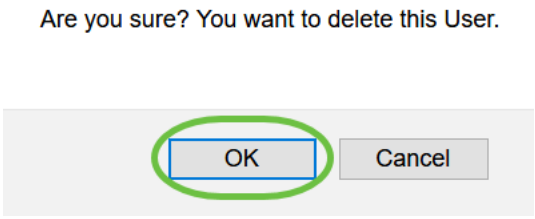
Schritt 2

Klicken Sie im *SNMP-Setup* auf das **X**-Symbol in der Zeile mit dem zu löschenden SNMPv3-Benutzer.



Schritt 3

Ein Popup-Fenster wird angezeigt, um die Aktion zu bestätigen. Klicken Sie auf **OK**.



Die SNMPv3-Benutzertabelle wird aktualisiert, und der gelöschte Eintrag wird aus der Tabelle entfernt.

Schlussfolgerung

Sie sind alle bereit! Sie haben nun erfolgreich SNMP in Ihrem CBW AP konfiguriert. Weitere Informationen erhalten Sie in den folgenden Artikeln. Sie können Ihr Netzwerk ganz einfach verwalten.

Häufig gestellte Fragen Firmware-Upgrade RLANs Erstellung von Anwendungsprofilen Client-Profilerstellung Master-AP-Tools Umbrella WLAN-Benutzer Protokollierung Traffic Shaping Schurken Störungsquelle Konfigurationsmanagement Mesh-Modus für die Portkonfiguration