Configurazione del protocollo SNMP (Simple Network Management Protocol) in Cisco Business Wireless Access Point

Obiettivo

L'obiettivo di questo documento è mostrare come configurare le impostazioni SNMP (Simple Network Management Protocol) sul punto di accesso Cisco Business Wireless (CBW).

Dispositivi interessati | Versione software

- 140AC (Scheda tecnica) | 10.0.1.0 (scarica la versione più recente)
- 145AC (Scheda tecnica) | 10.0.1.0 (scarica la versione più recente)
- 240AC (Scheda tecnica) | 10.0.1.0 (scarica la versione più recente)

Introduzione

I CBW AP supportano l'ultimo standard 802.11ac Wave 2 per prestazioni più elevate, accesso più ampio e reti a densità più elevata. Offrono prestazioni all'avanguardia con connessioni wireless sicure e affidabili, per un'esperienza utente mobile e affidabile.

L'SNMP è un diffuso protocollo di gestione della rete utilizzato per raccogliere informazioni da tutti i dispositivi della rete e per configurare e gestire tali dispositivi. È possibile configurare le modalità di accesso SNMP v2c e SNMP v3 utilizzando l'interfaccia Web del punto di accesso principale. SNMPv2c è il framework amministrativo basato su stringhe della community per SNMPv2. La stringa della community è un tipo di password, trasmessa in testo non crittografato. La funzione SNMP v3 fornisce un accesso sicuro ai dispositivi tramite l'autenticazione e la crittografia dei pacchetti di dati sulla rete.

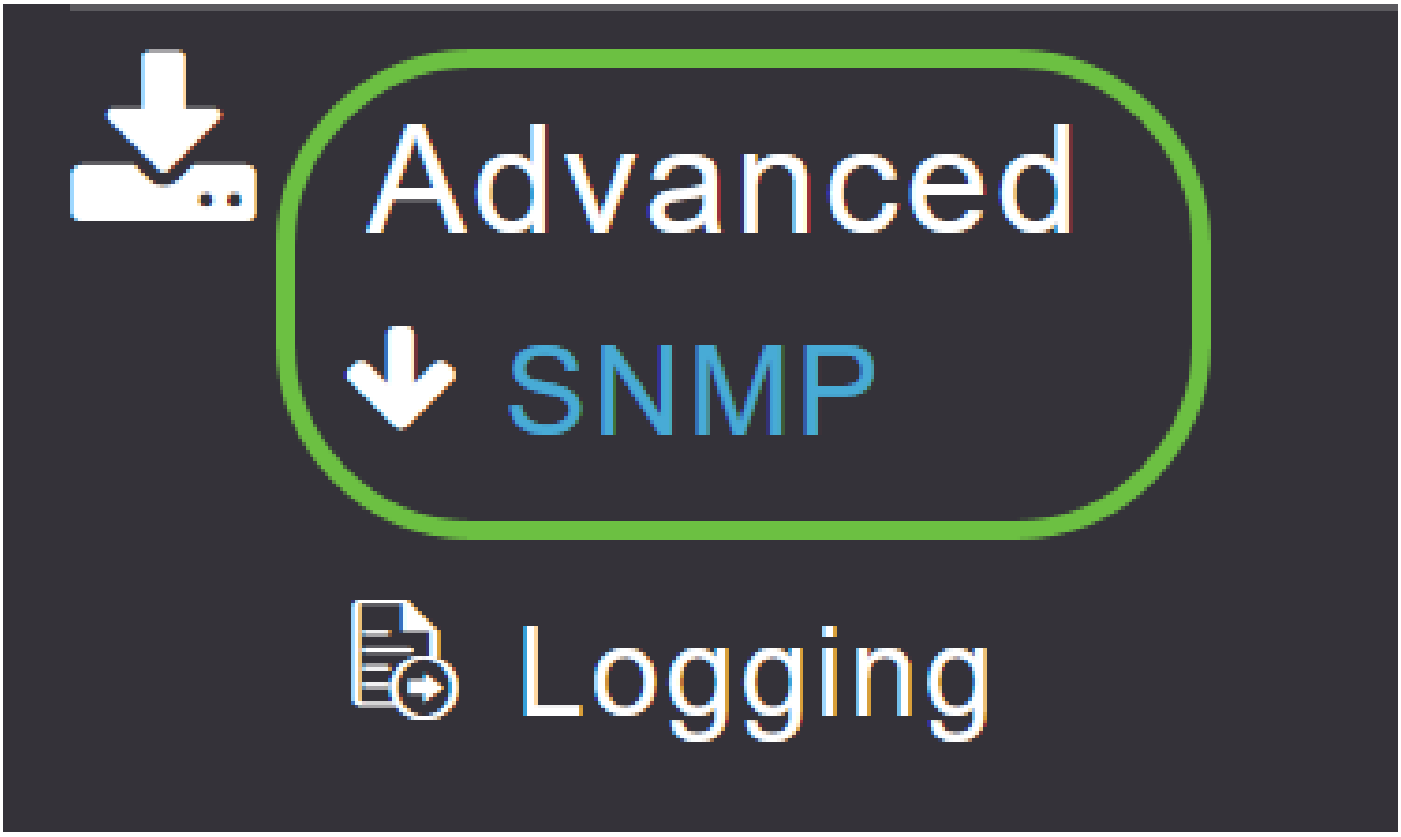
È possibile configurare le seguenti modalità di accesso SNMP per l'access point master:

- Solo SNMP v2c
- Solo SNMP v3
- Sia SNMP v2c che SNMP v3
- Né SNMP v2c né SNMP v3

Configurazione di SNMP

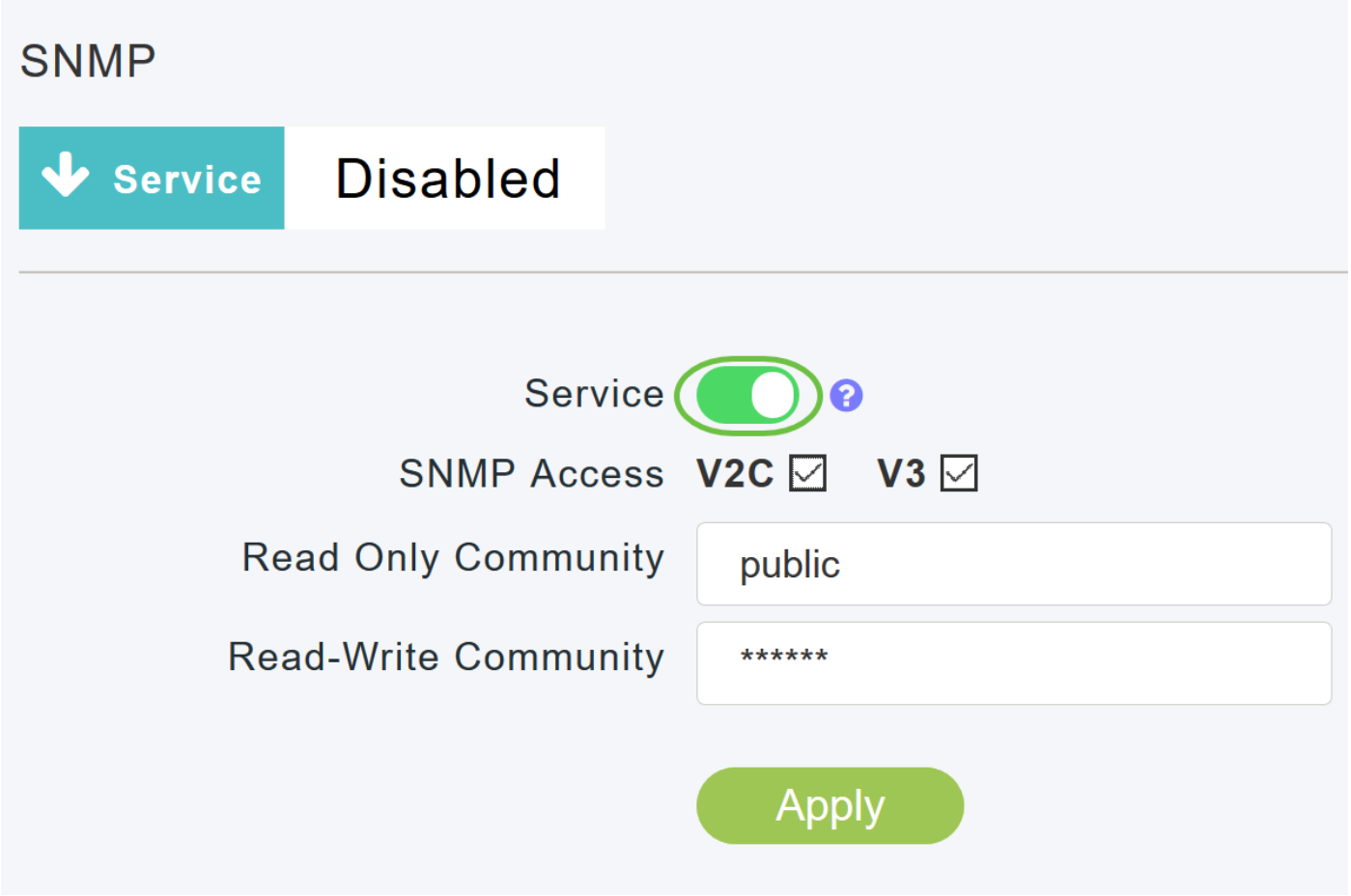
Passaggio 1

Scegliere Avanzate > SNMP.



Passaggio 2

Abilitare l'opzione del servizio SNMP per eseguire query sulla configurazione utilizzando il browser MIB.

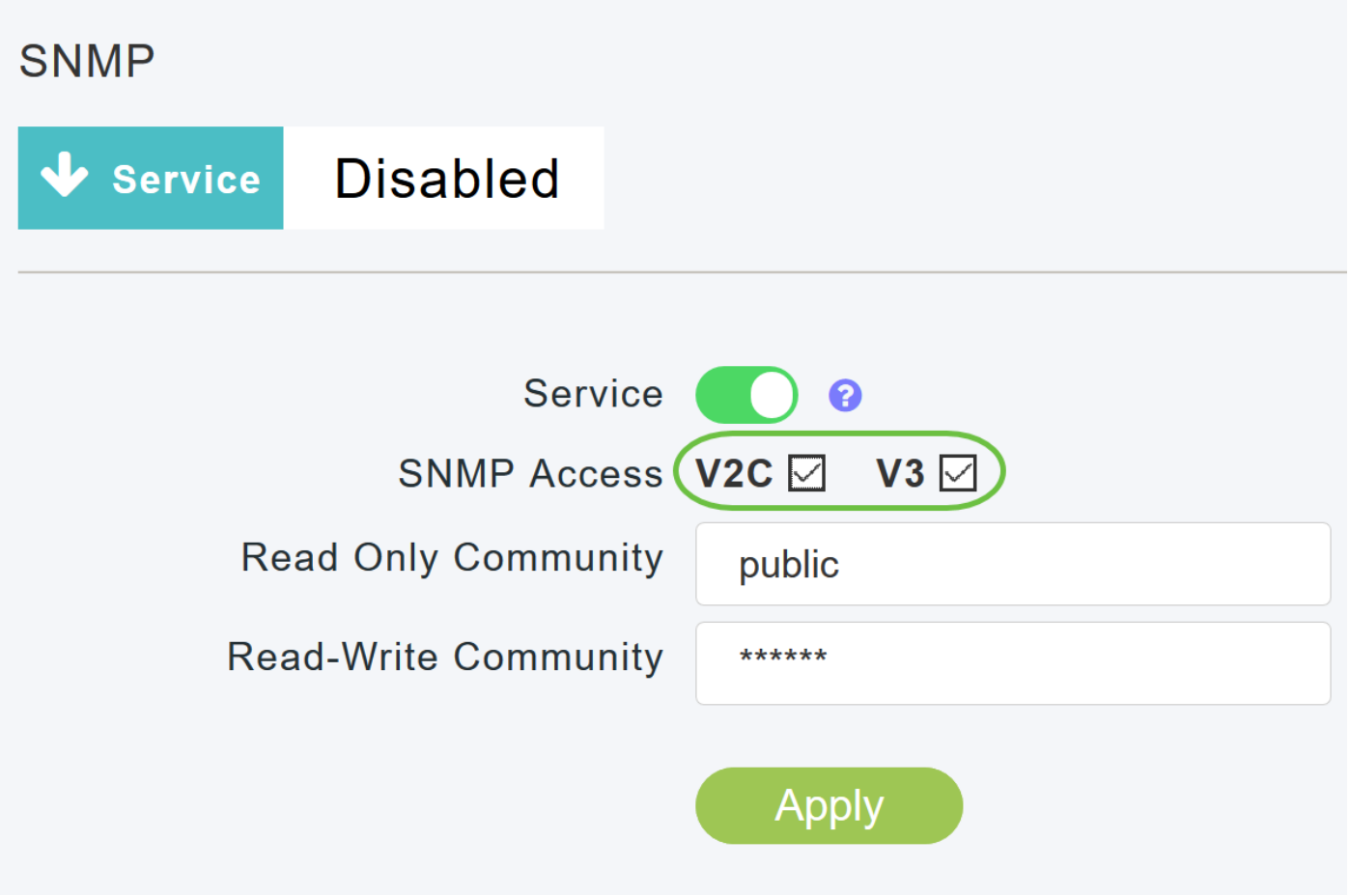


Passaggio 3

Nella finestra SNMP Setup (Impostazione SNMP), selezionare la casella di controllo appropriata accanto a SNMP Access (Accesso SNMP) per abilitare la modalità SNMP desiderata.

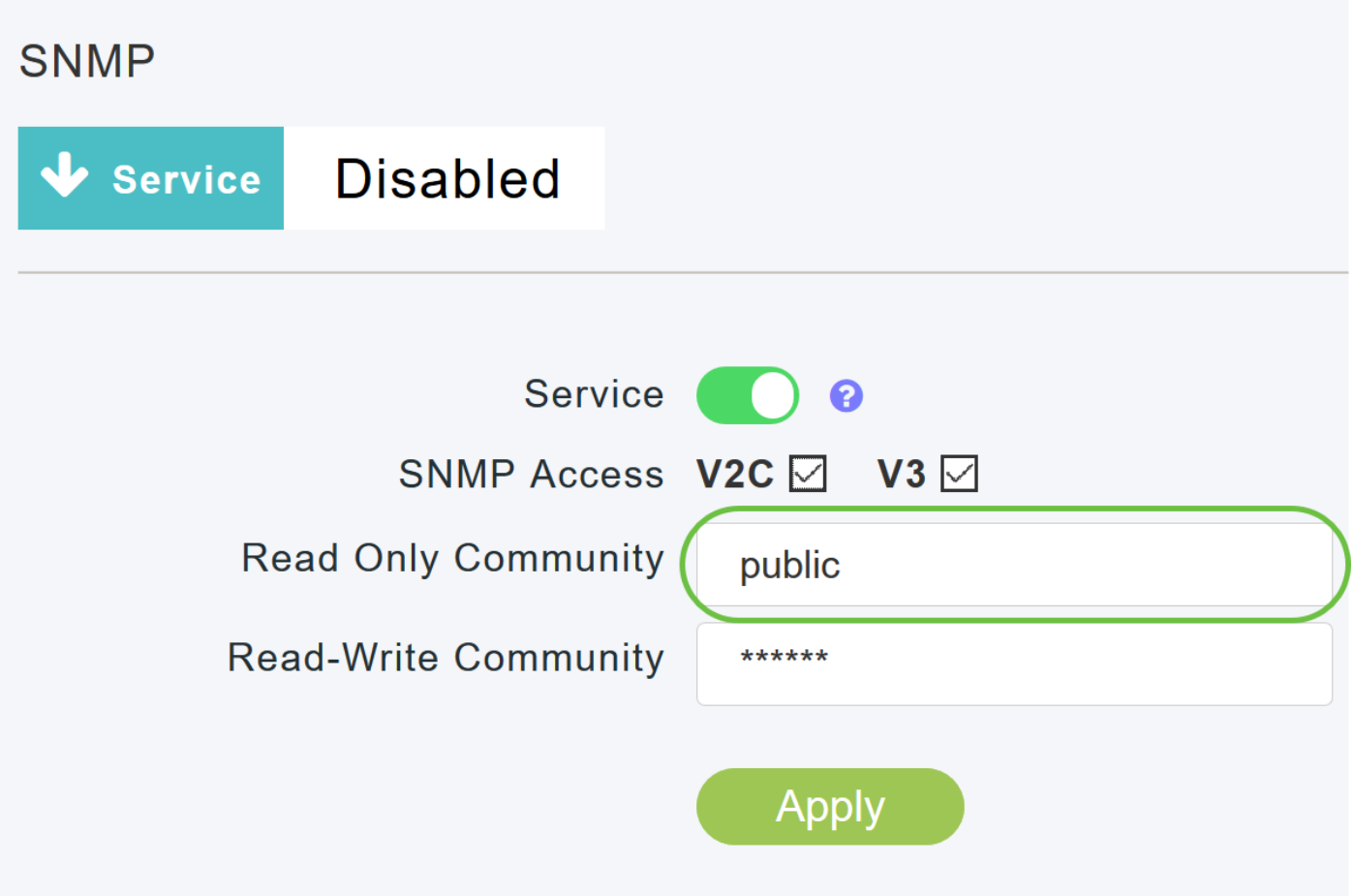
La modalità predefinita è v2c (o per impostazione predefinita, è selezionata una delle due modalità di accesso SNMP o nessuna delle due).

La modalità di accesso SNMP selezionata è attivata.



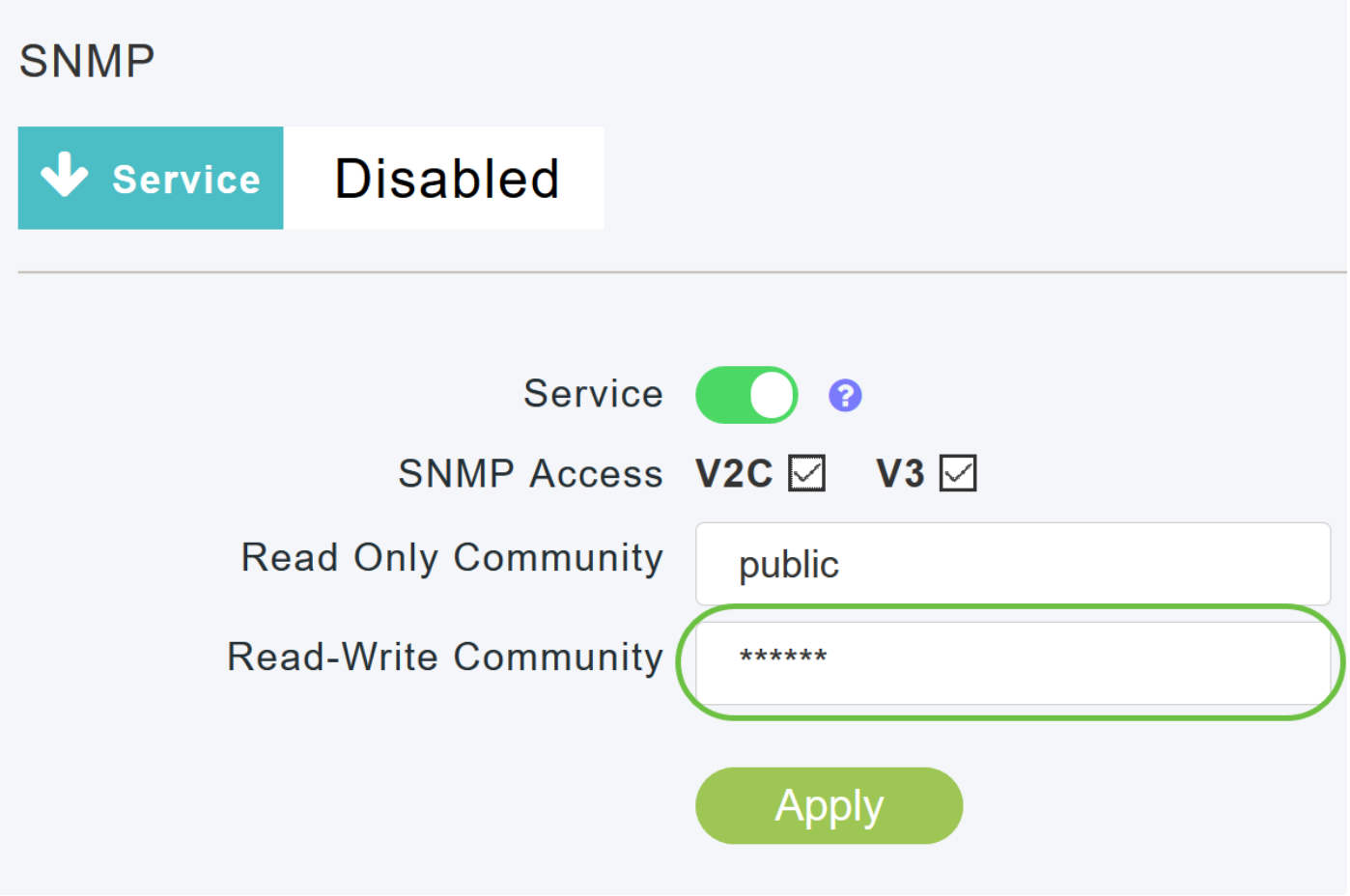
Passaggio 4

Nel campo Community di sola lettura, immettere il nome della community desiderato. Il nome predefinito è public.



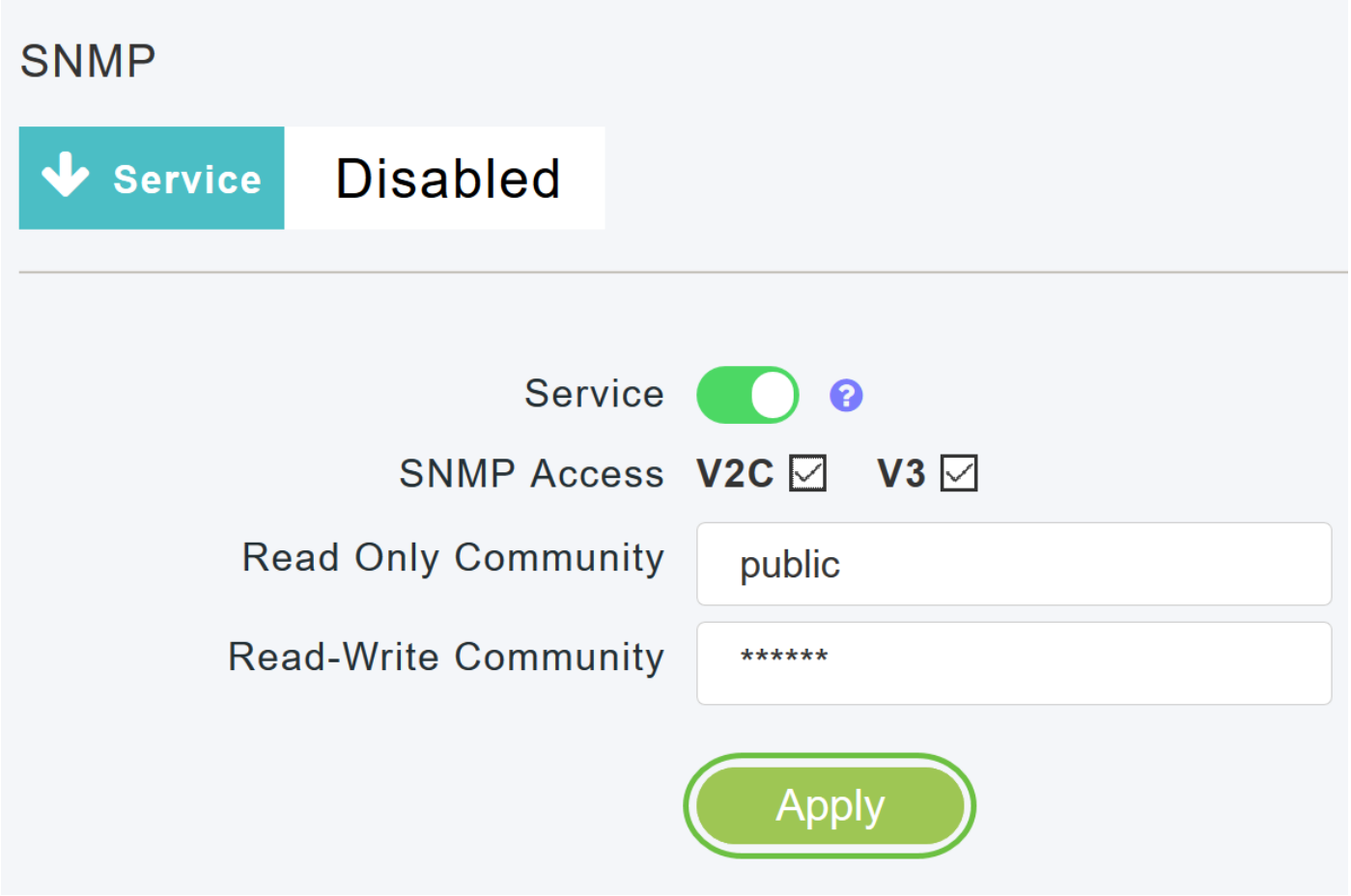
Passaggio 5

Nel campo Community di lettura/scrittura, immettere il nome della community desiderato. Il nome predefinito è private.



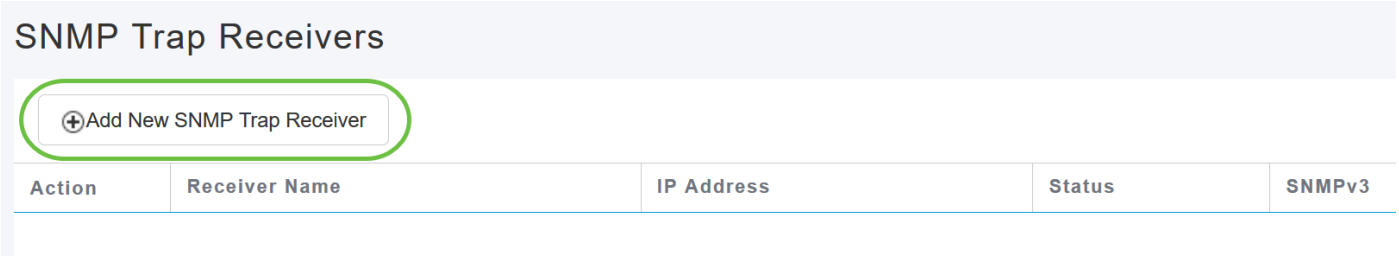
Passaggio 6

Fare clic su Apply (Applica).



Passaggio 7

Per configurare il ricevitore di trap SNMP, fare clic su Add New SNMP Trap Receiver (Aggiungi nuovo ricevitore di trap SNMP). Questo strumento riceve, registra e visualizza le trap SNMP inviate dai dispositivi di rete. L'impostazione predefinita è Disabilitato.



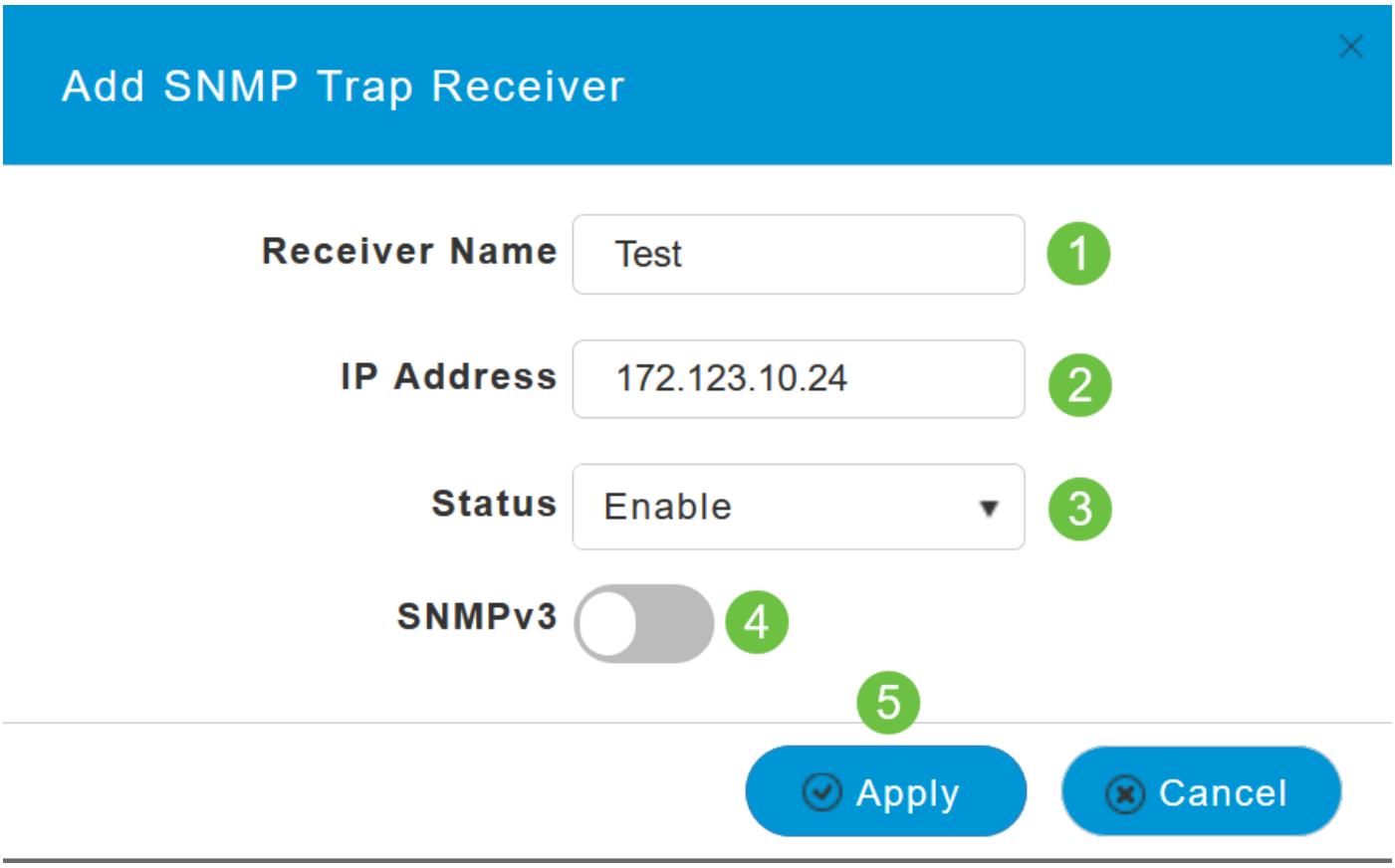
Passaggio 8

Nella finestra Add SNMP Trap Receiver, configurare quanto segue:

- Nome ricevitore
- Indirizzo IP del server a cui si desidera connettersi

- Stato
- Opzione per abilitare SNMPv3

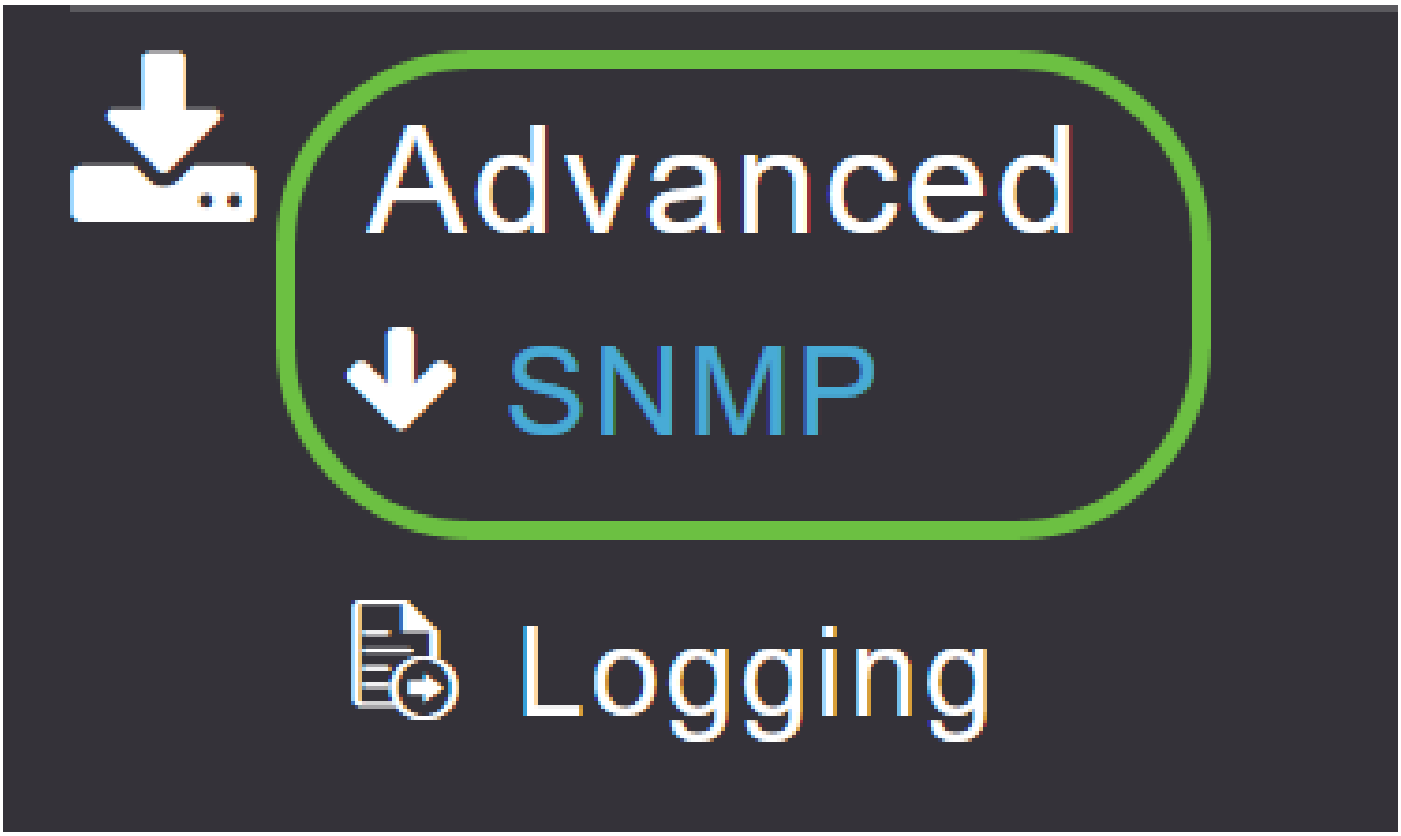
Fare clic su Apply (Applica).



Aggiunta di un utente SNMPv3

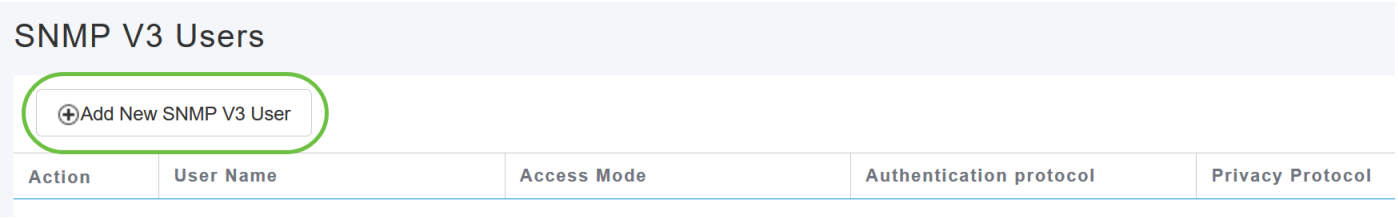
Passaggio 1

Scegliere Avanzate > SNMP.



Passaggio 2

Nella finestra SNMP Setup, nella sezione SNMPv3 Users, fare clic sul pulsante Add New SNMPv3 User.

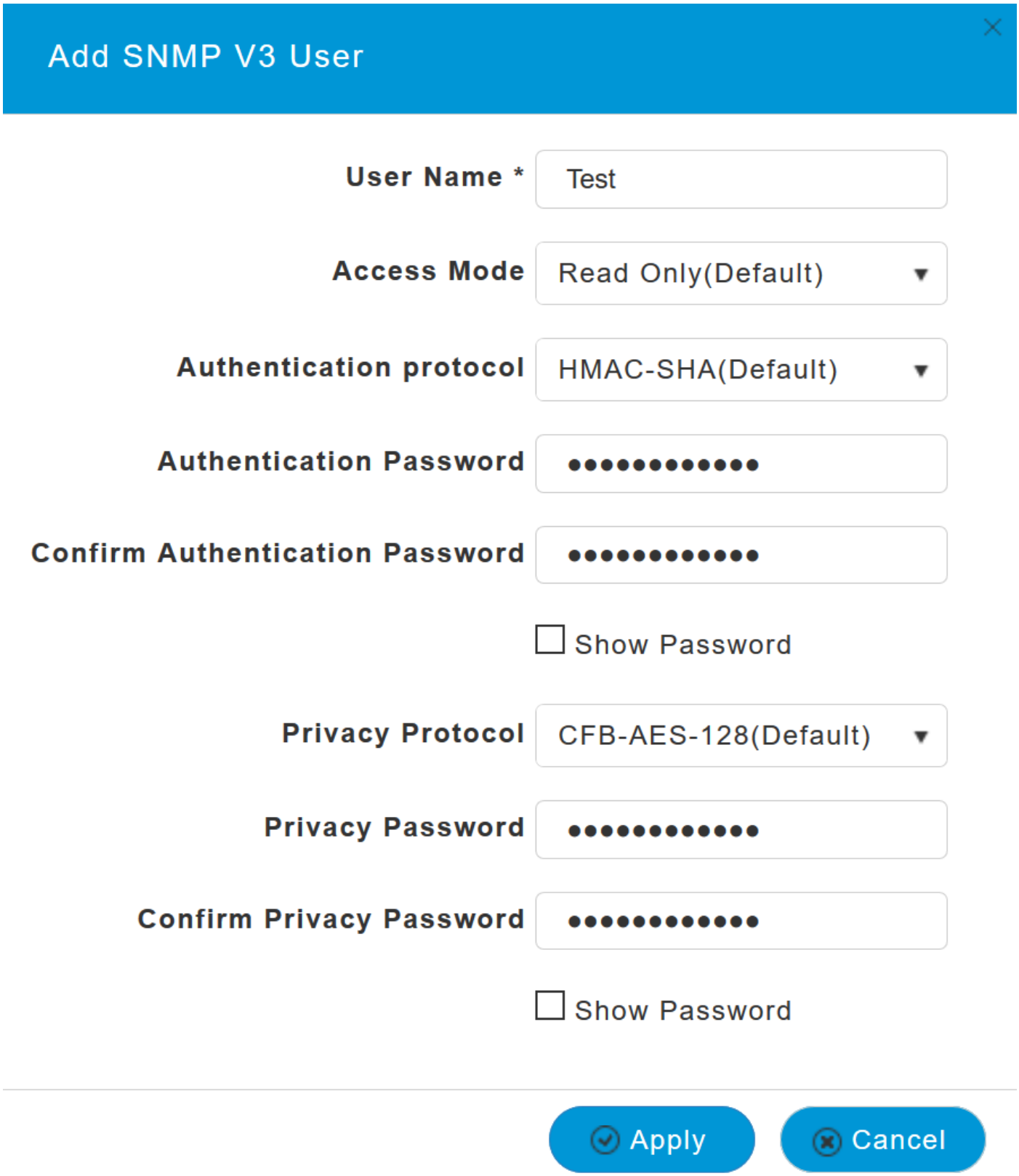


Passaggio 3

Nella finestra Add SNMP v3 User (Aggiungi utente SNMP v3), immettere i seguenti dettagli:

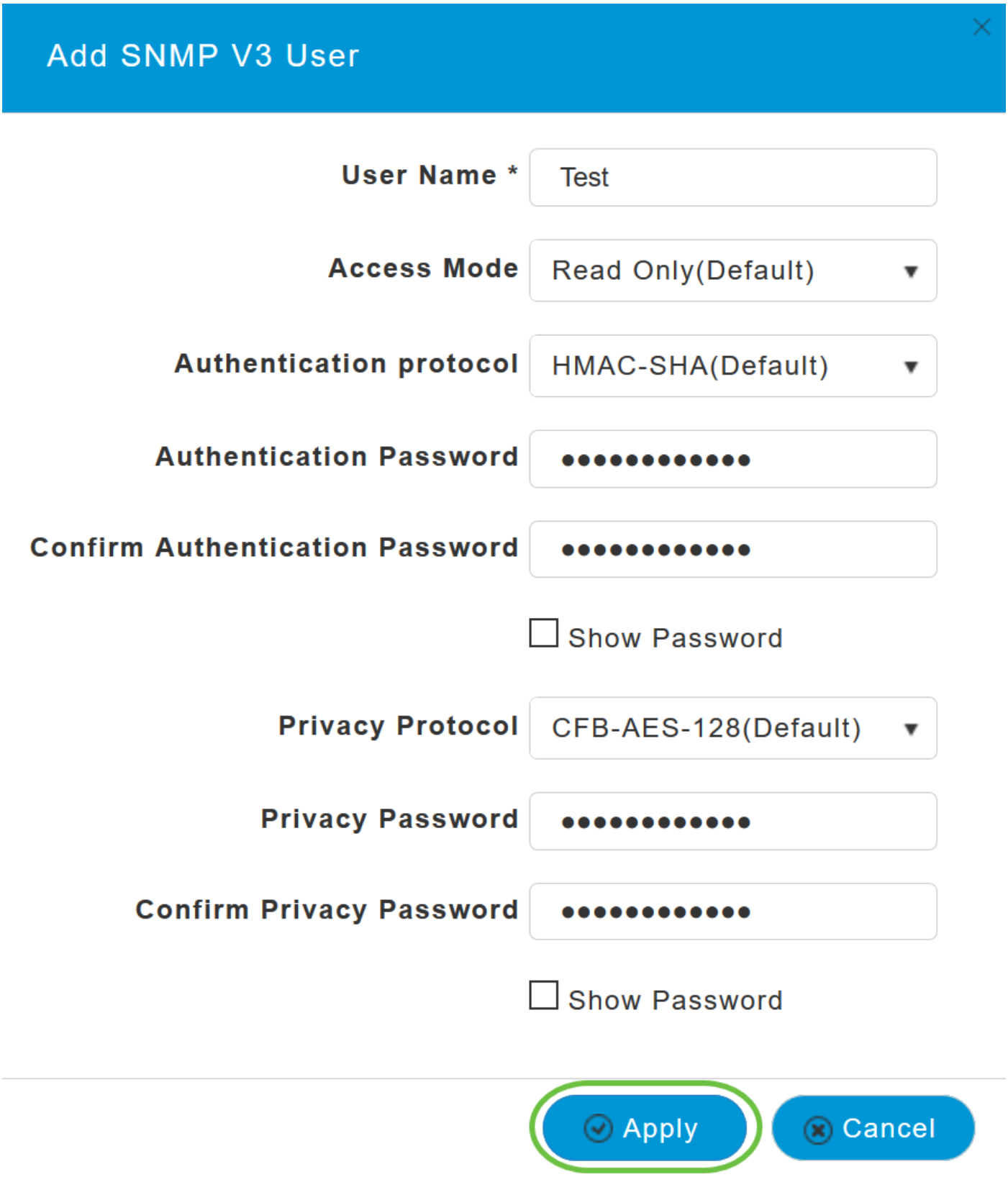
- Nome utente: immettere il nome utente desiderato per il nuovo utente SNMPv3.
- Modalità di accesso: dall'elenco a discesa, scegliere una delle modalità desiderate: Sola lettura o Lettura/scrittura. L'impostazione predefinita è Sola lettura.
- Protocollo di autenticazione: dall'elenco a discesa Protocollo di autenticazione scegliere una delle opzioni seguenti: HMAC-MD5, HMAC-SHA o Nessuno. Il protocollo di autenticazione predefinito è HMAC-SHA.

- Password di autenticazione: immettere la password di autenticazione desiderata. La lunghezza minima della password è di 12-31 caratteri.
- Conferma password di autenticazione: conferma la password di autenticazione specificata in precedenza. È possibile selezionare la casella di controllo Mostra password per visualizzare le voci nei campi Password di autenticazione e Conferma password di autenticazione e verificare se i caratteri corrispondono.
- Privacy Protocol: dall'elenco a discesa, selezionare una delle seguenti opzioni: CBC-DES, CFB-AES-128 o Nessuno. Il protocollo di privacy predefinito è CFB-AES-128.
- Password privacy - Immettere la password per la privacy desiderata. La lunghezza minima della password è di 12-31 caratteri.
- Confirm Privacy Password (Conferma password per la privacy) - Conferma la password per la privacy specificata sopra. È possibile selezionare la casella di controllo Mostra password per visualizzare le voci nei campi Password privacy e Conferma password privacy e verificare se i caratteri corrispondono.

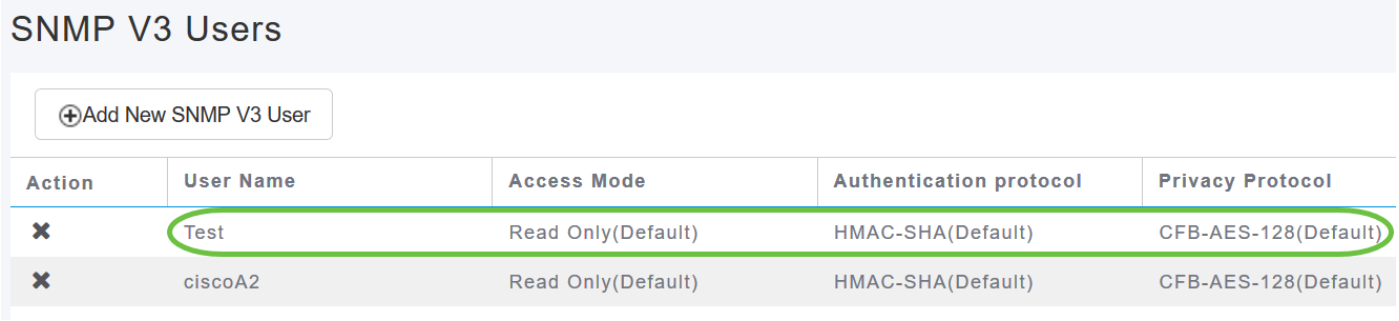


Passaggio 4

Fare clic su Apply (Applica) per creare un nuovo utente SNMPv3.



L'utente SNMPv3 appena aggiunto viene visualizzato nella tabella SNMP V3 Users della finestra SNMP Setup.

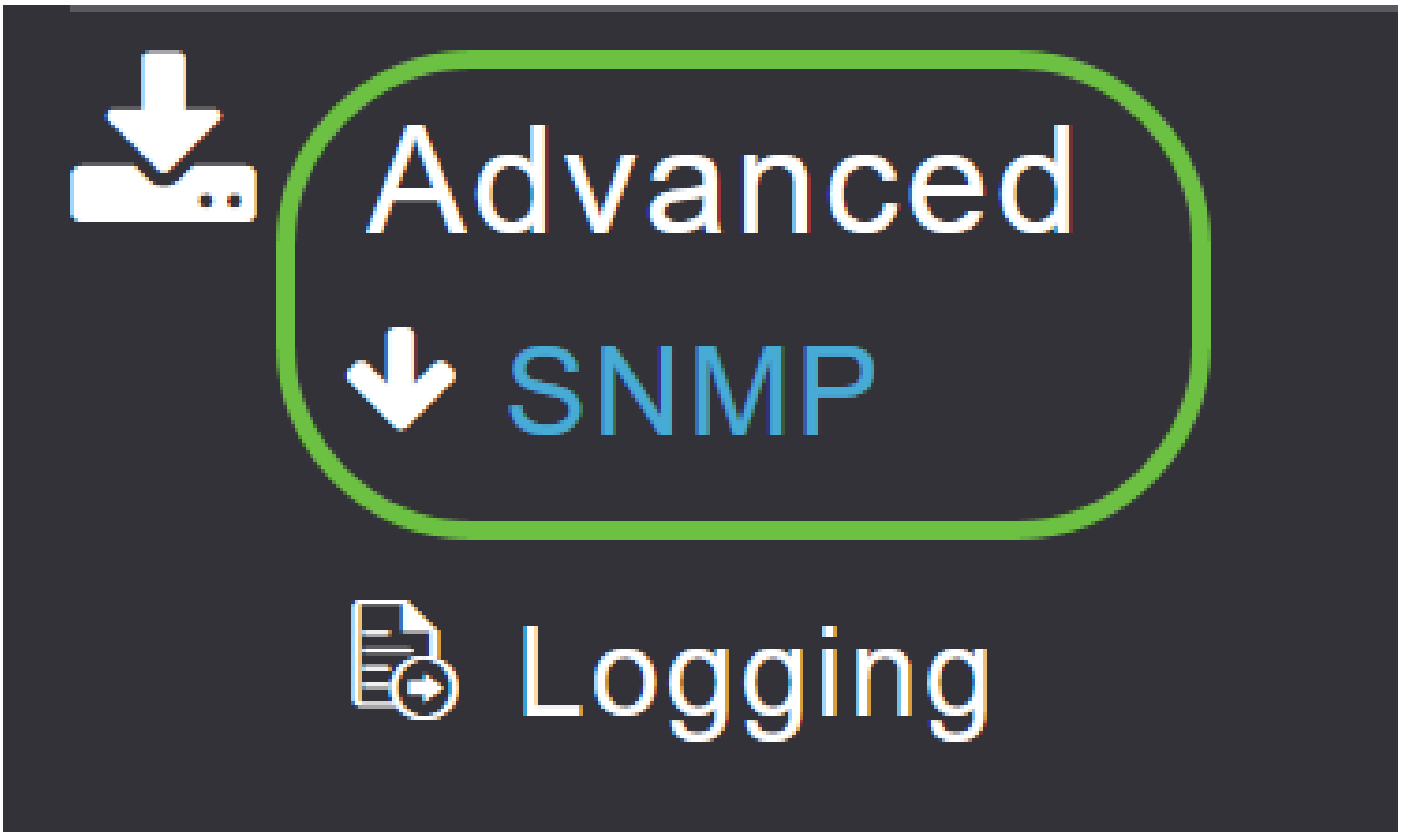


È possibile aggiungere un massimo di 7 utenti SNMPv3.

Elimina utente SNMPv3

Passaggio 1

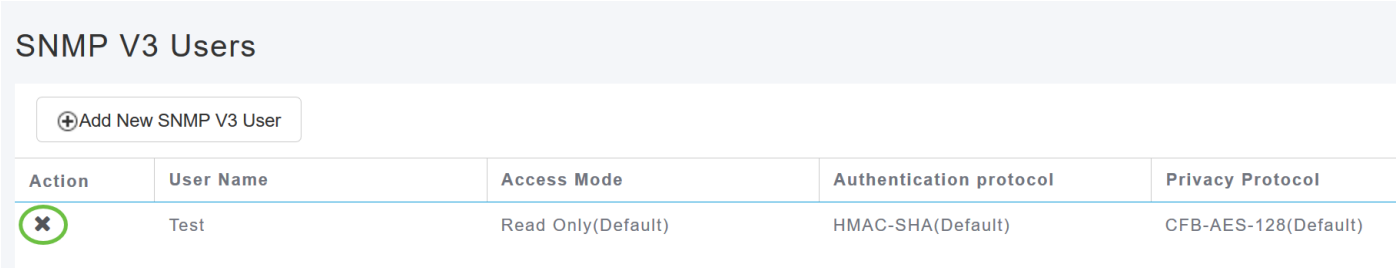
Scegliere Avanzate > SNMP.



Passaggio 2

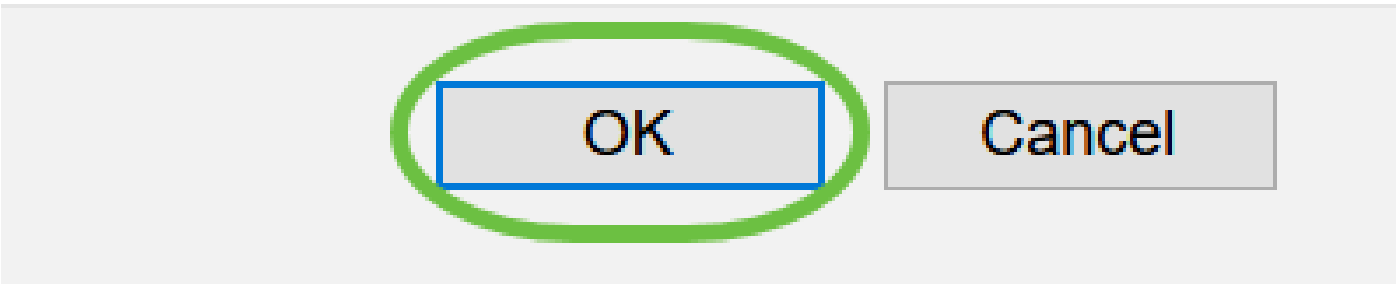
Nella finestra SNMP Setup, fare clic sull'icona X nella riga contenente l'utente SNMPv3 che si

desidera eliminare.



Passaggio 3

Viene visualizzata una finestra popup per confermare l'azione. Fare clic su OK.



La tabella Utenti SNMPv3 viene aggiornata e la voce eliminata viene rimossa dalla tabella.

Conclusioni

È tutto pronto! Il protocollo SNMP è stato configurato correttamente nell'access point CBW. Per ulteriori informazioni, leggere gli articoli seguenti e gestire la rete con facilità.

Domande frequenti Aggiornamento firmware RLAN Application Profiling Client Profiling

Master AP Tools Umbrella WLAN Users Logging Traffic Shaping Rogues Interferers Gestione configurazione Port Configuration Mesh Mode

Informazioni su questa traduzione
Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).