Configurazione rete totale: RV345P e Cisco Business Wireless tramite interfaccia utente Web

Obiettivo

In questa guida viene illustrato come configurare una rete mesh wireless utilizzando un router RV345P, un punto di accesso CBW140AC e due estensori mesh CBW142ACM.

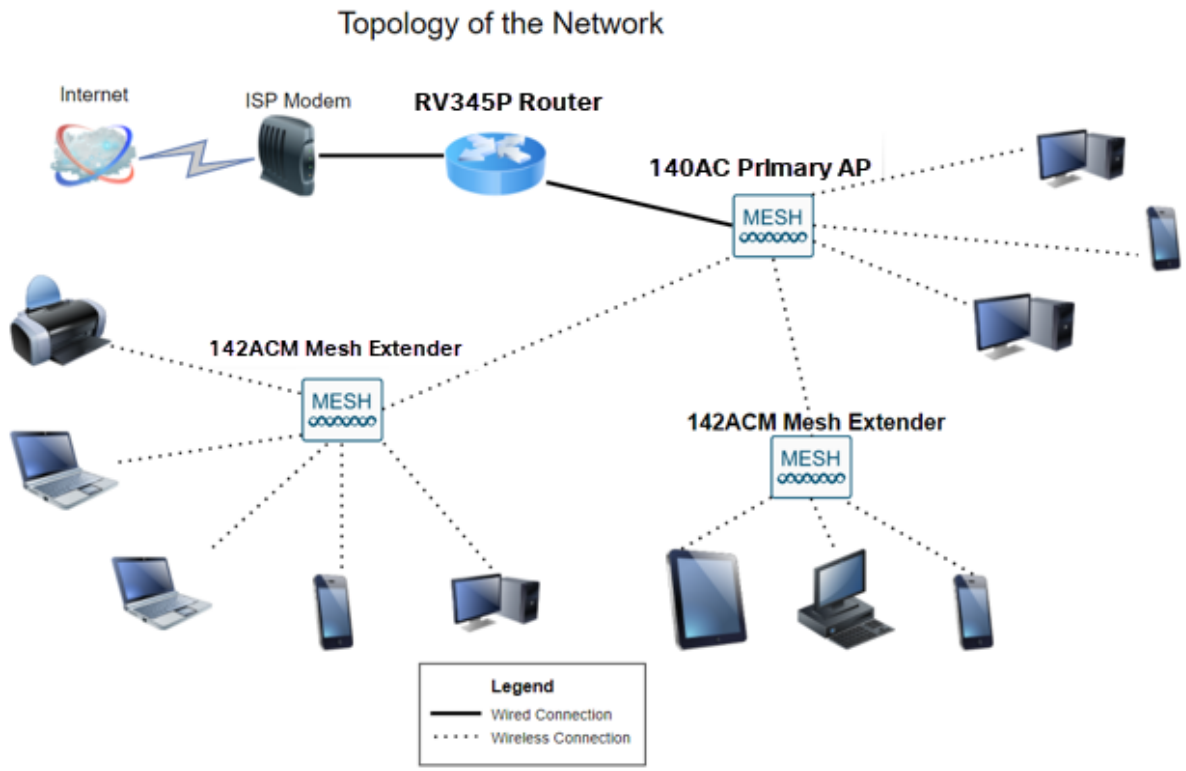
In questo articolo viene utilizzata l'interfaccia utente Web per impostare la rete wireless mesh. Se si preferisce utilizzare l'applicazione mobile, che è consigliata per una facile configurazione wireless, fare clic su per passare all'articolo che utilizza l'applicazione mobile.

Sommario

- Prerequisiti
  - Preparazione del router
  - Ottieni un account Cisco.com
- Configurazione del router RV345P
  - RV345P integrato
  - Configurazione del router
  - Risoluzione dei problemi relativi alla connessione Internet
  - Configurazione iniziale
  - Modificare un indirizzo IP se necessario (facoltativo)
  - Aggiorna firmware se necessario
  - Configurazione degli aggiornamenti automatici sul router serie RV345P
- Opzioni di sicurezza
  - Licenza RV Security (opzionale)
  - Filtro Web sul router RV345P
  - Licenza Umbrella RV Branch (opzionale)
  - Altre opzioni di sicurezza
- Opzioni VPN
  - VPN PassThrough
  - AnyConnect VPN
  - Mostra VPN soft
  - Altre opzioni VPN

- Configurazioni supplementari sul router RV345P
    - Configurazione delle VLAN (opzionale)
    - Assegnazione delle VLAN alle porte (facoltativo)
    - Aggiunta di un indirizzo IP statico (facoltativo)
    - Gestione dei certificati (facoltativo)
    - Configurazione di una rete mobile con un dongle e un router serie RV345P (opzionale)
- Configurazione di CBW140AC
    - CBW140AC
    - Configurazione del punto di accesso wireless primario 140AC sull'interfaccia utente Web
- Suggerimenti per la risoluzione dei problemi wireless
- Configurazione dei CBW142ACM Mesh Extender tramite interfaccia utente Web
- Controllo e aggiornamento del software tramite l'interfaccia utente Web
- Creazione di WLAN sull'interfaccia utente Web
- Configurazioni wireless opzionali
    - Creazione di una WLAN guest mediante l'interfaccia utente Web (facoltativo)
    - Creazione profilo applicazione mediante interfaccia utente Web (facoltativo)
    - Creazione profilo client tramite interfaccia utente Web (facoltativo)

Topologia



Introduzione

Dopo aver completato tutte le ricerche, avete acquistato le apparecchiature Cisco: fantastico! In questo scenario, viene utilizzato un router RV345P. Questo router offre funzionalità Power over Ethernet (PoE) che consentono di collegare il CBW140AC al router anziché a uno switch. I dispositivi di estensione mesh CBW140AC e CBW142ACM verranno utilizzati per creare una rete mesh wireless.

Il router avanzato offre inoltre la possibilità di aggiungere nuove funzionalità.

1. Il controllo delle applicazioni consente di controllare il traffico. Questa funzionalità può essere configurata per consentire il traffico ma per registrarlo, bloccarlo e registrarlo o semplicemente per bloccare il traffico.
2. Il filtro Web viene utilizzato per impedire il traffico Web verso siti Web non sicuri o inappropriati. Nessuna registrazione con questa funzionalità.
3. AnyConnect è una rete VPN (Virtual Private Network) SSL (Secure Sockets Layer) disponibile su Cisco. Le VPN consentono agli utenti e ai siti remoti di connettersi agli uffici aziendali o ai centri dati creando un tunnel sicuro tramite Internet.

Per utilizzare queste funzionalità, è necessario acquistare una licenza. I router e le

licenze sono registrati online, e saranno trattati in questa guida.

Se non si conoscono alcuni dei termini utilizzati in questo documento o si desiderano ulteriori dettagli su Mesh Networking, controllare gli articoli seguenti:

- Cisco Business: glossario dei nuovi termini
- Benvenuto in Cisco Business Wireless Mesh Networking
- Domande frequenti (FAQ) per una rete wireless aziendale Cisco

Dispositivi interessati | Versione software

- RV345P |1.0.03.21
- CBW140AC |10.4.1.0
- CBW142ACM | 10.4.1.0 (per la rete a maglie è necessaria almeno una rete a maglie)

Prerequisiti

Preparazione del router

1. Verificare di disporre di una connessione Internet corrente per la configurazione.
2. Contattare il provider di servizi Internet (ISP) per informazioni su eventuali istruzioni speciali relative all'utilizzo del router RV345P. Alcuni ISP offrono gateway con router integrati. Se si dispone di un gateway con un router integrato, potrebbe essere necessario disattivare il router e passare l'indirizzo IP WAN (Wide Area Network), ovvero l'indirizzo di protocollo Internet univoco assegnato dal provider Internet all'account, e tutto il traffico di rete attraverso il nuovo router.
3. Decidere dove posizionare il router. Se possibile, è necessario disporre di un'area aperta. Potrebbe non essere facile perché è necessario connettere il router al gateway a banda larga (modem) dal provider di servizi Internet (ISP).

Ottieni un account Cisco.com

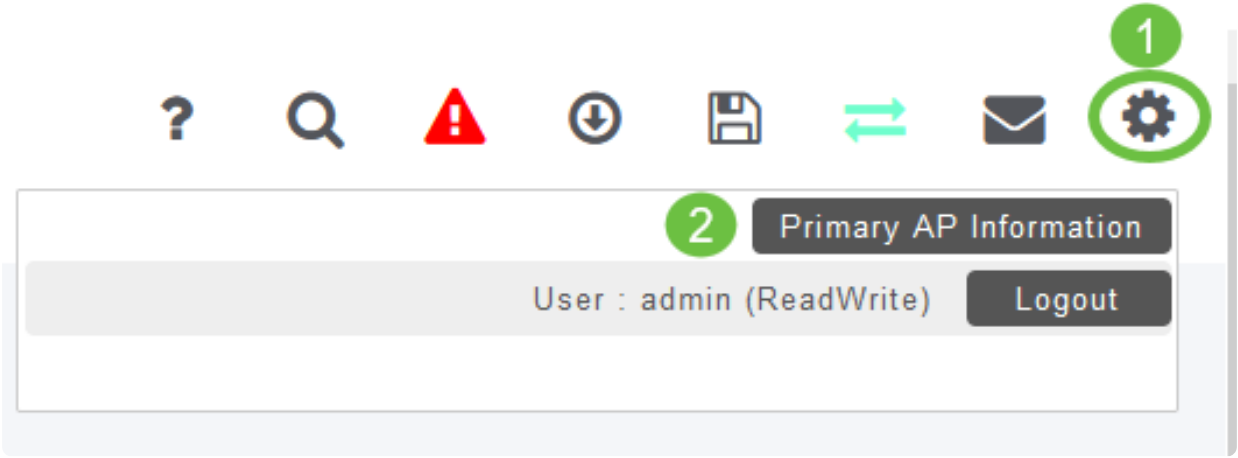
Ora che si possiede un'apparecchiatura Cisco, è necessario ottenere un account Cisco.com, a volte indicato come ID CCO (Cisco Connection Online Identification).

Nessun addebito per un account.

Se disponi già di un account, puoi passare alla sezione successiva di questo articolo.

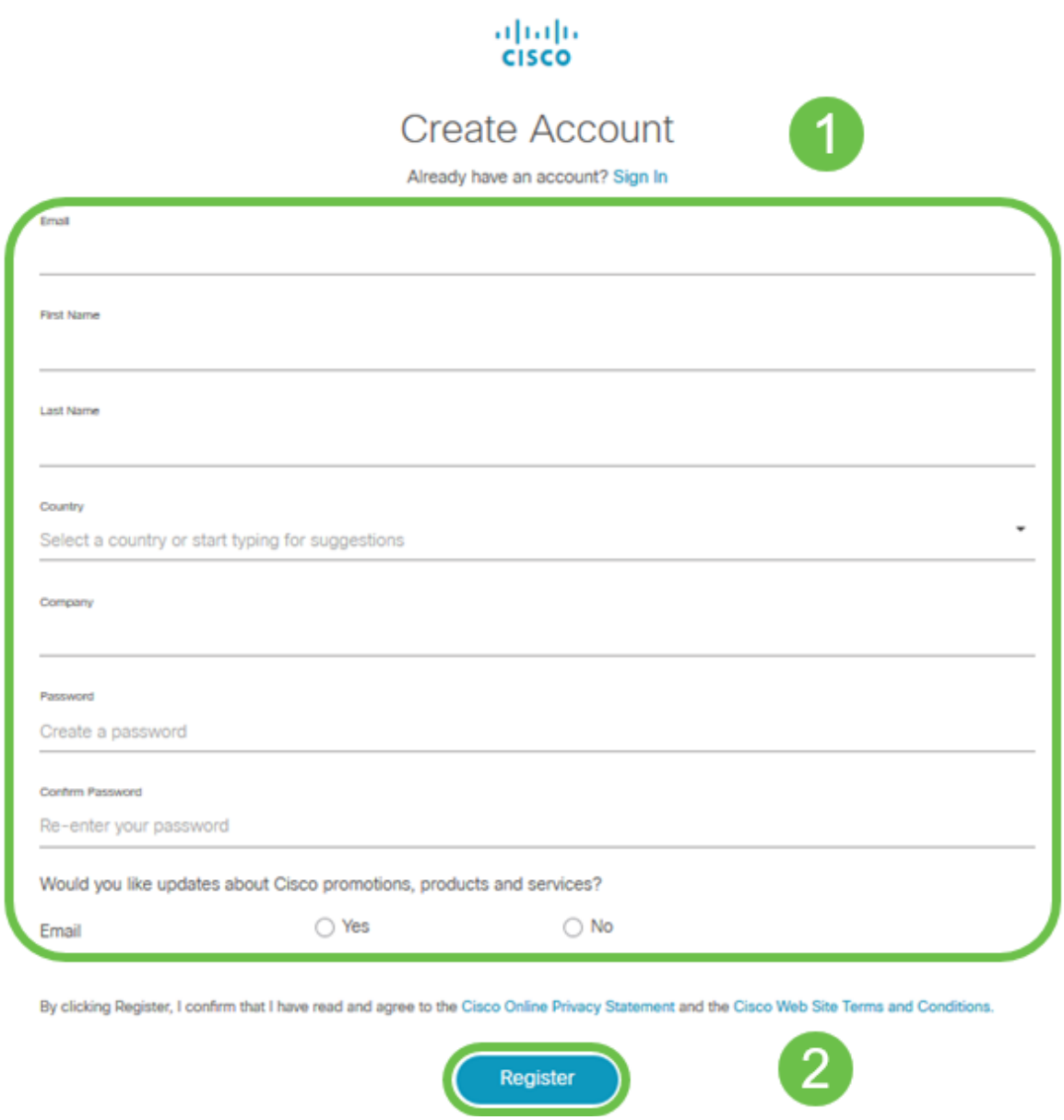
Passaggio 1

Visitare il sito Cisco.com. Fare clic sull'icona della persona, quindi creare un account.



Passaggio 2

Immettere i dettagli richiesti per creare l'account e fare clic su Registra. Seguire le istruzioni per completare il processo di registrazione.



In caso di problemi, fai clic su per accedere alla Cisco.com Guida alla registrazione dell'account.

Configurazione del router RV345P

Un router è essenziale in una rete perché instrada i pacchetti. Consente a un computer di comunicare con altri computer che non si trovano sulla stessa rete o subnet. Un router accede a una tabella di routing per determinare dove inviare i pacchetti. La tabella di routing elenca gli indirizzi di destinazione. Le configurazioni statiche e dinamiche possono essere entrambe elencate nella tabella di routing per portare i pacchetti alla destinazione specifica.

La stampante RV345P è dotata di impostazioni predefinite ottimizzate per molte piccole aziende. È tuttavia possibile che le esigenze della rete o del provider di servizi Internet (ISP) richiedano la modifica di alcune di queste impostazioni. Dopo aver contattato l'ISP per conoscere i requisiti necessari, è possibile apportare le modifiche utilizzando l'interfaccia utente Web.

Siete pronti? Andiamo!

RV345P integrato

Passaggio 1

Collegare il cavo Ethernet da una delle porte LAN (Ethernet) RV345P alla porta Ethernet del computer. Se il computer non dispone di una porta Ethernet, sarà necessario disporre di un adattatore. Per eseguire la configurazione iniziale, il terminale deve trovarsi nella stessa sottorete cablata dell'RV345P.

Passaggio 2

Assicurarsi di utilizzare l'adattatore di alimentazione in dotazione con RV345P. L'utilizzo di un adattatore di alimentazione diverso potrebbe danneggiare il router RV345P o causare il malfunzionamento dei dongle USB. L'interruttore di alimentazione è acceso per impostazione predefinita.

Collegare l'adattatore di alimentazione alla porta 12 V CC dell'RV345P, ma non collegarlo all'alimentazione.

Passaggio 3

Assicurarsi che il modem sia spento.

Passaggio 4

Utilizzare un cavo Ethernet per collegare il modem via cavo o DSL alla porta WAN

dell'RV345P.

Passaggio 5

Inserire l'altra estremità dell'adattatore RV345P in una presa elettrica. In questo modo si accende la RV345P. Ricollegare il modem in modo che possa accendersi. La spia di alimentazione sul pannello anteriore è verde fisso quando l'adattatore di alimentazione è collegato correttamente e l'avvio di RV345P è terminato.

Configurazione del router

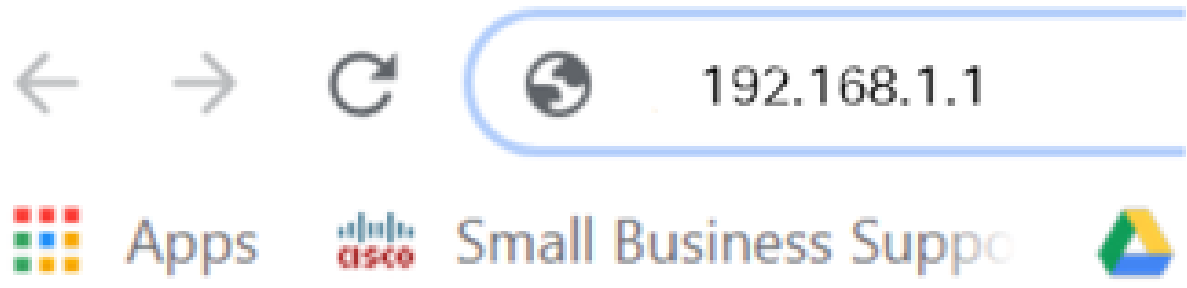
Il lavoro di preparazione è terminato, ora è il momento di arrivare ad alcune configurazioni! Per avviare l'interfaccia utente Web, eseguire la procedura seguente.

Passaggio 1

Se il computer è configurato per diventare un client DHCP (Dynamic Host Configuration Protocol), al computer viene assegnato un indirizzo IP compreso nell'intervallo 192.168.1.x. DHCP automatizza il processo di assegnazione di indirizzi IP, subnet mask, gateway predefiniti e altre impostazioni ai computer. Per ottenere un indirizzo, i computer devono essere impostati in modo da poter partecipare al processo DHCP. A tale scopo, selezionare per ottenere automaticamente un indirizzo IP nelle proprietà di TCP/IP nel computer.

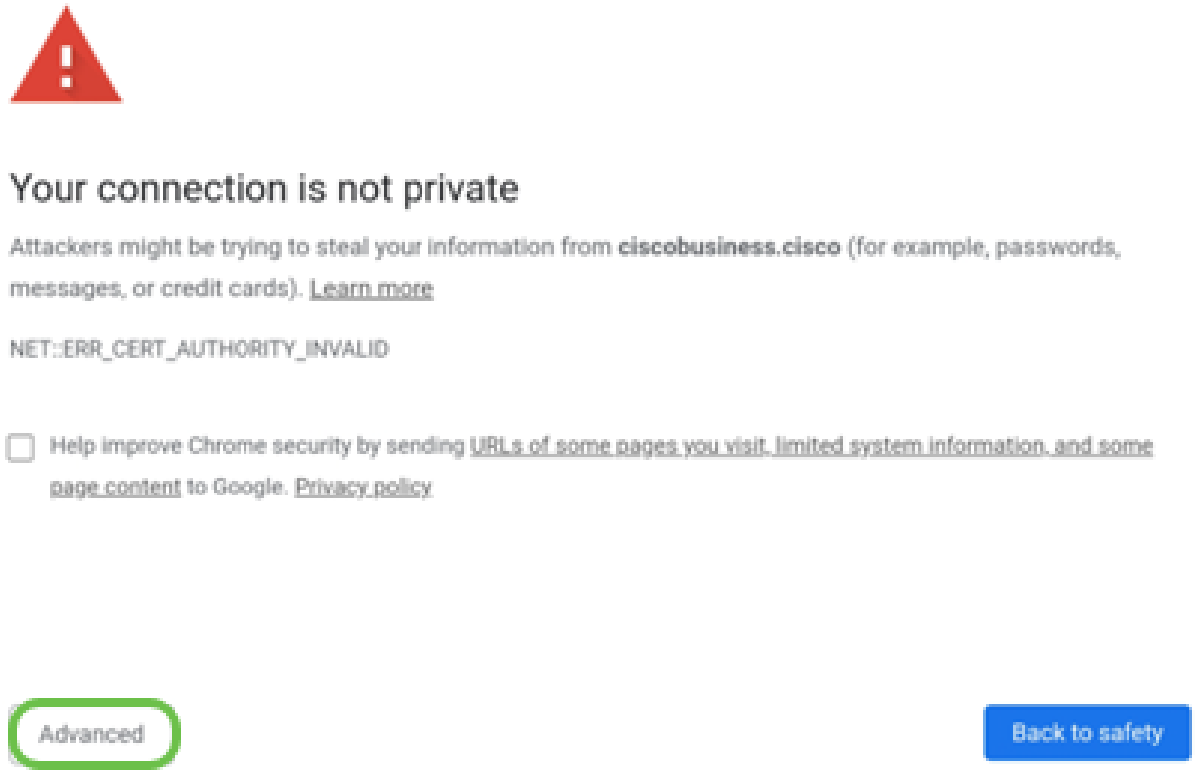
Passaggio 2

Aprire un browser Web come Safari, Internet Explorer o Firefox. Nella barra degli indirizzi, immettere l'indirizzo IP predefinito di RV345P, 192.168.1.1.



Passaggio 3

È possibile che il browser invii un avviso per segnalare che il sito Web non è attendibile. Accedere al sito Web. Se non si è connessi, passare alla sezione Risoluzione dei problemi di connessione Internet.

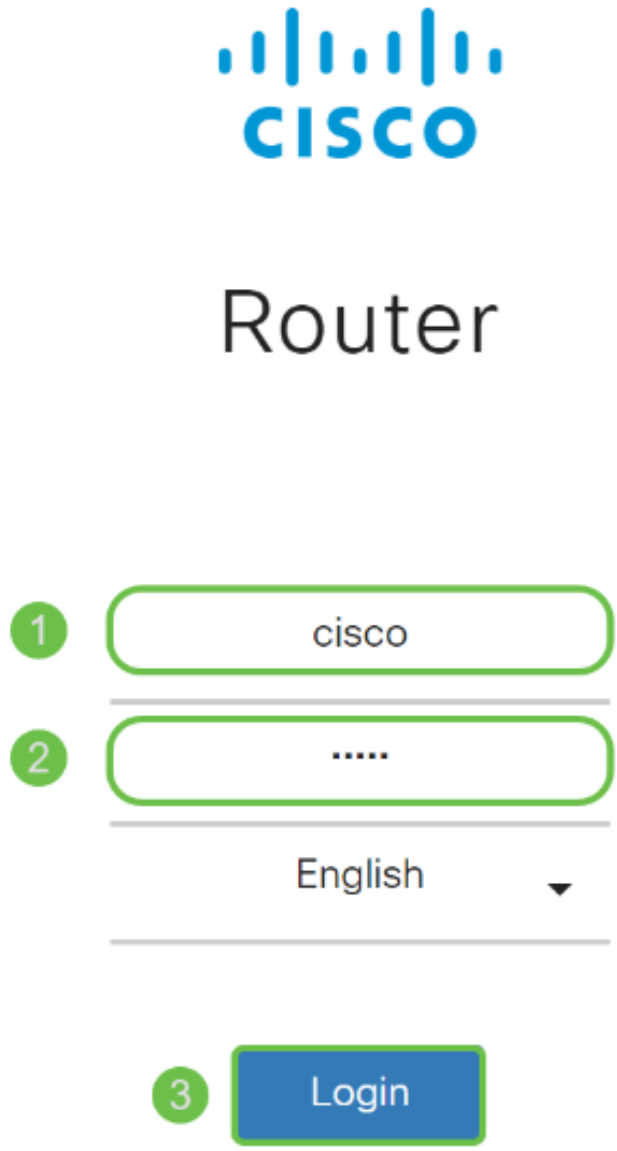


Passaggio 4

Quando viene visualizzata la pagina di accesso, immettere il nome utente predefinito cisco e la password predefinita cisco.

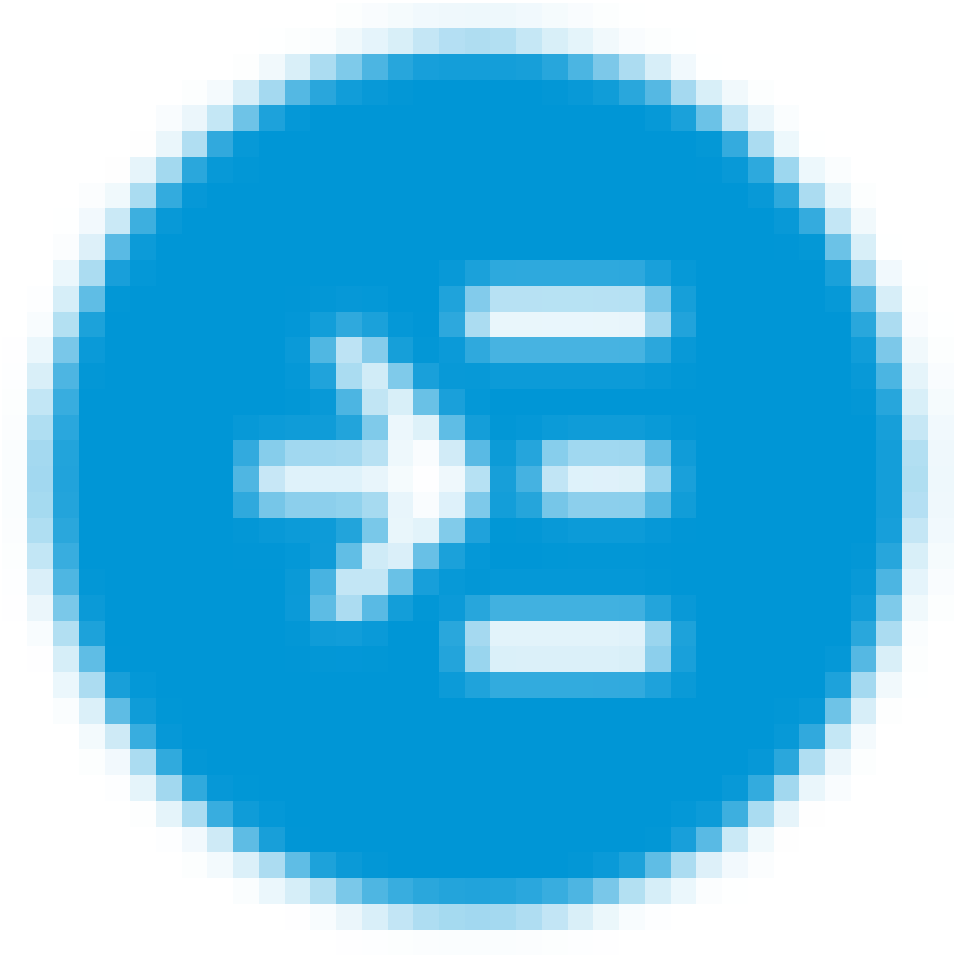
Fare clic su Login.

Per informazioni dettagliate, fare clic su Come accedere alla pagina di configurazione basata sul Web dei router VPN Cisco serie RV340.



Passaggio 5

Fare clic su Login. Viene visualizzata la pagina Riquadro attività iniziale. Se il riquadro di spostamento non è aperto, è possibile aprirlo facendo clic sull'icona del menu.



Dopo aver confermato la connessione e aver effettuato l'accesso al router, passare alla sezione Configurazione iniziale di questo articolo.

Risoluzione dei problemi relativi alla connessione Internet

Se si sta leggendo il file, è probabile che si verifichino problemi durante la connessione a Internet o all'interfaccia utente Web. Una di queste soluzioni dovrebbe essere d'aiuto.

Sul sistema operativo Windows connesso, è possibile verificare la connessione di rete aprendo il prompt dei comandi. Immettere ping 192.168.1.1 (indirizzo IP predefinito del router). Se la richiesta scade, non è possibile comunicare con il router.

Se la connettività non è attiva, consultare questo articolo sulla risoluzione dei problemi.

Altre cose da provare:

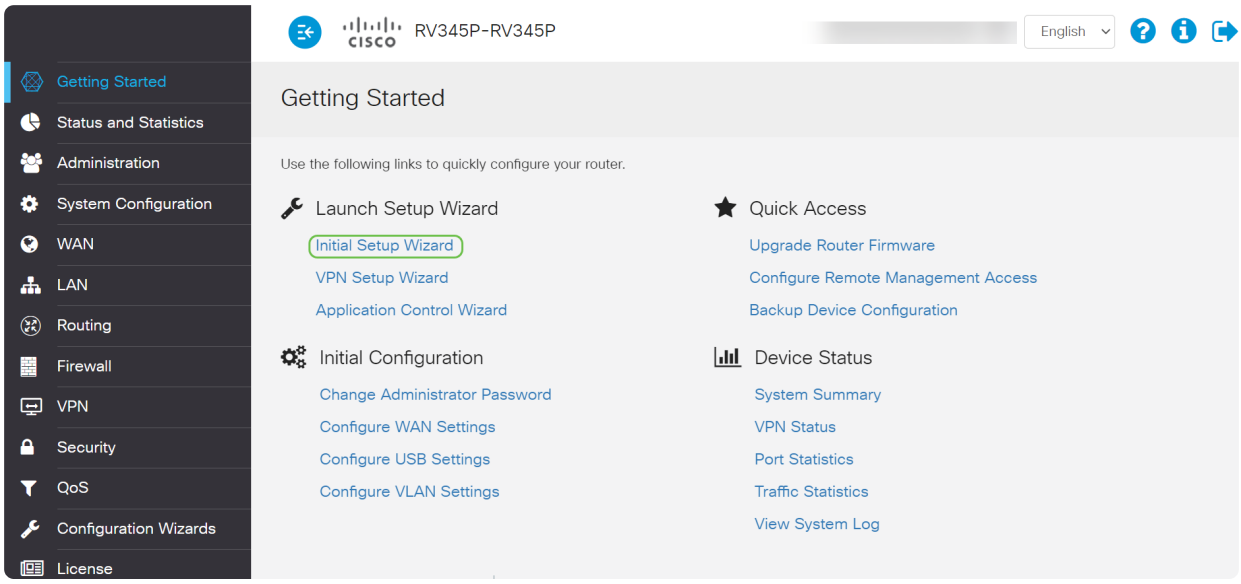
1. Verificare che il browser Web non sia impostato su Non in linea.
2. Verificare le impostazioni della connessione alla rete locale (LAN) per la scheda Ethernet. Il PC deve ottenere un indirizzo IP tramite DHCP. In alternativa, il PC può avere un indirizzo IP statico nell'intervallo 192.168.1.x con il gateway predefinito impostato su 192.168.1.1 (l'indirizzo IP predefinito dell'RV345P). Per connettersi, potrebbe essere necessario modificare le impostazioni di rete dell'RV345P. Se si utilizza Windows 10, controllare le istruzioni di Windows 10 per modificare le impostazioni di rete.
3. Se sono presenti apparecchiature che occupano l'indirizzo IP 192.168.1.1, sarà necessario risolvere il conflitto affinché la rete funzioni. Per maggiori informazioni, fai clic qui oppure fai clic qui.
4. Reimpostare il modem e il router RV345P spegnendo entrambi i dispositivi. Accendere quindi il modem e lasciarlo inattivo per circa 2 minuti. Accendere quindi RV345P. A questo punto, si dovrebbe ricevere un indirizzo IP WAN.
5. Se si dispone di un modem DSL, chiedere all'ISP di attivare la modalità bridge per il modem DSL.

Configurazione iniziale

È consigliabile eseguire i passaggi della Configurazione guidata iniziale elencati in questa sezione. È possibile modificare queste impostazioni in qualsiasi momento.

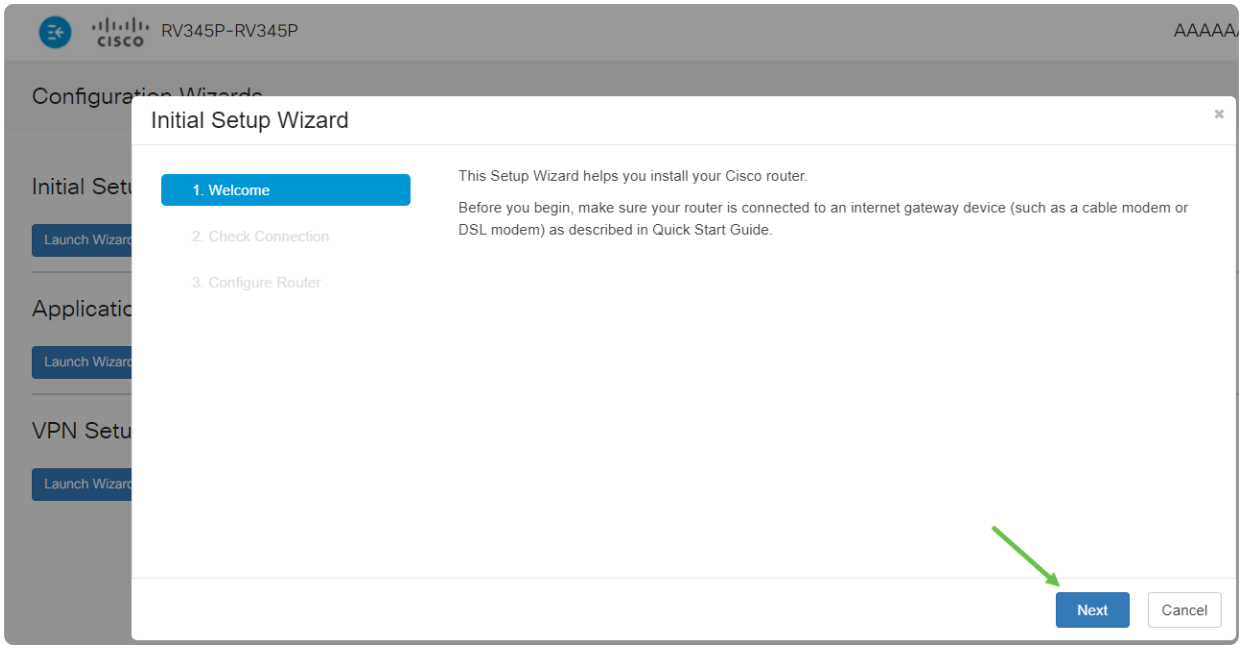
Passaggio 1

Fare clic su Installazione guidata iniziale nella pagina Guida introduttiva.



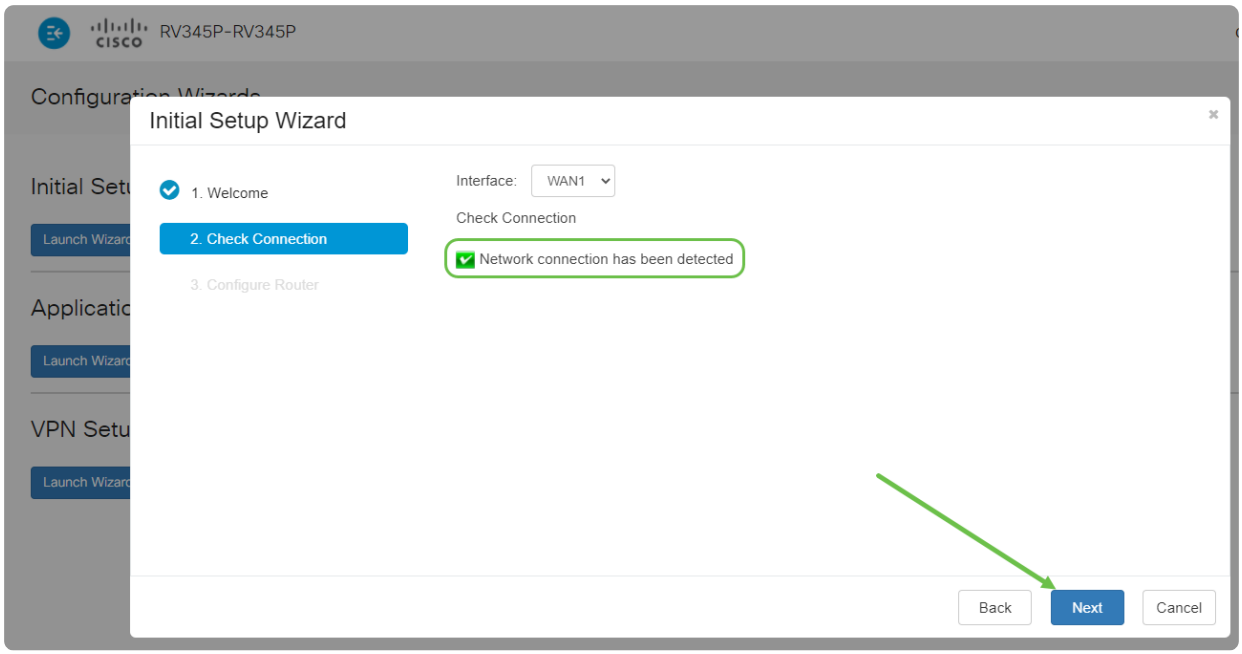
Passaggio 2

Questa operazione conferma la connessione dei cavi. Poiché l'operazione è già stata confermata, fare clic su Avanti.



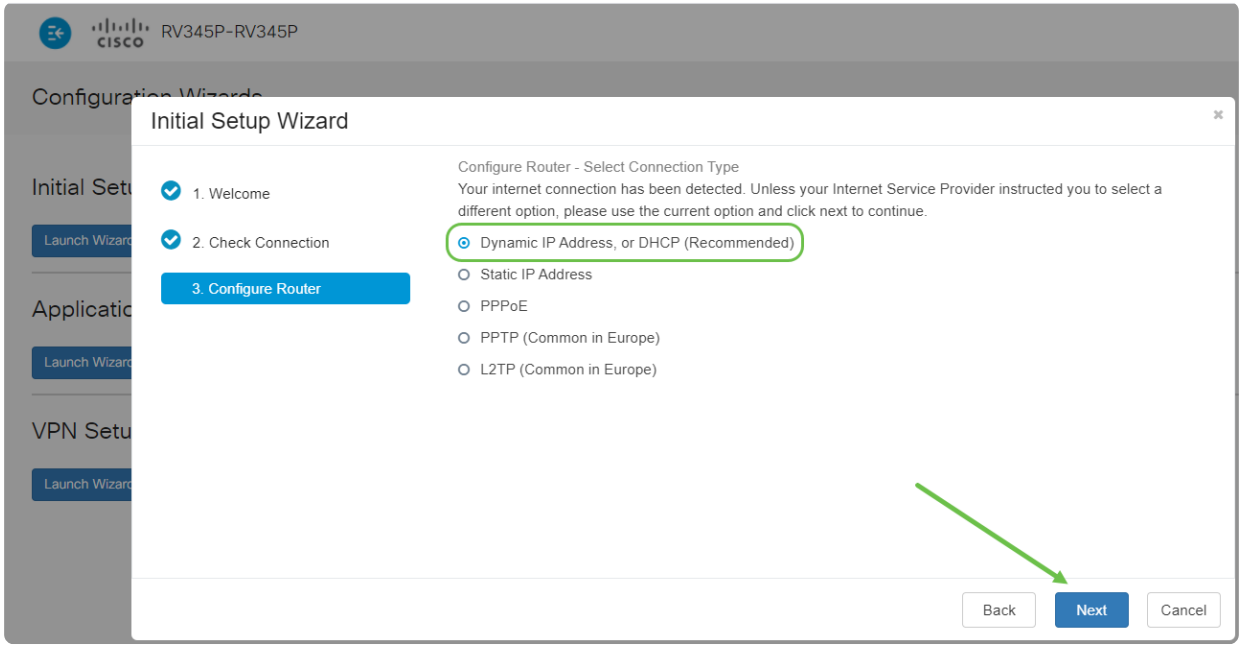
Passaggio 3

In questo passaggio vengono illustrati i passaggi di base per verificare che il router sia connesso. Poiché l'operazione è già stata confermata, fare clic su Avanti.



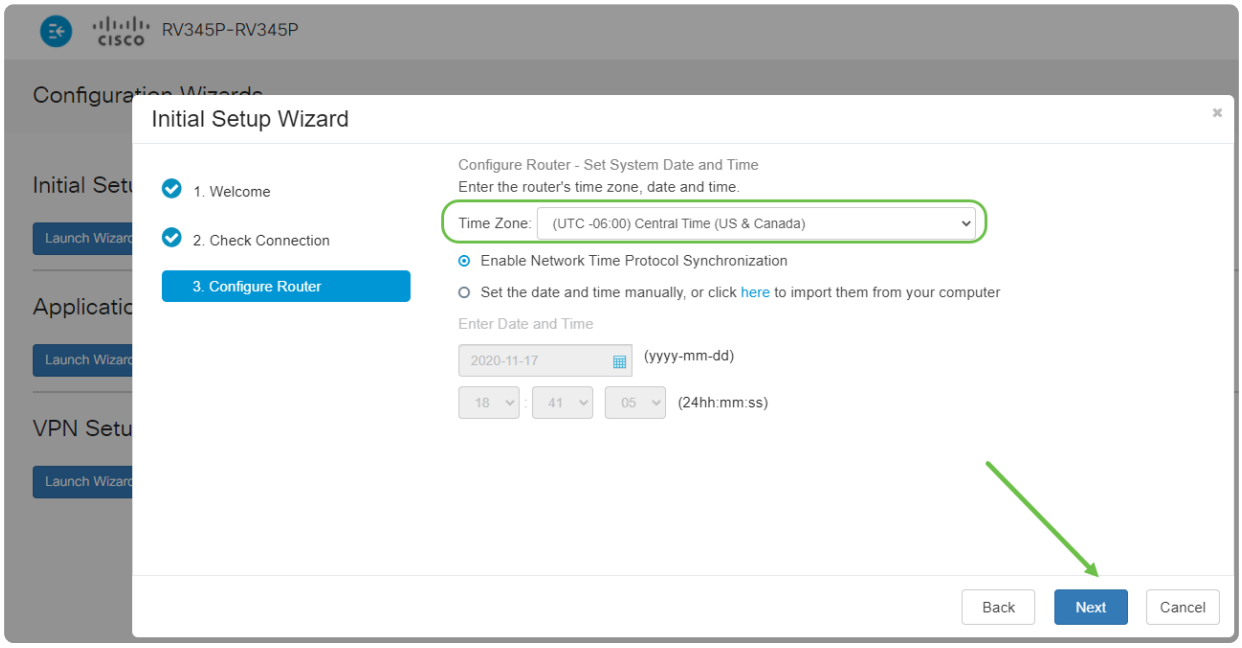
Passaggio 4

Nella schermata successiva vengono visualizzate le opzioni per l'assegnazione degli indirizzi IP al router. In questo scenario è necessario selezionare DHCP. Fare clic su Next (Avanti).



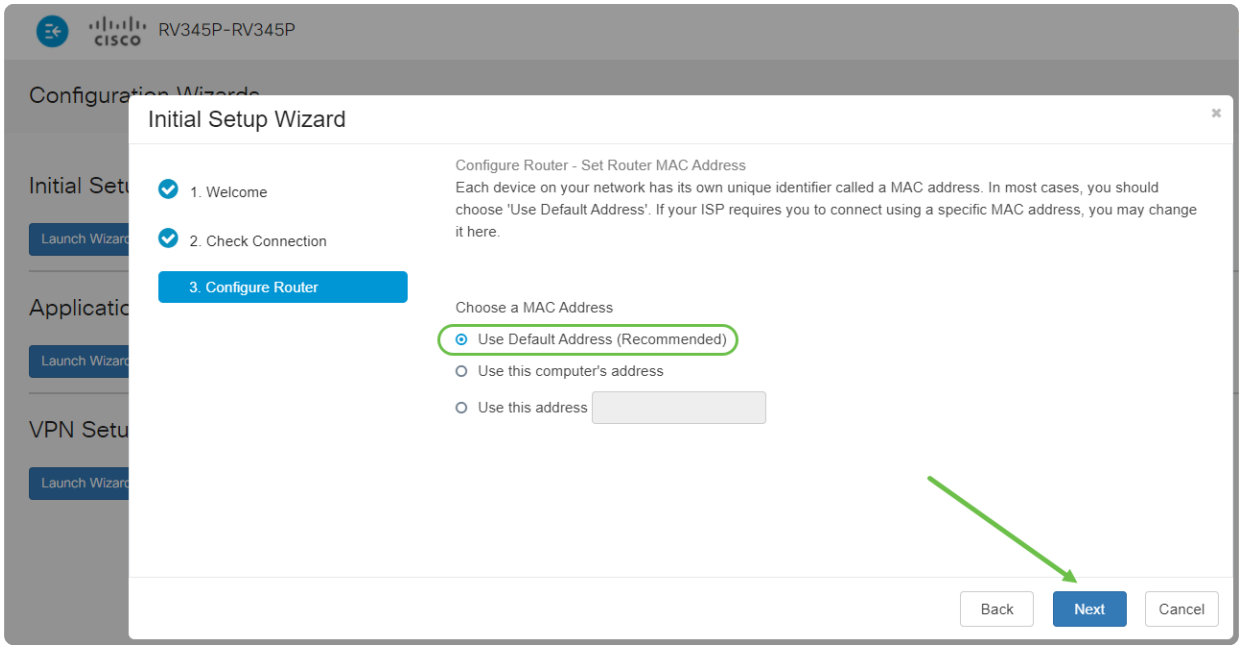
Passaggio 5

Verrà richiesto di impostare l'ora del router. Questa operazione è importante perché consente di ottenere la precisione durante l'analisi dei registri o la risoluzione degli eventi. Selezionare il fuso orario e fare clic su Avanti.



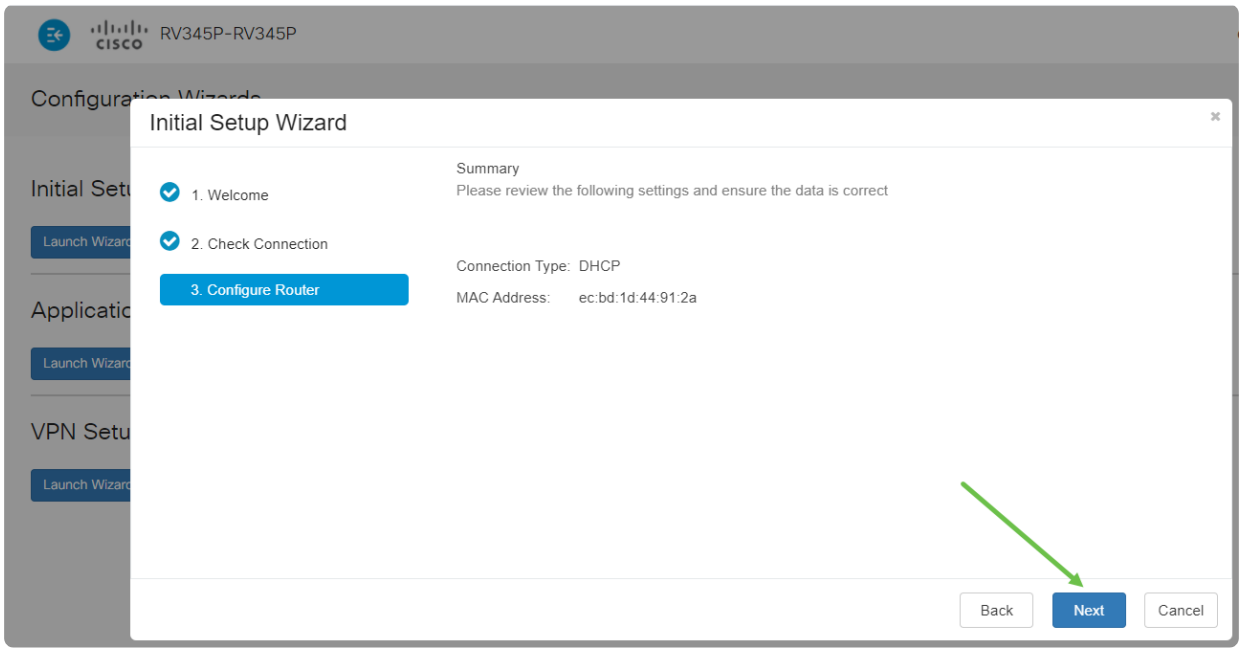
Passaggio 6

Selezionare gli indirizzi MAC da assegnare ai dispositivi. Nella maggior parte dei casi, verrà utilizzato l'indirizzo predefinito. Fare clic su Next (Avanti).



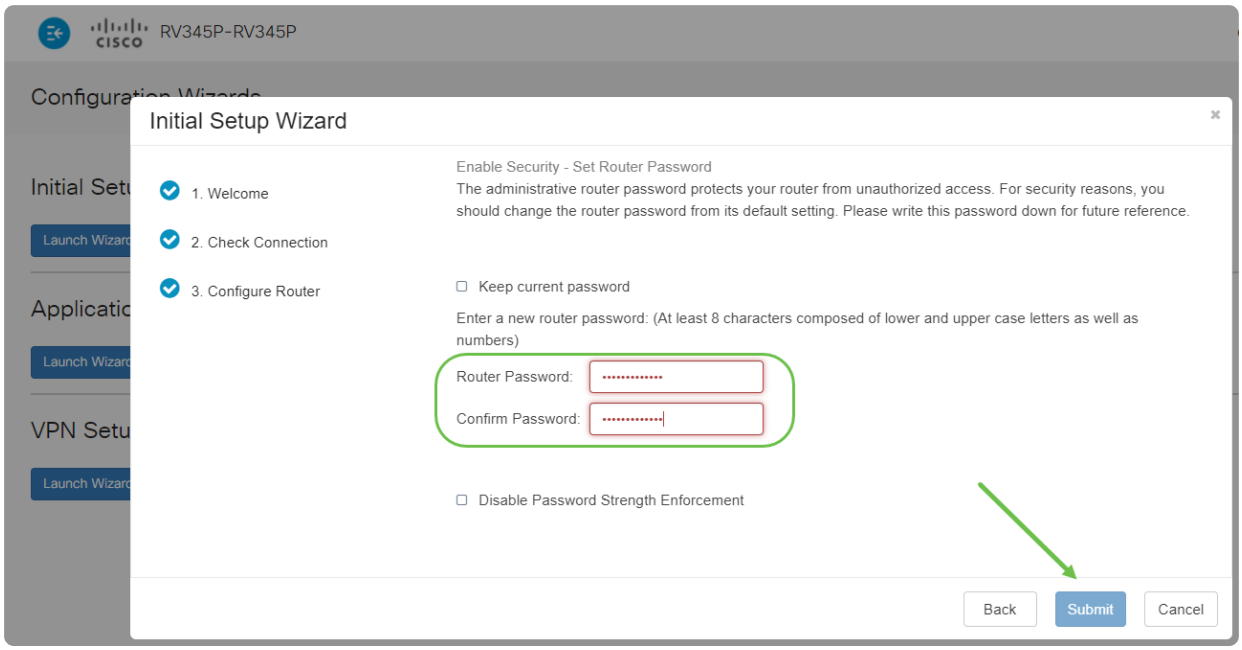
Passaggio 7

La pagina seguente è un riepilogo delle opzioni selezionate. Rivedere e fare clic su Avanti se soddisfatto.



Passaggio 8

Nel passaggio successivo, sarà necessario selezionare una password da utilizzare per accedere al router. Lo standard per le password deve contenere almeno 8 caratteri (maiuscoli e minuscoli) e includere numeri. Immettere una password conforme ai requisiti di protezione. Fare clic su Next (Avanti). Prendere nota della password per gli accessi futuri.



ⓘ Note: Non è consigliabile selezionare Disabilita applicazione della forza della password. Questa opzione consente di selezionare una password semplice come 123, che sarebbe facile come 1-2-3 per gli attori malintenzionati a crack.

Passaggio 9

Fare clic sull'icona Salva.

Per ulteriori informazioni su queste impostazioni, consultare il documento sulla configurazione delle impostazioni WAN DHCP sul router RV34x.

Per impostazione predefinita, la funzionalità Power over Ethernet (PoE) è abilitata su RV345P, ma è possibile apportare alcune modifiche. Per personalizzare le impostazioni, selezionare Configure Power over Ethernet (PoE) Settings (Configura

impostazioni Power over Ethernet) sul router RV345P.

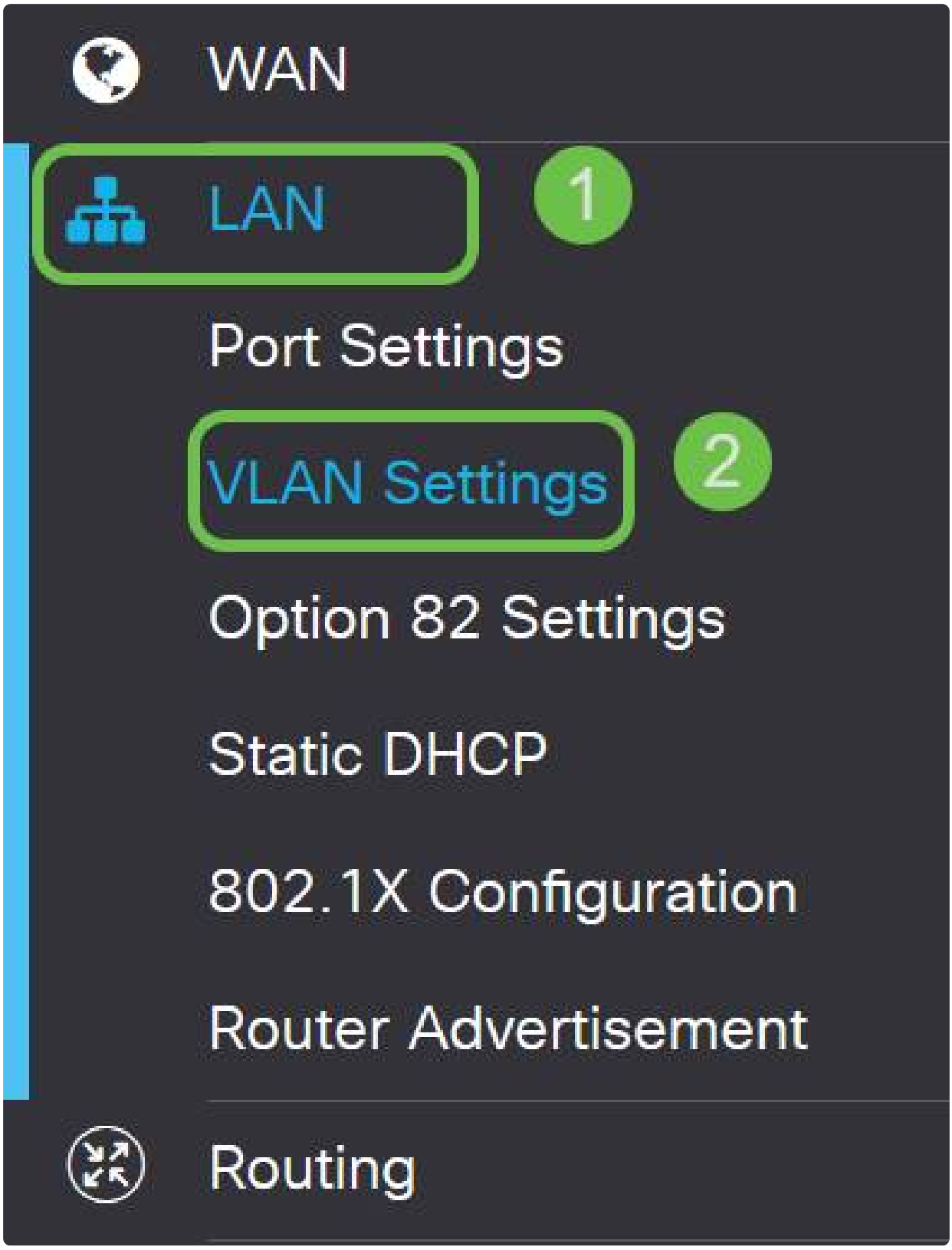
Modificare un indirizzo IP se necessario (facoltativo)

Dopo aver completato la Configurazione guidata iniziale, è possibile impostare un indirizzo IP statico sul router modificando le impostazioni della VLAN.

Questo processo è necessario solo se all'indirizzo IP del router deve essere assegnato un indirizzo specifico nella rete esistente. Se non occorre modificare un indirizzo IP, passare alla sezione successiva di questo articolo.

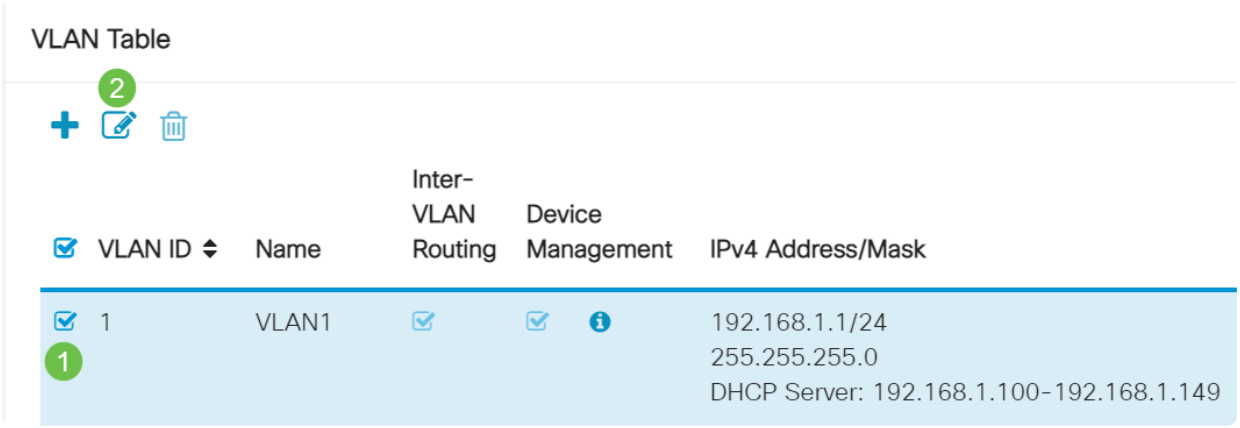
Passaggio 1

Nel menu a sinistra, fare clic su LAN > VLAN Settings (Impostazioni VLAN).



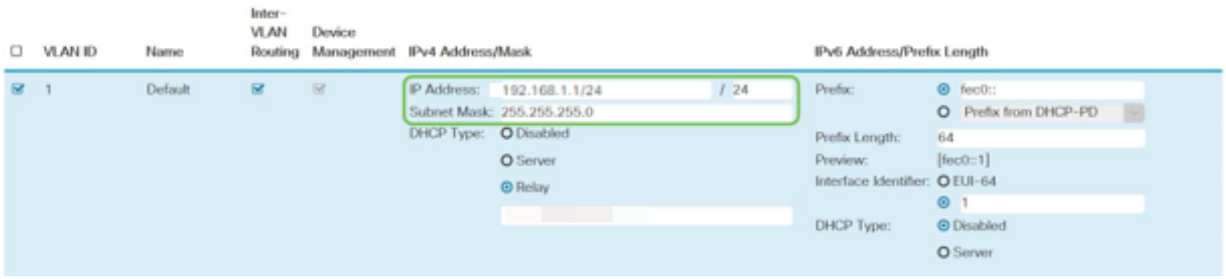
Passaggio 2

Selezionare la VLAN che contiene il dispositivo di routing, quindi fare clic sull'icona di modifica.



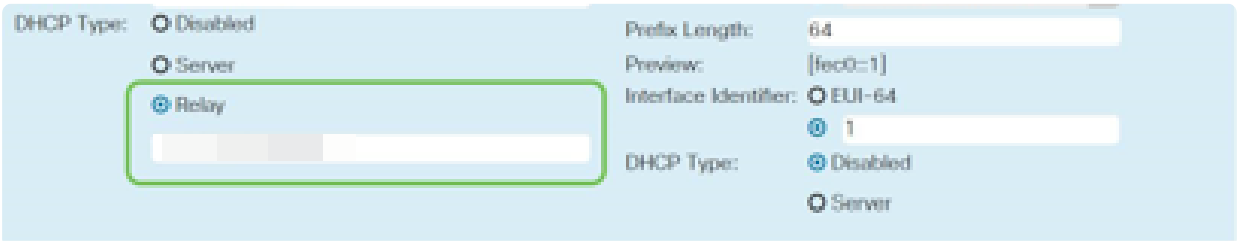
Passaggio 3

Immettere l'indirizzo IP statico desiderato e fare clic su Apply (Applica) nell'angolo in alto a destra.



Passaggio 4 (facoltativo)

Se il router in uso non è il server/dispositivo DHCP che assegna gli indirizzi IP, è possibile utilizzare la funzionalità di inoltro DHCP per indirizzare le richieste DHCP a un indirizzo IP specifico. È probabile che l'indirizzo IP sia il router connesso alla WAN o a Internet.

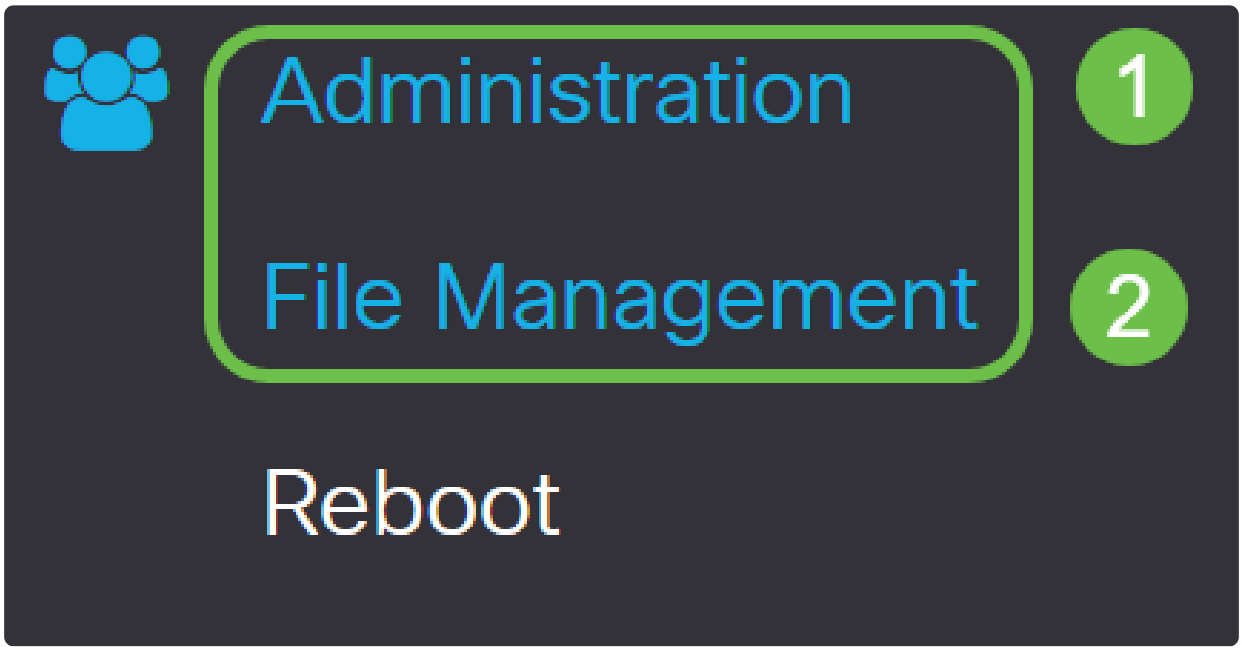


Aggiorna firmware se necessario

Questo è un passo importante, non saltarlo!

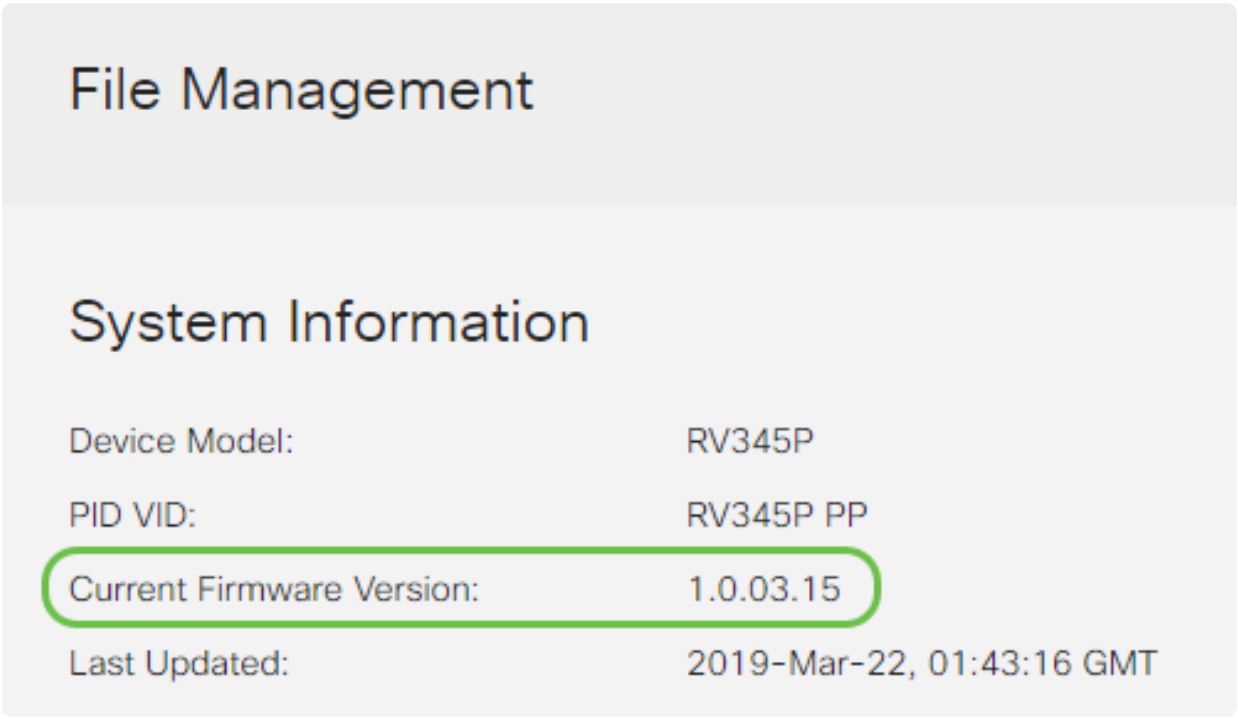
Passaggio 1

Scegliere Amministrazione > Gestione file.



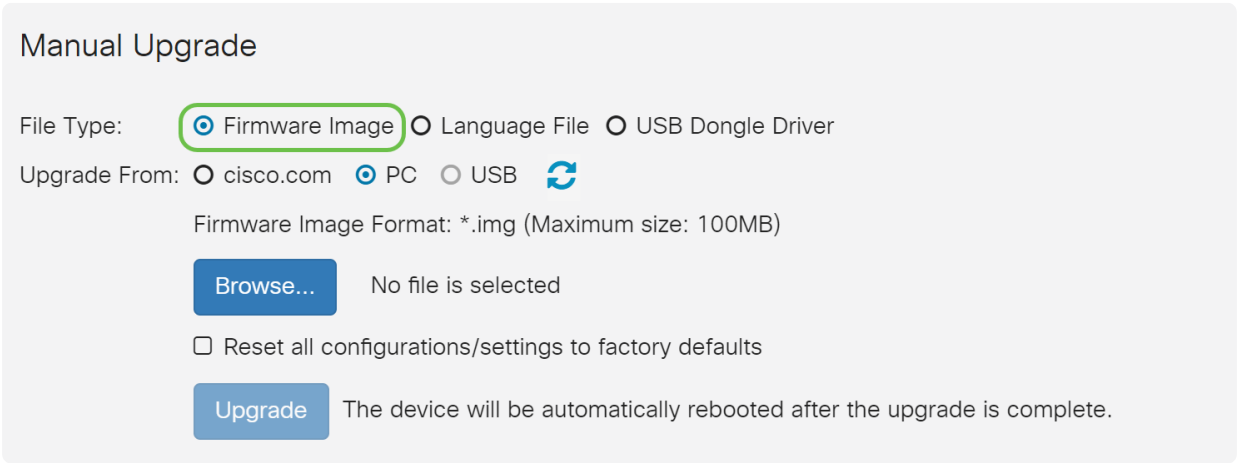
Nell'area System Information (Informazioni di sistema), le sottoaree seguenti descrivono:

- Modello dispositivo - Visualizza il modello del dispositivo.
- PID VID - ID prodotto e ID fornitore del router.
- Versione firmware corrente - Firmware attualmente in esecuzione sul dispositivo.
- Ultima versione Disponibile su Cisco.com - Ultima versione del software disponibile sul sito Web di Cisco.
- Ultimo aggiornamento firmware - Data e ora dell'ultimo aggiornamento firmware eseguito sul router.



Passaggio 2

Nella sezione Aggiornamento manuale, fare clic sul pulsante di opzione Firmware Image (Immagine firmware) per File Type (Tipo di file).



Passaggio 3

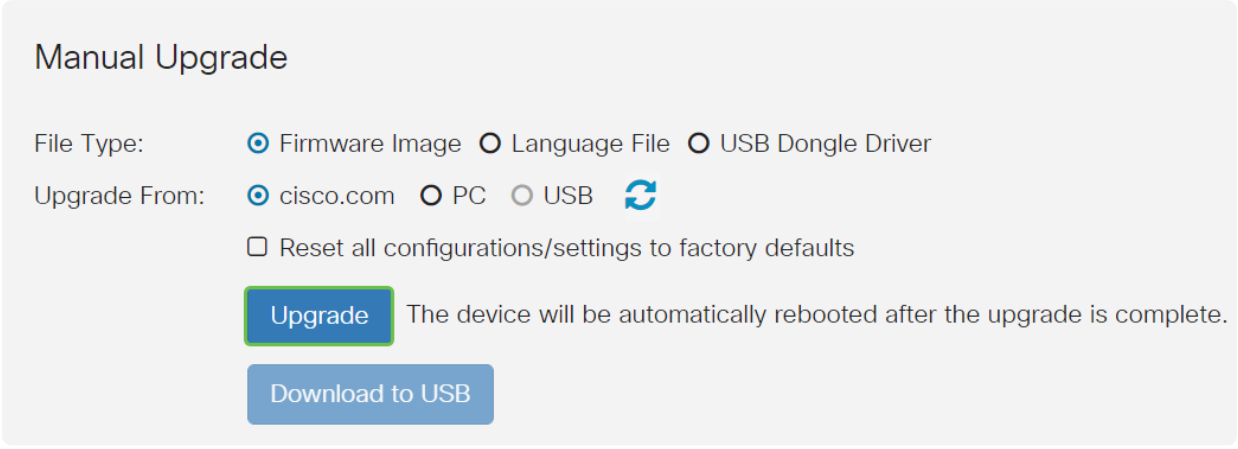
Nella pagina Manual Upgrade (Aggiornamento manuale), fare clic sul pulsante di opzione per selezionare cisco.com. Sono disponibili altre opzioni, ma questo è il modo più semplice per eseguire un aggiornamento. Questo processo installa il file

dell'aggiornamento più recente direttamente dalla pagina Web dei download di software Cisco.

> ⓘ Note: Se il dispositivo non è connesso a Internet o è stato disconnesso da Internet, non sarà possibile eseguire l'aggiornamento da cisco.com. Se questo è il tuo caso, qui puoi trovare delle opzioni alternative.

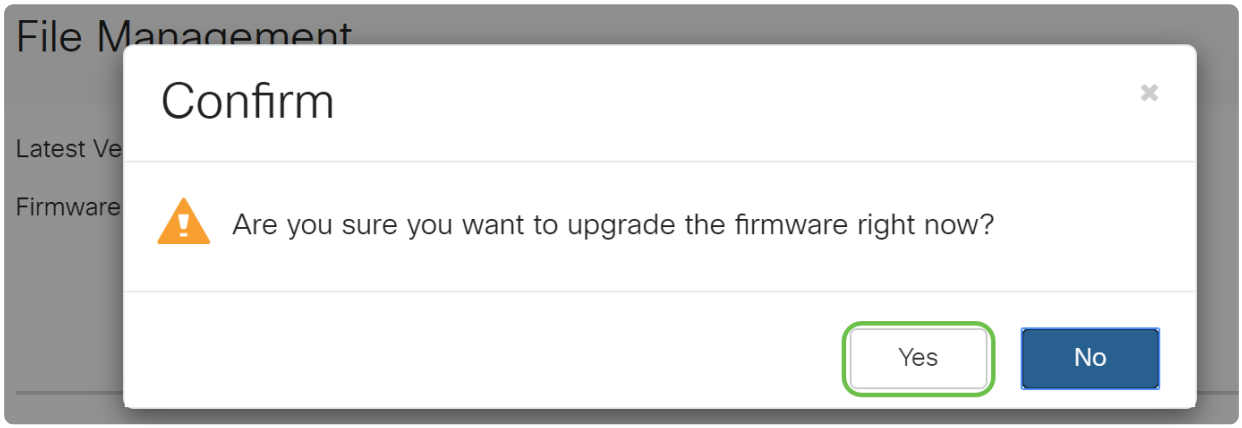
Passaggio 4

Fare clic su Aggiorna.

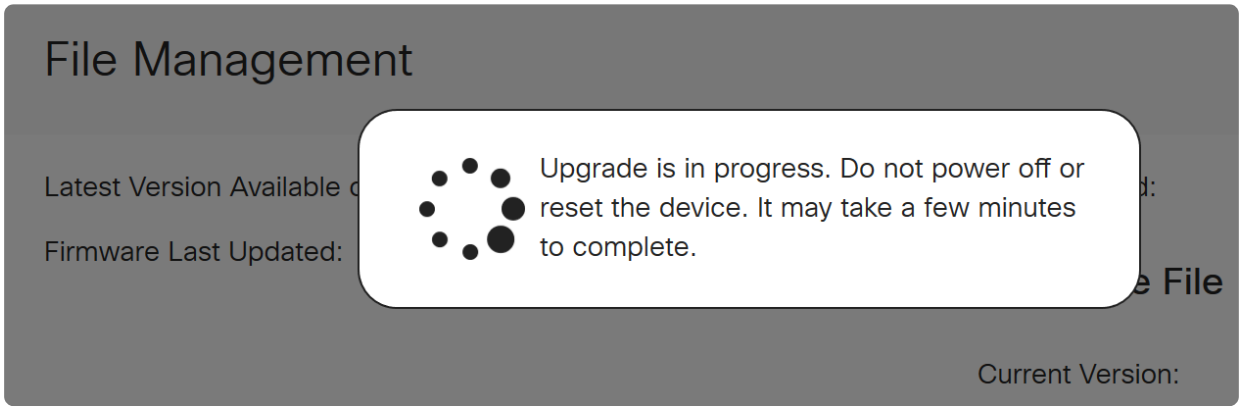


Passaggio 5

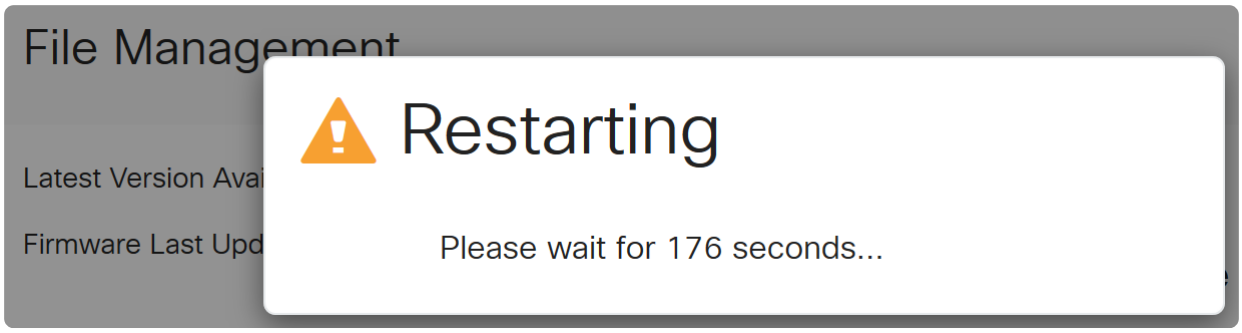
Fare clic su Sì nella finestra di conferma per continuare.



ⓘ Note: Il processo di aggiornamento deve essere eseguito senza interruzione. Durante l'aggiornamento verrà visualizzato il seguente messaggio.

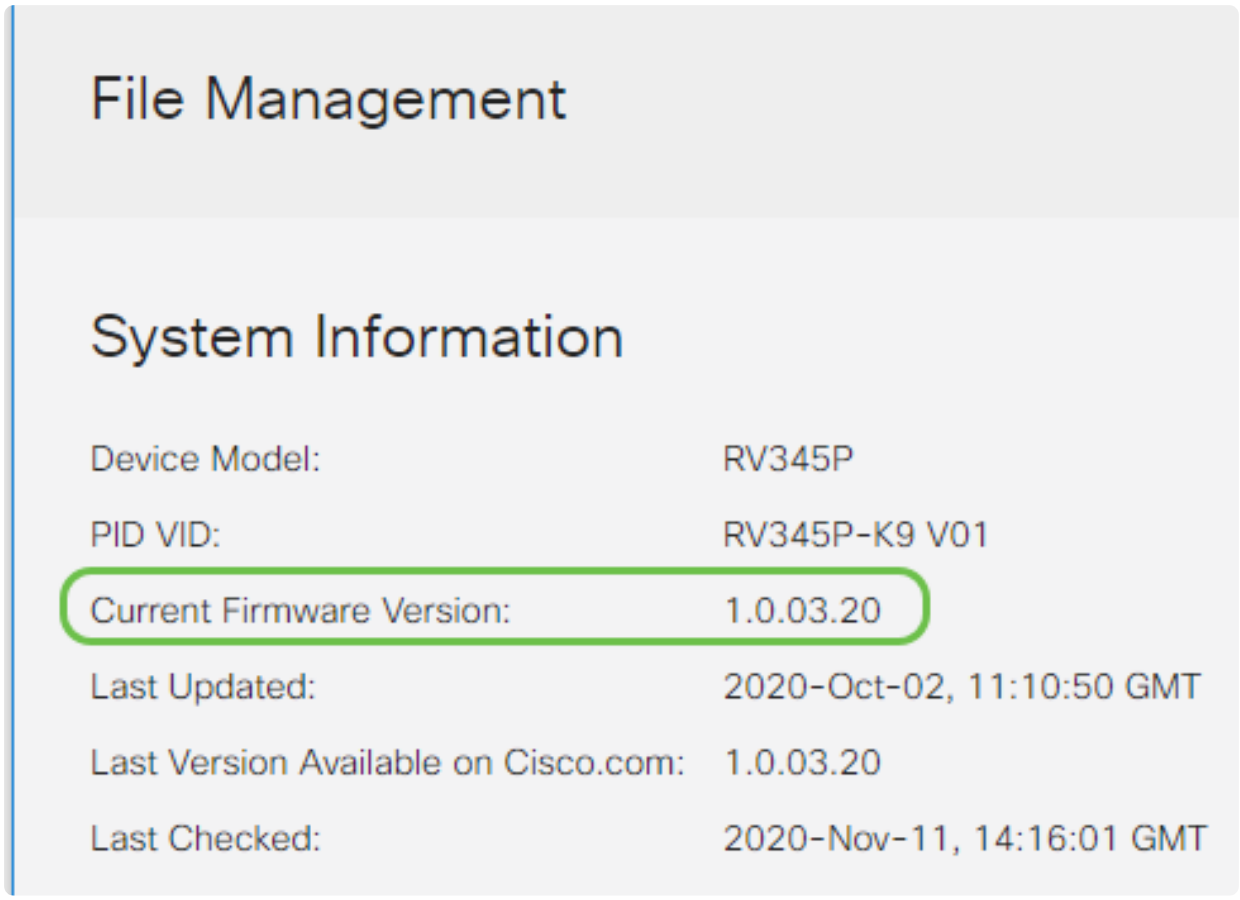


Una volta completato l'aggiornamento, viene visualizzata una finestra di notifica per informare che il router verrà riavviato con un conto alla rovescia del tempo stimato per il completamento del processo. In questo modo, l'utente verrà disconnesso.



Passaggio 6

Accedere nuovamente all'utility basata sul Web per verificare che il firmware del router sia stato aggiornato, quindi scorrere fino a System Information. Nell'area Current Firmware Version dovrebbe essere visualizzata la versione del firmware aggiornata.



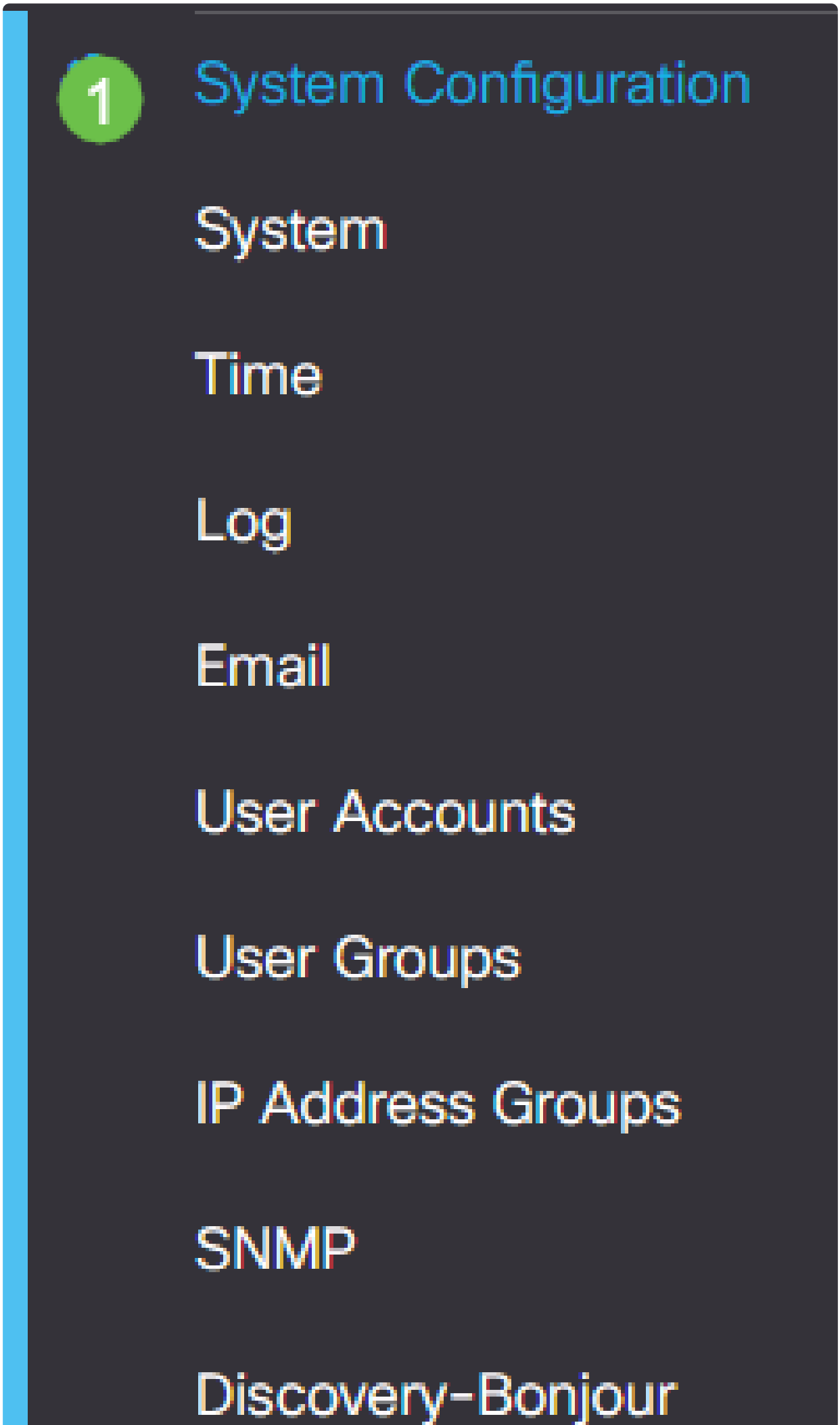
Configurazione degli aggiornamenti automatici sul router serie RV345P

Poiché gli aggiornamenti sono così importanti e si è molto occupati, è opportuno

configurare gli aggiornamenti automatici da qui in avanti.

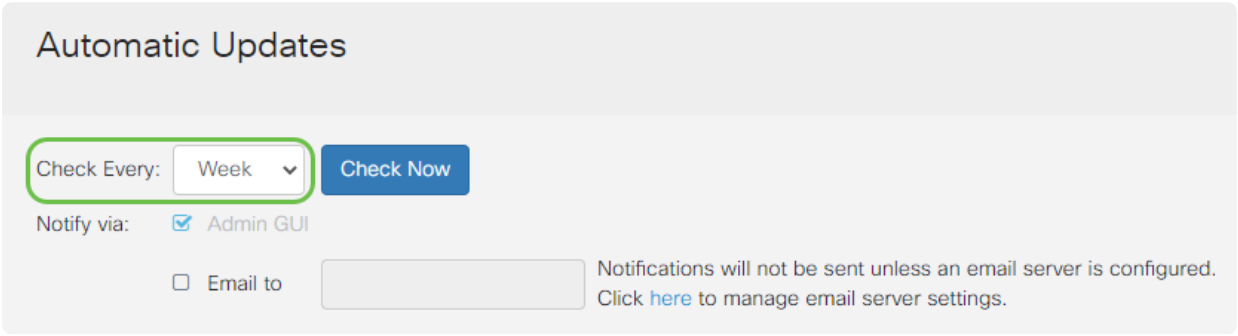
Passaggio 1

Accedere all'utility basata sul Web e scegliere Configurazione di sistema > Aggiornamenti automatici.


1
System Configuration
System
Time
Log
Email
User Accounts
User Groups
IP Address Groups
SNMP
Discovery-Bonjour

Passaggio 2

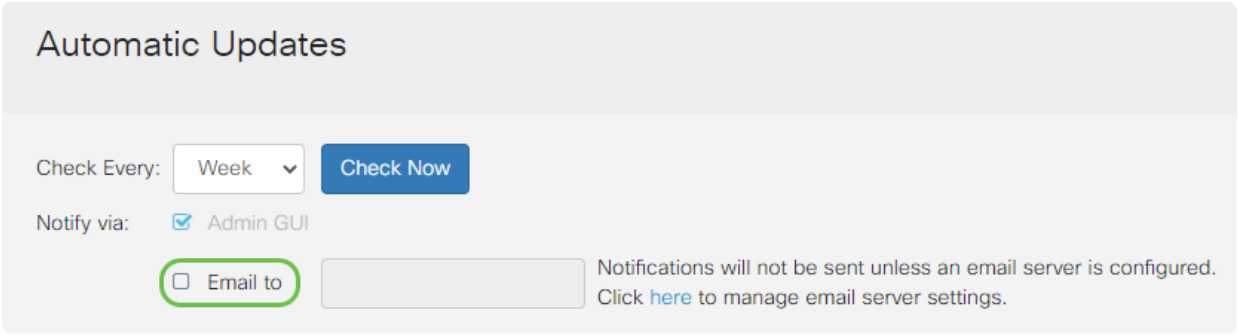
Dall'elenco a discesa Check Every (Controlla ogni), selezionare la frequenza con cui il router deve verificare la disponibilità di aggiornamenti.



Passaggio 3

Nell'area Notifica tramite selezionare la casella di controllo Invia a per ricevere gli aggiornamenti tramite posta elettronica. La casella di controllo Admin GUI (Interfaccia utente amministratore) è abilitata per impostazione predefinita e non può essere disabilitata. Una volta disponibile un aggiornamento, nella configurazione basata sul Web verrà visualizzata una notifica.

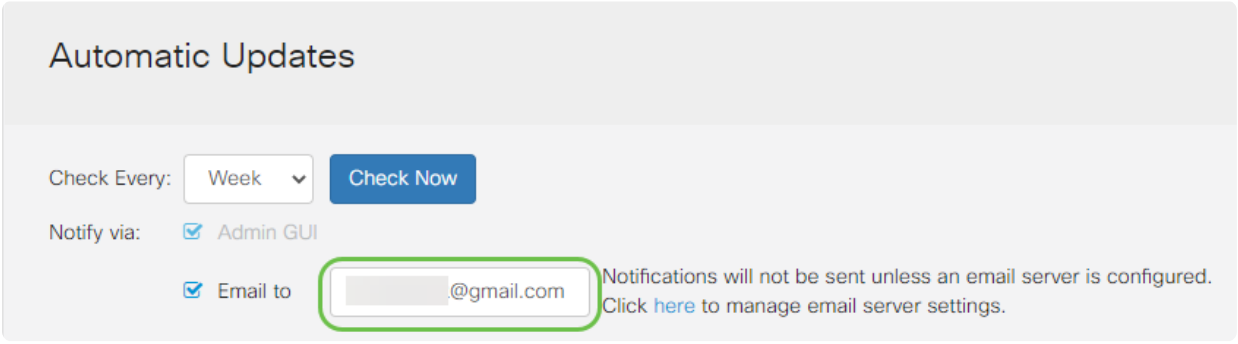
Per informazioni su come configurare le impostazioni del server e-mail, fare clic qui.



Passaggio 4

Immettere un indirizzo e-mail nel campo Indirizzo e-mail.

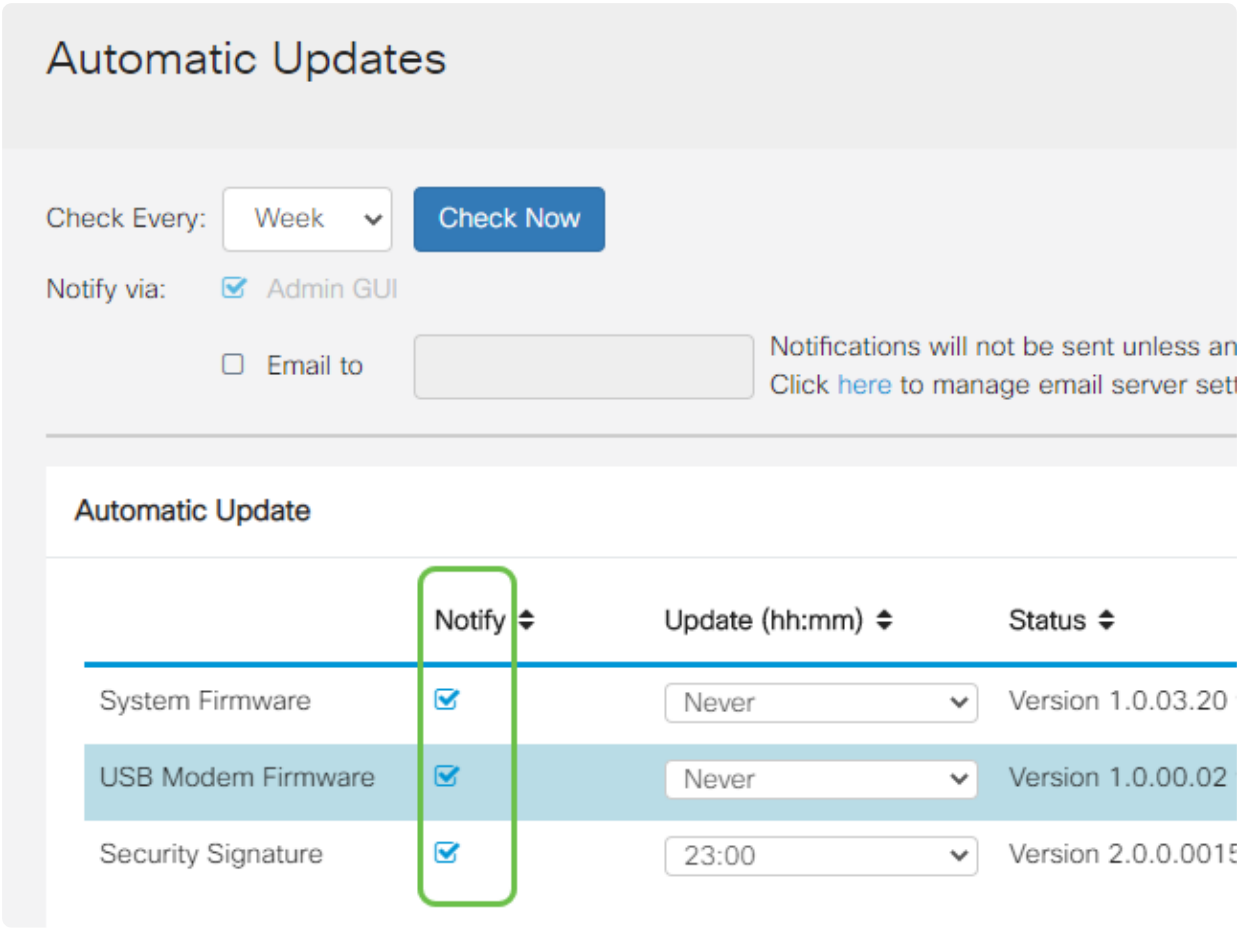
ⓘ Note: Si consiglia di utilizzare un account di posta elettronica distinto invece di utilizzare l'indirizzo di posta elettronica personale per mantenere la privacy.



Passaggio 5

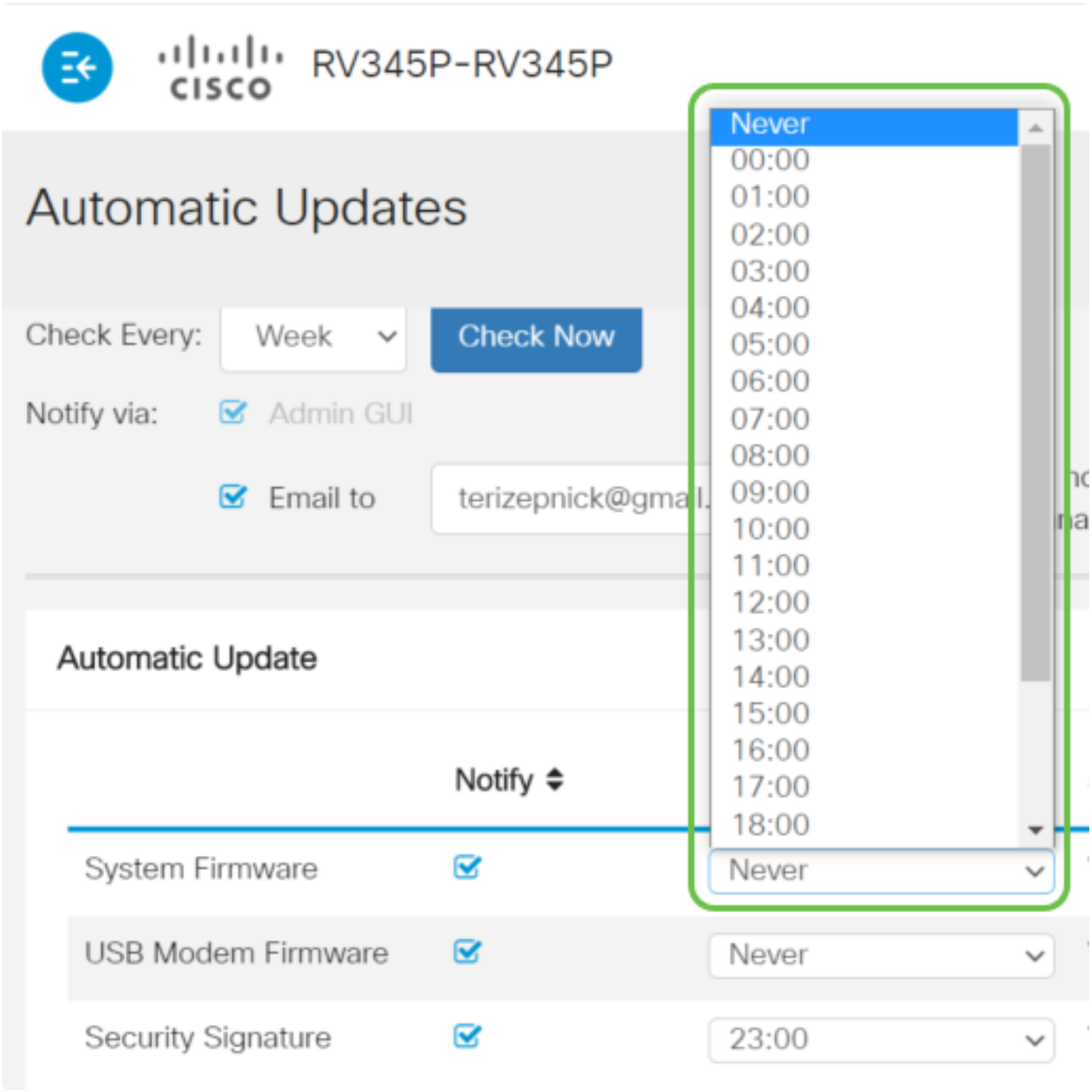
Nell'area Aggiorna automaticamente, selezionare le caselle di controllo Notifica relative al tipo di aggiornamenti per i quali si desidera ricevere una notifica. Le opzioni sono:

- Firmware di sistema — Il programma di controllo principale per il dispositivo.
- USB Modem Firmware: il programma di controllo o il driver per la porta USB.
- Firma di protezione: conterrà firme per il controllo dell'applicazione che consentono di identificare applicazioni, tipi di dispositivi, sistemi operativi e così via.



Passaggio 6

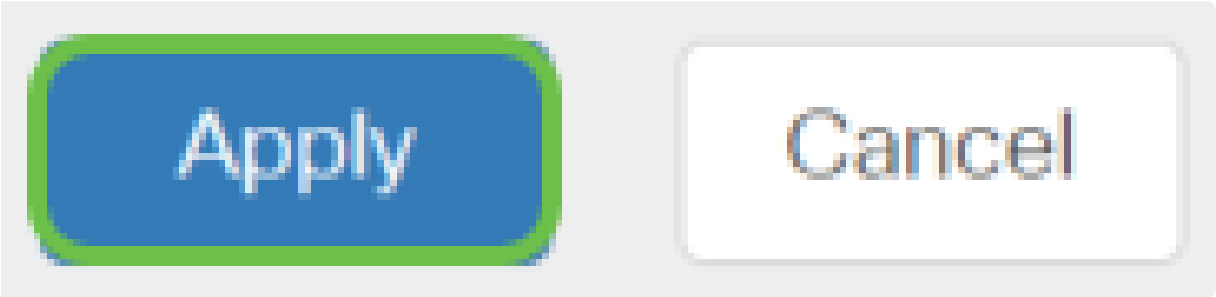
Dall'elenco a discesa Aggiornamento automatico, scegliere l'ora del giorno in cui si desidera eseguire l'aggiornamento automatico. Alcune opzioni possono variare a seconda del tipo di aggiornamento scelto. La firma di protezione è l'unica opzione che consente un aggiornamento immediato. Si consiglia di impostare l'ora di chiusura dell'ufficio in modo che il servizio non venga interrotto in un momento non opportuno.



Lo stato indica la versione corrente del firmware o la firma di protezione.

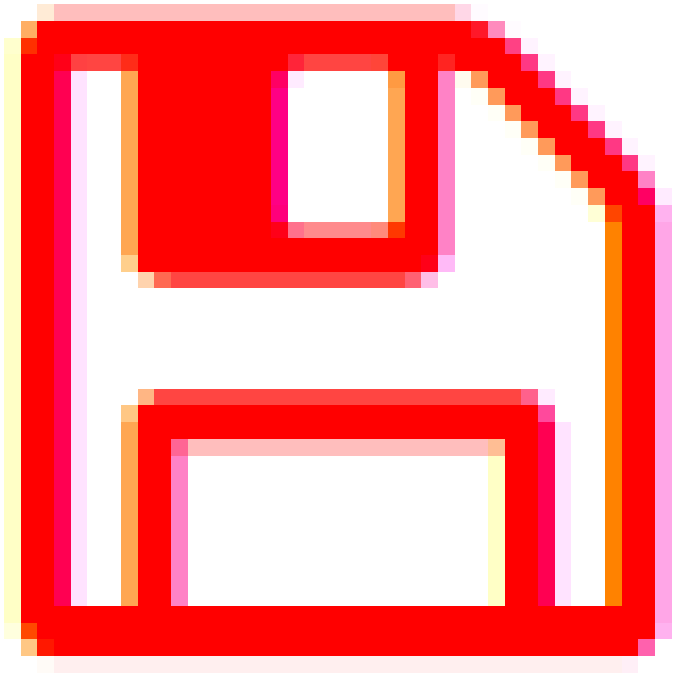
Passaggio 7

Fare clic su Apply (Applica).



Passaggio 8

Per salvare la configurazione in modo permanente, andare alla pagina Copia/Salva configurazione o fare clic sull'icona Salva nella parte superiore della pagina.



Straordinario, le impostazioni di base sul router sono state completate! A questo punto è possibile esplorare alcune opzioni di configurazione.

Opzioni di sicurezza

Naturalmente, si desidera che la rete sia sicura. Ci sono alcune semplici opzioni, come avere una password complessa, ma se si desidera prendere provvedimenti per una rete ancora più sicura controllare questa sezione sulla sicurezza.

Licenza RV Security (opzionale)

Le caratteristiche della presente licenza di sicurezza RV proteggono la rete dagli attacchi provenienti da Internet:

- IPS (Intrusion Prevention System): Controlla i pacchetti di rete, i registri e/o blocca un'ampia gamma di attacchi di rete. Garantisce una maggiore disponibilità della rete, una più rapida risoluzione dei problemi e una protezione completa delle minacce.
- Antivirus: Protezione dai virus attraverso la scansione delle applicazioni per vari protocolli come HTTP, FTP, allegati di posta elettronica SMTP, allegati di posta elettronica POP3 e allegati di posta elettronica IMAP che passano attraverso il router.
- Sicurezza Web: Consente l'efficienza e la sicurezza aziendali durante la connessione a Internet, consente di definire policy di accesso a Internet per i dispositivi terminali e le applicazioni Internet al fine di garantire prestazioni e sicurezza. È basato su cloud e contiene più di 80 categorie con più di 450 milioni di domini classificati.
- Identificazione applicazione: Identificare e assegnare criteri alle applicazioni Internet. Vengono identificate automaticamente 500 applicazioni univoche.
- Identificazione client: Identificare e classificare i client in modo dinamico. La capacità di assegnare policy basate sulla categoria del dispositivo finale e sul sistema operativo.

La licenza di sicurezza RV fornisce il filtro Web. Il filtro Web è una funzionalità che consente di gestire l'accesso a siti Web inappropriati. Può esaminare le richieste di accesso al Web di un client per determinare se consentire o negare tale sito.

> ⓘ Note: Le funzioni di sicurezza con licenza possono essere provate gratuitamente per 90 giorni. Se si desidera continuare a utilizzare le funzionalità di sicurezza avanzate sul router dopo il periodo di valutazione, è necessario acquistare e attivare una licenza.

Un'altra opzione di sicurezza è Cisco Umbrella. Clicca qui se vuoi passare alla sezione Umbrella.

Se non si desidera avere una licenza di sicurezza, fare clic per passare alla sezione VPN di questo documento.

Introduzione agli Smart Account

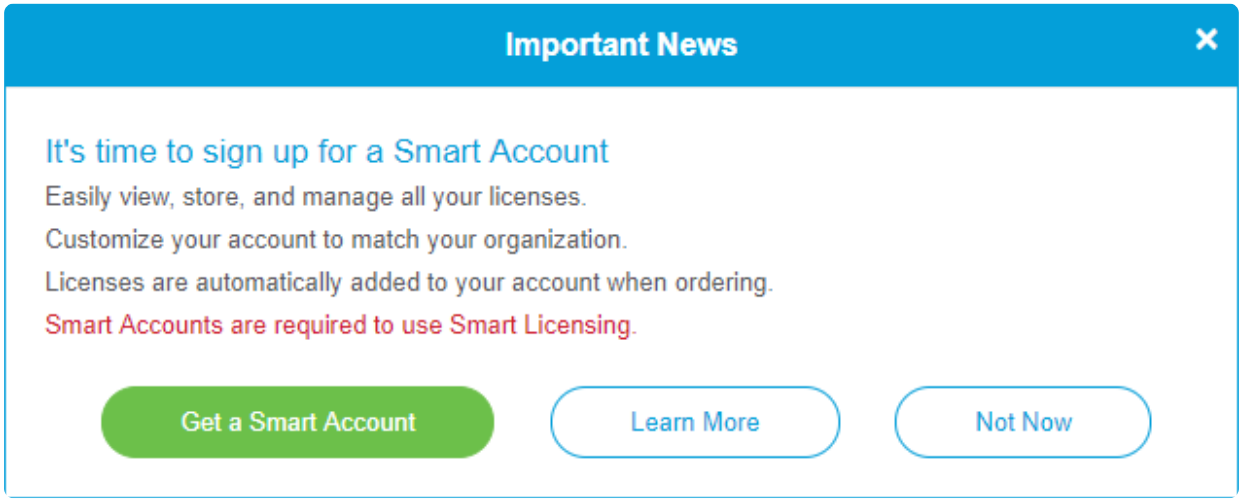
Per acquistare la licenza RV Security, è necessario uno Smart Account.

Autorizzando l'attivazione di questo Smart Account, l'utente accetta di essere autorizzato a creare account e a gestire diritti relativi a prodotti e servizi, contratti di licenza e accesso degli utenti agli account per conto dell'organizzazione. I partner Cisco non possono autorizzare la creazione di account per conto dei clienti.

La creazione di un nuovo Smart Account è un evento unico e la gestione da quel momento in poi viene fornita attraverso lo strumento.

Crea uno Smart Account

Quando si accede al proprio account Cisco generale utilizzando il proprio Cisco.com account o ID CCO (quello creato all'inizio di questo documento), è possibile che un messaggio ti saluti per creare uno Smart Account.



Se non lo hai ancora fatto, puoi fare clic per andare alla pagina di creazione dello Smart Account. Potrebbe essere necessario eseguire l'accesso con le credenziali dell'account Cisco.com.

Per ulteriori informazioni sui passaggi da seguire per richiedere lo Smart Account, fare clic qui.

Prendere nota del nome account e di altri dettagli per la registrazione.

Suggerimento rapido: se è necessario immettere un dominio e non si dispone di un dominio, è possibile immettere l'indirizzo di posta elettronica nel formato name@domain.com. I domini più comuni sono gmail, yahoo e così via, a seconda della società o del provider.

> ⓘ Note: Prima di acquistare la licenza per la sicurezza RV, è molto importante avere un account Cisco.com (ID CCO) e uno Cisco Smart Account.

Acquista licenza di sicurezza RV

È necessario acquistare una licenza dal distributore Cisco o dal partner Cisco. Per individuare un partner Cisco, fare clic qui.

Nella tabella seguente viene visualizzato il numero di parte della licenza.

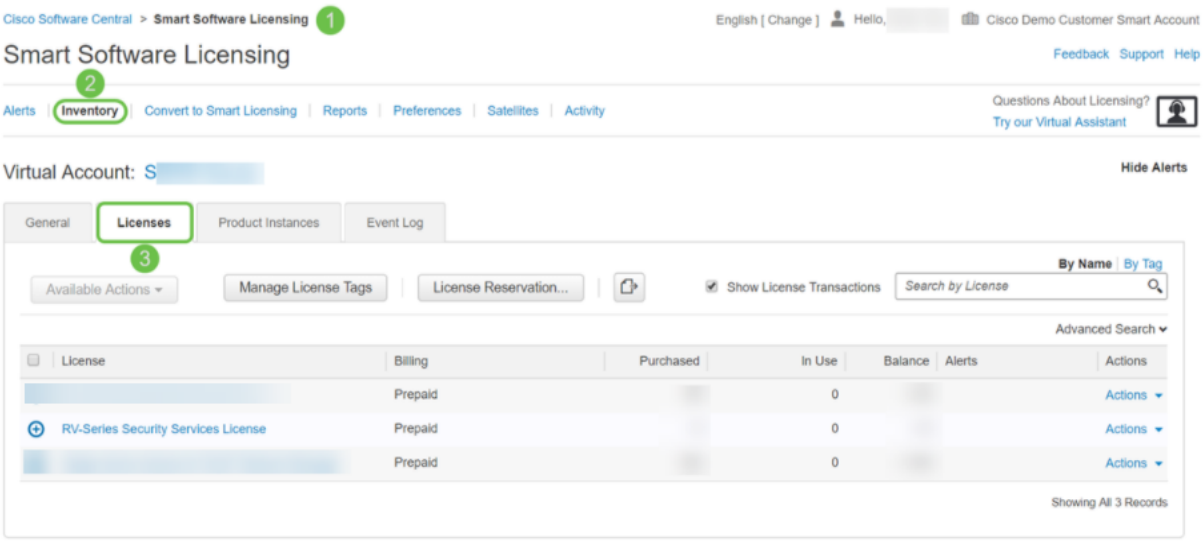
Tipo	ID prodotto	Descrizione
Licenza RV Security	LS-RV34X-SEC-1YR= LS-RV34X	Sicurezza RV: 1 anno: Dynamic Web Filter, Application Visibility, Client Identification and Statistics, Gateway Antivirus e Intrusion Prevention System IPS.

La chiave di licenza non viene immessa direttamente nel router, ma viene assegnata

allo Smart Account Cisco dopo aver ordinato la licenza. Il tempo necessario per visualizzare la licenza sull'account dipende dal momento in cui il partner accetta l'ordine e dal momento in cui il rivenditore collega le licenze al proprio account, ossia 24-48 ore.

Conferma licenza nello Smart Account

Passare alla pagina dell'account Smart License, quindi fare clic su Pagina licenza Smart Software > Inventario > Licenze.

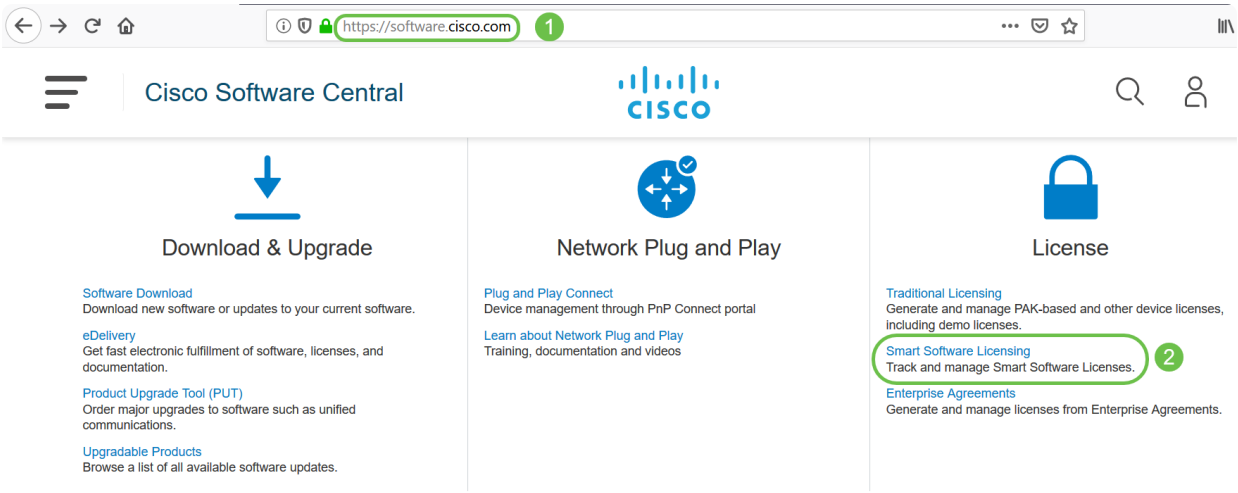


> ⓘ Note: Se la licenza non viene visualizzata nello Smart Account, contattare il partner Cisco.

Configurazione della licenza RV Security sul router serie RV345P

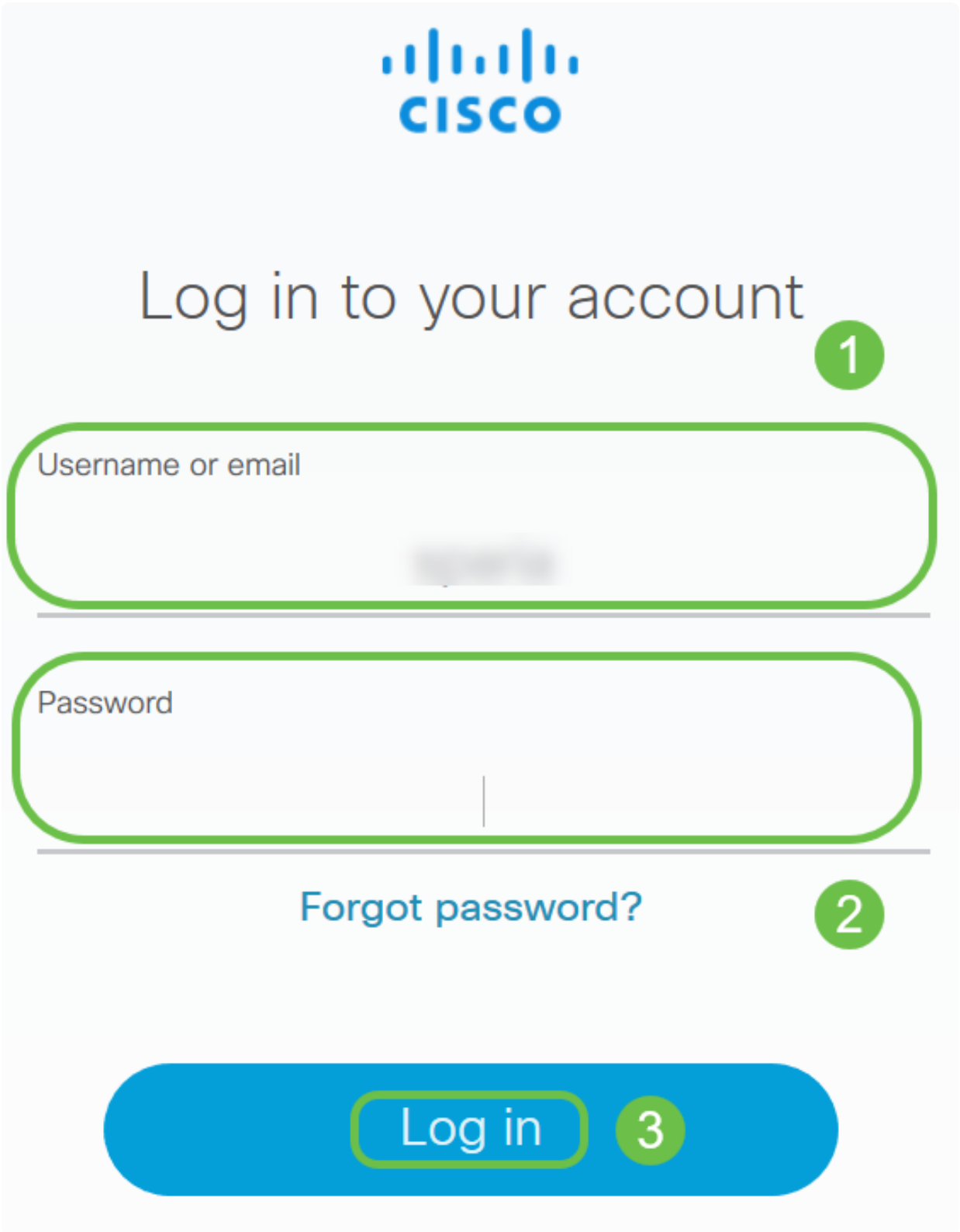
Passaggio 1

Accedere al software Cisco e selezionare Smart Software Licensing.



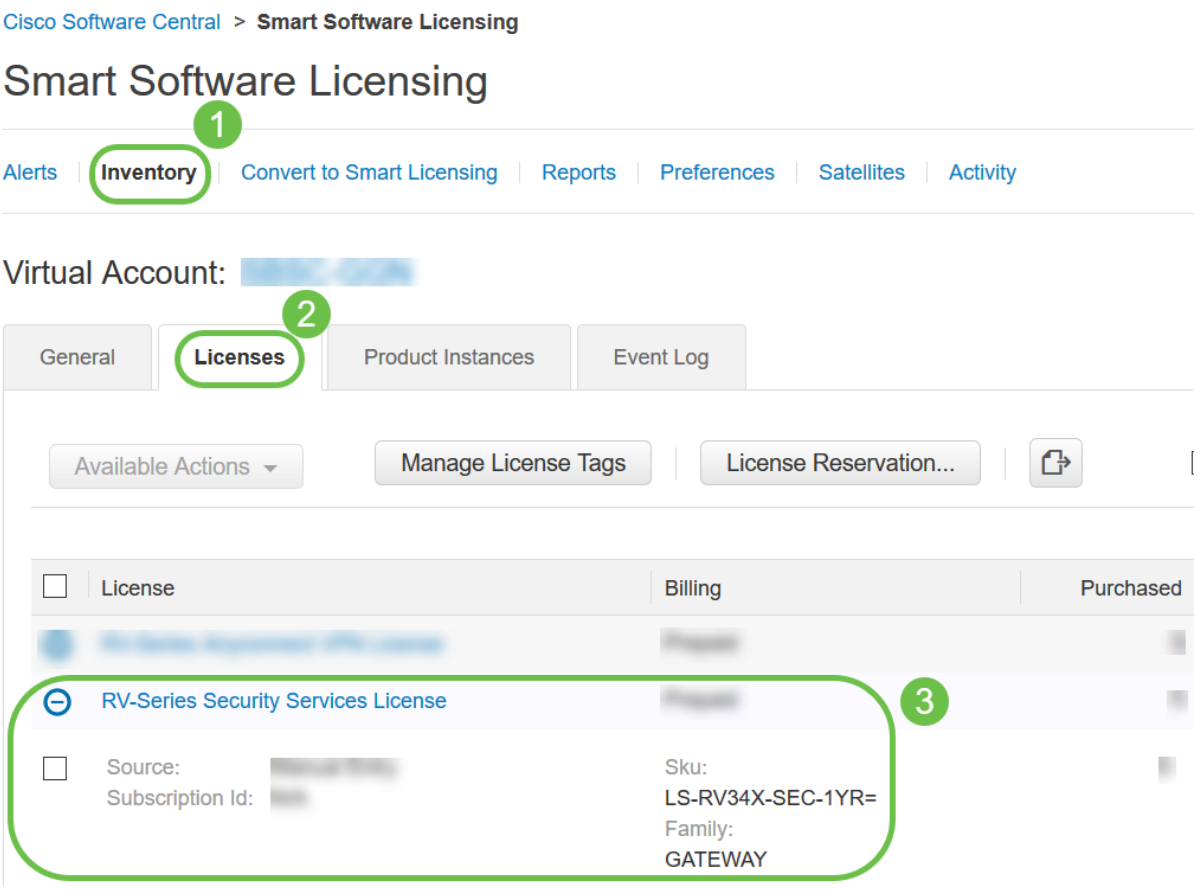
Passaggio 2

Immettere il nome utente o l'indirizzo di posta elettronica e la password per accedere allo Smart Account. Fare clic su Log in (Accedi).



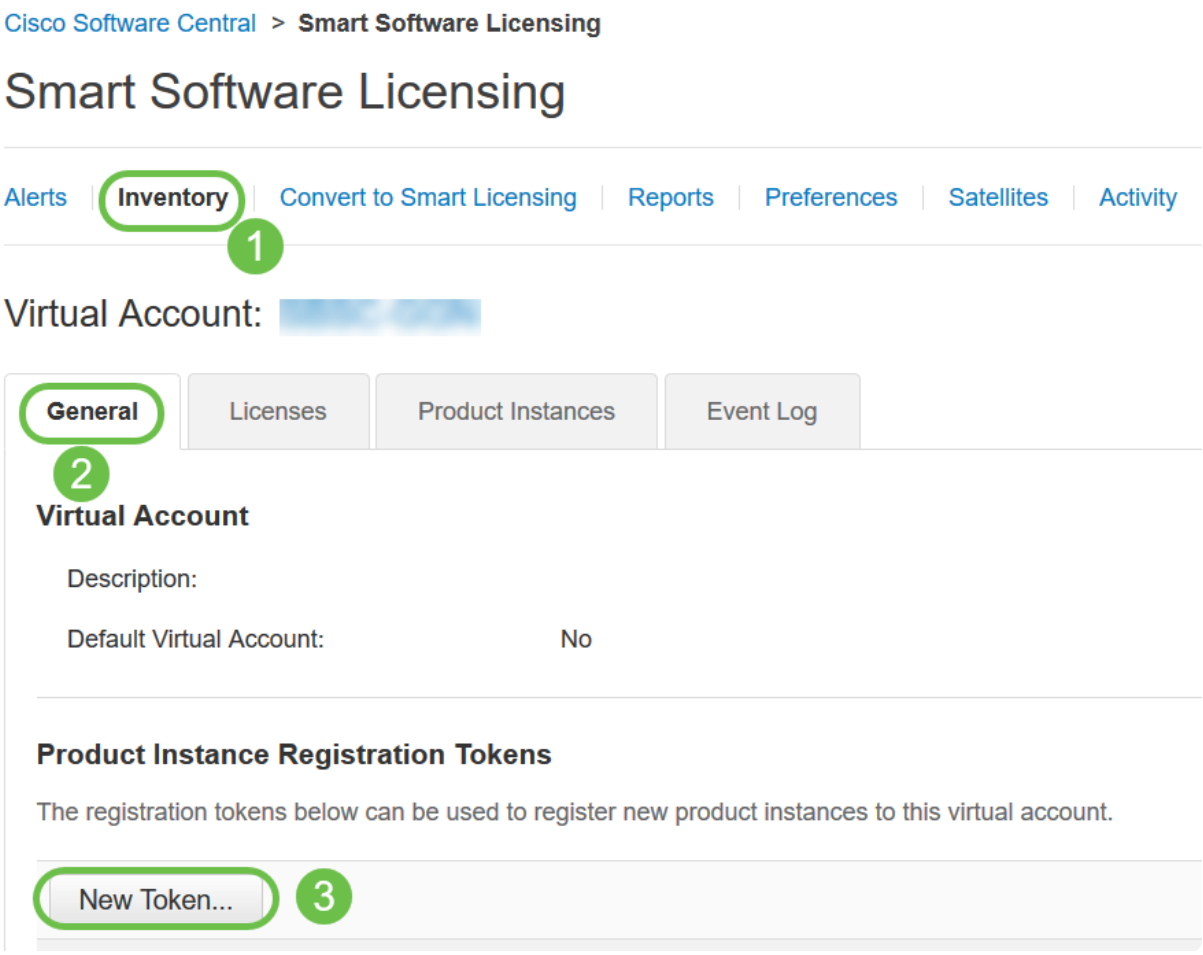
Passaggio 3

Selezionare Inventario > Licenze e verificare che la licenza dei servizi di sicurezza della serie RV sia presente nello Smart Account. Se la licenza non viene visualizzata, contattare il partner Cisco.



Passaggio 4

Passare a Magazzino > Generale. In Token di registrazione dell'istanza del prodotto fare clic su Nuovo token.



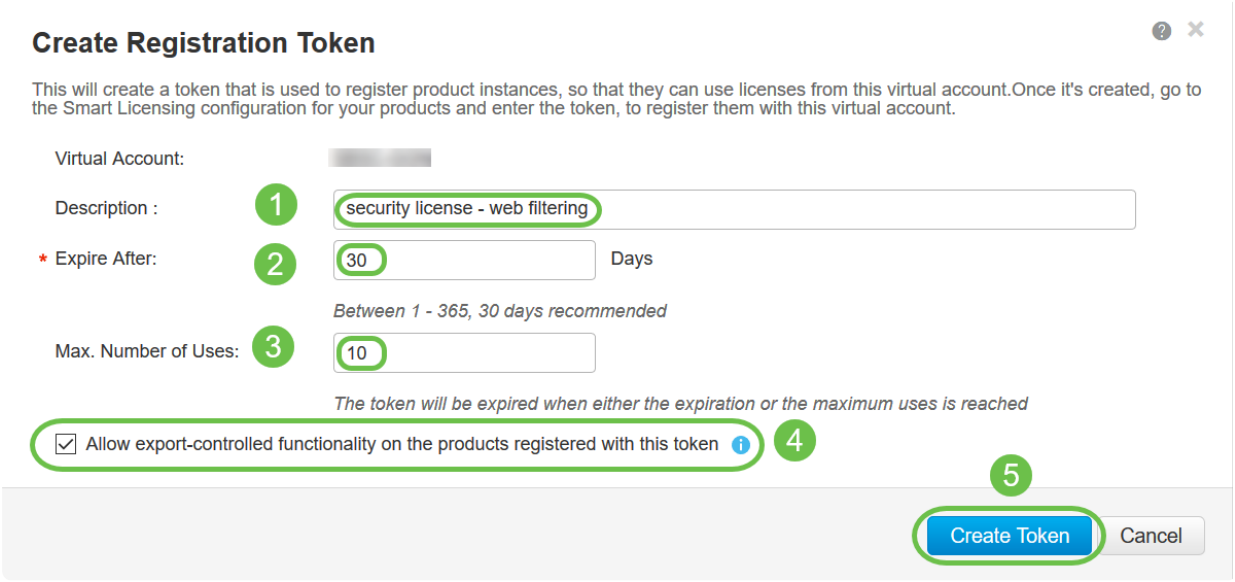
Passaggio 5

Viene visualizzata la finestra Crea token di registrazione. Nell'area Account virtuale viene visualizzato l'account virtuale in cui verrà creato il token di registrazione. Nella pagina Crea token di registrazione, effettuare le operazioni riportate di seguito.

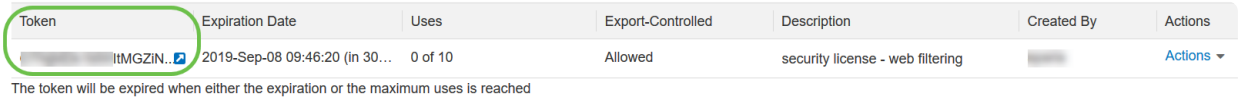
- Nel campo Description (Descrizione), immettere una descrizione univoca per il token. In questo esempio, viene immesso security license - web filtering (licenza di protezione - filtro Web).
- Nel campo Scadenza immettere un valore compreso tra 1 e 365 giorni. Cisco consiglia di impostare questo campo su 30 giorni; tuttavia, è possibile modificare il valore in base alle proprie esigenze.
- Nella scheda Max. Campo Numero di utilizzi immettere un valore per definire il numero di utilizzi del token. Il token scadrà quando viene raggiunto il numero di giorni o il numero massimo di utilizzi.
- Selezionare la casella di controllo Consenti funzionalità di controllo dell'esportazione sui prodotti registrati con questo token per abilitare la funzionalità di controllo dell'esportazione per i token di un'istanza del prodotto nell'account virtuale. Deselezionare la casella di controllo se non si desidera consentire l'utilizzo della

funzionalità di controllo dell'esportazione con questo token. Utilizzare questa opzione solo se si è conformi alla funzionalità di esportazione controllata. Alcune funzionalità sottoposte ai controlli per l'esportazione sono soggette a restrizioni da parte del Dipartimento del Commercio degli Stati Uniti. Queste funzionalità sono limitate per i prodotti registrati con questo token quando si deseleziona la casella di controllo. Qualsiasi violazione è soggetta a sanzioni e a sanzioni amministrative.

- Fare clic su Create Token per generare il token.

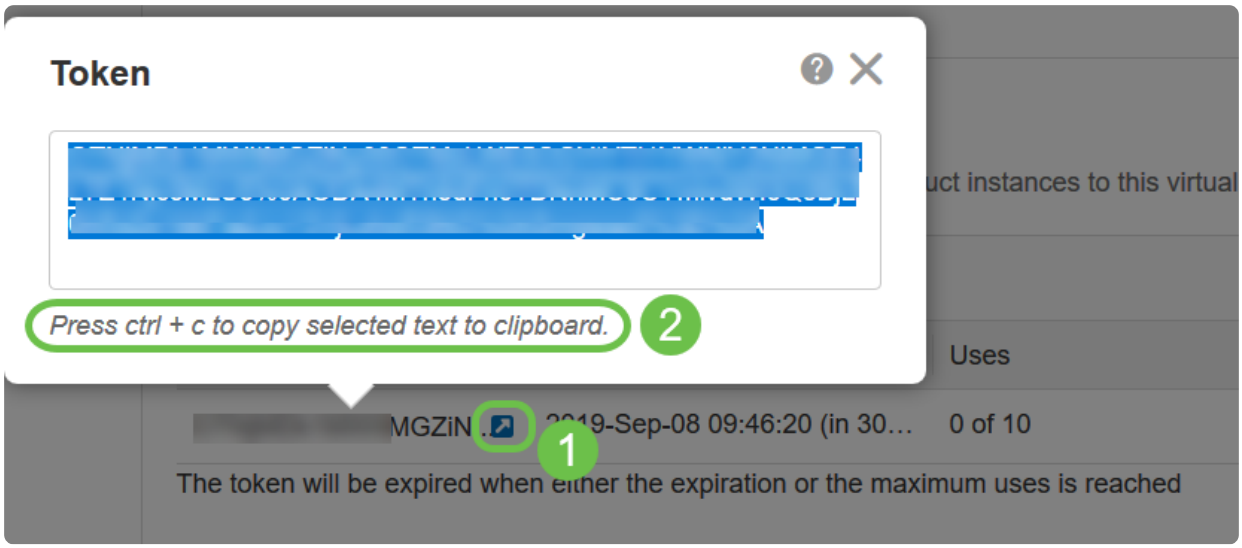


È stato generato correttamente un token di registrazione dell'istanza del prodotto.



Passaggio 6

Fare clic sull'icona a forma di freccia nella colonna Token per copiare il token negli Appunti, premere ctrl + c sulla tastiera.

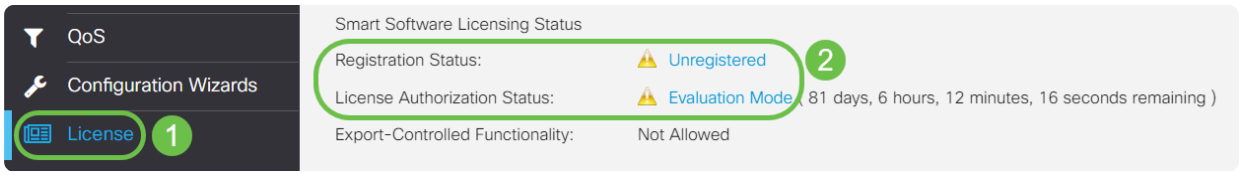


Passaggio 7 (facoltativo)

Fare clic sul menu a discesa Azioni, scegliere Copia per copiare il token negli Appunti o Scarica... per scaricare una copia del file di testo del token da cui è possibile copiare.

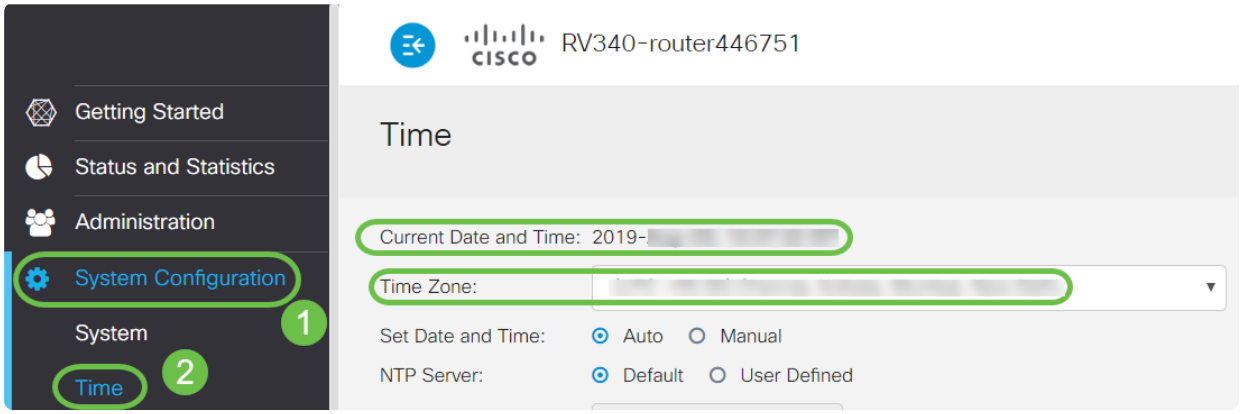
Passaggio 8

Passare a Licenza e verificare che lo stato di registrazione sia indicato come Non registrato e che lo stato di autorizzazione della licenza sia indicato come modalità di valutazione.



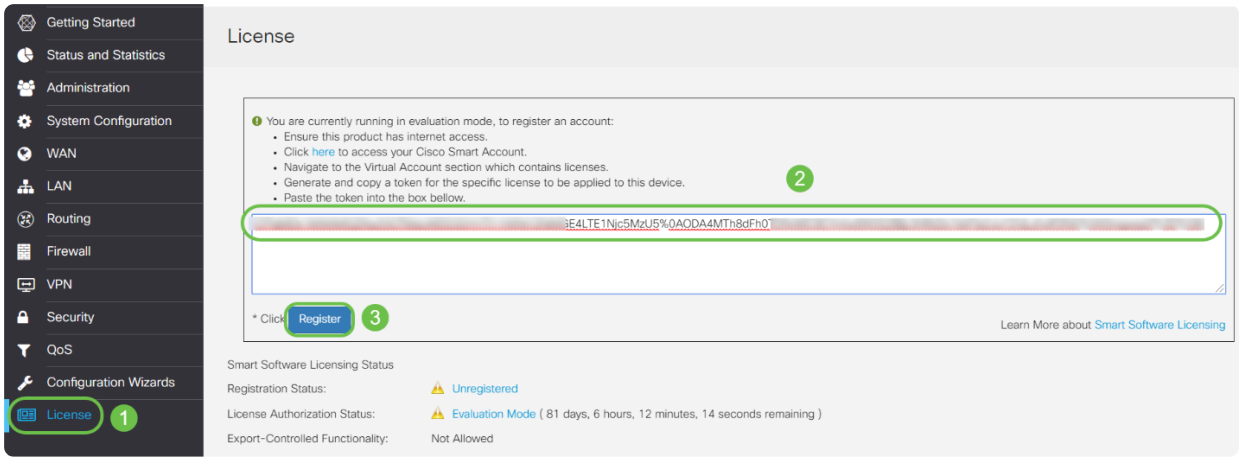
Passaggio 9

Passare a Configurazione di sistema > Ora e verificare che la data e l'ora correnti e il fuso orario si riflettano correttamente in base al fuso orario.



Passaggio 10

Passare a Licenza. Incollare il token copiato al passaggio 6 nella casella di testo nella scheda Licenza selezionando ctrl + v sulla tastiera. Fare clic su Registra.

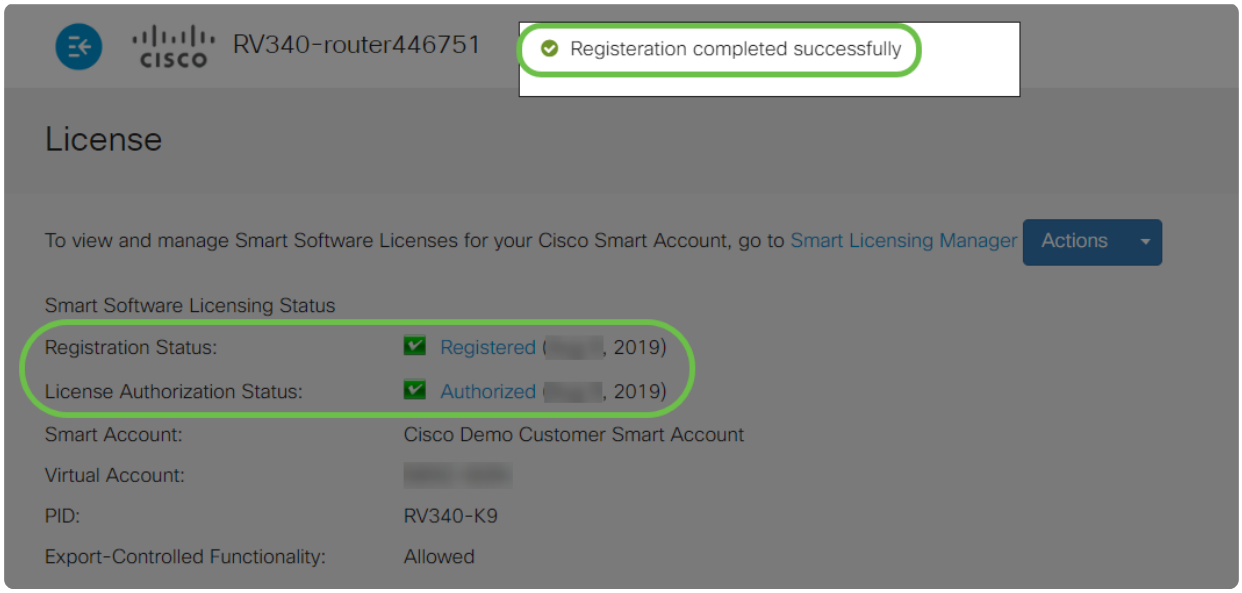


La registrazione potrebbe richiedere alcuni minuti. Non uscire dalla pagina perché il router tenta di contattare il server licenze.

Passaggio 11

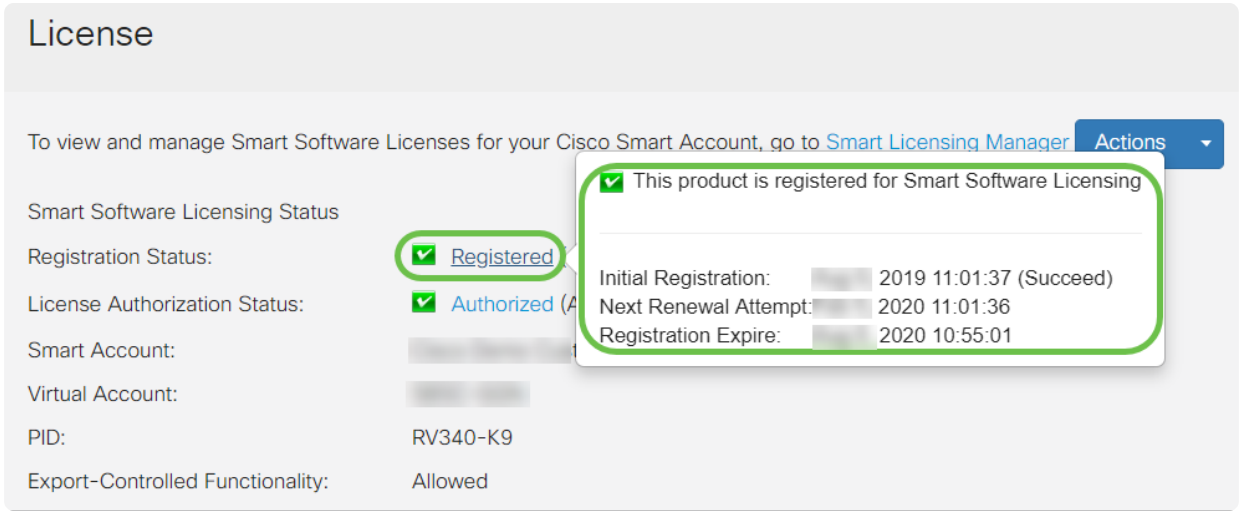
A questo punto, è necessario aver registrato e autorizzato il router serie RV345P con una Smart License. Sullo schermo verrà visualizzata una notifica indicante che la

registrazione è stata completata. Inoltre, è possibile verificare che lo stato della registrazione sia indicato come Registrato e lo stato di autorizzazione della licenza come Autorizzato.



Passaggio 12 (facoltativo)

Per visualizzare ulteriori dettagli sullo stato di registrazione della licenza, posizionare il puntatore del mouse sullo stato Registrato. Viene visualizzata una finestra di dialogo con le seguenti informazioni:



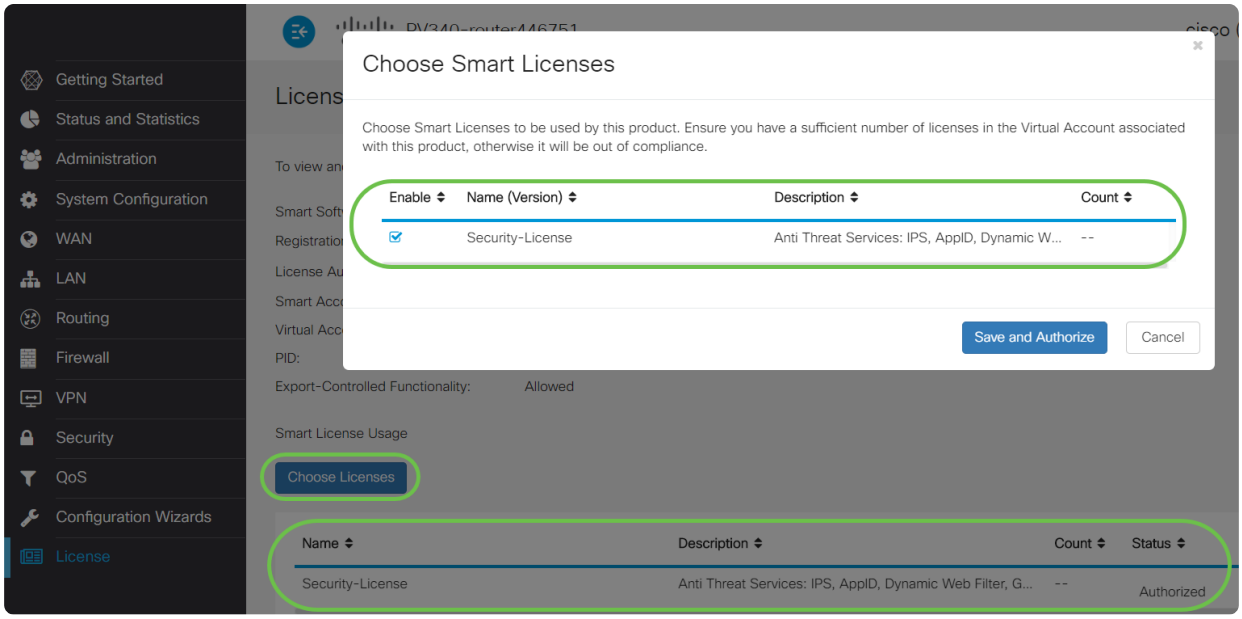
- Registrazione iniziale - Quest'area indica la data e l'ora in cui la licenza è stata registrata.

- Next Renewal Tentate - Quest'area indica la data e l'ora in cui il router tenterà di rinnovare la licenza.
- Scadenza registrazione — quest'area indica la data e l'ora di scadenza della registrazione.

Passaggio 13

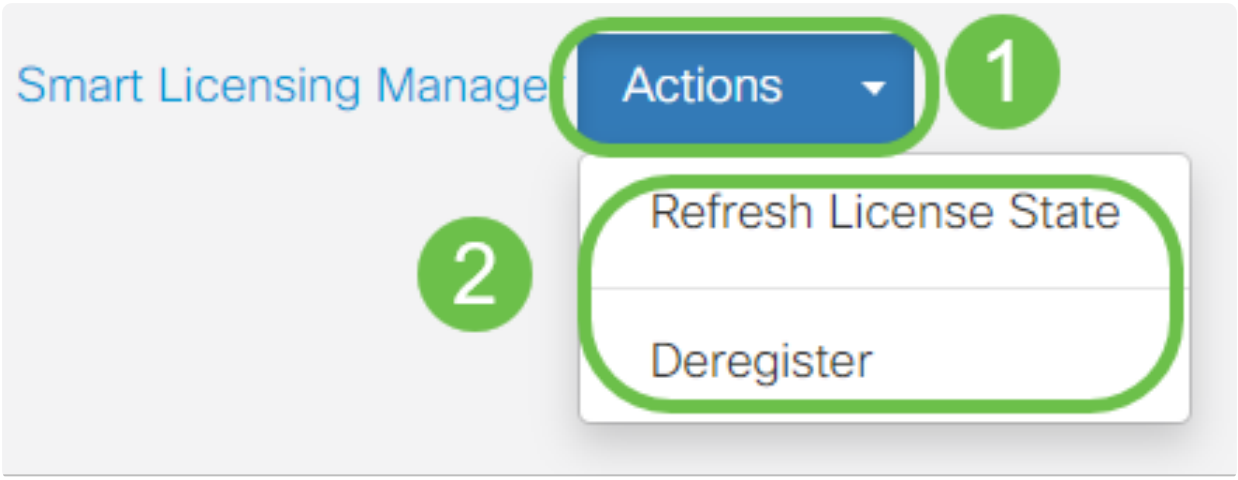
Nella pagina Licenza verificare che lo stato Security-License sia Authorized (Autorizzata). È inoltre possibile fare clic sul pulsante Choose License (Scegli licenza) per verificare che Security-License sia abilitato.

> ⓘ Note: In caso di problemi in questo passaggio, potrebbe essere necessario riavviare il router.



Passaggio 14 (facoltativo)

Per aggiornare lo stato della licenza o annullare la registrazione della licenza dal router, fare clic sul menu a discesa Azioni di Smart Licensing Manager e selezionare un'azione.



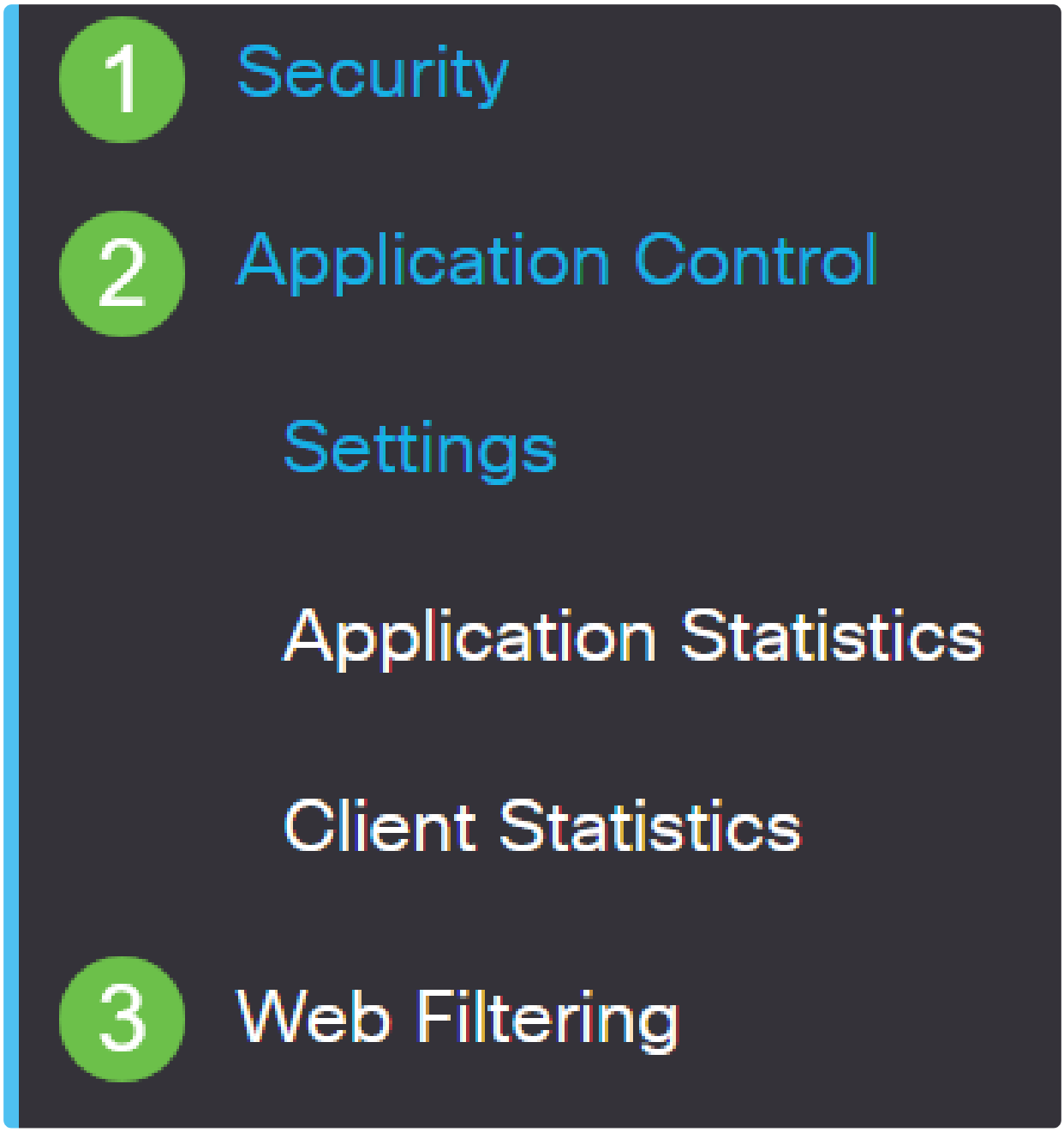
Ora che si dispone della licenza sul router, è necessario completare la procedura descritta nella sezione successiva.

Filtro Web sul router RV345P

Sono trascorsi 90 giorni dall'attivazione per utilizzare gratuitamente il filtro Web. Dopo la versione di valutazione gratuita, se si desidera continuare a utilizzare questa funzionalità, è necessario acquistare una licenza. Fare clic per tornare alla sezione.

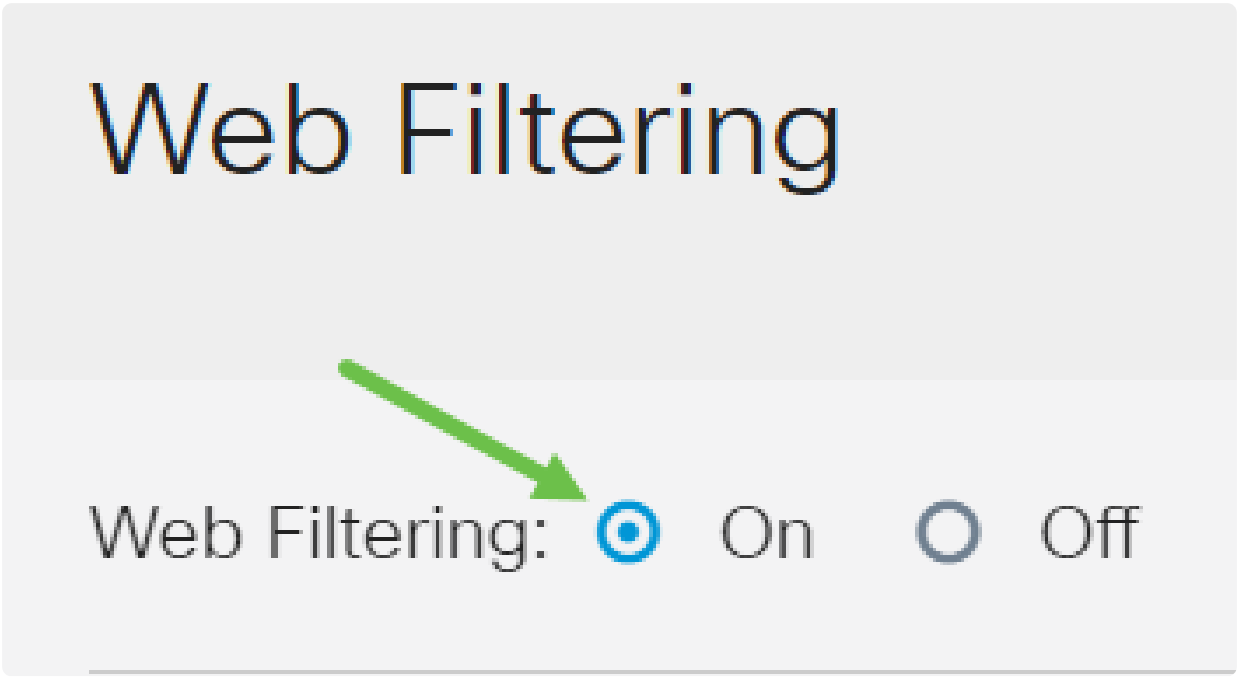
Passaggio 1

Accedere all'utility basata sul Web e scegliere Protezione > Controllo applicazione > Filtro Web.



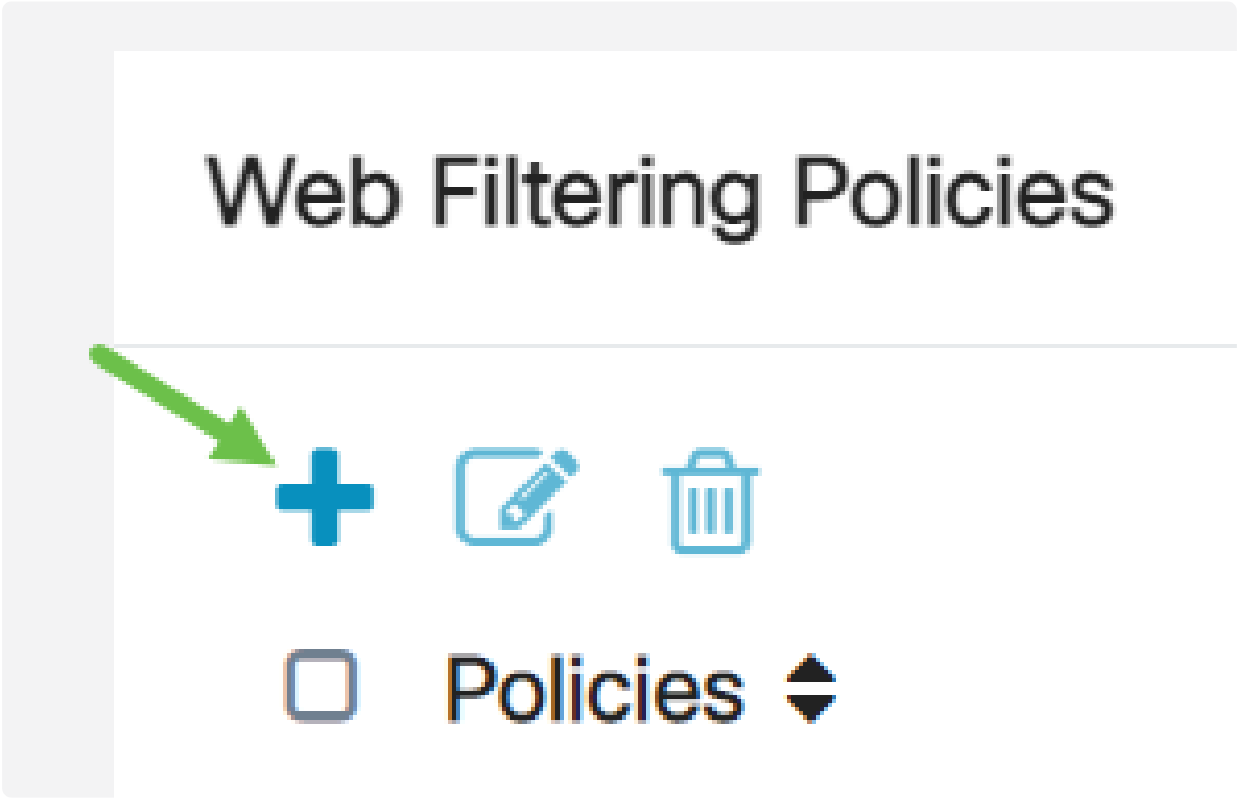
Passaggio 2

Selezionare il pulsante di opzione On.



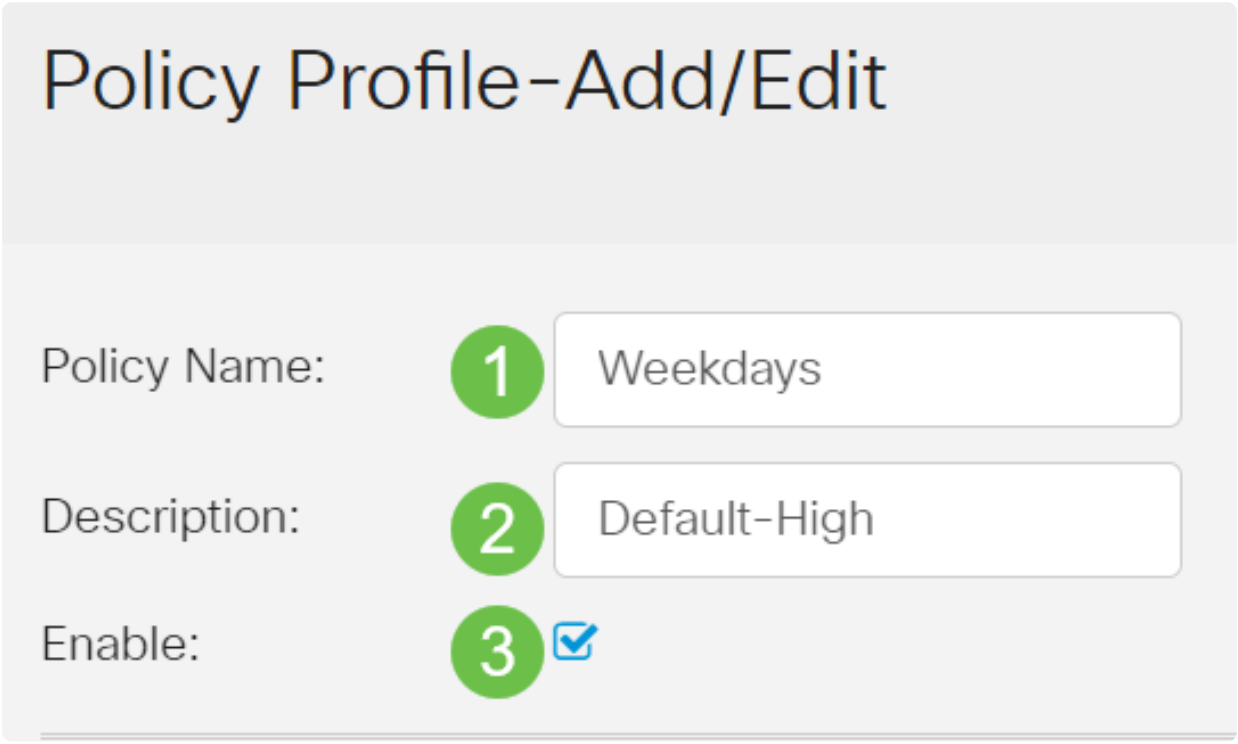
Passaggio 3

Fare clic sull'icona Aggiungi.



Passaggio 4

Immettere il Nome criterio, la Descrizione e la casella di controllo Abilita.



ⓘ Note: Se sul router è attivato il filtro contenuti, verrà visualizzata una notifica per informare che il filtro è stato disattivato e che le due funzionalità non possono essere attivate contemporaneamente. Fare clic su Apply (Applica) per continuare con la configurazione.

Passaggio 5

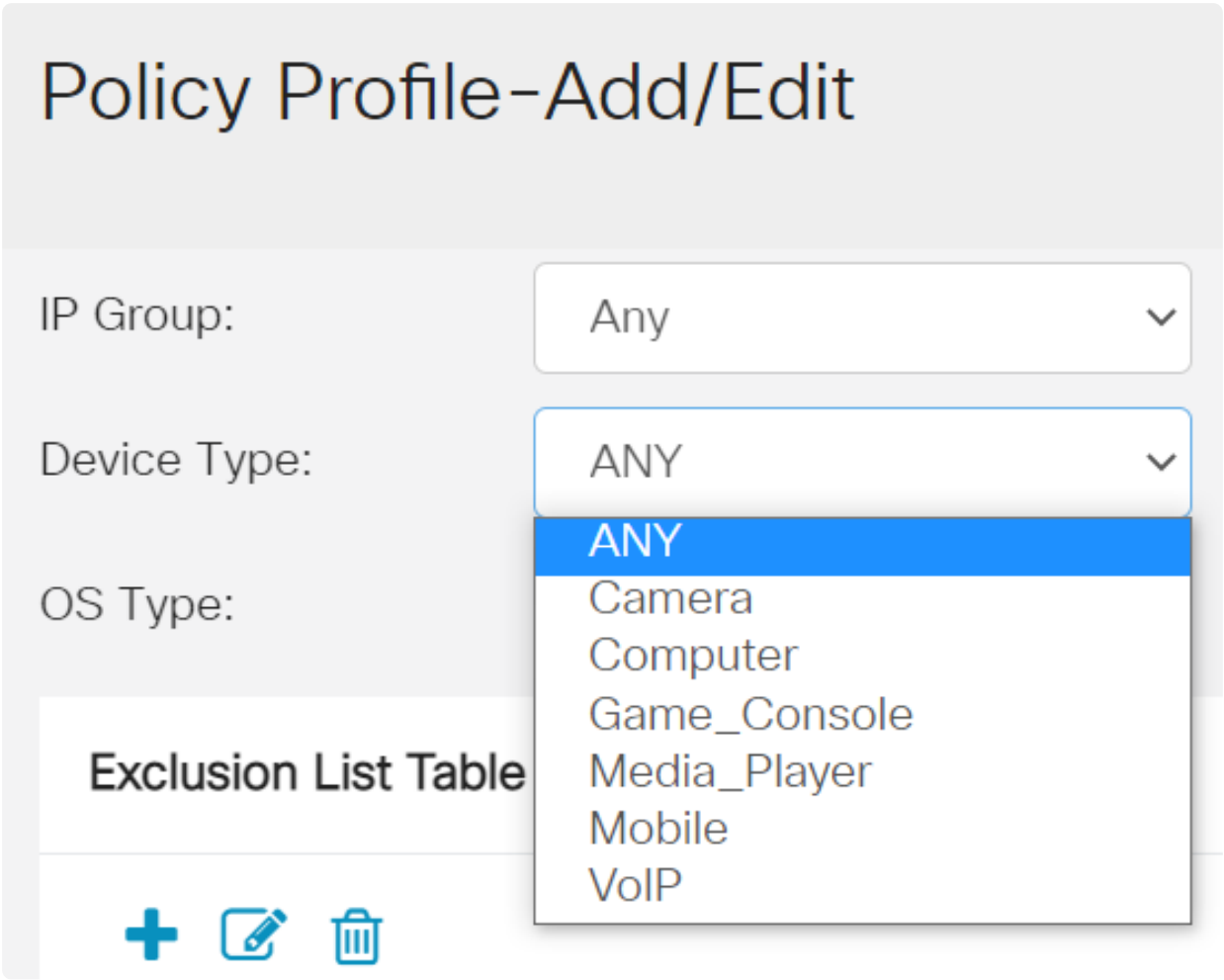
Selezionare la casella di controllo Reputazione Web per abilitare il filtro in base a un indice di reputazione Web.

ⓘ Note: I contenuti verranno filtrati in base alla notorietà di un sito Web o di un URL in base a un indice di reputazione Web. Se il punteggio scende al di sotto di 40, il sito verrà bloccato. Per ulteriori informazioni sulla tecnologia di reputazione Web, fare clic qui per ulteriori dettagli.

Passaggio 6

Dall'elenco a discesa Device Type (Tipo di dispositivo), selezionare l'origine o la destinazione dei pacchetti da filtrare. È possibile scegliere una sola opzione alla volta. Le opzioni sono:

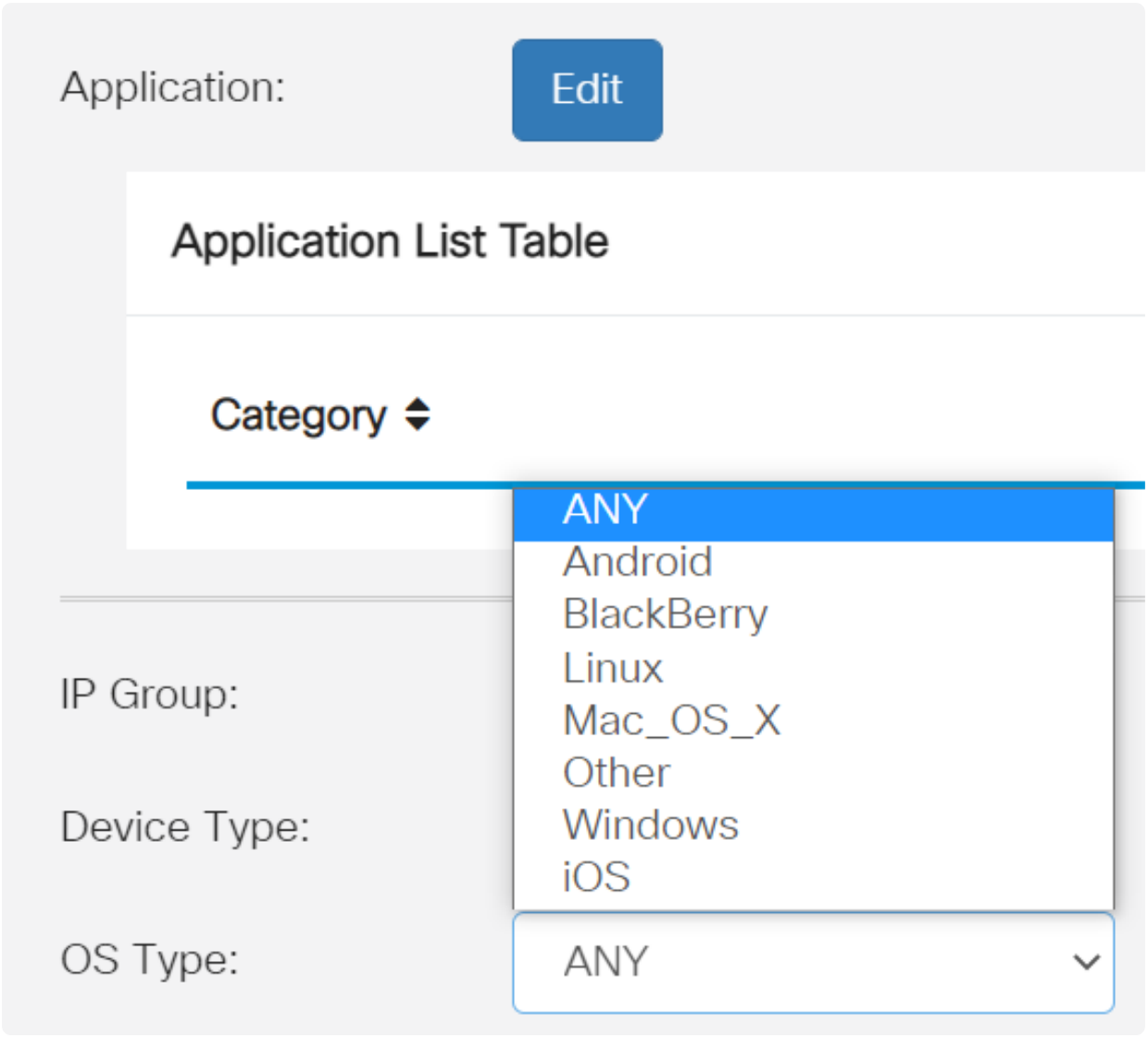
- ANY - Consente di applicare il criterio a qualsiasi dispositivo.
- Fotocamera: selezionare questa opzione per applicare il criterio alle videocamere (ad esempio, le videocamere di sicurezza IP).
- Computer — scegliere questa opzione per applicare il criterio ai computer.
- Game_Console: scegliere questa opzione per applicare la policy alle console di gioco.
- Media_Player: scegliere questa opzione per applicare il criterio a Media Player.
- Mobile: scegliere questa opzione per applicare il criterio ai dispositivi mobili.
- VoIP: scegliere questa opzione per applicare il criterio ai dispositivi Voice over Internet Protocol.



Passaggio 7

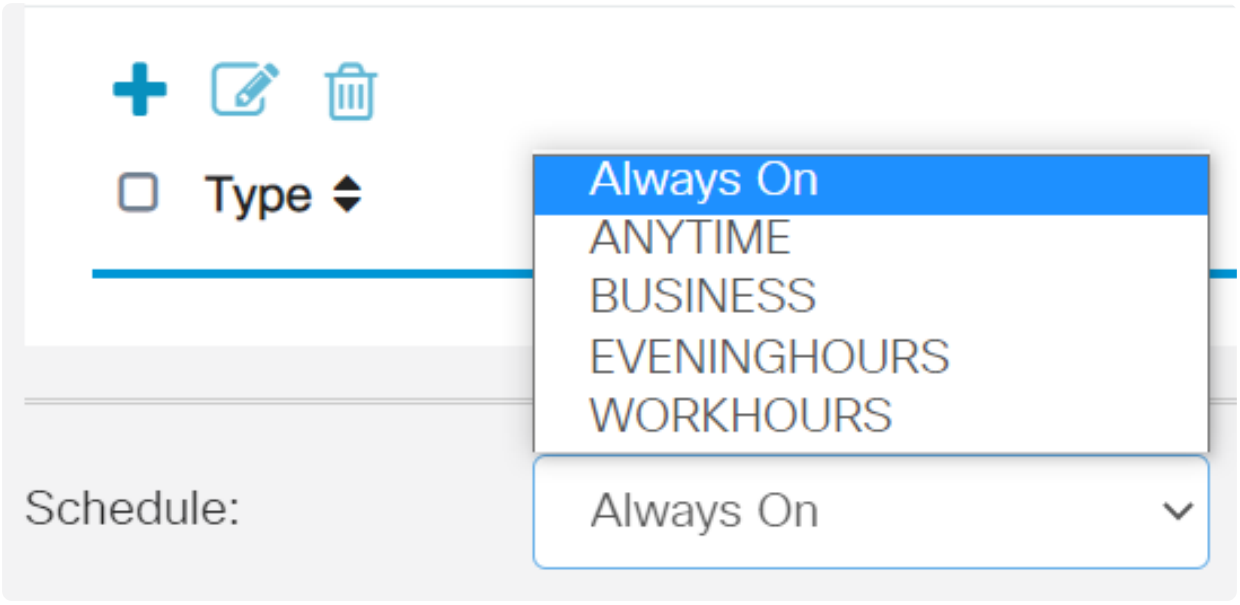
Dall'elenco a discesa Tipo di sistema operativo, scegliere un sistema operativo a cui applicare il criterio. È possibile scegliere una sola opzione alla volta. Le opzioni sono:

- ANY - Applica il criterio a qualsiasi tipo di sistema operativo. Questa è l'impostazione predefinita.
- Android — Applica il criterio solo al sistema operativo Android.
- BlackBerry: applica il criterio solo al sistema operativo Blackberry.
- Linux: applica la policy solo al sistema operativo Linux.
- Mac_OS_X — applica il criterio solo a Mac OS.
- Altro - Applica il criterio a un sistema operativo non elencato.
- Windows: applica il criterio al sistema operativo Windows.
- iOS: applica la policy solo a iOS OS.



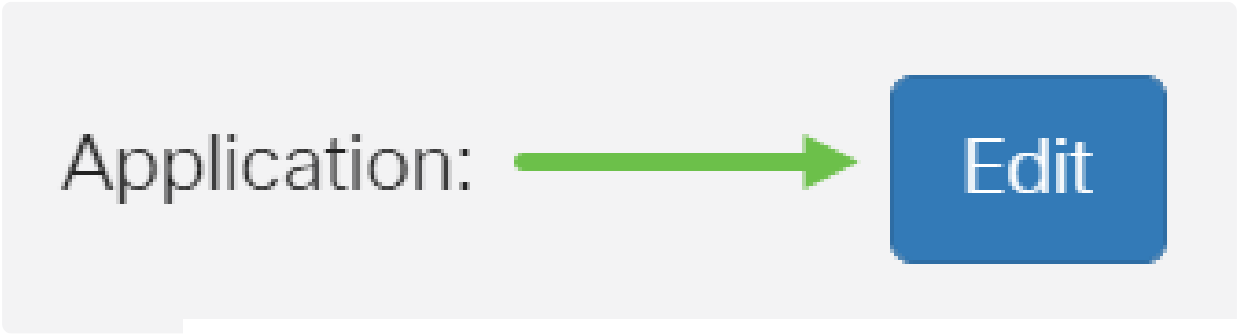
Passaggio 8

Scorrere fino alla sezione Pianificazione e selezionare l'opzione più adatta alle proprie esigenze.



Passaggio 9

Fare clic sull'icona Modifica.

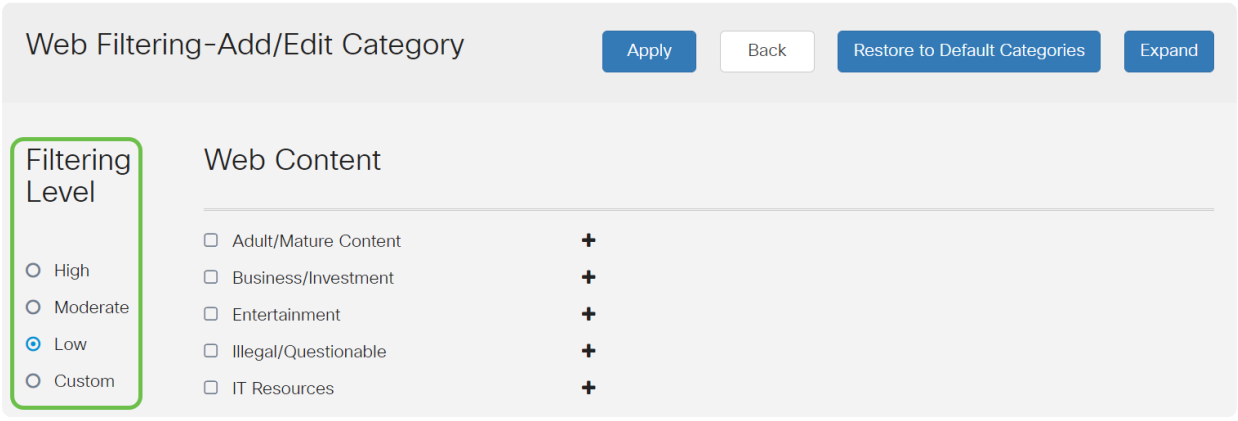


Passaggio 10

Nella colonna Livello filtro fare clic su un pulsante di opzione per definire rapidamente l'estensione di filtro più adatta ai criteri di rete. Le opzioni disponibili sono Alta, Sufficiente, Bassa e Personalizzata. Fare clic su uno dei livelli di filtro seguenti per conoscere le sottocategorie predefinite specifiche filtrate per ciascuna delle categorie di contenuti Web abilitate. I filtri predefiniti non possono essere modificati ulteriormente e sono disattivati.

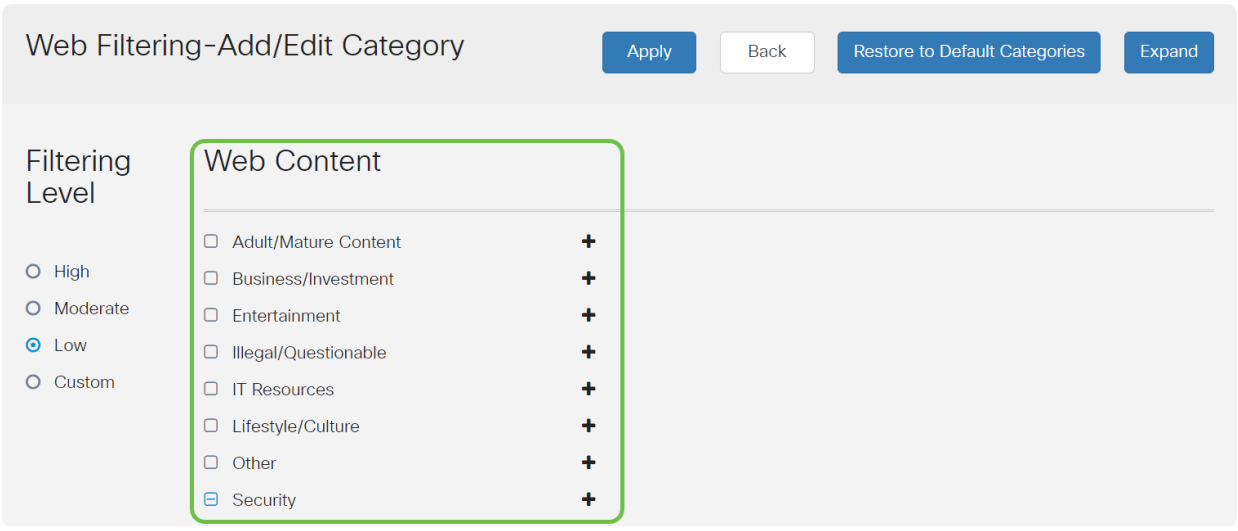
- Basso - questa è l'opzione predefinita. Questa opzione consente di abilitare la protezione.

- Sufficiente: questa opzione consente di abilitare i contenuti per adulti/adulti, illeciti/discutibili e di sicurezza.
- Elevato: questa opzione consente di gestire contenuti per adulti/adulti, attività commerciali/investimenti, informazioni illecite/discutibili, risorse IT e sicurezza.
- Personalizzato - Non sono impostati valori predefiniti per consentire l'uso di filtri definiti dall'utente.



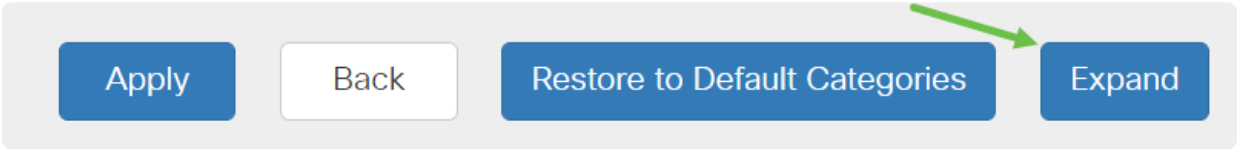
Passaggio 11

Immettere il contenuto Web da filtrare. Fare clic sull'icona più se si desidera visualizzare ulteriori dettagli su una sezione.



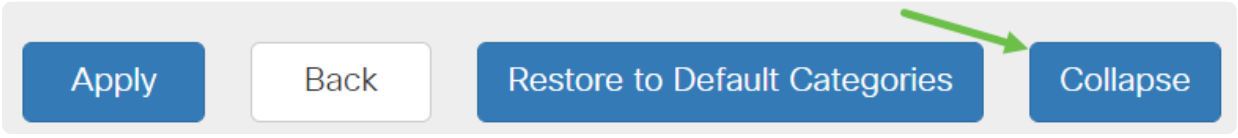
Passaggio 12 (facoltativo)

Per visualizzare tutte le sottocategorie e le descrizioni del contenuto Web, è possibile fare clic sul pulsante Espandi.



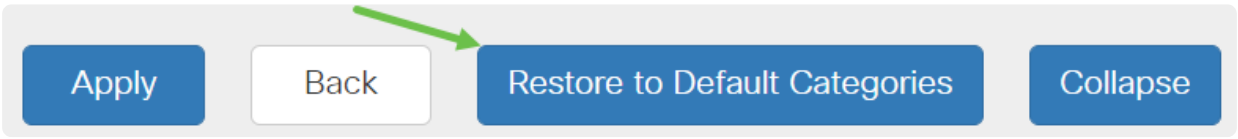
Passaggio 13 (facoltativo)

Fare clic su Comprimi per comprimere le sottocategorie e le descrizioni.



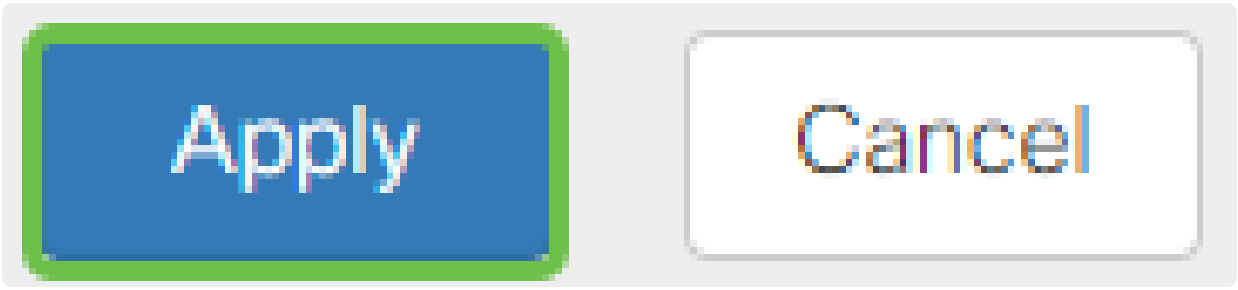
Passaggio 14 (facoltativo)

Per tornare alle categorie predefinite, fare clic su Ripristina categorie predefinite.



Passaggio 15

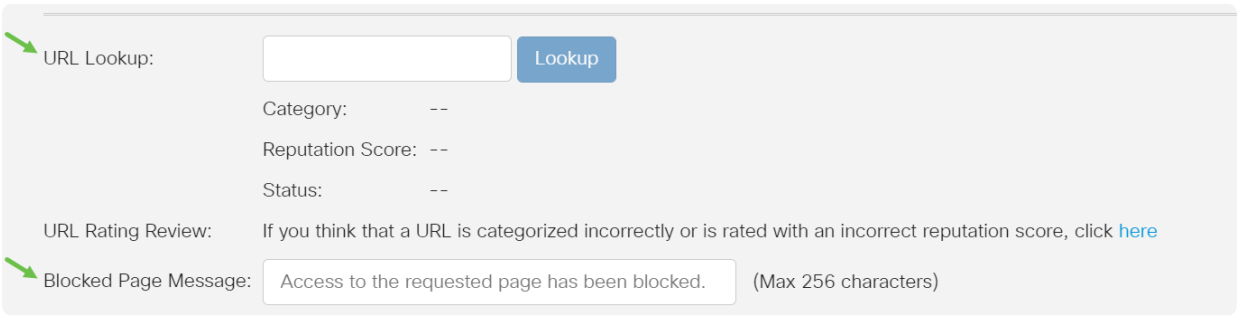
Fare clic su Apply (Applica) per salvare la configurazione e tornare alla pagina Filter (Filtro) per continuare l'installazione.



ⓘ Note: Nella tabella Elenco applicazioni verranno inserite le sottocategorie corrispondenti basate sul livello di filtro scelto.

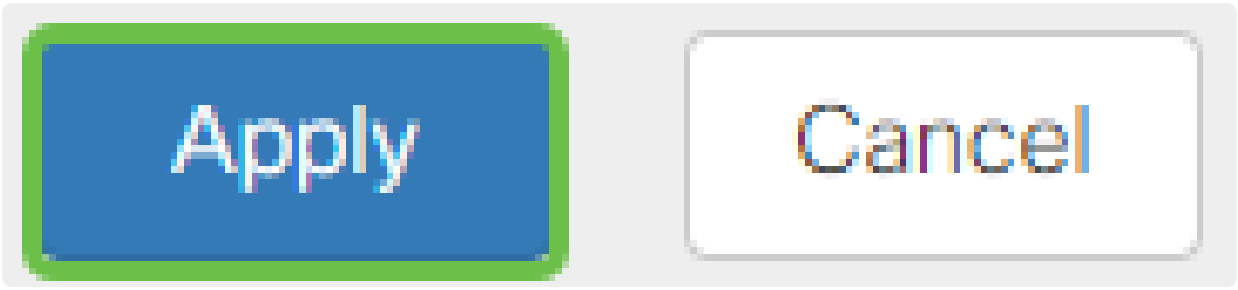
Passaggio 16 (Facoltativo)

Altre opzioni includono Ricerca URL e il messaggio che viene visualizzato quando una pagina richiesta è stata bloccata.



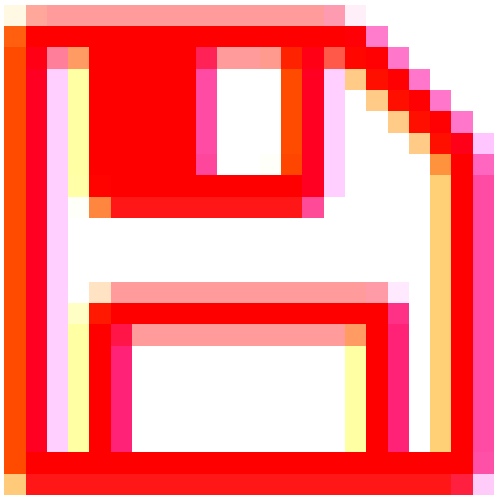
Passaggio 17 (facoltativo)

Fare clic su Apply (Applica).



Passaggio 18

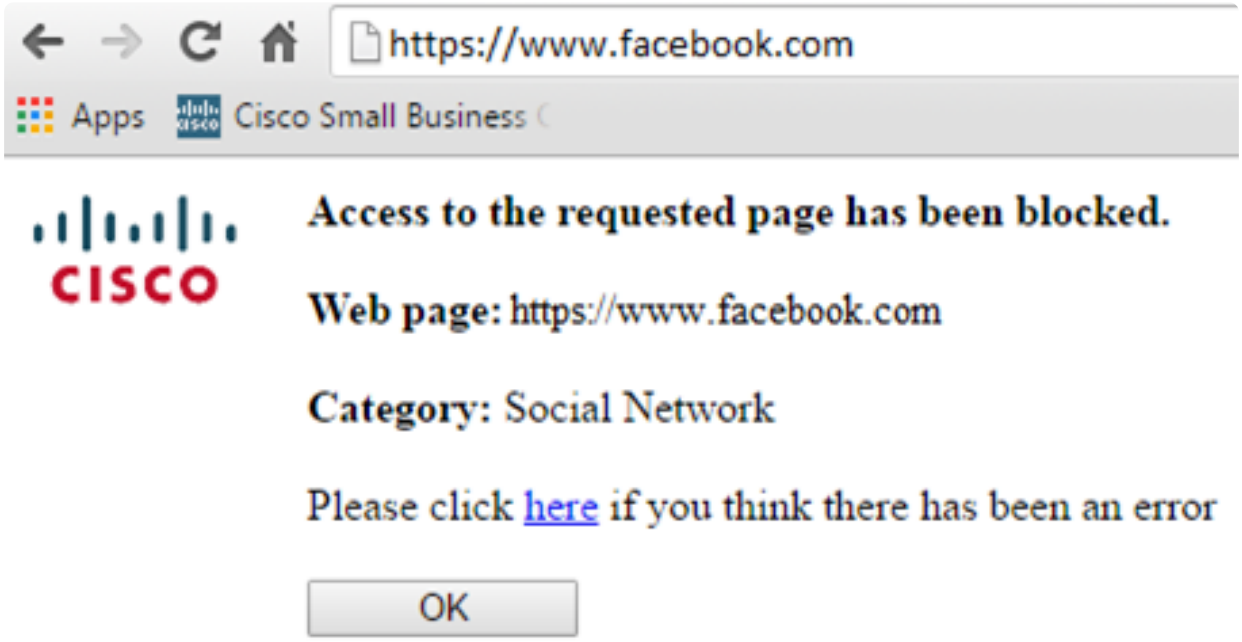
Per salvare la configurazione in modo permanente, andare alla pagina Copia/Salva configurazione o fare clic sull'icona Salva nella parte superiore della pagina.



Passaggio 19 (Facoltativo)

Per verificare che un sito Web o un URL sia stato filtrato o bloccato, avviate un browser Web o aprite una nuova scheda nel browser. Immetti il nome di dominio che hai bloccato elencato o che hai filtrato per essere bloccato o rifiutato.

Nell'esempio viene utilizzato www.facebook.com.



A questo punto, il filtro Web sul router RV345P deve essere configurato correttamente. Poiché si sta utilizzando la RV Security License per il filtro Web, probabilmente non è necessario Umbrella. Se vuoi anche Umbrella, clicca qui. Se si dispone di un livello di protezione sufficiente, fare clic su per passare alla sezione successiva.

Risoluzione dei problemi

Se la licenza è stata acquistata ma non è visualizzata nell'account virtuale, sono disponibili due opzioni:

1. Contattare il rivenditore per richiedere il trasferimento.
2. Contattateci per contattare il rivenditore.

Idealmente non dovreste fare neanche una cosa, ma se arrivate a questo incrocio siamo felici di aiutarvi! Per rendere il processo il più rapido possibile, sono necessarie le credenziali riportate nella tabella precedente e quelle descritte di seguito.

Informazioni obbligatorie	Individuazione delle informazioni
Fattura licenza	Dopo aver completato l'acquisto delle licenze, riceverete un'e-mail di conferma.
Numero ordine di vendita Cisco	Per ottenere questo, potrebbe essere necessario tornare al rivenditore.
Schermata della pagina della licenza dello Smart Account	La cattura di uno screenshot consente di acquisire il contenuto dello schermo per condividerlo con il team. Se non si ha dimestichezza con gli screenshot, è possibile utilizzare i metodi seguenti.

Schermate

Una volta ottenuto un token, o se state risolvendo il problema, si consiglia di acquisire una schermata per acquisire il contenuto dello schermo.

Date le differenze nelle procedure richieste per acquisire uno screenshot, vedere di seguito per i collegamenti specifici del sistema operativo.

- Windows
- MAC
- iPhone/iPad
- Android

Licenza Umbrella RV Branch (opzionale)

Umbrella è una piattaforma Cisco per la sicurezza cloud semplice ma molto efficace.

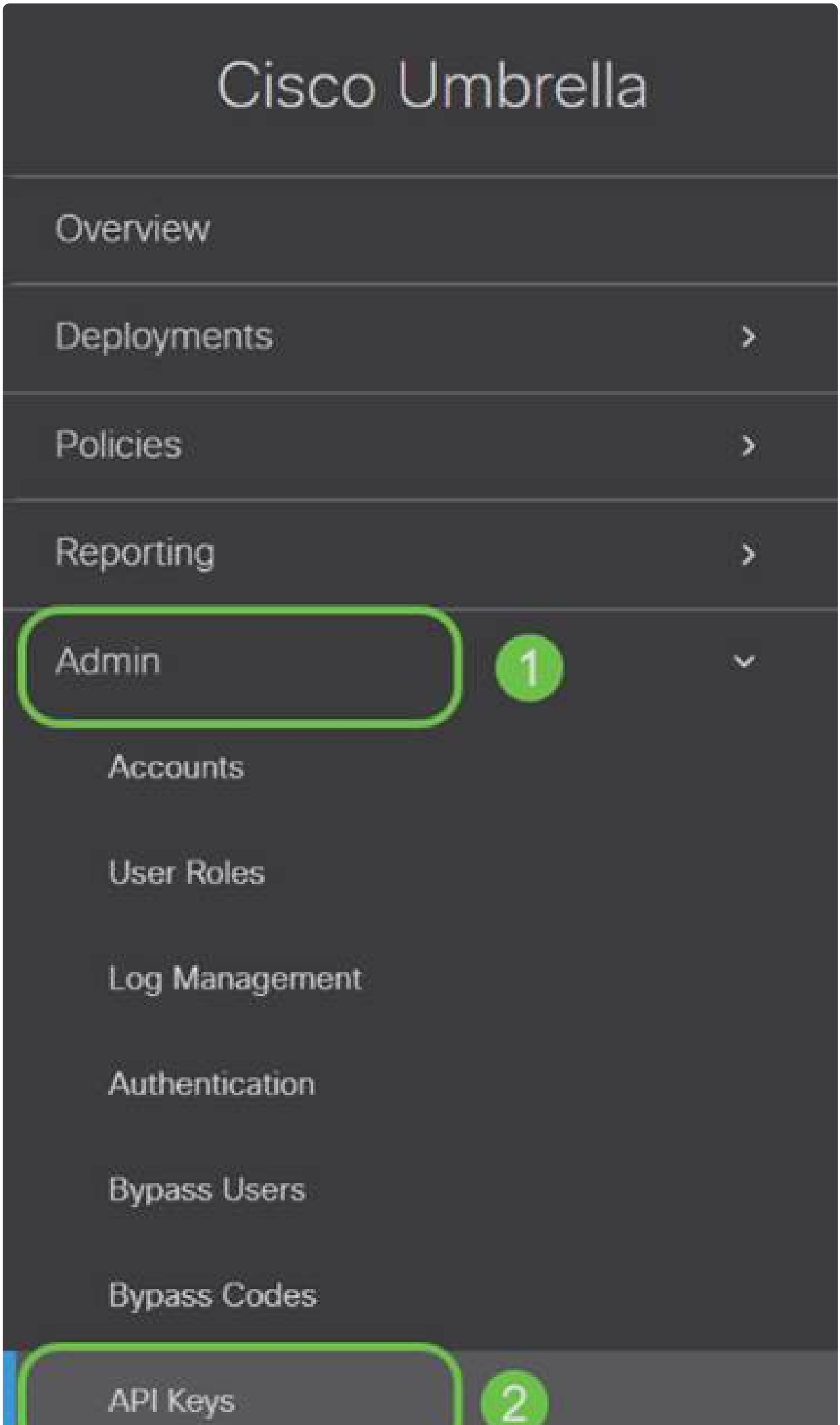
Umbrella opera nel cloud ed esegue molti servizi legati alla sicurezza. Dalla minaccia emergente all'indagine post-evento. Umbrella individua e previene gli attacchi attraverso tutte le porte e i protocolli.

Umbrella utilizza il DNS come vettore principale per la difesa. Quando gli utenti immettono un URL nella barra del browser e premono Invio, Umbrella partecipa al trasferimento. Tale URL passa al resolver DNS di Umbrella e, se al dominio viene associato un avviso di sicurezza, la richiesta viene bloccata. Questi dati di telemetria vengono trasferiti e analizzati in microsecondi, senza aggiungere alcuna latenza. I dati di telemetria utilizzano registri e strumenti per tenere traccia di miliardi di richieste DNS in tutto il mondo. Quando questi dati sono diffusi, la correlazione a livello globale consente una risposta rapida agli attacchi non appena si verificano. Per ulteriori informazioni, vedere l'informativa sulla privacy di Cisco: informativa completa, versione di riepilogo. I dati di telemetria possono essere paragonati ai dati derivati da strumenti e registri.

Per ulteriori informazioni e per creare un account, visita Cisco Umbrella. In caso di problemi, consultare la documentazione e qui le opzioni di supporto Umbrella.

Passaggio 1

Dopo aver effettuato l'accesso all'account Umbrella, dalla schermata Dashboard fare clic su Amministrazione > Chiavi API.


Cisco Umbrella
Overview
Deployments
Policies
Reporting
Admin
1
Accounts
User Roles
Log Management
Authentication
Bypass Users
Bypass Codes
API Keys
2

Anatomia della schermata delle chiavi API (con chiave API preesistente)

1 Add API Key (Aggiungi chiave API) - Avvia la creazione di una nuova chiave da utilizzare con l'API Umbrella.

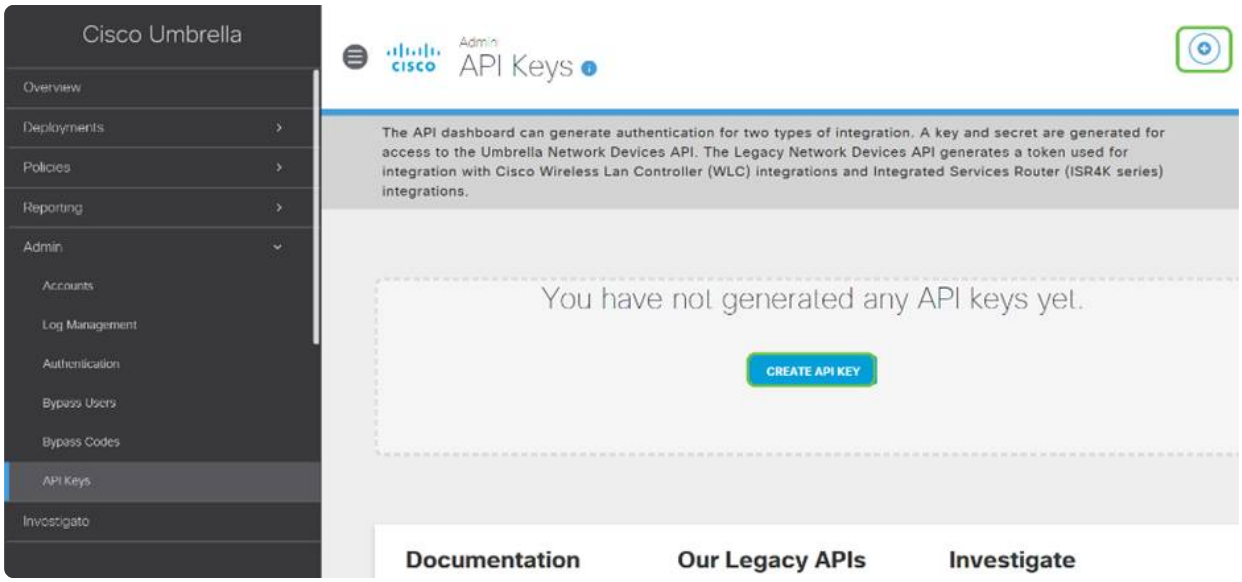
2 Informazioni aggiuntive - Visualizza le diapositive verso il basso/verso l'alto con un'illustrazione per questa schermata.

3 Finestra Token - Contiene tutte le chiavi e i token creati da questo account. (Popola dopo la creazione di una chiave)

4 Documenti di supporto - Collegamenti alla documentazione sul sito Umbrella relativa agli argomenti di ciascuna sezione.

Passaggio 2

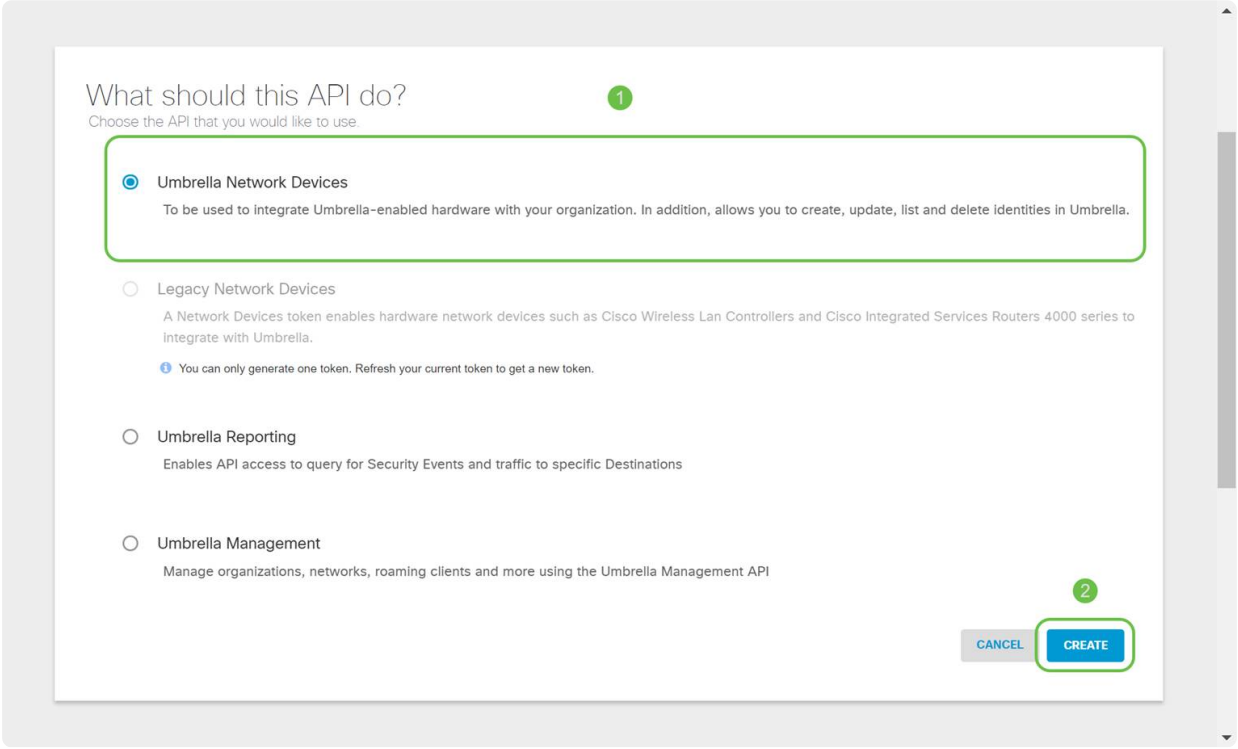
Fare clic sul pulsante Add API Key nell'angolo in alto a destra o fare clic sul pulsante Create API Key. Funzionano entrambi allo stesso modo.



ⓘ Note: La schermata precedente sarebbe simile a quella che vedreste aprire questo menu per la prima volta.

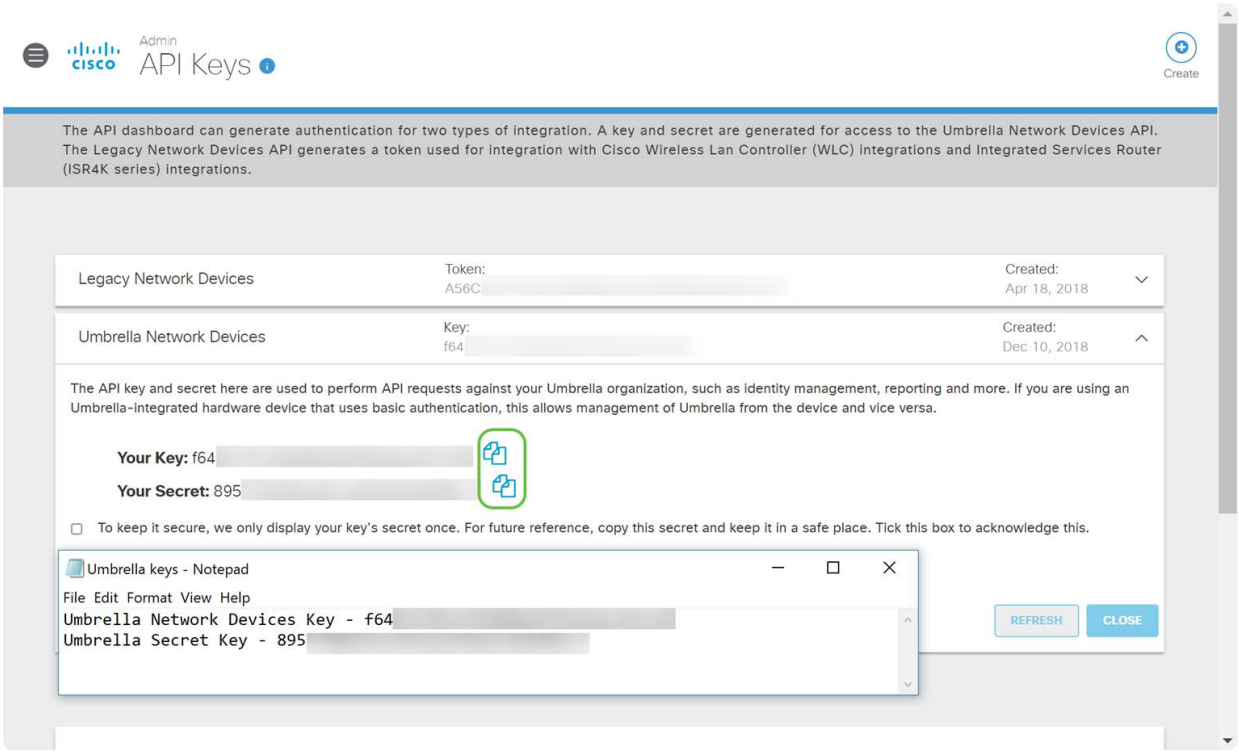
Passaggio 3

Selezionare Periferiche di rete ombrello, quindi fare clic sul pulsante Crea.



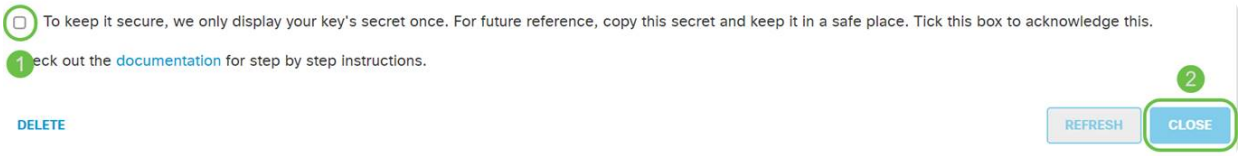
Passaggio 4

Aprire un editor di testo come il Blocco note, quindi fare clic sull'icona di copia a destra dell'API e della chiave segreta API. Una notifica a comparsa confermerà che la chiave è stata copiata negli Appunti. Incollare una alla volta il segreto e la chiave API nel documento, etichettandoli per riferimento futuro. In questo caso, l'etichetta è "Umbrella network devices key". Salvare quindi il file di testo in una posizione sicura, facilmente accessibile in seguito.



Passaggio 5

Dopo aver copiato la chiave e la chiave segreta in un luogo sicuro, dalla schermata Umbrella API fare clic sulla casella di spunta per confermare il completamento della visualizzazione temporanea della chiave segreta, quindi fare clic sul pulsante Chiudi.



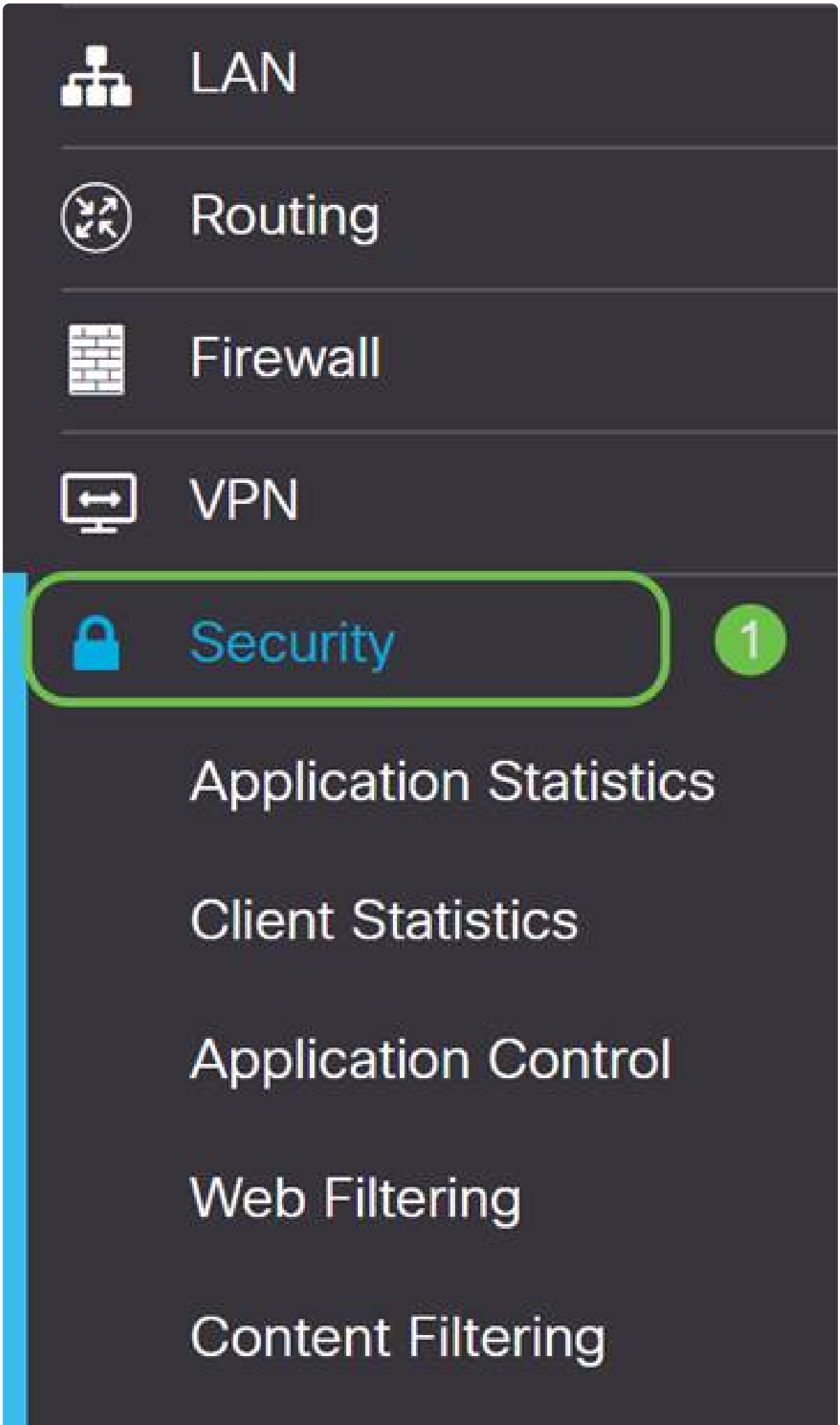
> ⓘ Note: Se si perde o si elimina accidentalmente la chiave segreta, non sarà disponibile alcuna funzione o numero di supporto da chiamare per recuperare la chiave. In caso di perdita, sarà necessario eliminare la chiave e autorizzare nuovamente la nuova chiave API con ciascun dispositivo che si desidera proteggere con Umbrella.

Configurazione di Umbrella su RV345P

Ora che abbiamo creato le chiavi API all'interno di Umbrella, è possibile prendere quelle chiavi e installarle sul vostro RV345P.

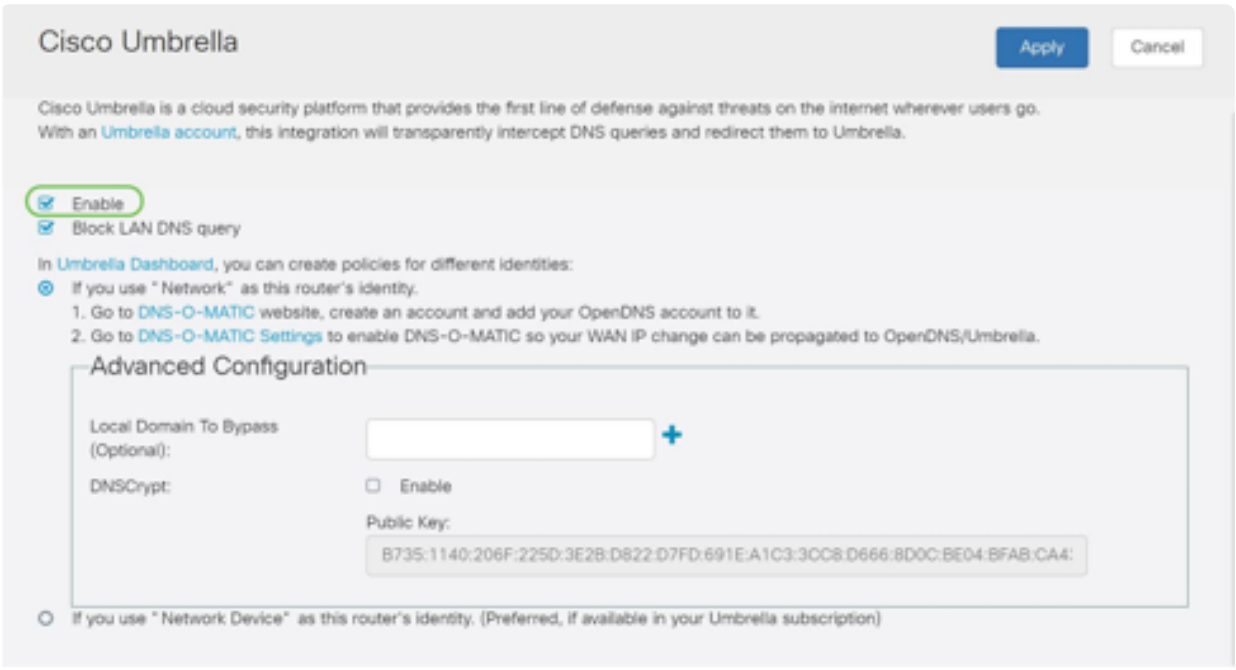
Passaggio 1

Dopo aver effettuato l'accesso al router RV345P, fare clic su Sicurezza > Umbrella nel menu della barra laterale.


LAN
Routing
Firewall
VPN
Security
1
Application Statistics
Client Statistics
Application Control
Web Filtering
Content Filtering

Passaggio 2

La schermata Umbrella API presenta una serie di opzioni, per iniziare ad abilitare Umbrella, fare clic sulla casella di controllo Abilita.

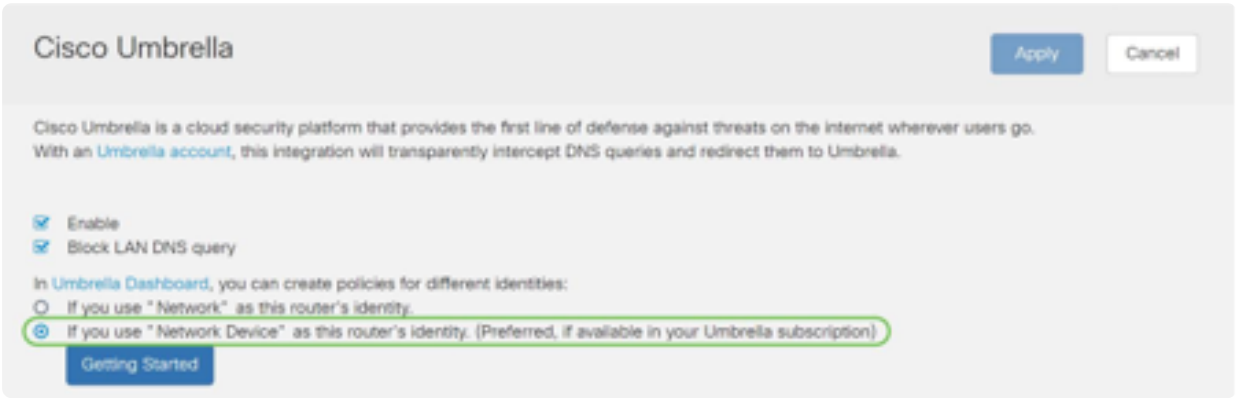


Passaggio 3 (facoltativo)

Per impostazione predefinita, la casella Blocca query DNS LAN è selezionata. Questa funzionalità avanzata consente di creare automaticamente elenchi di controllo di accesso sul router, impedendo al traffico DNS di accedere a Internet. Questa funzione forza tutte le richieste di traduzione del dominio a essere indirizzate attraverso RV345P ed è una buona idea per la maggior parte degli utenti.

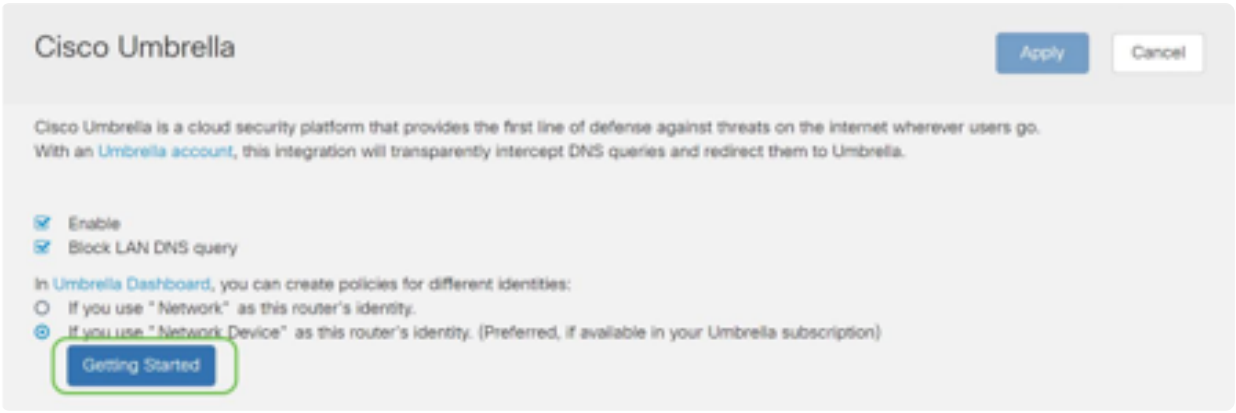
Passaggio 4

Il passaggio successivo viene eseguito in due modi diversi. Entrambi dipendono dalla configurazione della rete. Se si utilizza un servizio come DynDNS o NoIP, si lascia lo schema di denominazione predefinito "Network". Sarà necessario accedere a tali account per garantire l'interfaccia Umbrella con tali servizi in quanto fornisce protezione. Per i nostri scopi ci affidiamo a "Dispositivo di rete", quindi clicchiamo sul pulsante radio inferiore.



Passaggio 5

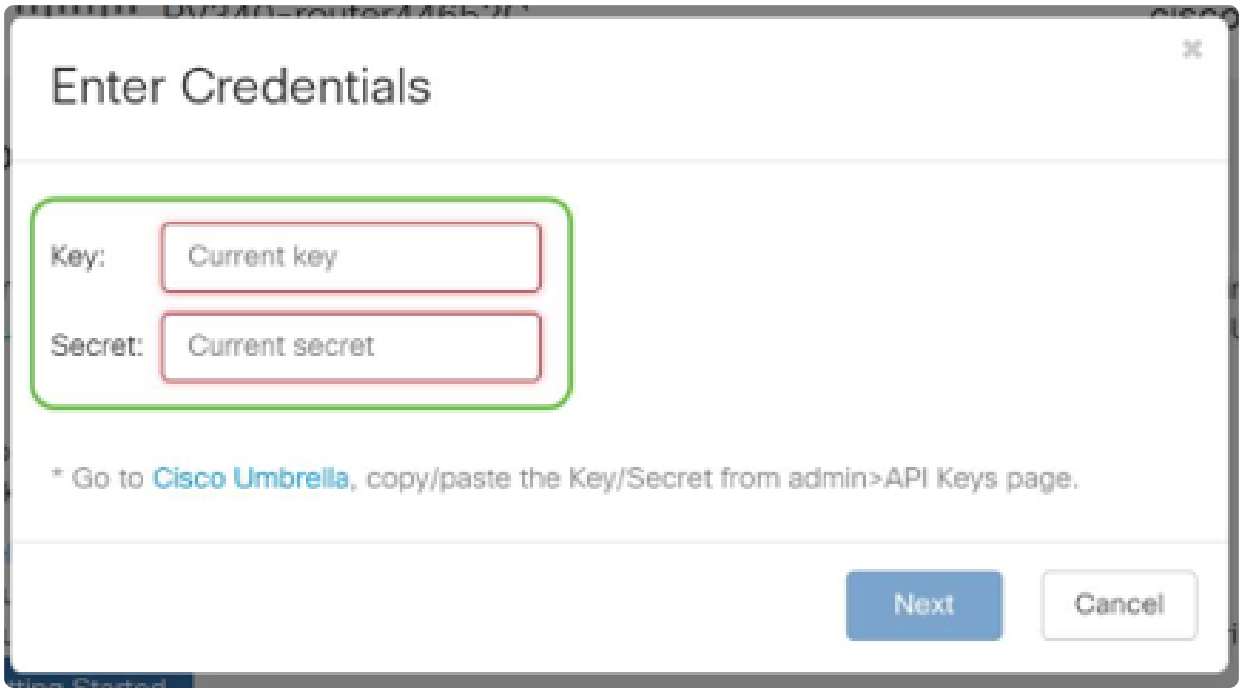
Fare clic su Guida introduttiva.



Passaggio 6

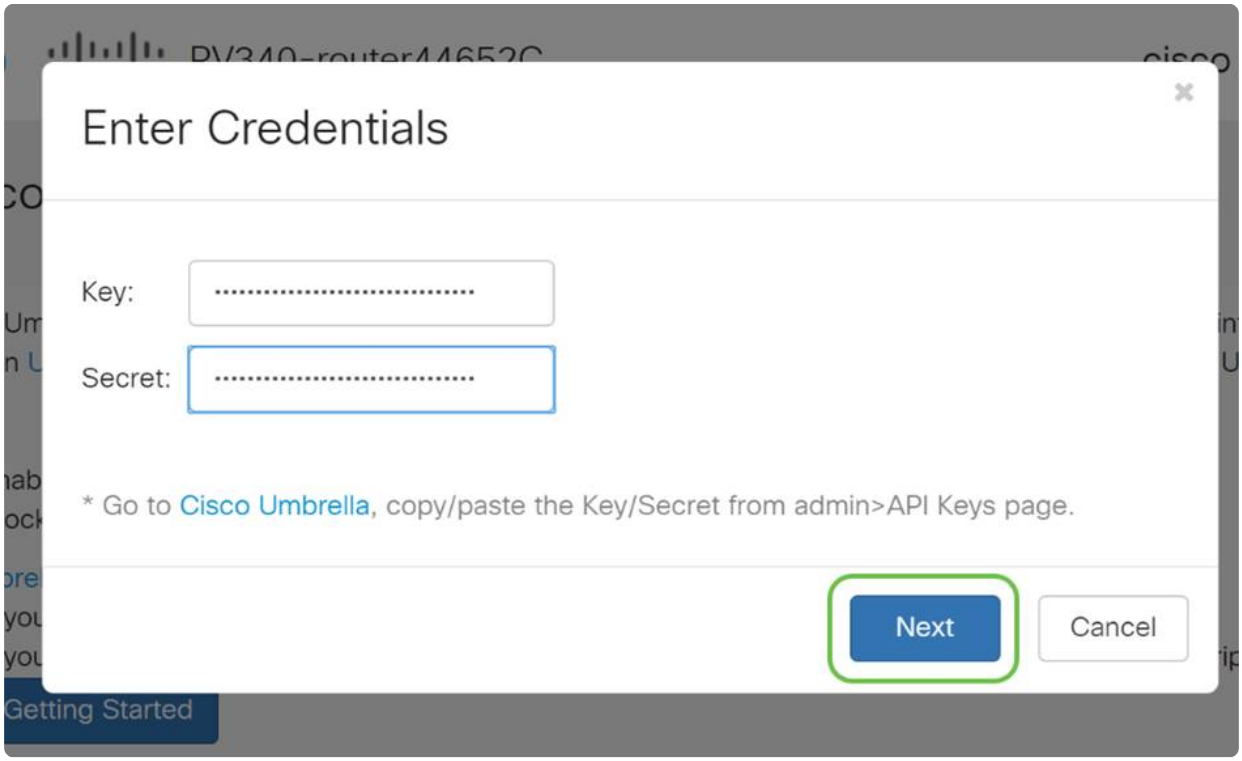
Immettere la Chiave API e la Chiave segreta nelle caselle di testo.

> ⓘ Note: Dillo due volte, cosi' sai che e' importante! Se si perde o si elimina accidentalmente la chiave segreta, non sarà disponibile alcuna funzione o numero di supporto da chiamare per recuperare la chiave. Mantenerla segreta e sicura. In caso di perdita, sarà necessario eliminare la chiave e autorizzare nuovamente la nuova chiave API con ciascun dispositivo che si desidera proteggere con Umbrella.



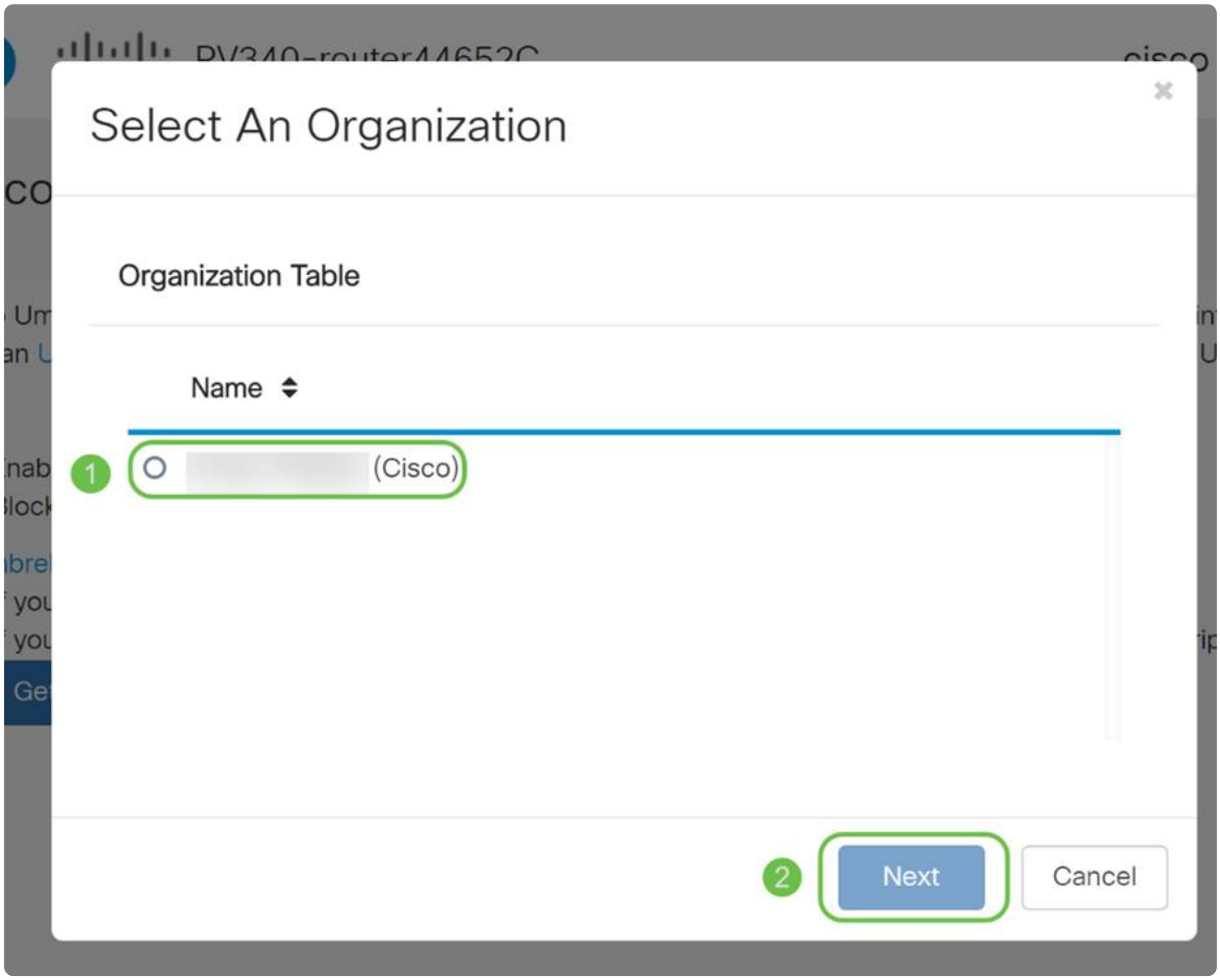
Passaggio 7

Dopo aver inserito l'API e la chiave privata, fare clic sul pulsante Next (Avanti).



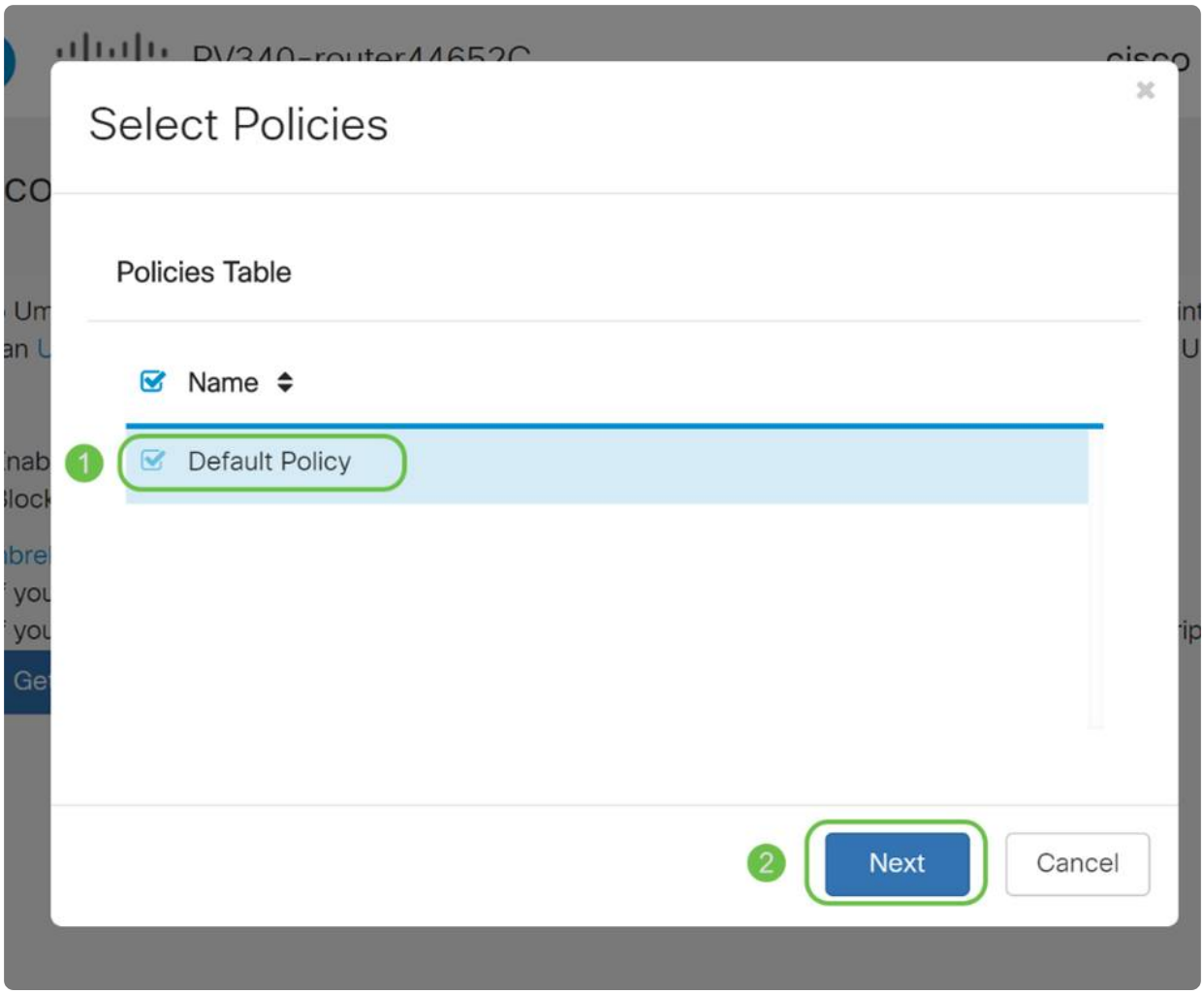
Passaggio 8

Nella schermata successiva, selezionare l'organizzazione che si desidera associare al router. Fare clic su Next (Avanti).



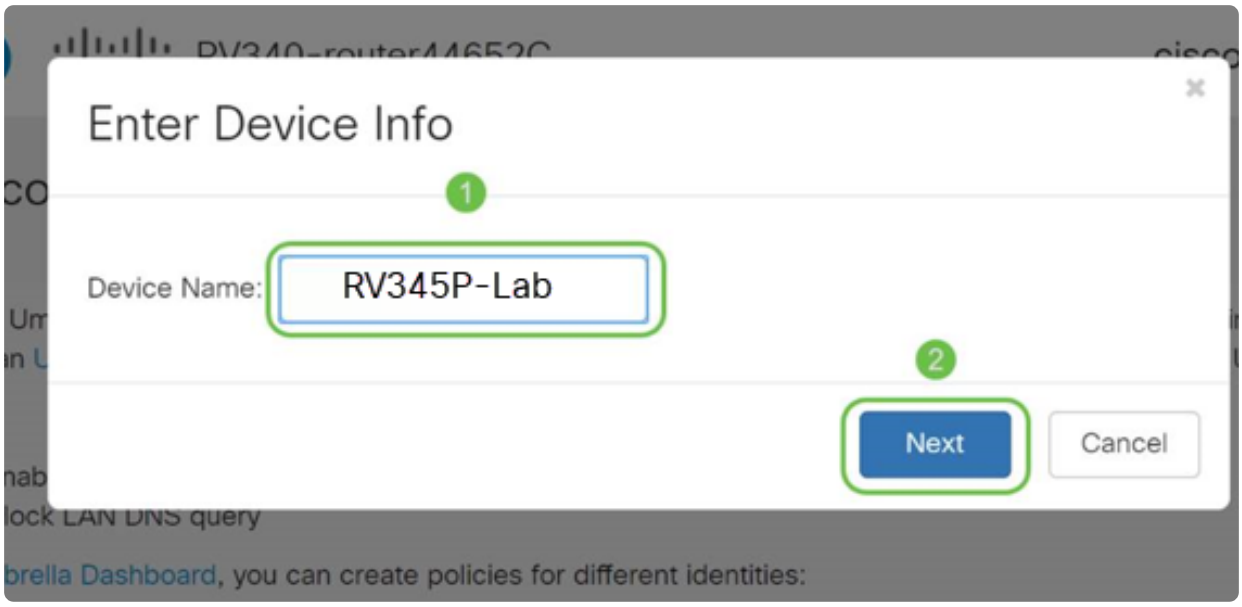
Passaggio 9

Selezionare la policy da applicare al traffico instradato dalla RV345P. Per la maggior parte degli utenti, il criterio predefinito fornisce una copertura sufficiente.



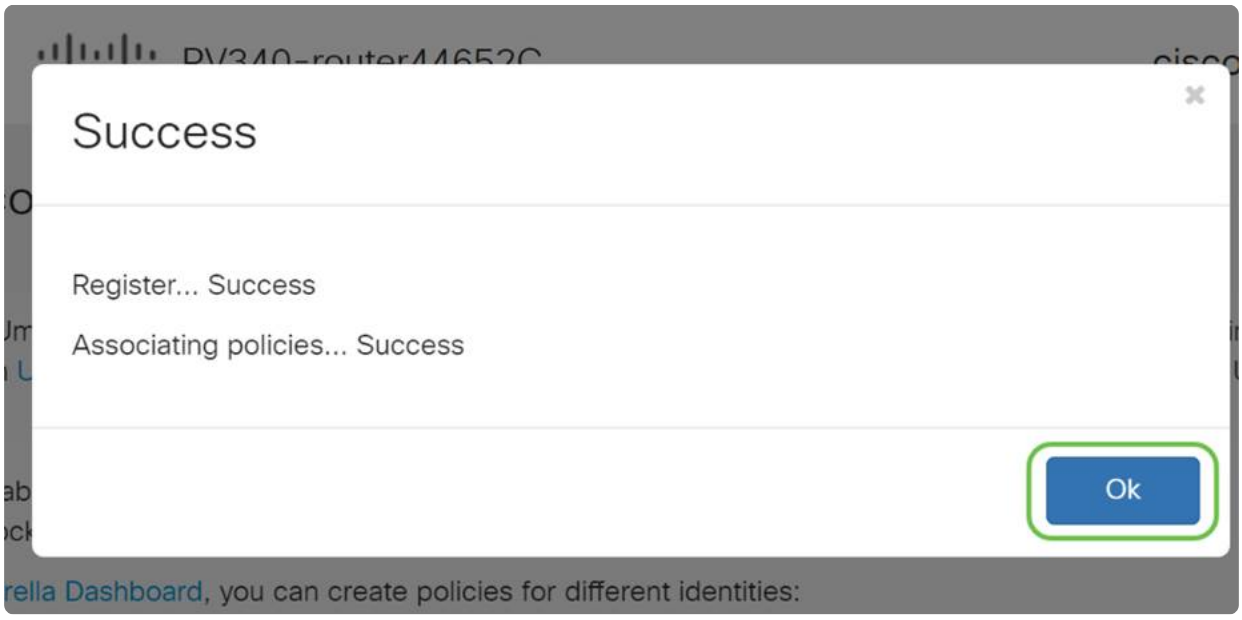
Passaggio 10

Assegnare un nome al dispositivo in modo che possa essere designato in Umbrella reporting. Nella configurazione, è stato denominato RV345P-Lab.



Passaggio 11

La schermata successiva convaliderà le impostazioni scelte e fornirà un aggiornamento quando l'associazione riesce. Fare clic su OK.

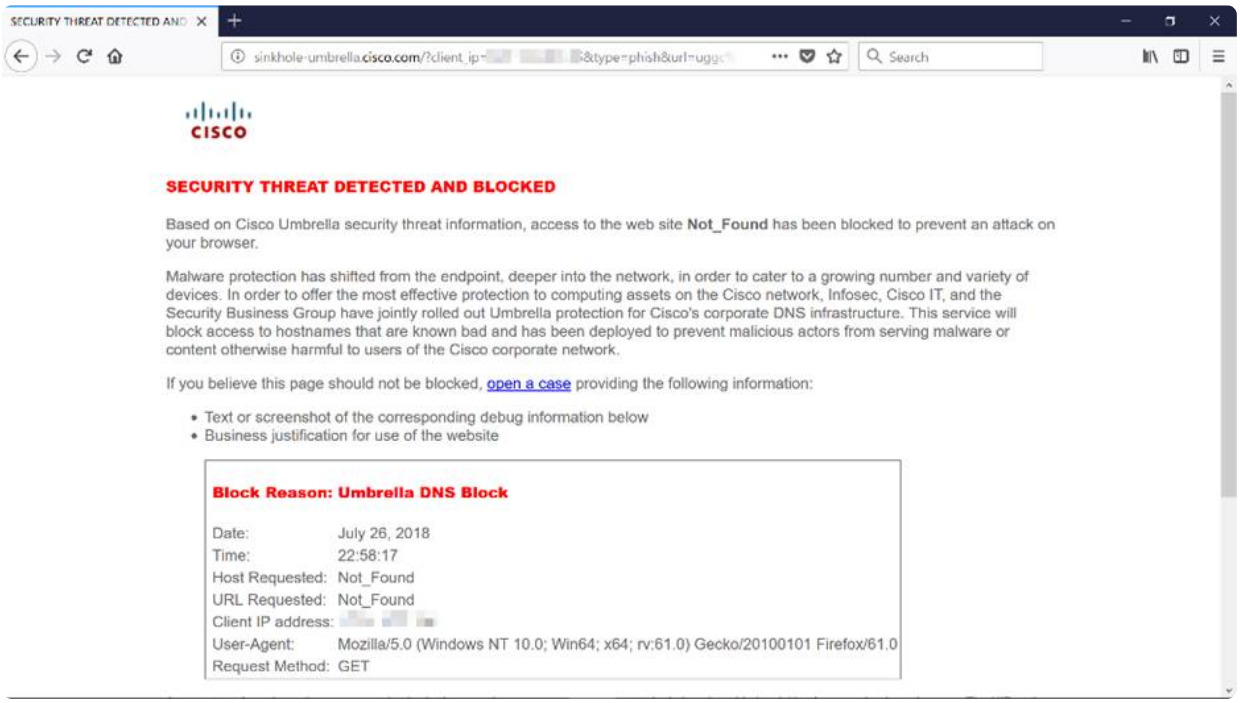


Conferma

Congratulazioni, ora sei protetto da Cisco Umbrella. O lo sei? Tramite un doppio controllo con un esempio dal vivo, Cisco ha creato un sito Web dedicato a determinare

la velocità di caricamento della pagina. Fare clic qui o digitare https://InternetBadGuys.com nella barra del browser.

Se Umbrella è configurato correttamente, verrà visualizzata una schermata simile a questa.



Altre opzioni di sicurezza

Si è preoccupati che qualcuno possa tentare di accedere alla rete senza autorizzazione scollegando un cavo Ethernet da un dispositivo di rete e collegandolo? In questo caso, è importante registrare un elenco di host autorizzati a connettersi direttamente al router con i rispettivi indirizzi IP e MAC. Per le istruzioni, consultare l'articolo Configure IP Source Guard sul router serie RV34x.

Opzioni VPN

Una connessione VPN (Virtual Private Network) consente agli utenti di accedere, inviare e ricevere dati da e verso una rete privata tramite una rete pubblica o condivisa, ad esempio Internet, ma garantisce comunque una connessione sicura a un'infrastruttura di rete sottostante per proteggere la rete privata e le relative risorse.

Un tunnel VPN stabilisce una rete privata in grado di inviare i dati in modo sicuro utilizzando la crittografia e l'autenticazione. Le filiali utilizzano per lo più connessioni VPN in quanto è utile e necessario consentire ai dipendenti di accedere alla rete privata anche quando si trovano fuori sede.

La VPN consente a un host remoto di agire come se si trovasse sulla stessa rete locale. Il router supporta fino a 50 tunnel. È possibile configurare una connessione VPN tra il router e un endpoint dopo che il router è stato configurato per la connessione Internet. Il client VPN dipende interamente dalle impostazioni del router VPN per poter stabilire una connessione.

Se non sei sicuro di quale VPN soddisfi al meglio le tue esigenze, consulta la panoramica e le best practice di Cisco Business VPN.

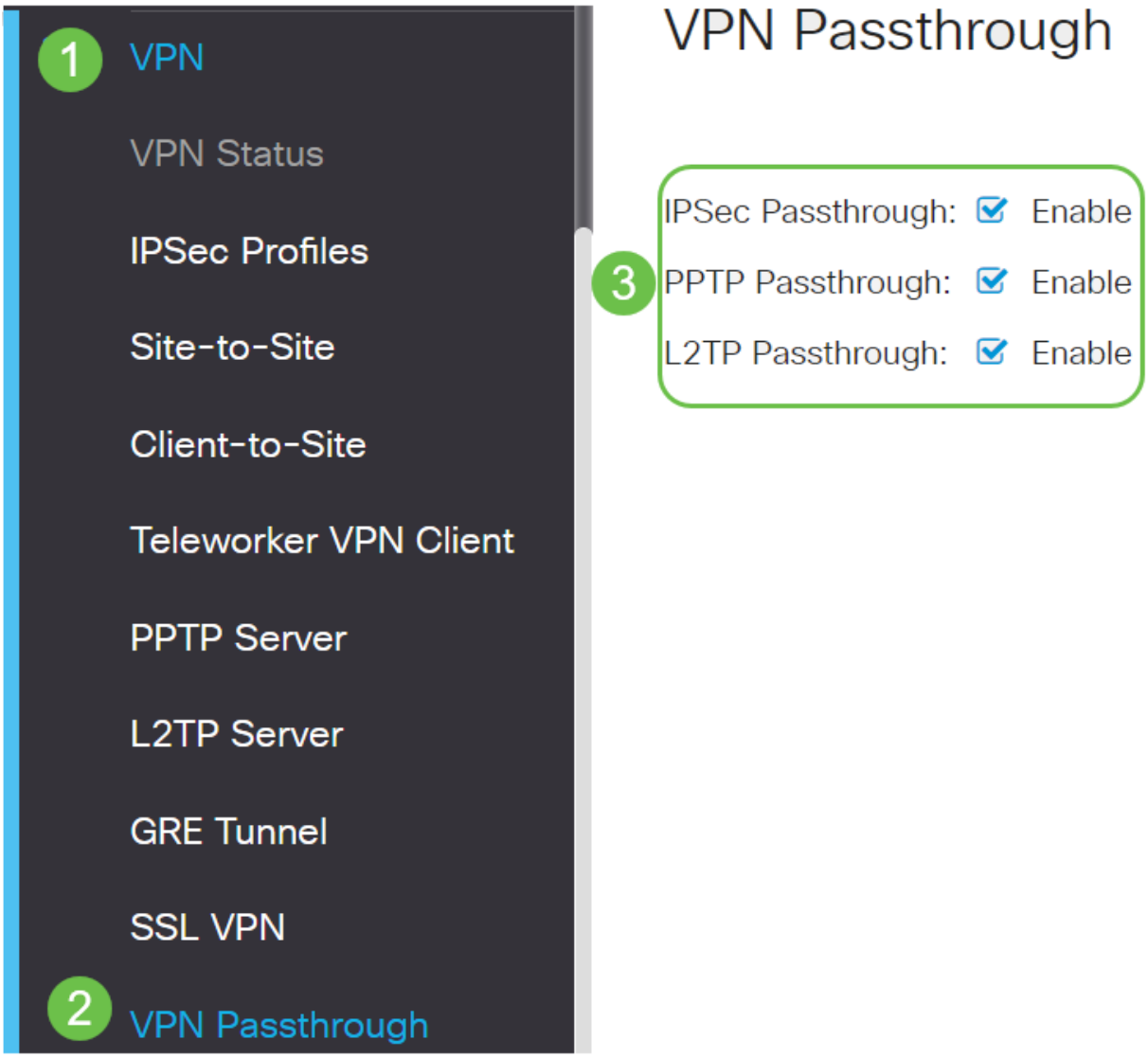
> ⓘ Note: AnyConnect VPN è l'unico prodotto Cisco VPN supportato elencato in questa guida alla configurazione. I prodotti di terze parti non Cisco, tra cui TheGreenBow e Shrew Soft, non sono supportati da Cisco. Sono inclusi esclusivamente a scopo orientativo. Se hai bisogno di supporto su questi oltre l'articolo, è necessario contattare quella terza parte per il supporto.

Se non hai intenzione di configurare una VPN, puoi fare clic per passare alla sezione successiva.

VPN PassThrough

In genere, ogni router supporta Network Address Translation (NAT) per conservare gli indirizzi IP quando si desidera supportare più client con la stessa connessione Internet. Tuttavia, il protocollo PPTP (Point-to-Point Tunneling Protocol) e la VPN IPsec (Internet Protocol Security) non supportano NAT. A questo punto entra in gioco la VPN PassThrough. Una VPN PassThrough è una funzionalità che consente al traffico VPN generato dai client VPN connessi a questo router di passare attraverso questo router e connettersi a un endpoint VPN. Il protocollo VPN PassThrough consente solo al protocollo PPTP e alla VPN IPsec di passare a Internet, che viene avviato da un client VPN, e quindi di raggiungere il gateway VPN remoto. Questa funzione si trova in genere sui router domestici che supportano NAT.

Per impostazione predefinita, IPsec, PPTP e L2TP Passthrough sono abilitati. Per visualizzare o modificare queste impostazioni, selezionare VPN > VPN PassThrough. Visualizzare o regolare in base alle esigenze.



AnyConnect VPN

L'uso di Cisco AnyConnect offre diversi vantaggi:

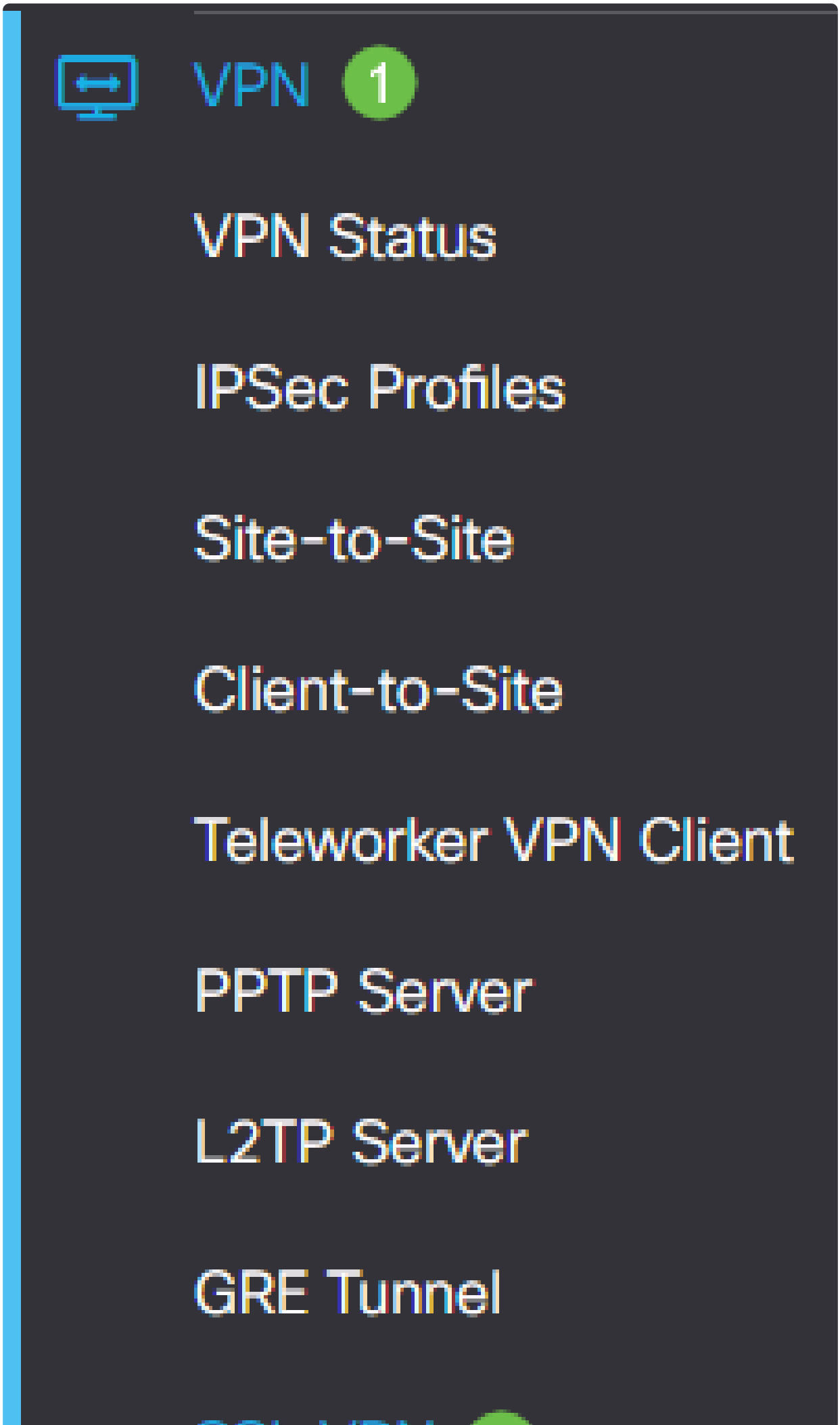
1. Connettività sicura e persistente
2. Sicurezza costante e applicazione delle policy
3. Installabile da Adaptive Security Appliance (ASA) o da sistemi di distribuzione software aziendali

4. Personalizzabile e traducibile
5. Facile configurazione
6. Supporta sia IPsec (Internet Protocol Security) che SSL (Secure Sockets Layer)
7. Supporto del protocollo Internet Key Exchange versione 2.0 (IKEv2.0)

Configurazione di AnyConnect SSL VPN su RV345P

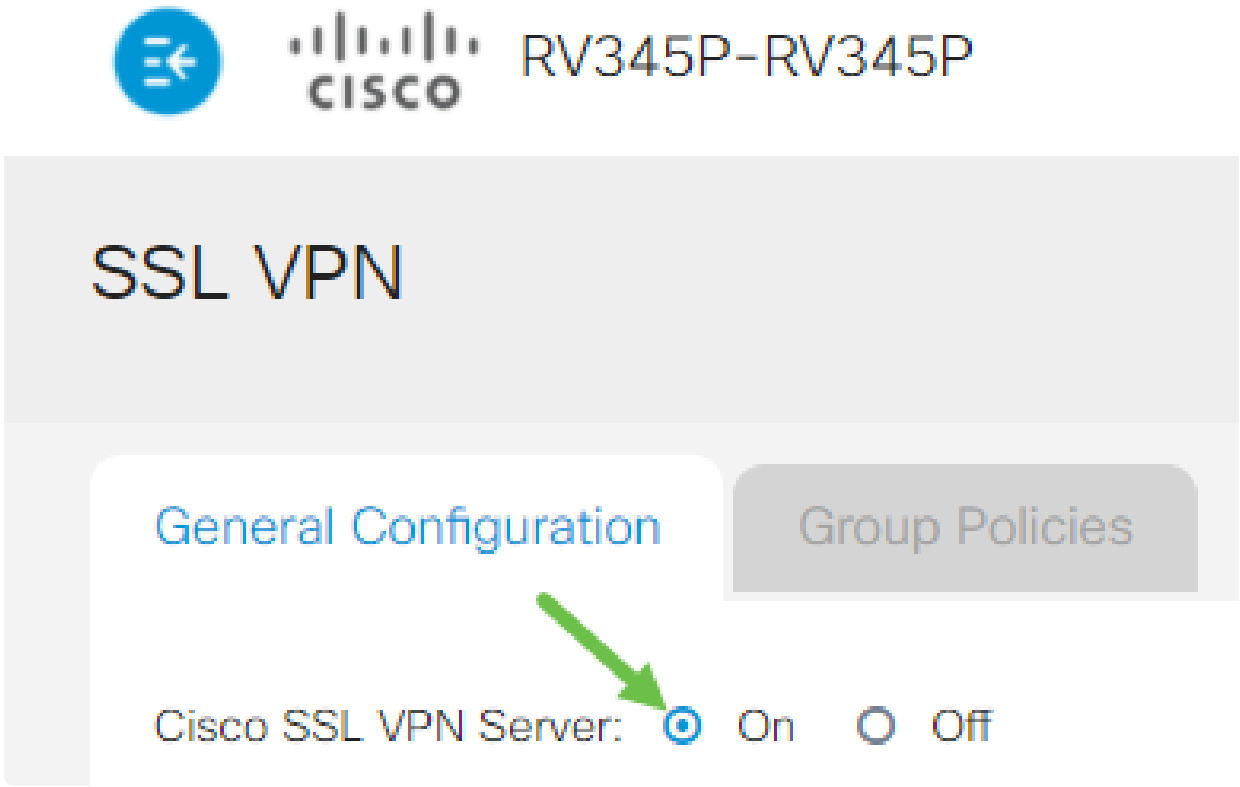
Passaggio 1

Accedere all'utility basata sul Web del router e scegliere VPN > SSL VPN.


VPN
1
VPN Status
IPSec Profiles
Site-to-Site
Client-to-Site
Teleworker VPN Client
PPTP Server
L2TP Server
GRE Tunnel

Passaggio 2

Fare clic sul pulsante di opzione On per abilitare Cisco SSL VPN Server.



Impostazioni gateway obbligatorie

Passaggio 1

Le seguenti impostazioni di configurazione sono obbligatorie:

1 Selezionare Interfaccia gateway dall'elenco a discesa. Questa sarà la porta che verrà utilizzata per passare il traffico attraverso i tunnel VPN SSL. Le opzioni includono: WAN1, WAN2, USB1, USB2

2 Immettere il numero di porta utilizzato per il gateway VPN SSL nel campo Porta gateway, compreso tra 1 e 65535.

3 Scegliere il file di certificato dall'elenco a discesa. Questo certificato autentica gli utenti che tentano di accedere alla risorsa di rete tramite i tunnel VPN SSL. L'elenco a discesa contiene un certificato predefinito e i certificati importati.

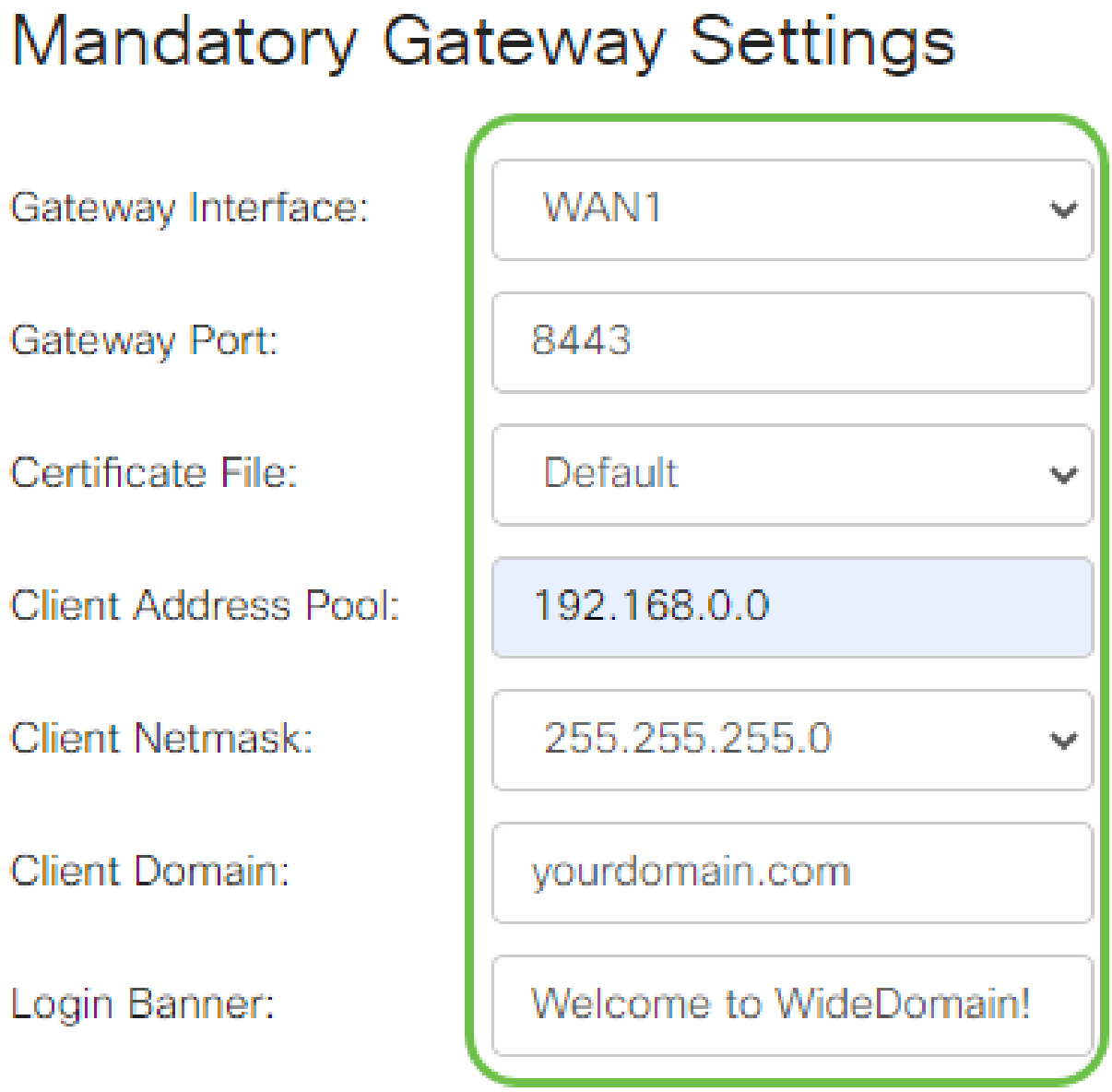
4 Immettere l'indirizzo IP del pool di indirizzi client nel campo Pool di indirizzi client. Questo pool sarà l'intervallo di indirizzi IP che verranno allocati ai client VPN remoti.

Verificare che l'intervallo di indirizzi IP non si sovrapponga ad alcun indirizzo IP della rete locale.

5 Selezionare la maschera di rete client dall'elenco a discesa.

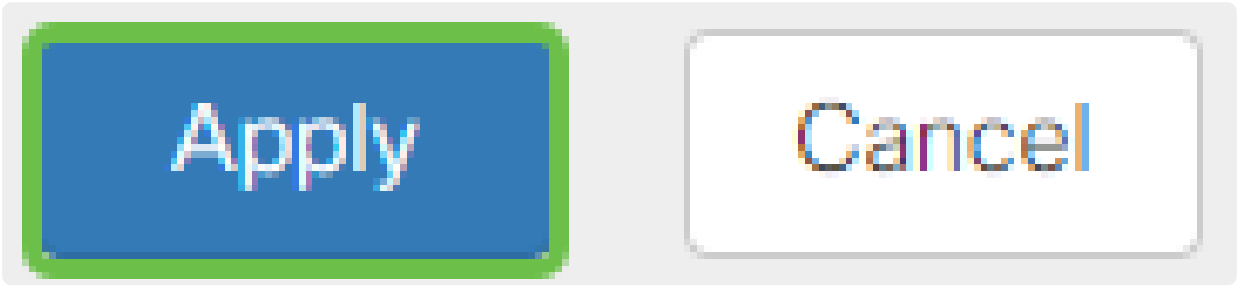
6 Immettere il nome del dominio del client nel campo Dominio client. Questo sarà il nome di dominio da inviare ai client VPN SSL.

7 Immettere il testo che verrà visualizzato come banner di accesso nel campo Banner di accesso. Questo sarà il banner che verrà visualizzato ogni volta che un client esegue l'accesso.



Passaggio 2

Fare clic su Apply (Applica).



Impostazioni gateway opzionali

Passaggio 1

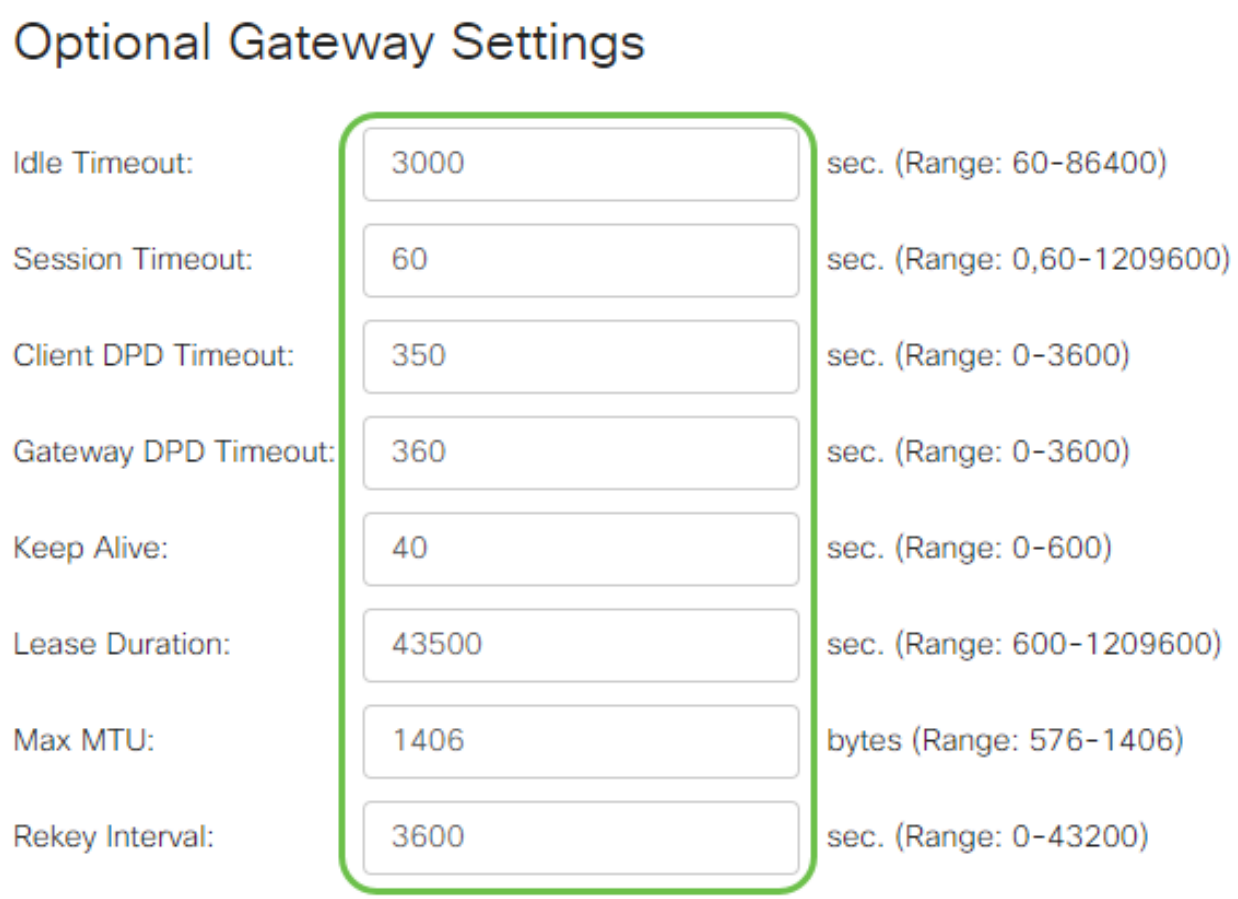
Le seguenti impostazioni di configurazione sono facoltative:

1. Immettere un valore in secondi per il timeout di inattività compreso tra 60 e 86400. Questo valore indica il periodo di tempo durante il quale la sessione VPN SSL può rimanere inattiva.
2. Immettere un valore in secondi nel campo Timeout sessione. Tempo necessario per il timeout della sessione TCP (Transmission Control Protocol) o UDP (User Datagram Protocol) dopo il tempo di inattività specificato. L'intervallo ammesso è compreso tra 60 e 1209600.
3. Immettere un valore compreso tra 0 e 3600 in secondi nel campo Timeout DPD client. Questo valore specifica l'invio periodico di messaggi HELLO/ACK per controllare lo stato del tunnel VPN. Questa funzionalità deve essere abilitata su entrambe le estremità del tunnel VPN.
4. Immettere un valore in secondi nel campo GatewayDPD Timeout (Timeout DPD) compreso tra 0 e 3600. Questo valore specifica l'invio periodico di messaggi HELLO/ACK per controllare lo stato del tunnel VPN. Questa funzionalità deve essere abilitata su entrambe le estremità del tunnel VPN.
5. Immettere un valore in secondi nel campo Keep Alive compreso tra 0 e 600. Questa funzione assicura che il router sia sempre connesso a Internet. Tenterà di ristabilire la connessione VPN se viene interrotta.
6. Immettere un valore in secondi per la durata del tunnel da connettere nel campo Durata

lease. L'intervallo ammesso è compreso tra 600 e 1209600.

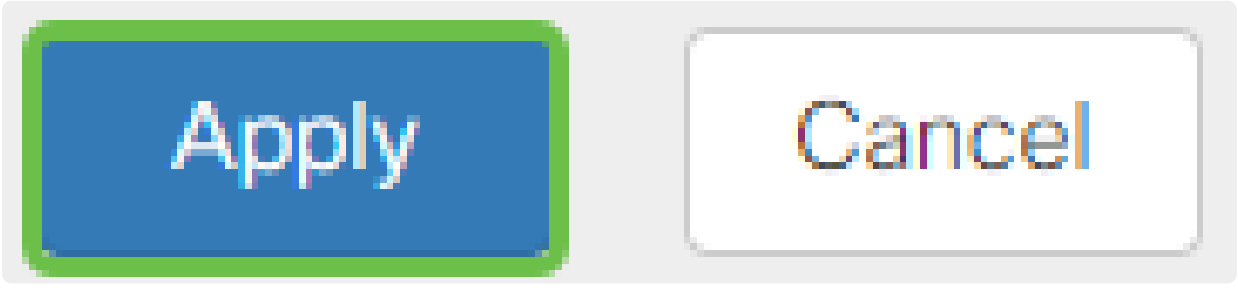
7 Immettere le dimensioni in byte del pacchetto che può essere inviato sulla rete. L'intervallo ammesso è compreso tra 576 e 1406.

8 Immettere il tempo dell'intervallo di inoltro nel campo Intervallo di reimpostazione chiavi. La funzione Rekey consente alle chiavi SSL di rinegoziare dopo la creazione della sessione. L'intervallo ammesso è compreso tra 0 e 43200.



Passaggio 2

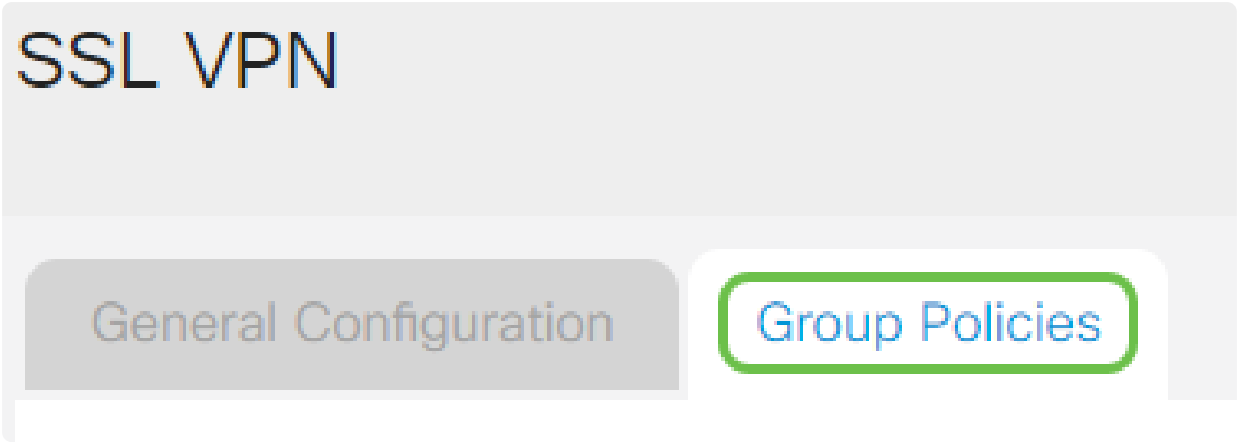
Fare clic su Apply (Applica).



Configura Criteri di gruppo

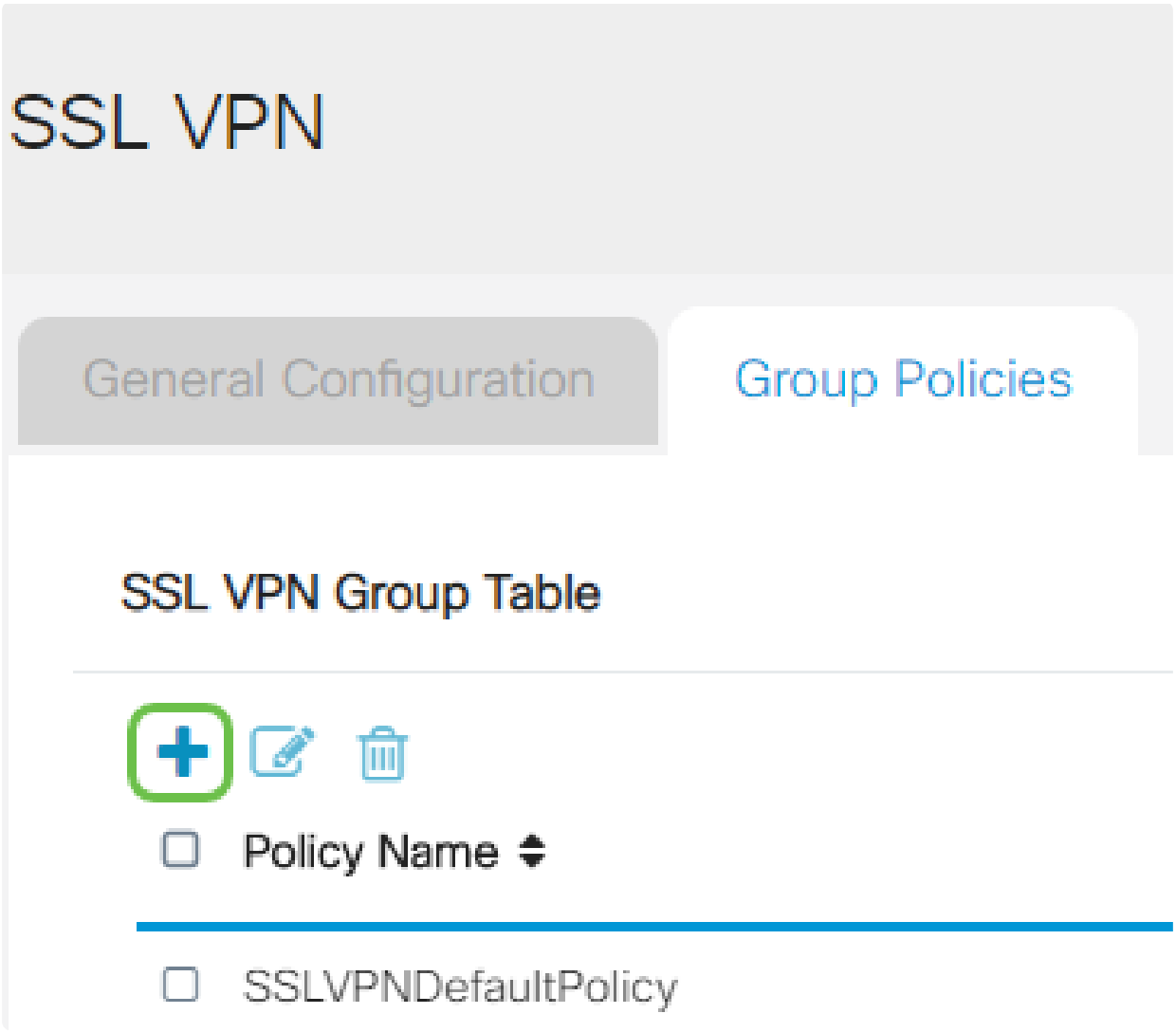
Passaggio 1

Fare clic sulla scheda Criteri di gruppo.



Passaggio 2

Per aggiungere un criterio di gruppo, fare clic sull'icona Aggiungi nella tabella Gruppo VPN SSL.

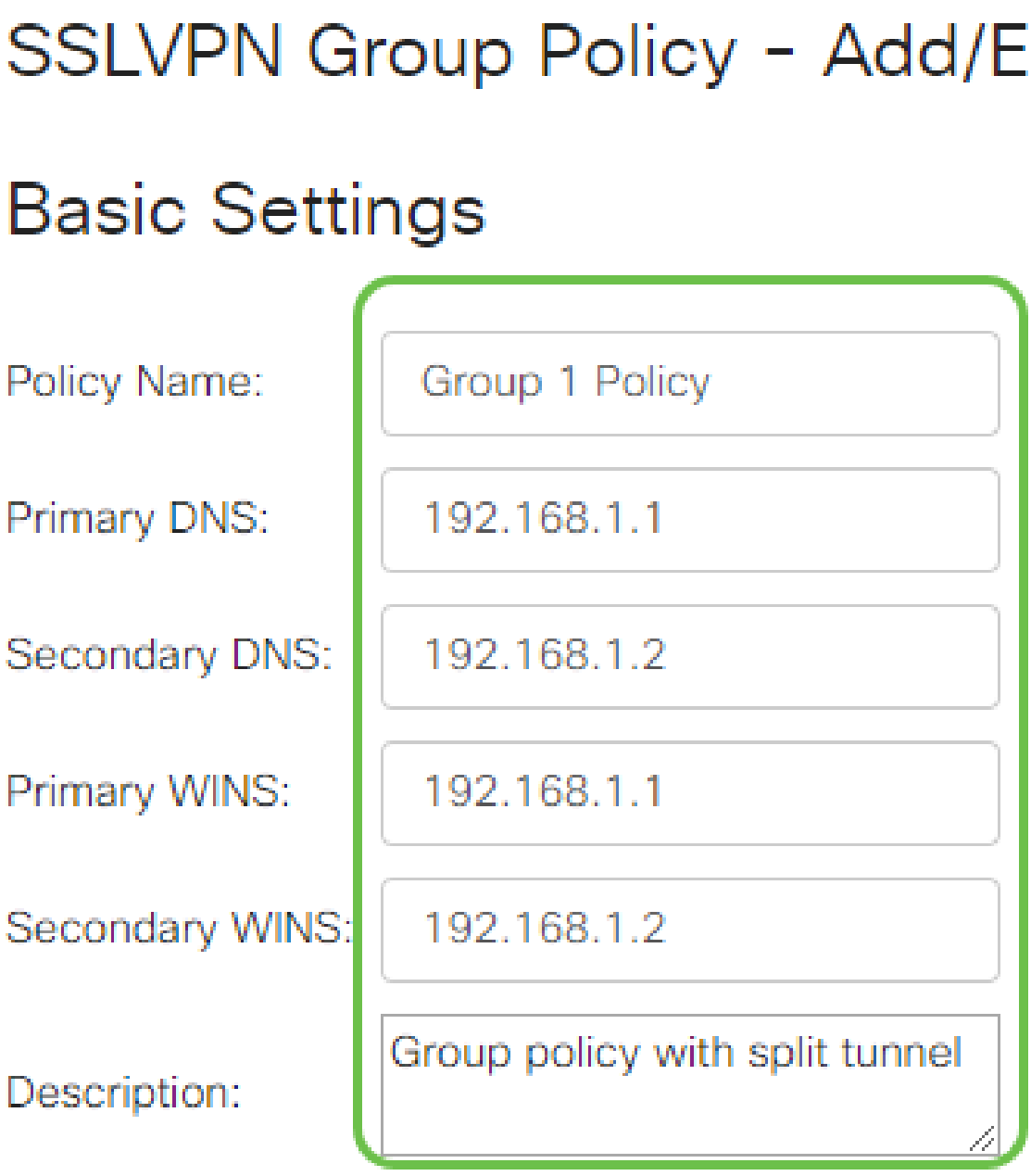


ⓘ Note: Nella tabella Gruppo VPN SSL verrà visualizzato l'elenco dei criteri di gruppo nel dispositivo. È inoltre possibile modificare il primo criterio di gruppo dell'elenco, denominato SSLVPNDefaultPolicy. Si tratta del criterio predefinito fornito dal dispositivo.

Passaggio 3

1. Immettere il nome del criterio desiderato nel campo Nome criterio.
2. Immettere l'indirizzo IP del DNS primario nel campo fornito. Per impostazione predefinita, questo indirizzo IP è già specificato.
3. (Facoltativo) Immettere l'indirizzo IP del DNS secondario nell'apposito campo. Questo fungerà da backup in caso di errore del DNS primario.

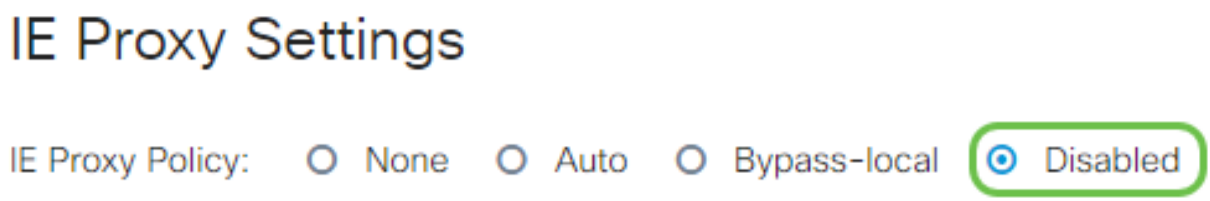
4. (Facoltativo) Immettere l'indirizzo IP del server WINS primario nell'apposito campo.
5. (Facoltativo) Immettere l'indirizzo IP del server WINS secondario nell'apposito campo.
6. (Facoltativo) Immettere una descrizione del criterio nel campo Descrizione.



Passaggio 4 (facoltativo)

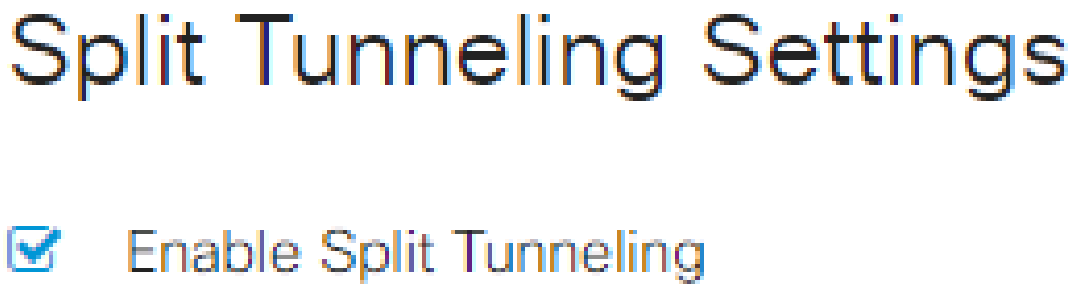
Fare clic su un pulsante di opzione per scegliere i criteri proxy di Internet Explorer per abilitare le impostazioni proxy di Microsoft Internet Explorer (MSIE) per stabilire il tunnel VPN. Le opzioni sono:

- None - Consente al browser di non utilizzare le impostazioni proxy.
- Auto - Consente al browser di rilevare automaticamente le impostazioni del proxy.
- Bypass-local: consente al browser di ignorare le impostazioni proxy configurate sull'utente remoto.
- Disabled - Disattiva le impostazioni del proxy MSIE.



Passaggio 5 (facoltativo)

Nell'area Impostazioni tunneling ripartito, selezionare la casella di controllo Abilita tunneling ripartito per consentire l'invio del traffico Internet non crittografato direttamente a Internet. Il tunneling completo invia tutto il traffico al dispositivo terminale, dove viene instradato alle risorse di destinazione, eliminando la rete aziendale dal percorso per l'accesso al Web.



Passaggio 6 (facoltativo)

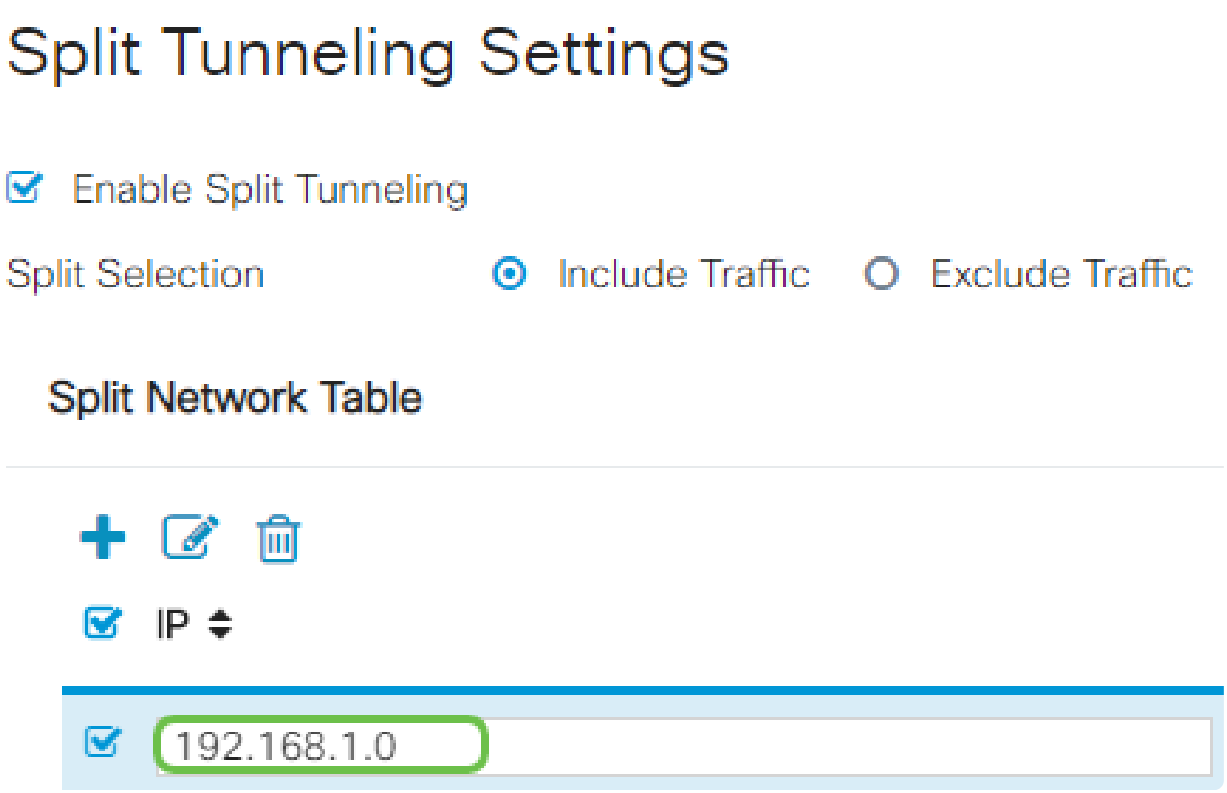
Fare clic su un pulsante di opzione per scegliere se includere o escludere il traffico quando si applica il tunneling suddiviso.

Passaggio 7

Nella tabella Dividi rete fare clic sull'icona Aggiungi per aggiungere un'eccezione Dividi rete.

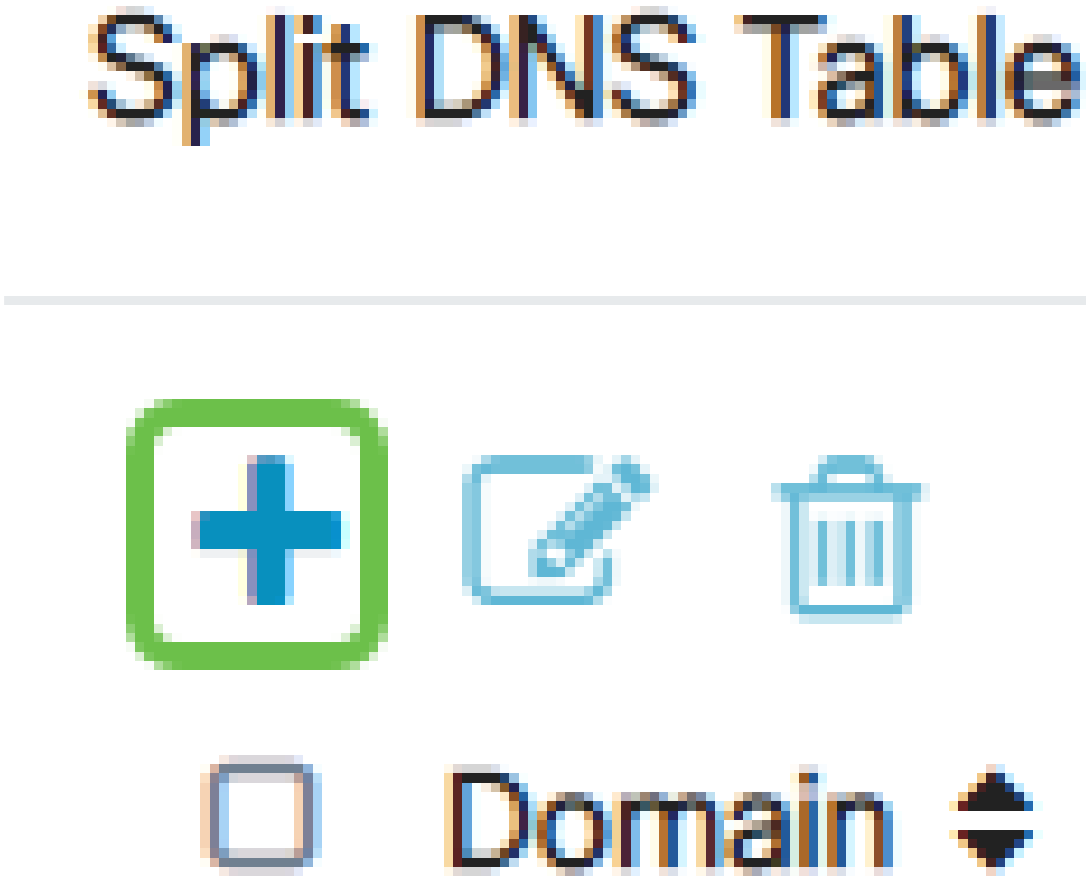
Passaggio 8

Immettere l'indirizzo IP della rete nell'apposito campo.



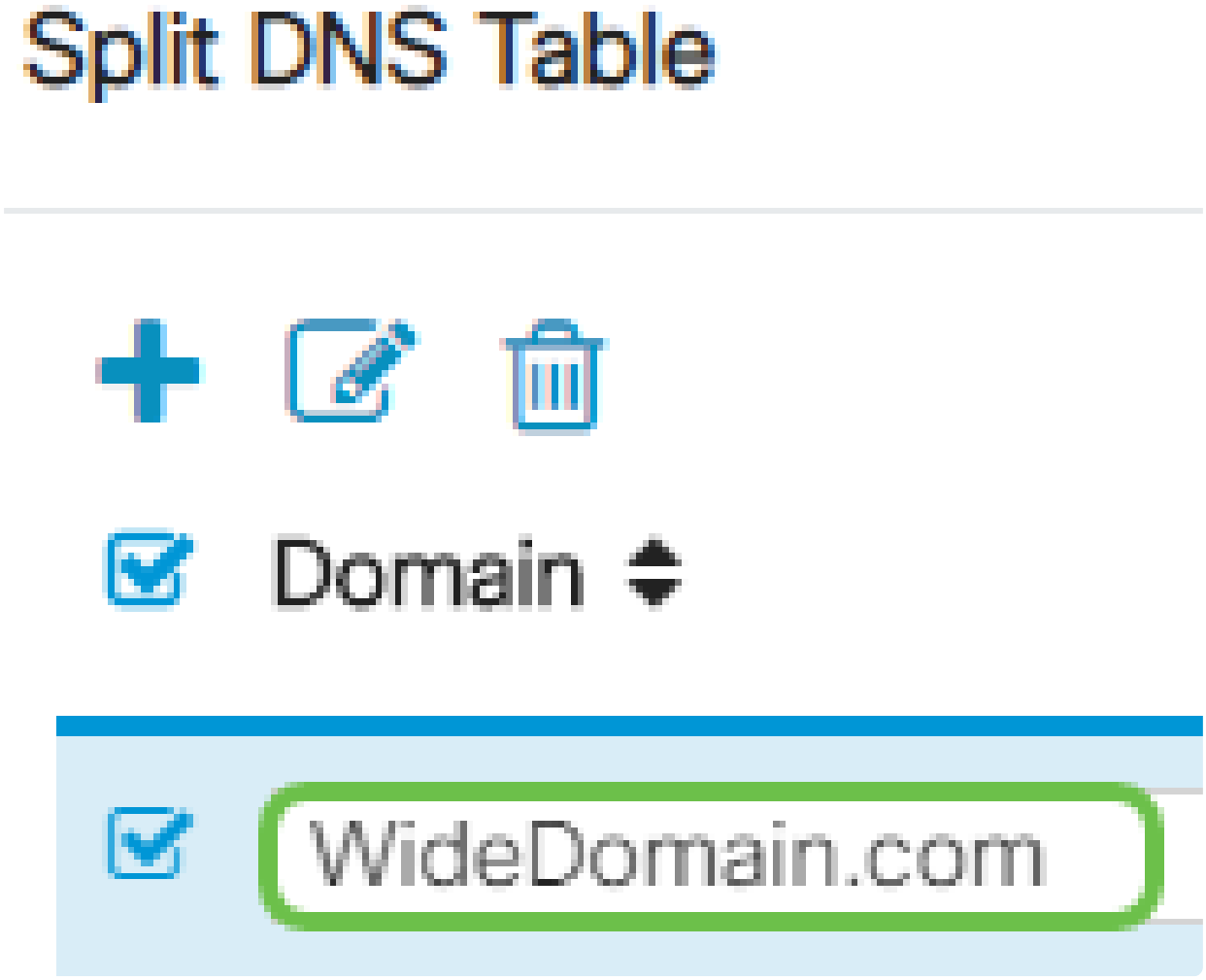
Passaggio 9

Nella tabella DNS divisa fare clic sull'icona di aggiunta per aggiungere un'eccezione DNS divisa.



Passaggio 10

Immettere il nome del dominio nell'apposito campo e fare clic su Applica.



Per impostazione predefinita, il router è provvisto di 2 licenze AnyConnect per server. Ciò significa che, una volta ottenute le licenze per i client AnyConnect, è possibile stabilire 2 tunnel VPN contemporaneamente a qualsiasi altro router serie RV340.

In breve, il router RV345P non ha bisogno di una licenza, ma tutti i client ne avranno bisogno. Le licenze client AnyConnect consentono ai client desktop e mobili di accedere alla rete VPN in remoto.

In questa sezione viene descritto come ottenere le licenze per i client.

AnyConnect Mobility Client

Un client VPN è un software installato ed eseguito su un computer che desidera

connettersi alla rete remota. Questo software client deve essere configurato con la stessa configurazione del server VPN, ad esempio l'indirizzo IP e le informazioni di autenticazione. Queste informazioni di autenticazione includono il nome utente e la chiave già condivisa che verrà utilizzata per crittografare i dati. A seconda della posizione fisica delle reti da connettere, un client VPN può anche essere un dispositivo hardware. Ciò si verifica in genere se la connessione VPN viene utilizzata per connettere due reti che si trovano in percorsi diversi.

Cisco AnyConnect Secure Mobility Client è un'applicazione software per la connessione a una VPN che funziona su diversi sistemi operativi e configurazioni hardware. Questa applicazione software consente di rendere accessibili le risorse remote di un'altra rete come se l'utente fosse connesso direttamente alla rete, ma in modo sicuro.

Dopo aver registrato e configurato il router con AnyConnect, il client può installare le licenze sul router dal pool di licenze disponibili che è stato acquistato, descritto nella sezione successiva.

Acquista licenza

È necessario acquistare una licenza dal distributore Cisco o dal partner Cisco. Quando si ordina una licenza, è necessario fornire l'ID dello Smart Account o del dominio Cisco nel formato name@domain.com.

Se non disponi di un distributore o di un partner Cisco, puoi trovarne uno qui.

Al momento della stesura del presente documento, le seguenti SKU possono essere usate per acquistare altre licenze in pacchetti da 25. Tenere presente che sono disponibili altre opzioni per le licenze dei client AnyConnect, come descritto nella Guida agli ordini di Cisco AnyConnect. Tuttavia, l'ID prodotto elencato costituisce il requisito minimo per la piena funzionalità.

Lo SKU delle licenze AnyConnect per i client, elencato per primo, fornisce le licenze per un periodo di 1 anno e richiede l'acquisto di almeno 25 licenze. Sono inoltre disponibili altre SKU di prodotti applicabili ai router della serie RV340 con diversi livelli di abbonamento, come indicato di seguito:

- LS-AC-PLS-1Y-S1 — licenza client Cisco AnyConnect Plus per 1 anno

- LS-AC-PLS-3Y-S1 — Licenza client Cisco AnyConnect Plus di 3 anni
- LS-AC-PLS-5Y-S1: licenza client Cisco AnyConnect Plus per 5 anni
- LS-AC-PLS-P-25-S — Confezione da 25 licenze Cisco AnyConnect Plus per client perpetui
- LS-AC-PLS-P-50-S: pacchetto da 50 licenze Cisco AnyConnect Plus per client perpetui

Informazioni sul client

Quando il client configura uno dei seguenti collegamenti, è necessario inviarli:

- Windows: AnyConnect su un computer Windows
- Mac: installa AnyConnect su Mac.
- Desktop Ubuntu: Installazione e uso di AnyConnect su Ubuntu Desktop
- In caso di problemi, è possibile consultare il documento sulla raccolta di informazioni per la risoluzione dei problemi di base sugli errori del client Cisco AnyConnect Secure Mobility.

Verifica della connettività VPN di AnyConnect

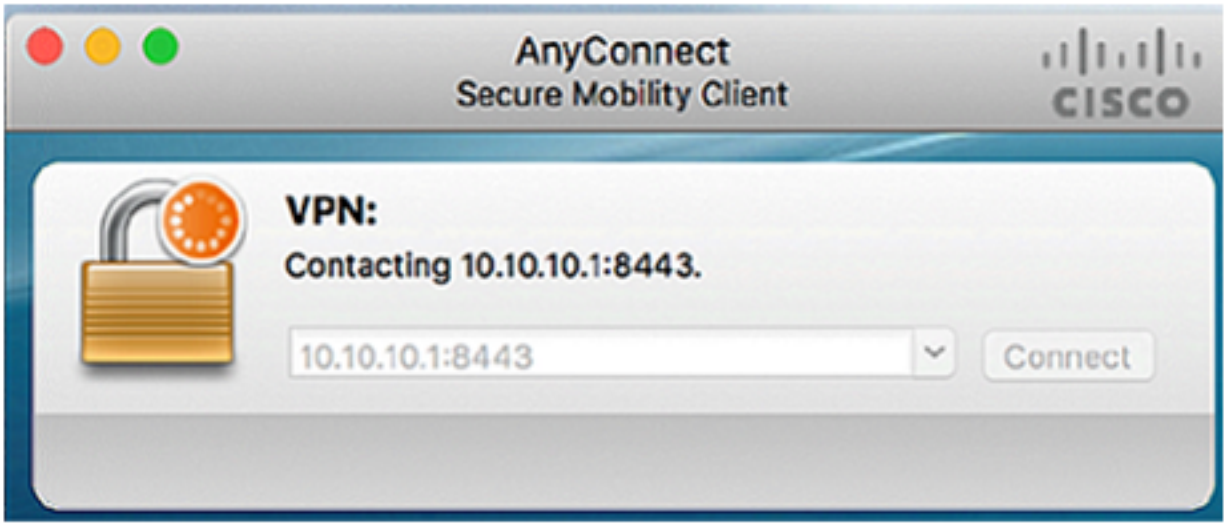
Passaggio 1

Fare clic sull'icona AnyConnect Secure Mobility Client.

Passaggio 2

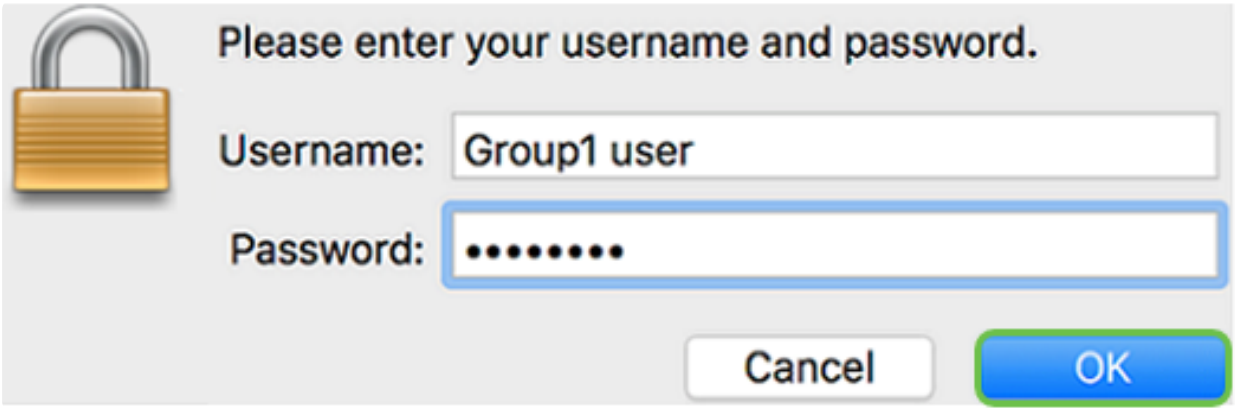
Nella finestra AnyConnect Secure Mobility Client, immettere l'indirizzo IP del gateway e il numero di porta del gateway separati da due punti (:), quindi fare clic su Connect.

Il software mostrerà ora che sta contattando la rete remota.



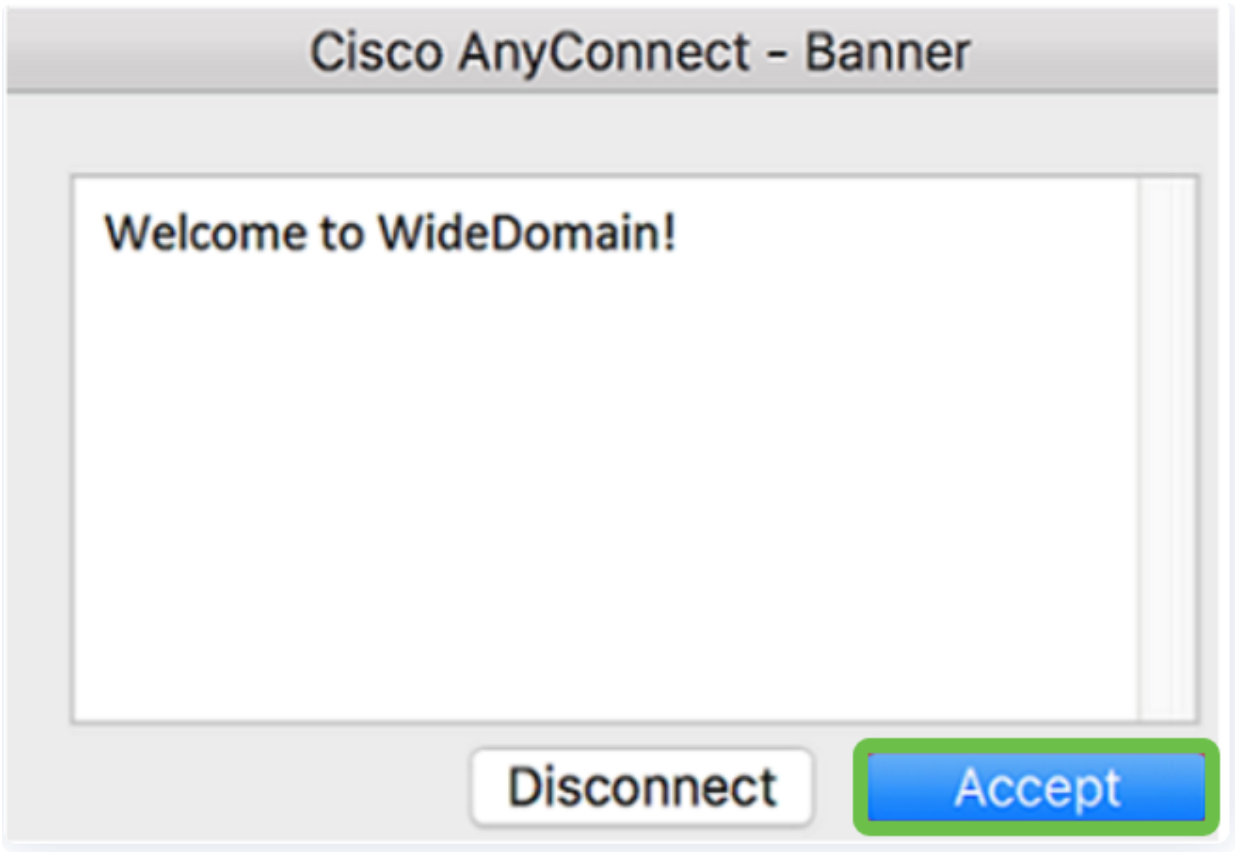
Passaggio 3

Immettere il nome utente e la password del server nei campi corrispondenti e quindi fare clic su OK.

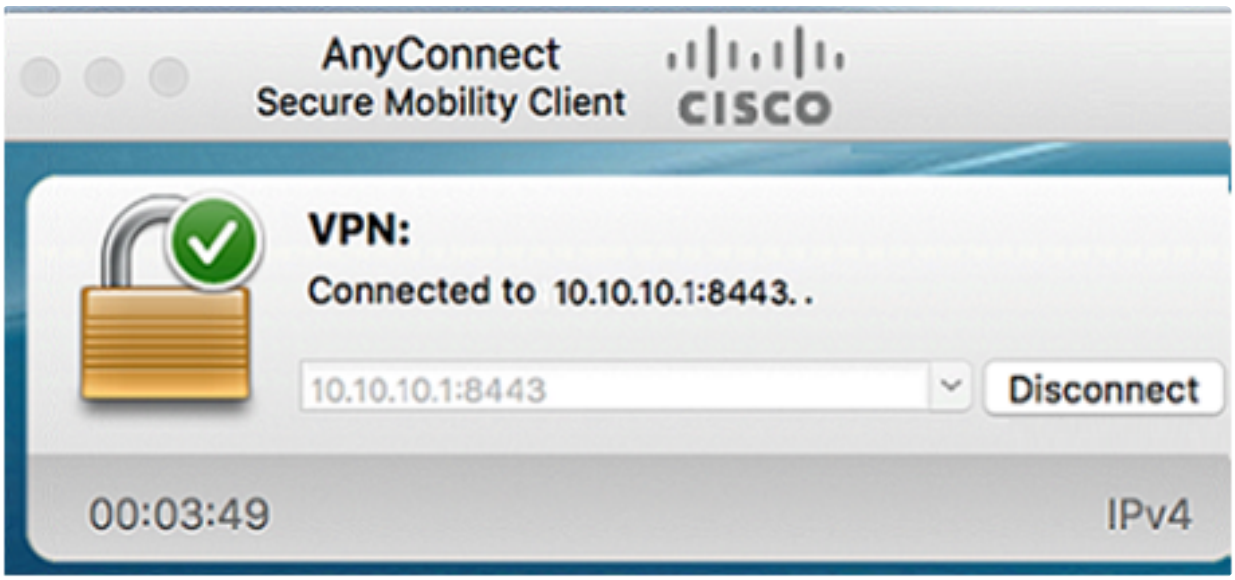


Passaggio 4

Non appena la connessione è stabilita, il banner di accesso viene visualizzato. Fare clic su Accetta.



A questo punto, la finestra AnyConnect dovrebbe indicare la connessione VPN alla rete riuscita.



Se al momento si usa AnyConnect VPN, è possibile ignorare le altre opzioni VPN e passare alla sezione successiva.

Mostra VPN soft

Una VPN IPsec consente di ottenere risorse remote in modo sicuro stabilendo un tunnel crittografato su Internet. I router della serie RV34X funzionano come server VPN IPsec e supportano il client Show Soft VPN. In questa sezione viene illustrato come configurare il router e il soft client Shrew per proteggere una connessione a una VPN.

> ⓘ Note: Cisco non supporta Shrew Soft. Questo esempio viene fornito solo a scopo dimostrativo. In caso di problemi con Shrew Soft, contattateli per assistenza.

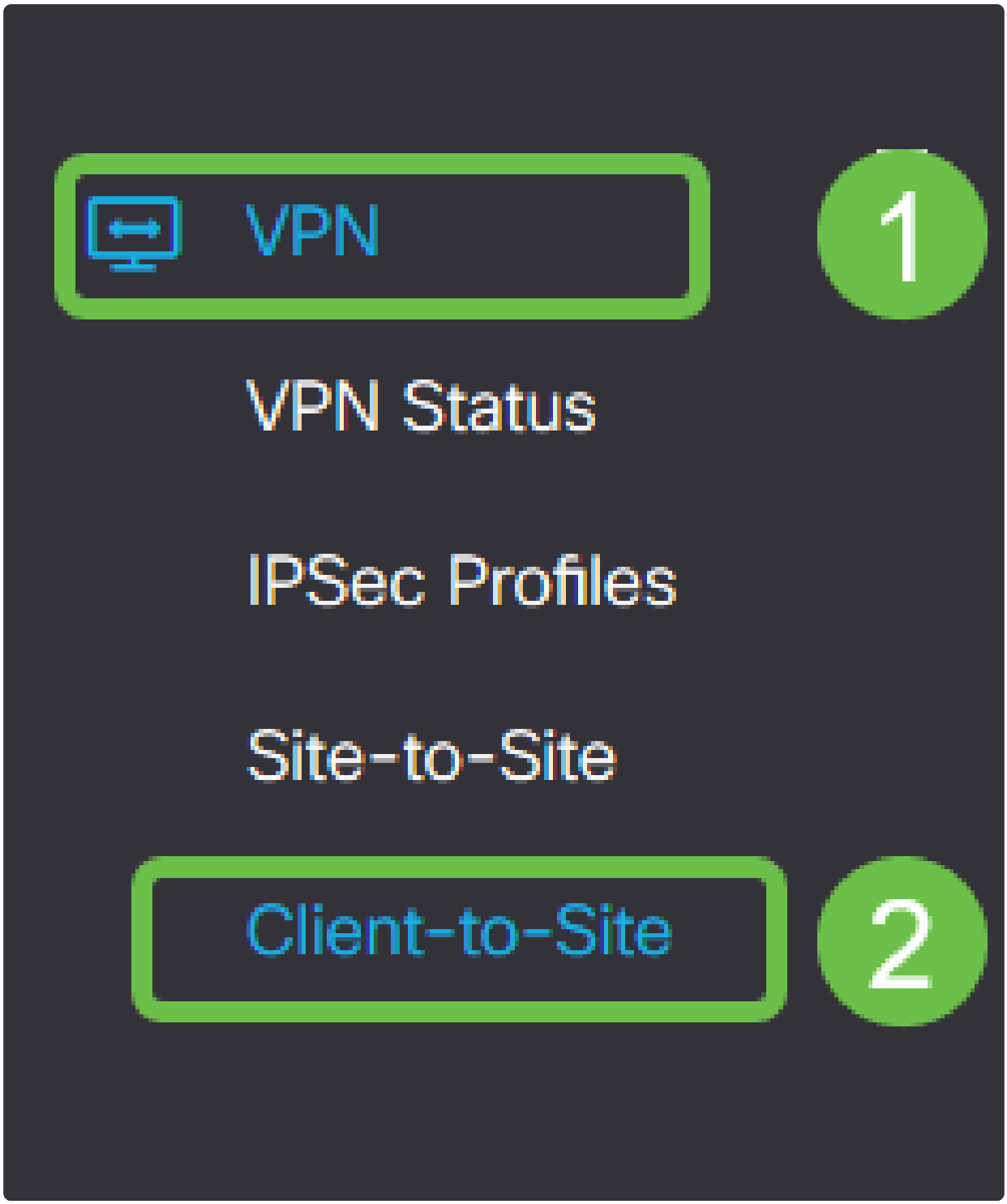
È possibile scaricare la versione più recente del software client Shrew Soft VPN qui: https://www.shrew.net/download/vpn

Configurazione di Shrew Soft sui router serie RV345P

Inizieremo configurando la VPN da client a sito sull'RV345P.

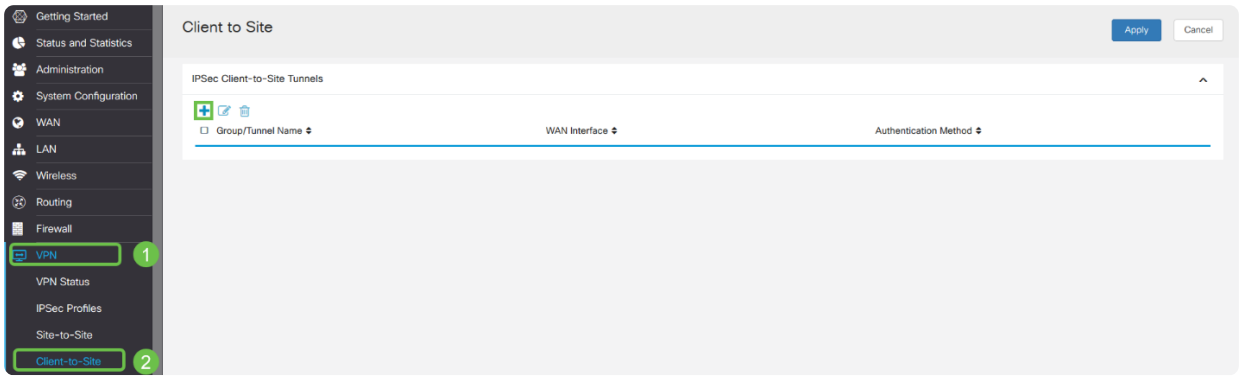
Passaggio 1

Selezionare VPN > Da client a sito.



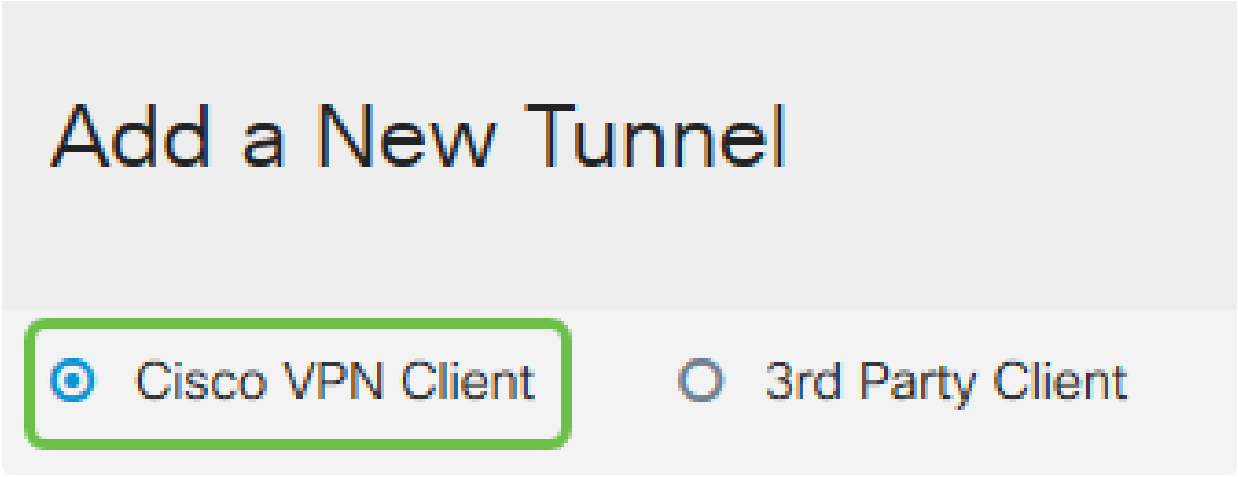
Passaggio 2

Aggiungere un profilo VPN da client a sito.



Passaggio 3

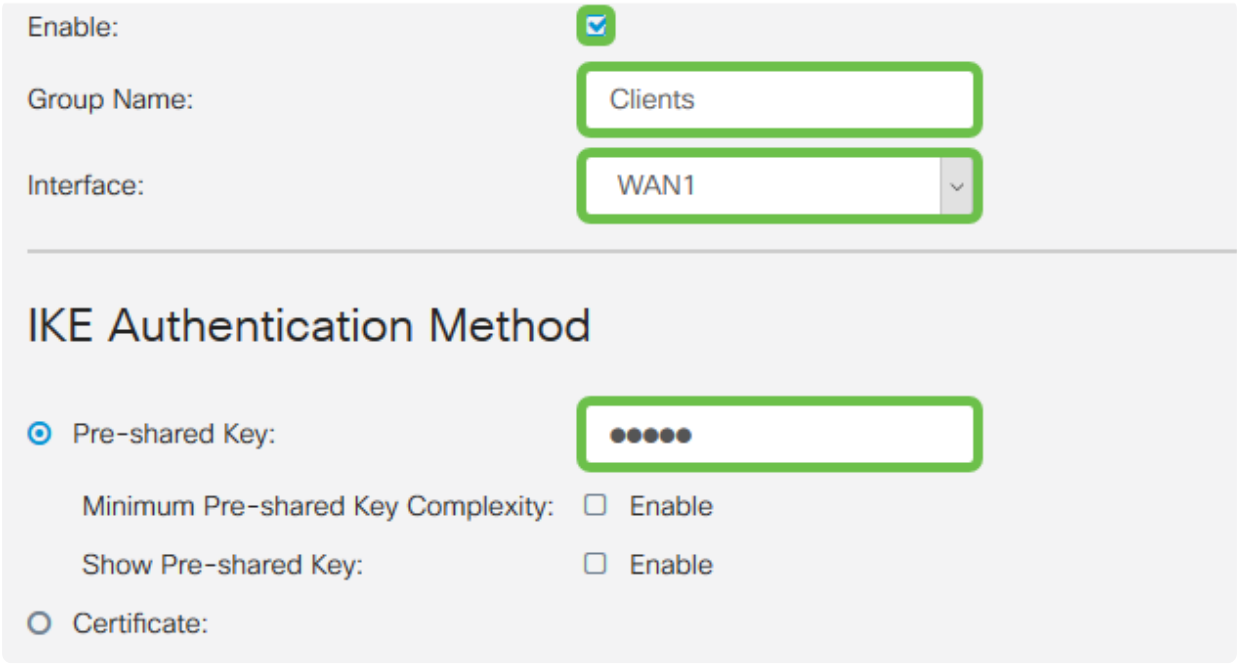
Selezionare l'opzione Cisco VPN Client.



Passaggio 4

Selezionare la casella Enable (Abilita) per rendere attivo il profilo client VPN. Inoltre, configureremo il Nome gruppo, selezioneremo l'interfaccia WAN e immetteremo una Chiave già condivisa.

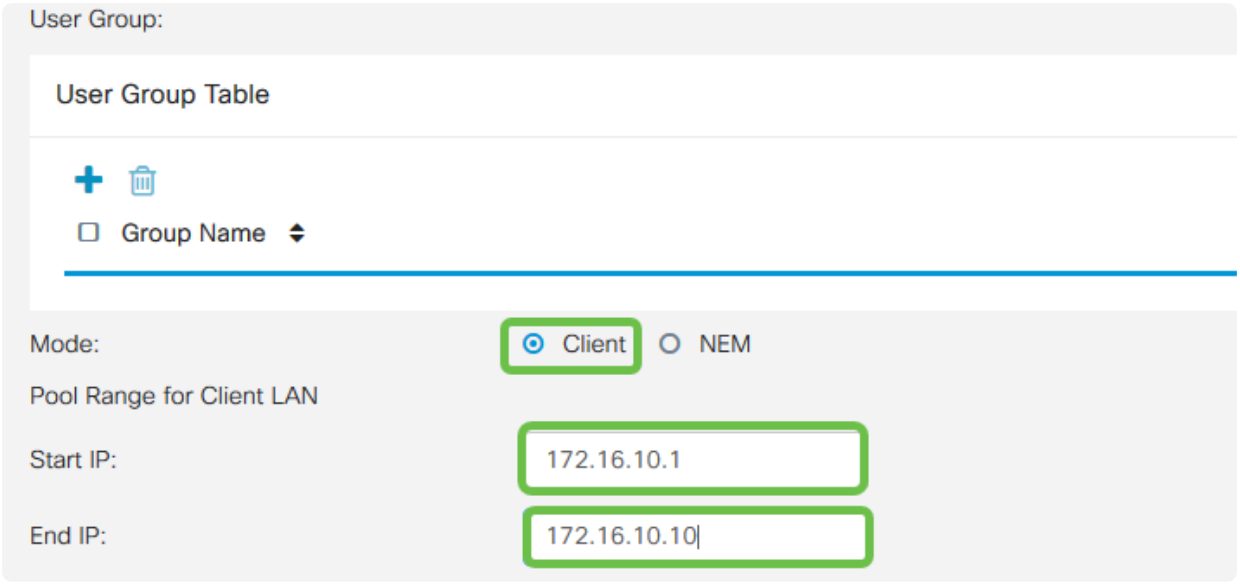
ⓘ Note: Prendere nota del nome del gruppo e della chiave già condivisa poiché verranno utilizzati in seguito durante la configurazione del client.



Passaggio 5

Per il momento, lasciare vuota la tabella Gruppo utenti. Questa operazione è relativa al gruppo di utenti sul router, ma non è ancora stata configurata. Verificare che la modalità sia impostata su Client. Immettere l'intervallo del pool per la LAN client. Utilizzeremo da 172.16.10.1 a 172.16.10.10.

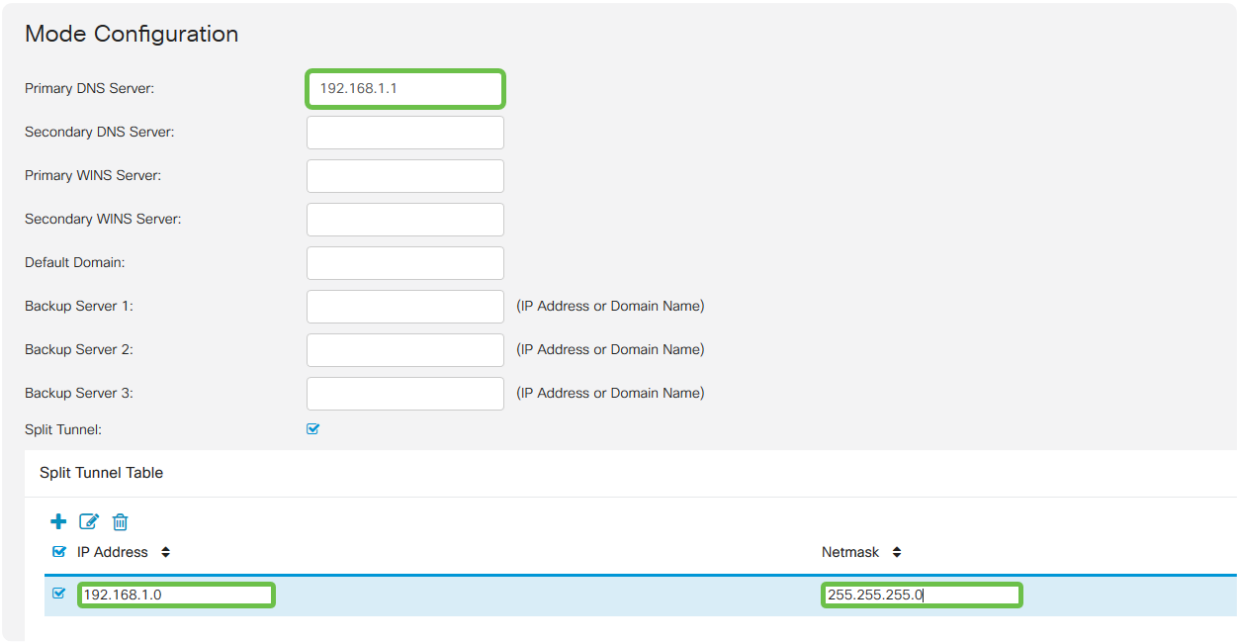
ⓘ Note: L'intervallo di pool deve utilizzare una subnet univoca che non viene utilizzata in altre posizioni della rete.



Passaggio 6

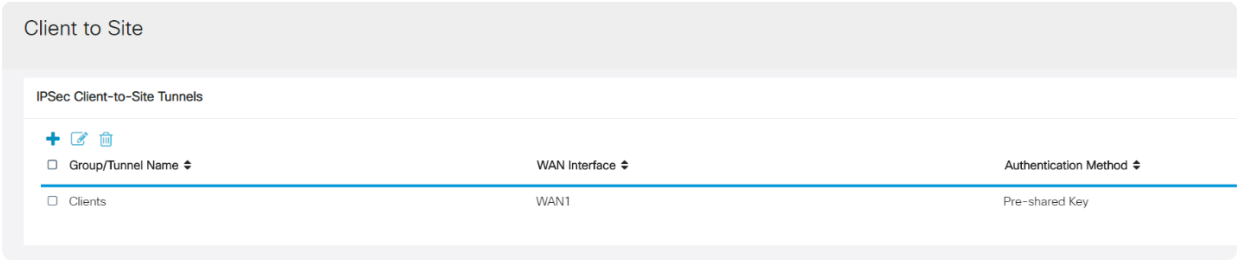
Qui è possibile configurare le impostazioni di Configurazione modalità. Ecco le impostazioni che utilizzeremo:

- Server DNS primario: Se si dispone di un server DNS interno o si desidera utilizzare un server DNS esterno, è possibile immetterlo qui. In caso contrario, per impostazione predefinita viene utilizzato l'indirizzo IP della LAN RV345P. Nell'esempio verrà utilizzata l'impostazione predefinita.
- Tunnel ripartito: selezionare per abilitare il tunneling ripartito. Questa opzione viene usata per specificare il traffico che passerà attraverso il tunnel VPN. Nel nostro esempio utilizzeremo Split Tunnel.
- Tabella tunnel suddiviso: immettere le reti a cui il client VPN deve avere accesso tramite la VPN. In questo esempio viene utilizzata la rete LAN RV345P.



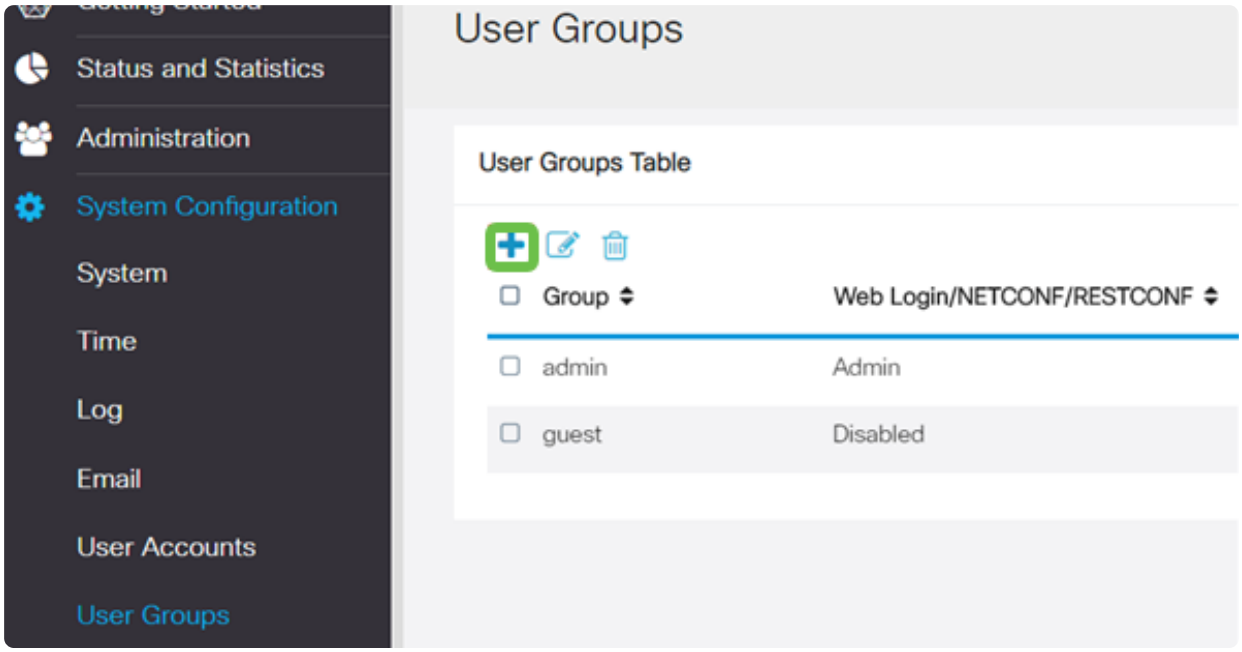
Passaggio 7

Dopo aver fatto clic su Save, è possibile visualizzare il profilo nell'elenco dei gruppi da client a sito IPsec.



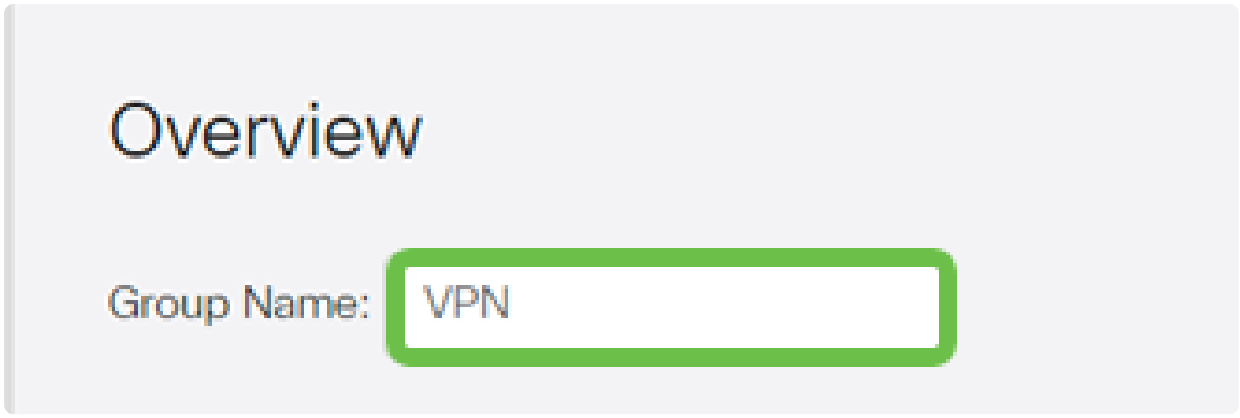
Passaggio 8

Configurare un gruppo di utenti da utilizzare per l'autenticazione degli utenti client VPN. In Configurazione di sistema > Gruppi di utenti, fare clic sull'icona con il segno più (+) per aggiungere un gruppo di utenti.



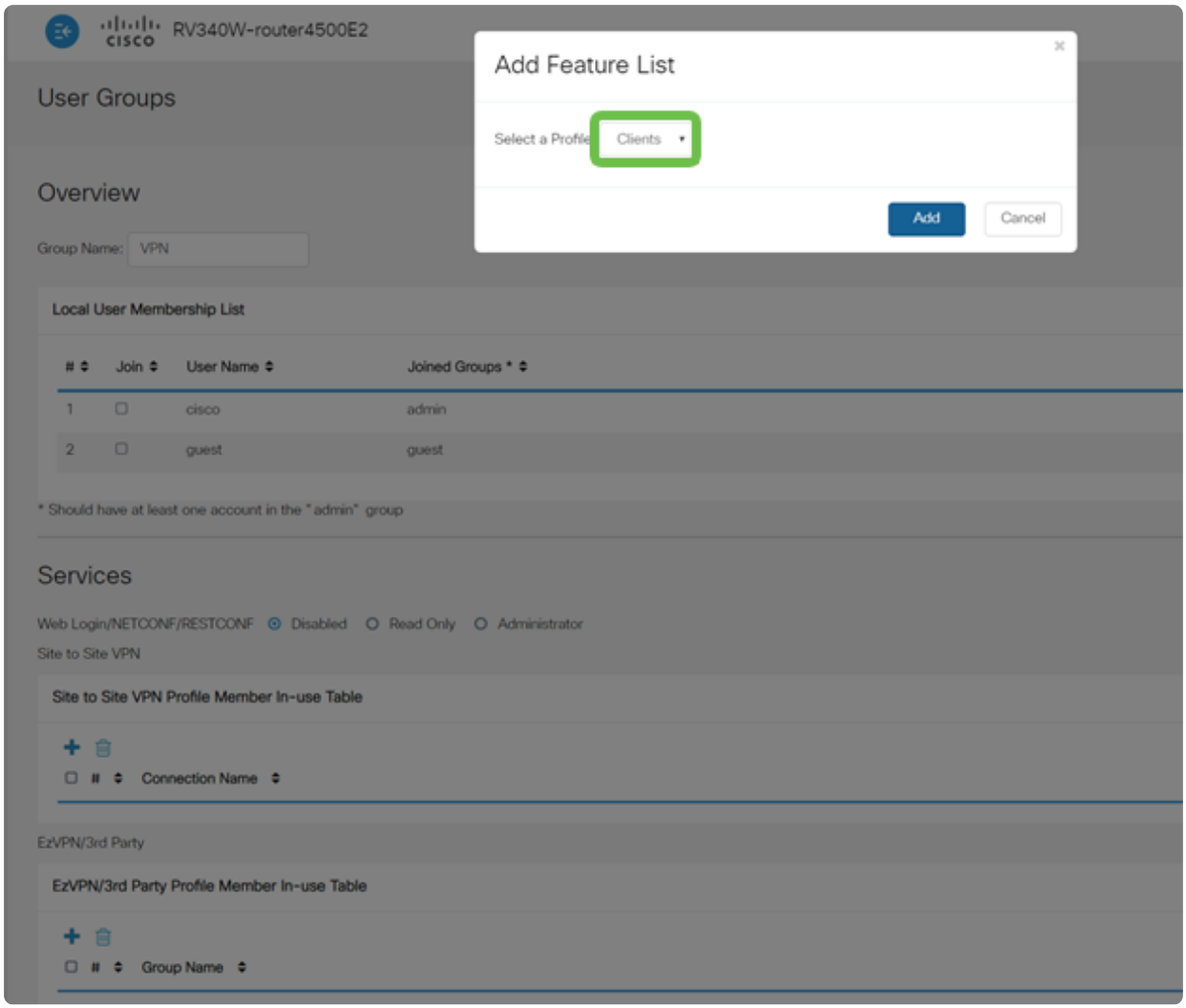
Passaggio 9

Immettere il nome di un gruppo.



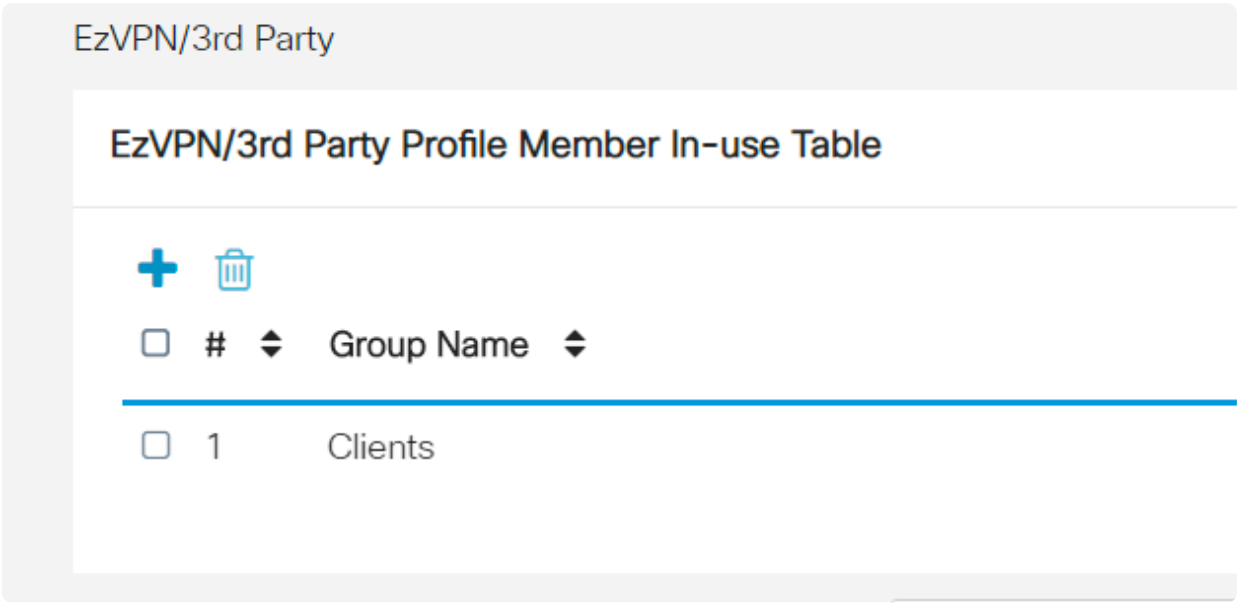
Passaggio 10

In Servizi > EzVPN/terze parti, fare clic su Aggiungi per collegare questo gruppo di utenti al profilo da client a sito configurato in precedenza.



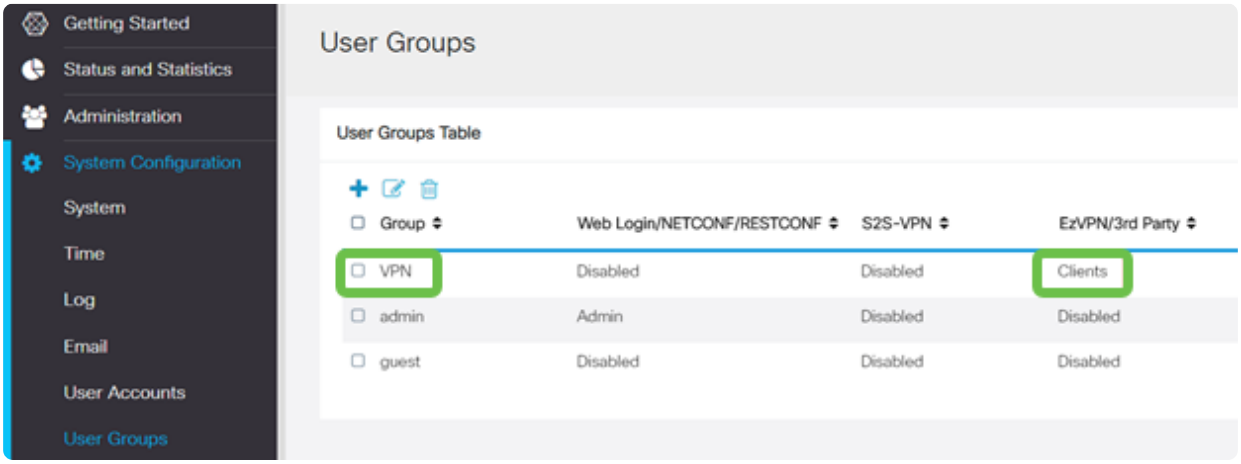
Passaggio 11

Il nome del gruppo da client a sito dovrebbe essere visualizzato nell'elenco di EzVPN/terze parti.



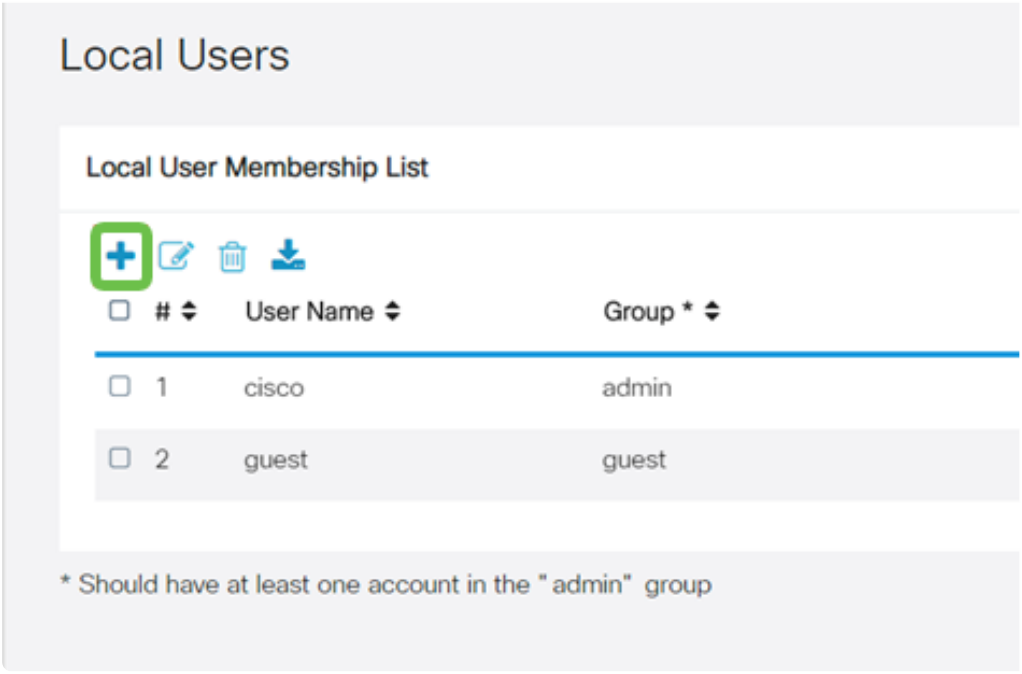
Passaggio 12

Dopo aver applicato la configurazione del gruppo di utenti, questa verrà visualizzata nell'elenco Gruppi di utenti e mostrerà che il nuovo gruppo di utenti verrà utilizzato con il profilo da client a sito creato in precedenza.



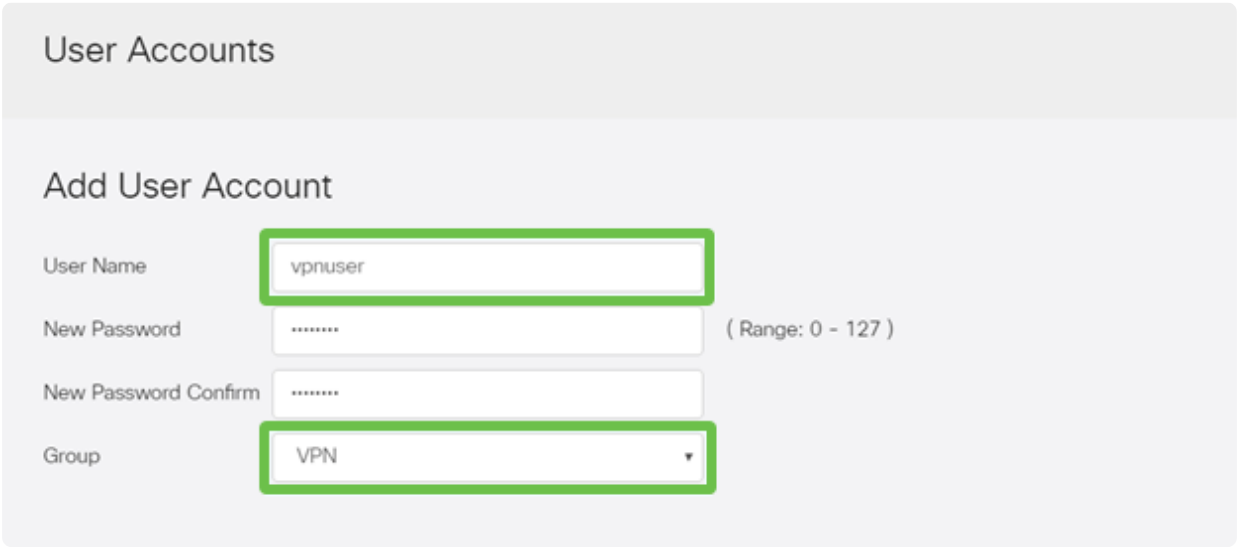
Passaggio 13

Configurare un nuovo utente in Configurazione di sistema > Account utente. Fare clic sull'icona più per creare un nuovo utente.



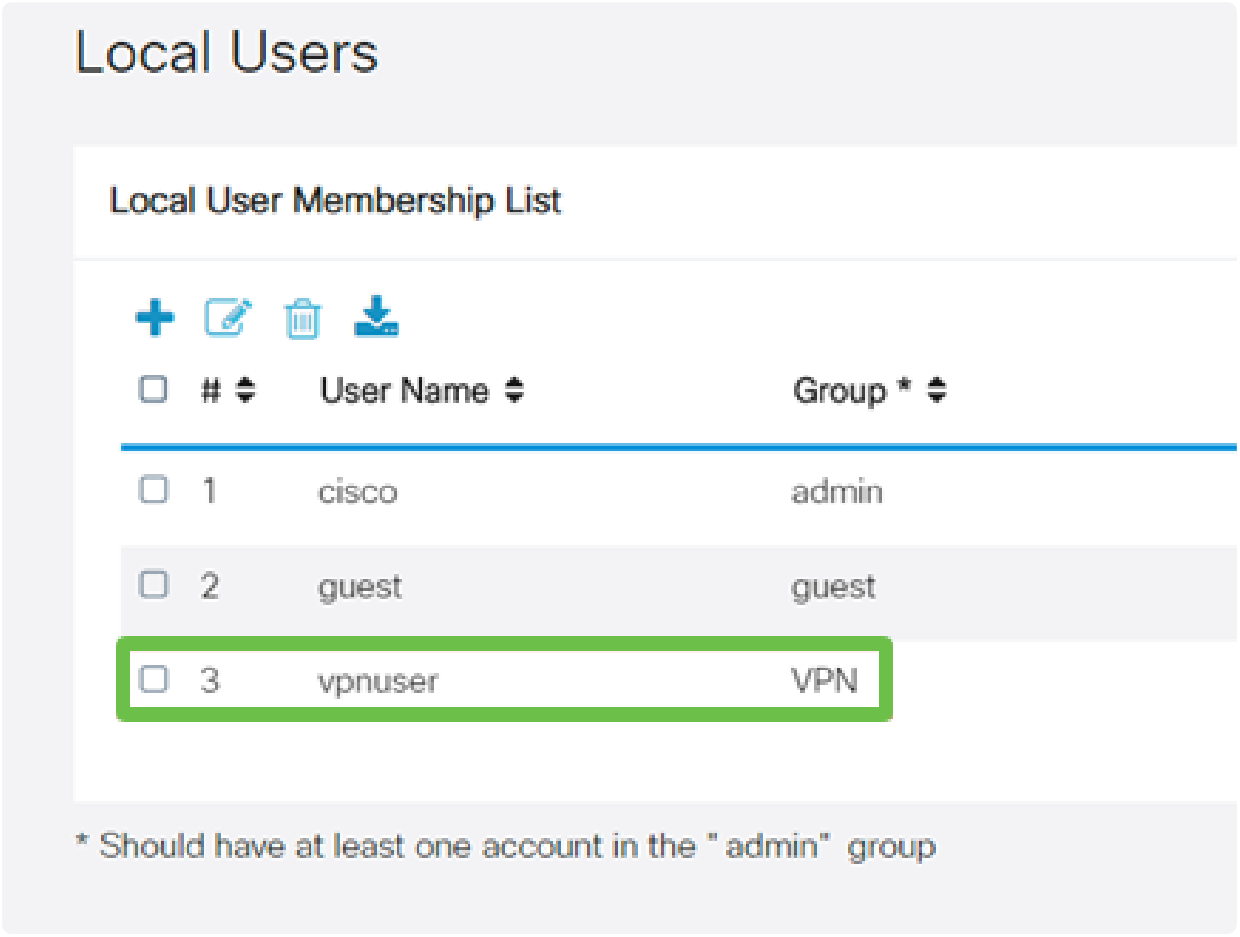
Passaggio 14

Immettere il nuovo nome utente insieme alla nuova password. Verificare che il gruppo sia impostato sul nuovo gruppo utenti appena configurato. Al termine, fare clic su Apply (Applica).



Passaggio 15

Il nuovo utente verrà visualizzato nell'elenco degli utenti locali.



La configurazione del router serie RV345P è stata completata. Successivamente, si configurerà il client Shrew Soft VPN.

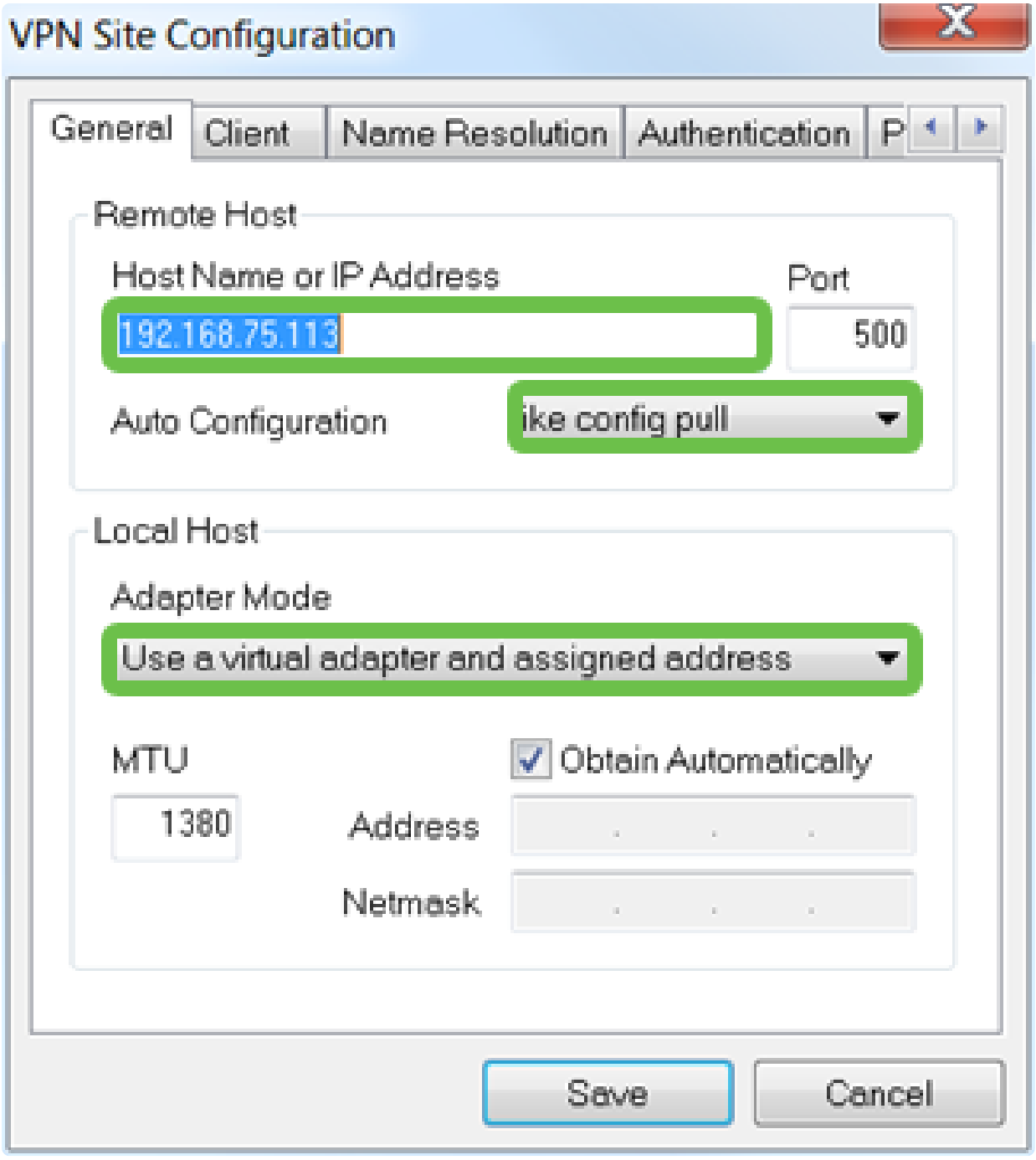
Configurare il client Show Soft VPN

Attenersi alla procedura seguente.

Passaggio 1

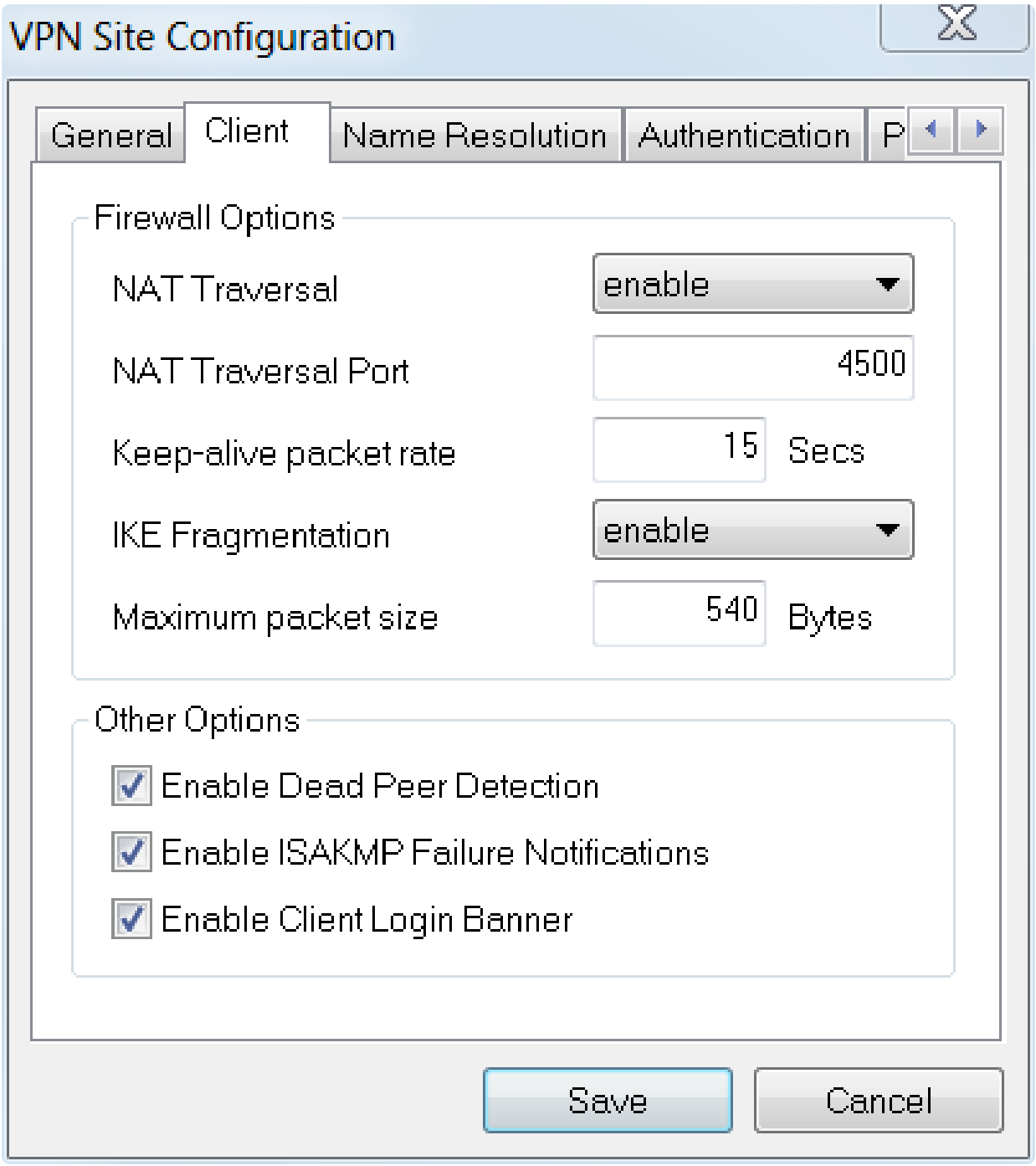
Aprire Show Soft VPN Access Manager e fare clic su Add per aggiungere un profilo. Nella finestra Configurazione sito VPN che viene visualizzata, configurare la scheda Generale:

- Nome host o indirizzo IP: Usare l'indirizzo IP WAN (o il nome host dell'RV345P)
- Configurazione automatica: Selezionare Ike config pull
- Modalità scheda di rete: Selezionare Usa scheda virtuale e indirizzo assegnato



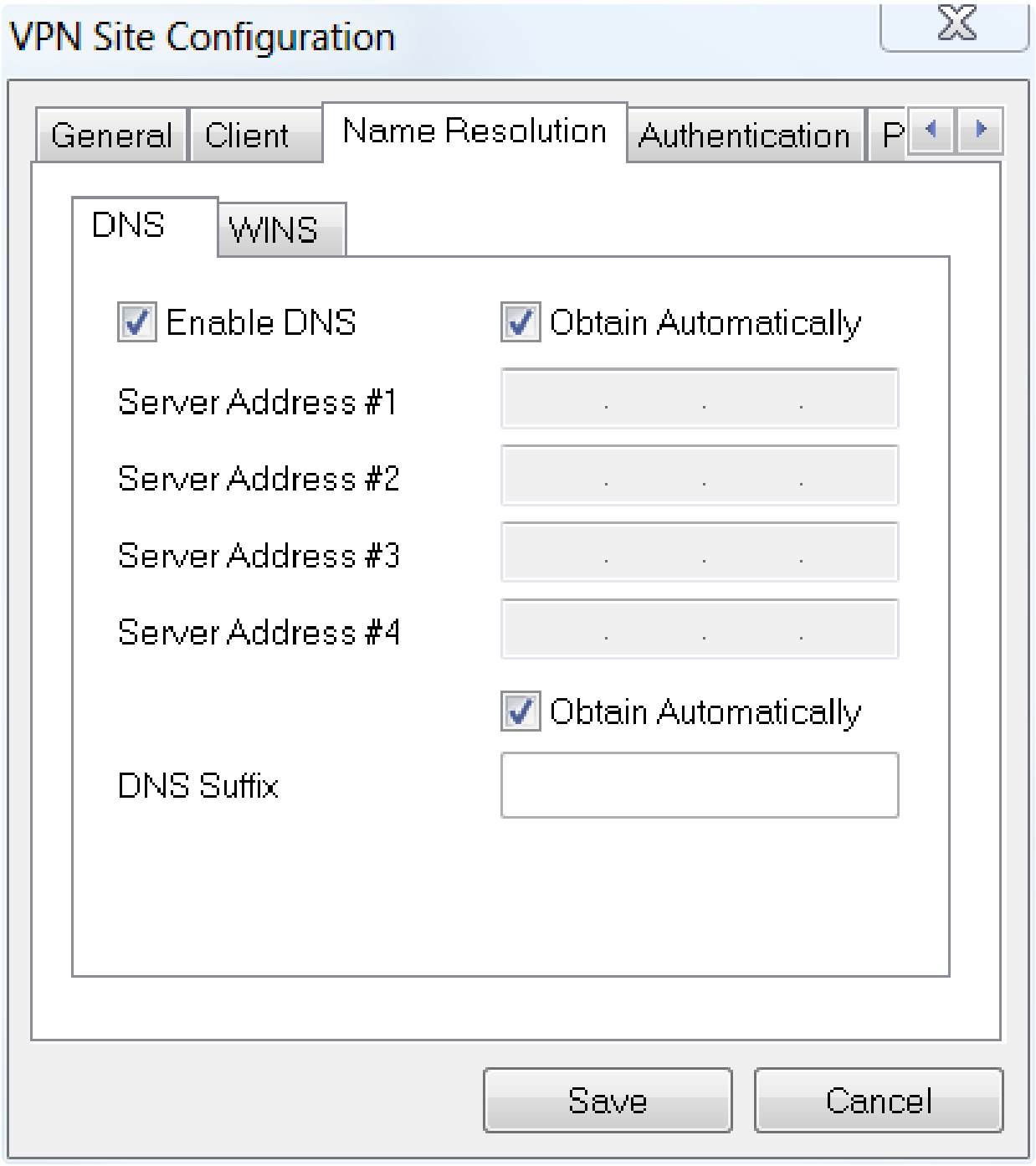
Passaggio 2

Configurare la scheda Client. In questo esempio sono state mantenute le impostazioni predefinite.



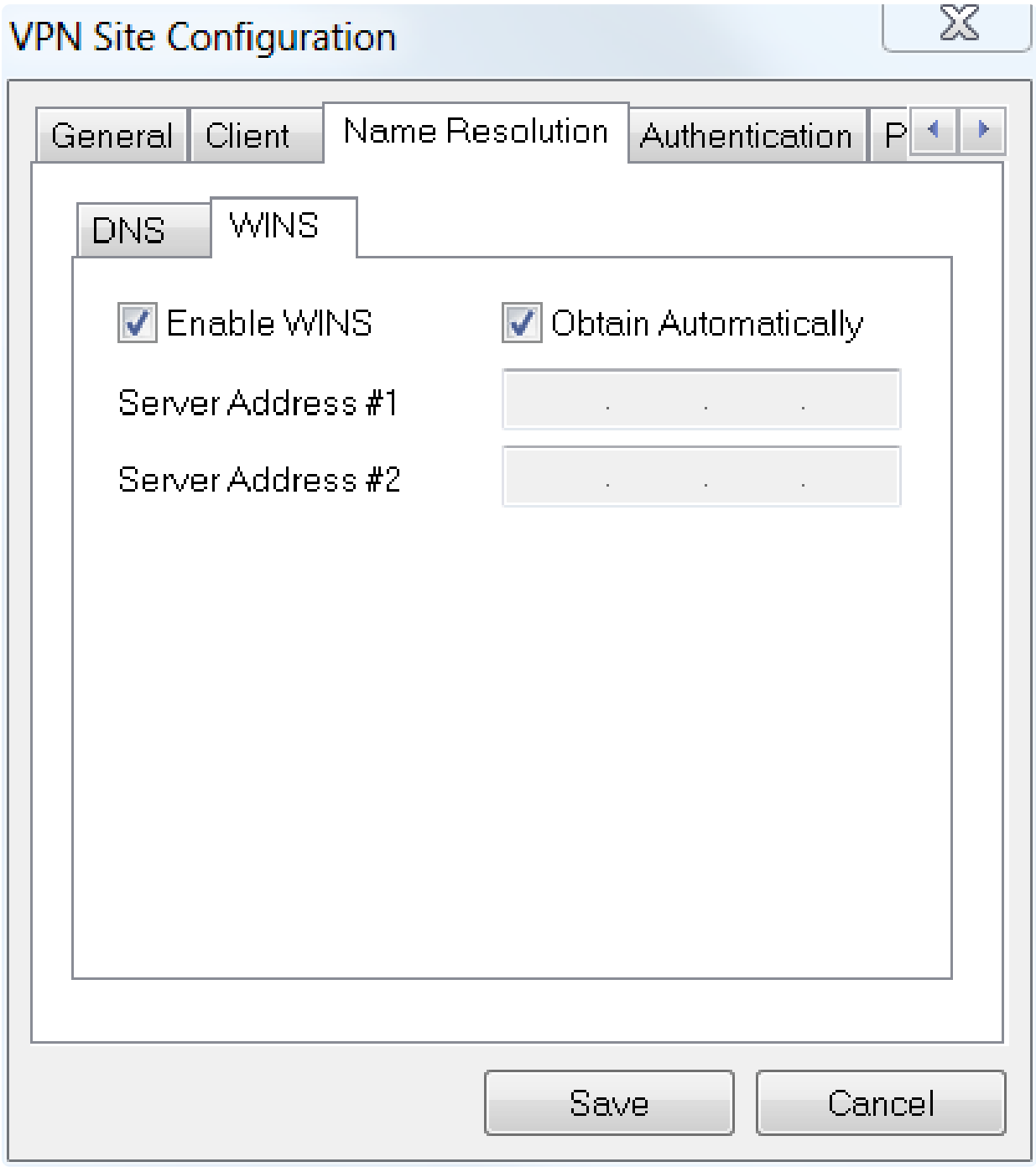
Passaggio 3

In Risoluzione dei nomi > DNS, selezionare la casella Abilita DNS e lasciare selezionate le caselle Ottieni automaticamente.



Passaggio 4

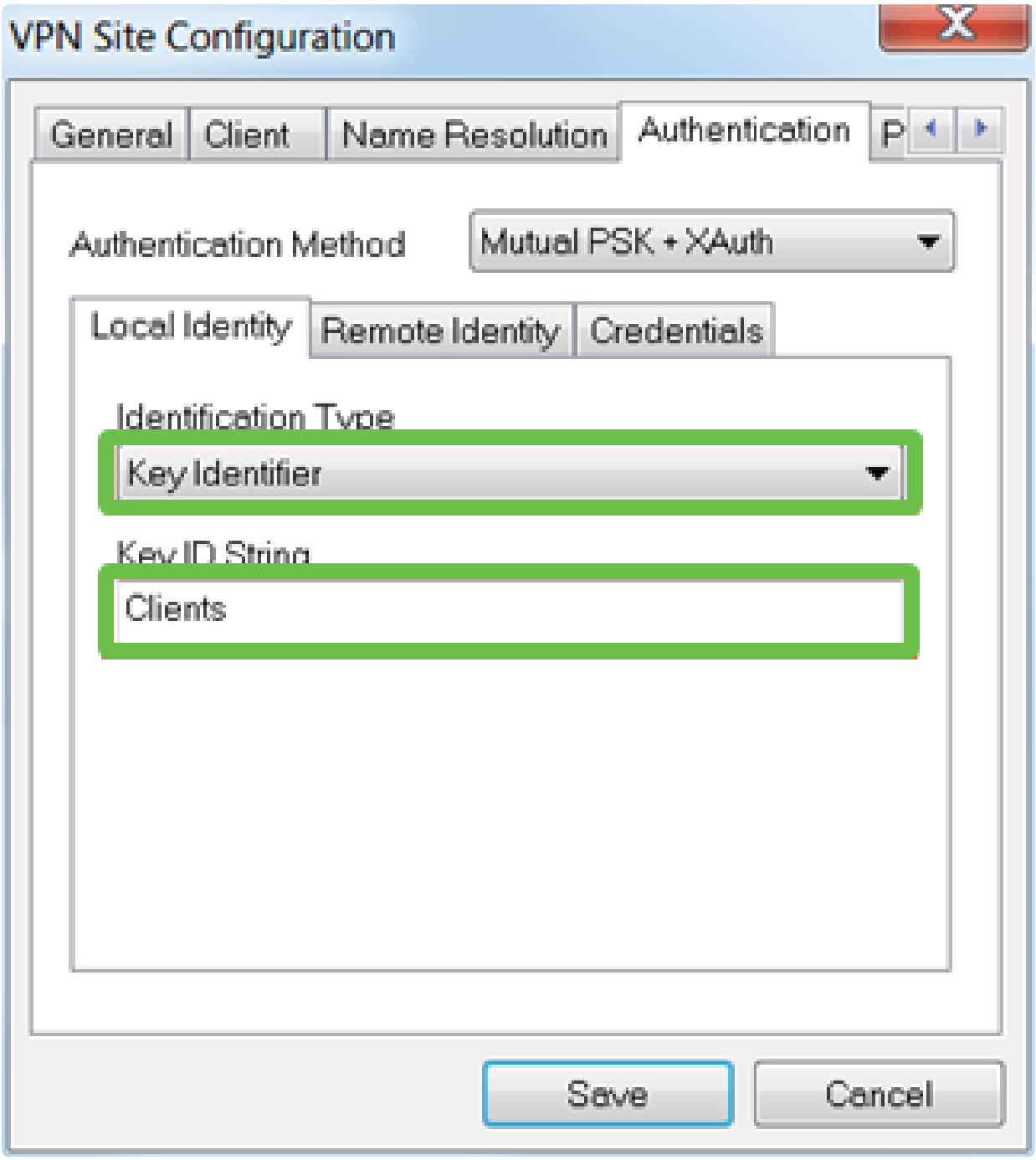
In Risoluzione nome > scheda WINS, selezionare la casella Abilita WINS e lasciare la casella di controllo Ottieni automaticamente selezionata.



Passaggio 5

Fare clic su Autenticazione > Identità locale.

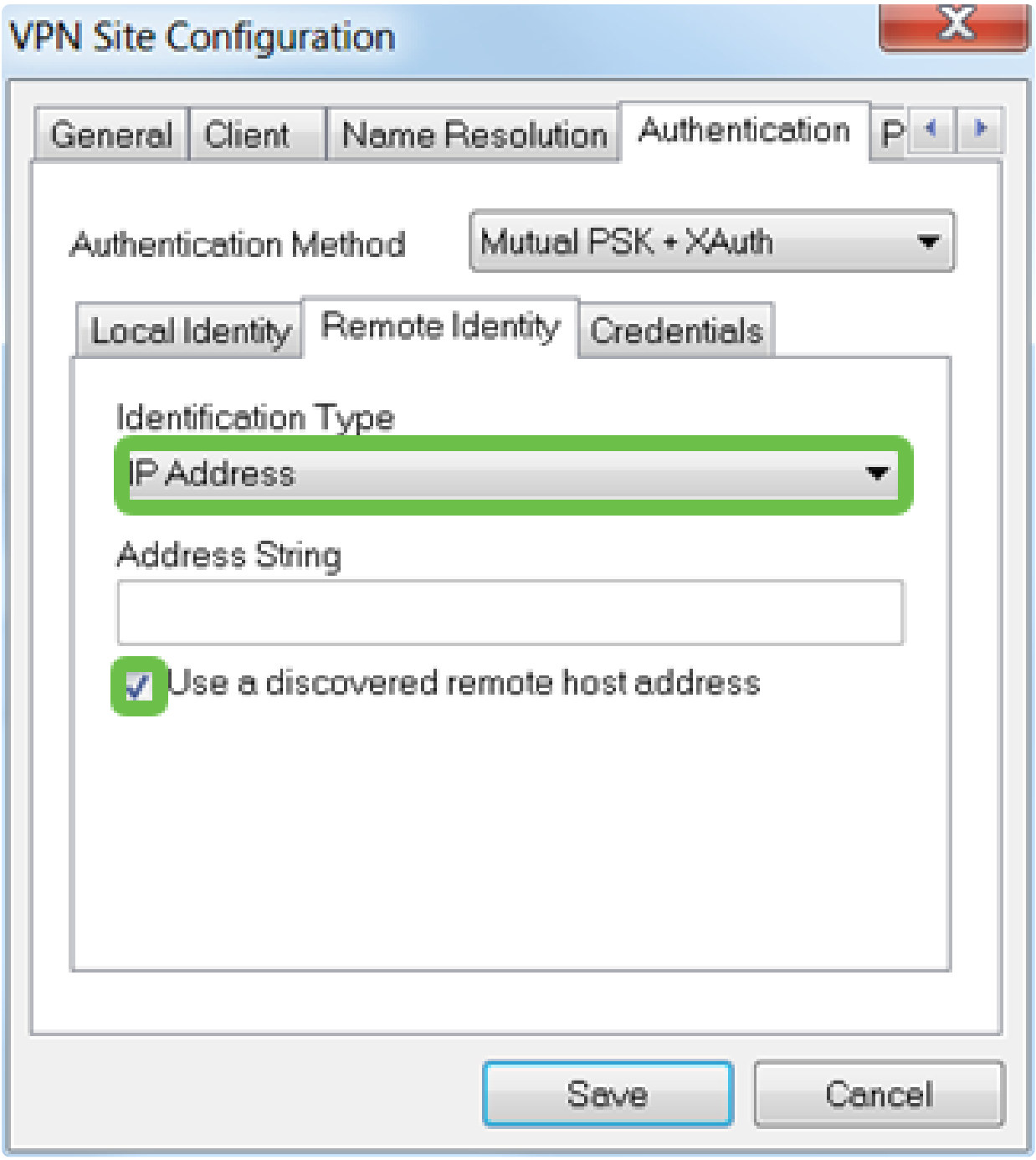
- Tipo di identificazione: Seleziona identificatore chiave
- Stringa ID chiave: Immettere il nome del gruppo configurato sull'RV345P



Passaggio 6

In Autenticazione > Identità Remota. In questo esempio sono state mantenute le impostazioni predefinite.

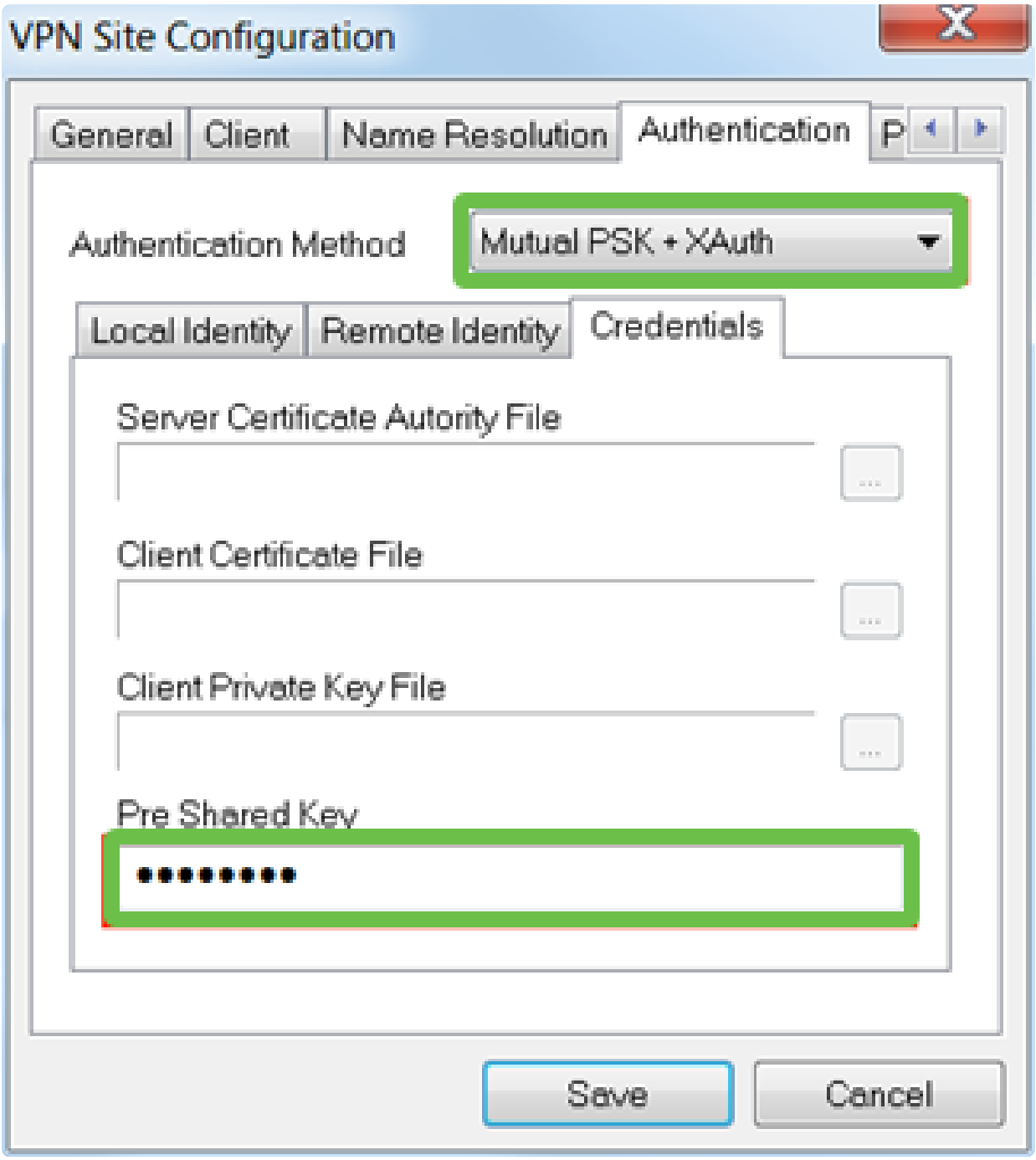
- Tipo di identificazione: Indirizzo IP
- Stringa indirizzo: <vuoto>
- Utilizzare la casella dell'indirizzo di un host remoto individuato: Controllato



Passaggio 7

In Autenticazione > Credenziali, configurare quanto segue:

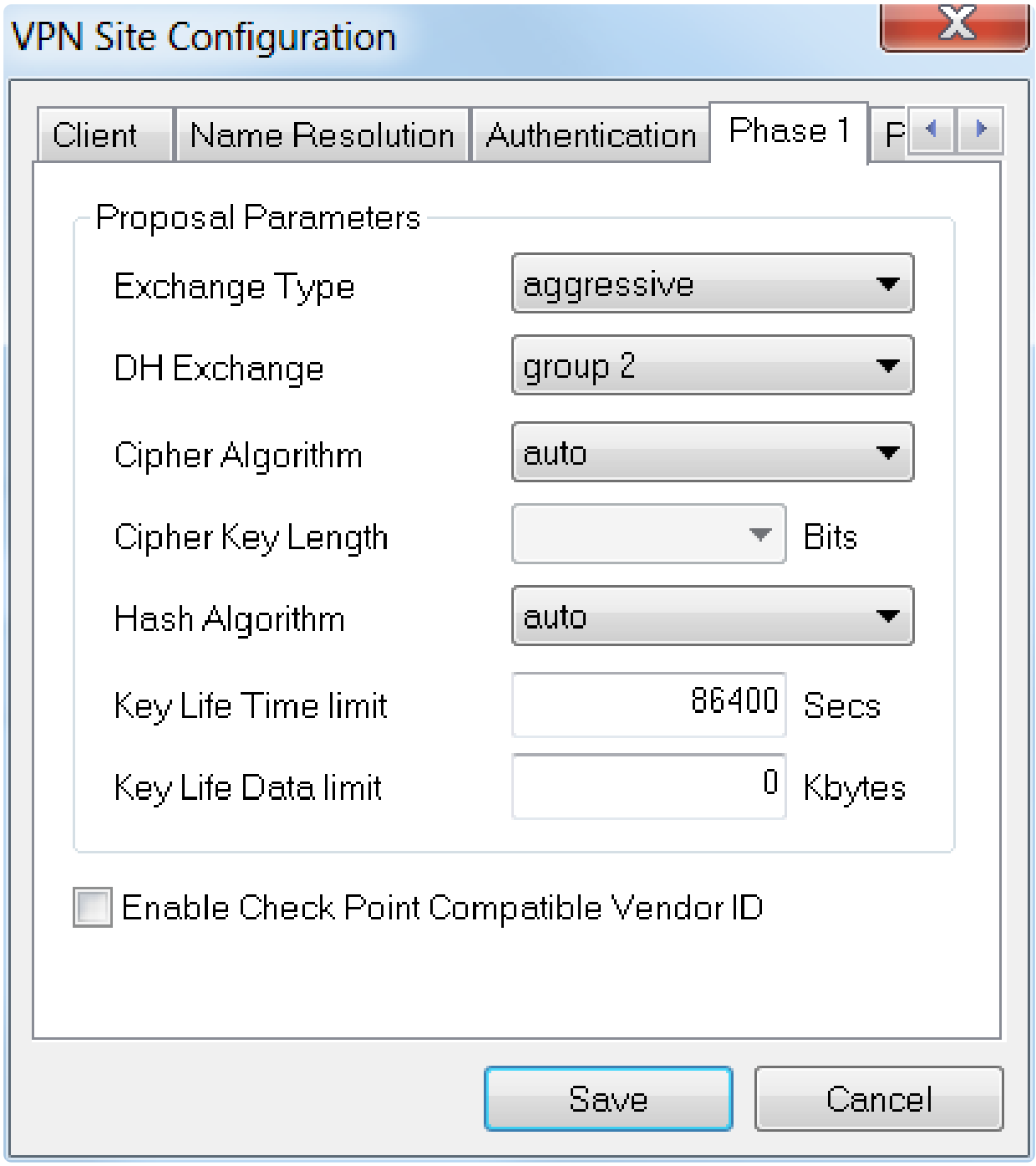
- Metodo di autenticazione: Selezionare Mutual PSK + XAuth
- Chiave già condivisa: Immettere la chiave già condivisa configurata nel profilo client RV345P



Passaggio 8

Per la scheda Fase 1. In questo esempio sono state mantenute le impostazioni predefinite:

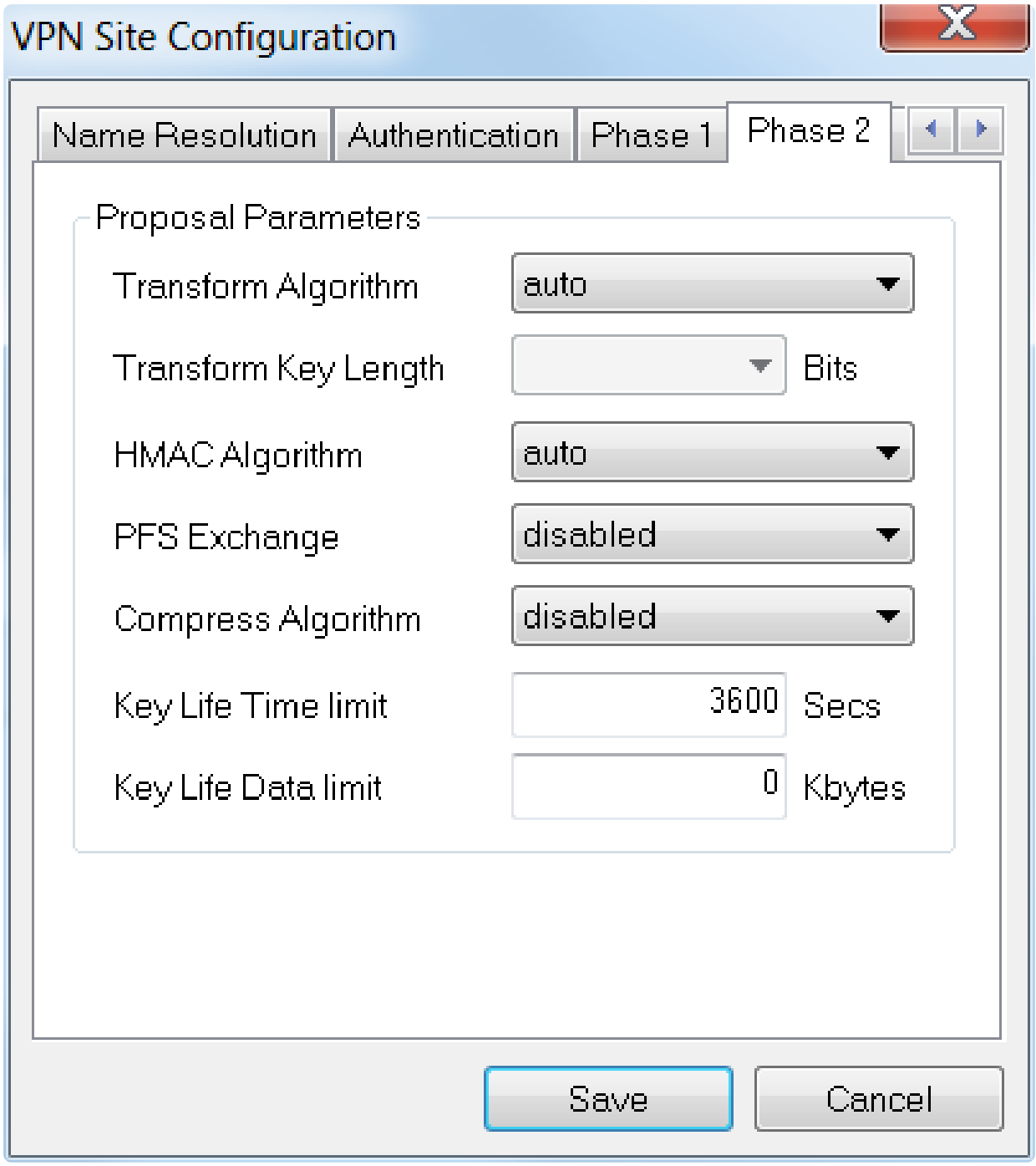
- Tipo di scambio: aggressivo
- DH Exchange: gruppo 2
- Algoritmo di crittografia: automatico
- Algoritmo hash: automatico



Passaggio 9

In questo esempio, i valori predefiniti per la scheda Fase 2 sono rimasti invariati.

- Algoritmo di trasformazione: automatico
- Algoritmo HMAC: automatico
- Scambio PFS: Disabilitato
- Algoritmo di compressione: disabilitato

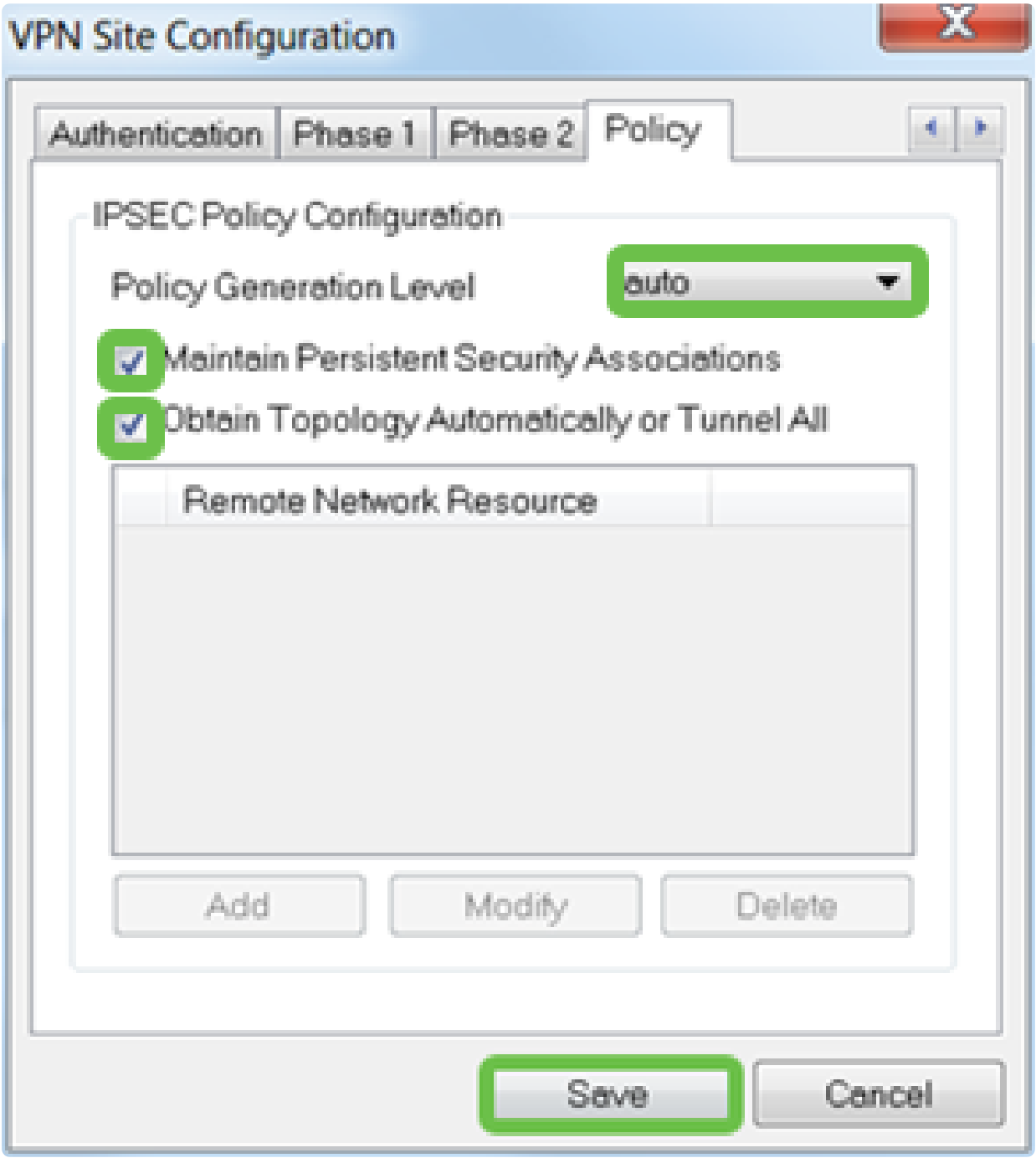


Passaggio 10

Per l'esempio della scheda Criterio sono state utilizzate le impostazioni seguenti:

- Livello di generazione dei criteri: automatico
- Gestisci Associazioni Di Sicurezza Persistenti: Selezionato
- Ottieni topologia automaticamente o Tunnel tutto: selezionata

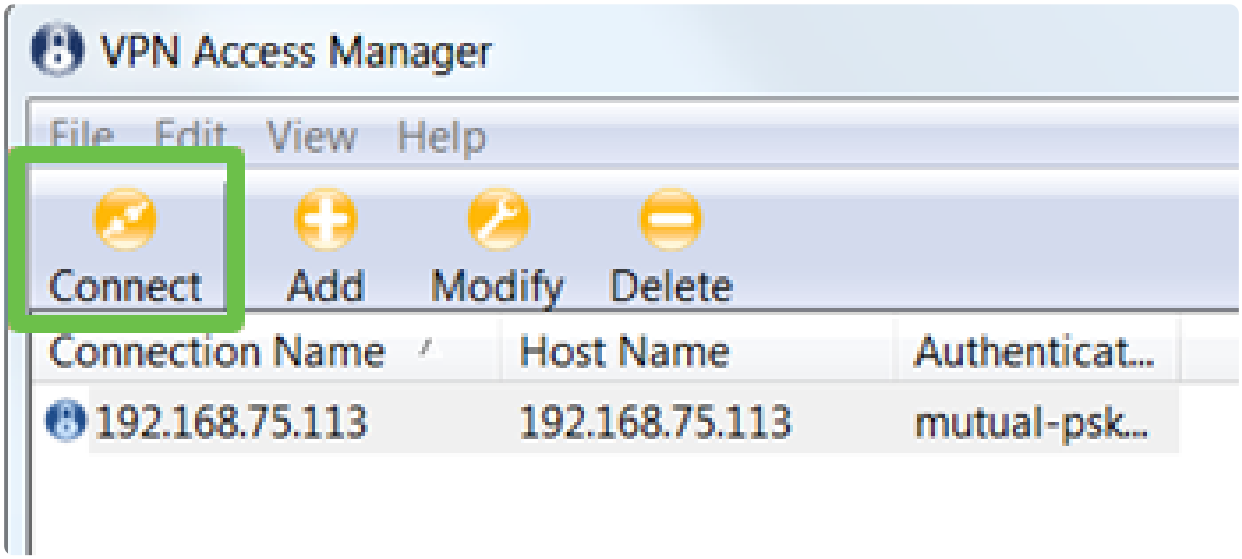
Poiché è stato configurato lo split-tunneling sull'RV345P, non è necessario configurarlo qui.



Al termine, fare clic su Salva.

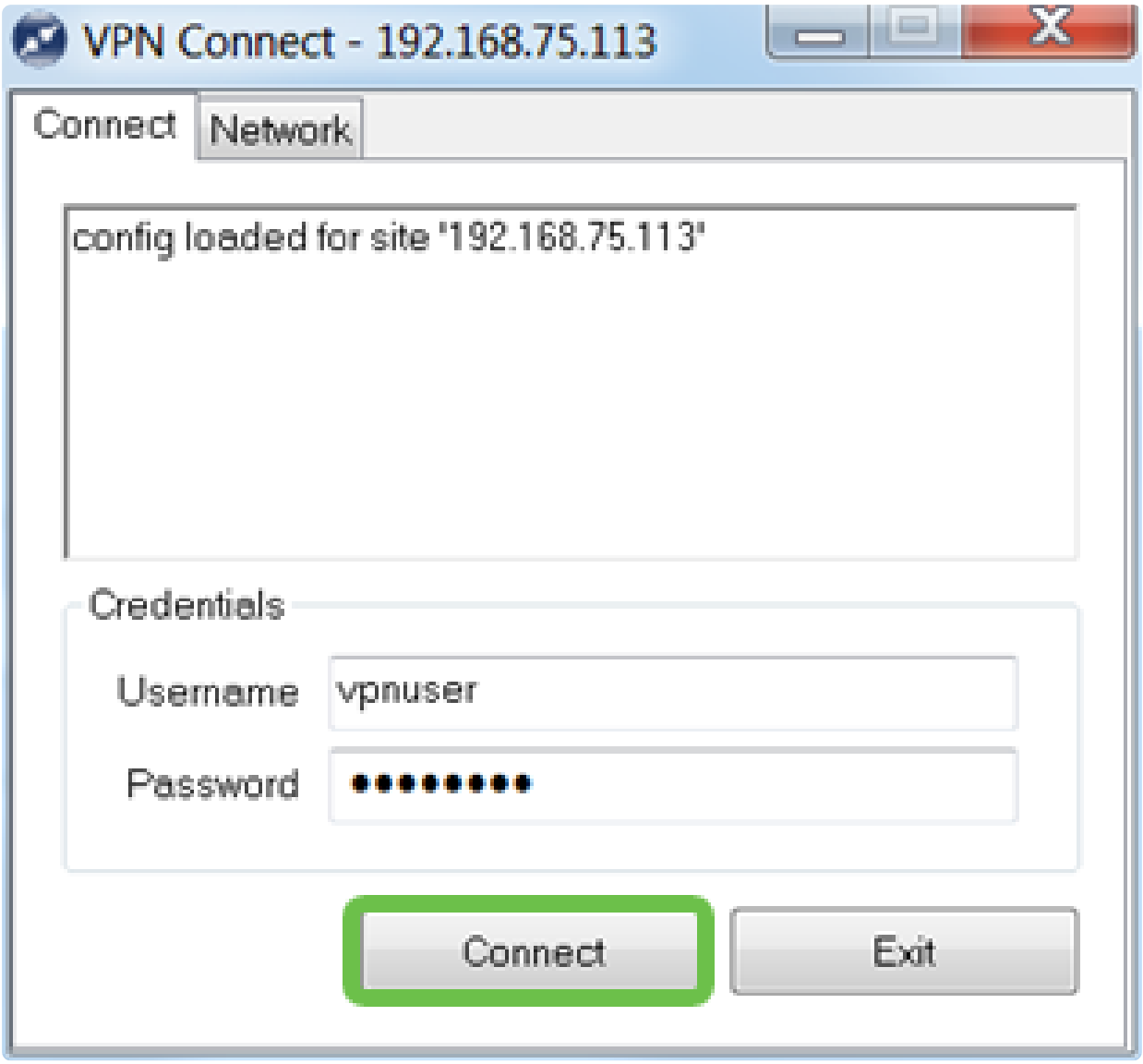
Passaggio 11

È ora possibile eseguire il test della connessione. In VPN Access Manager, evidenziare il profilo di connessione e fare clic sul pulsante Connect (Connetti).



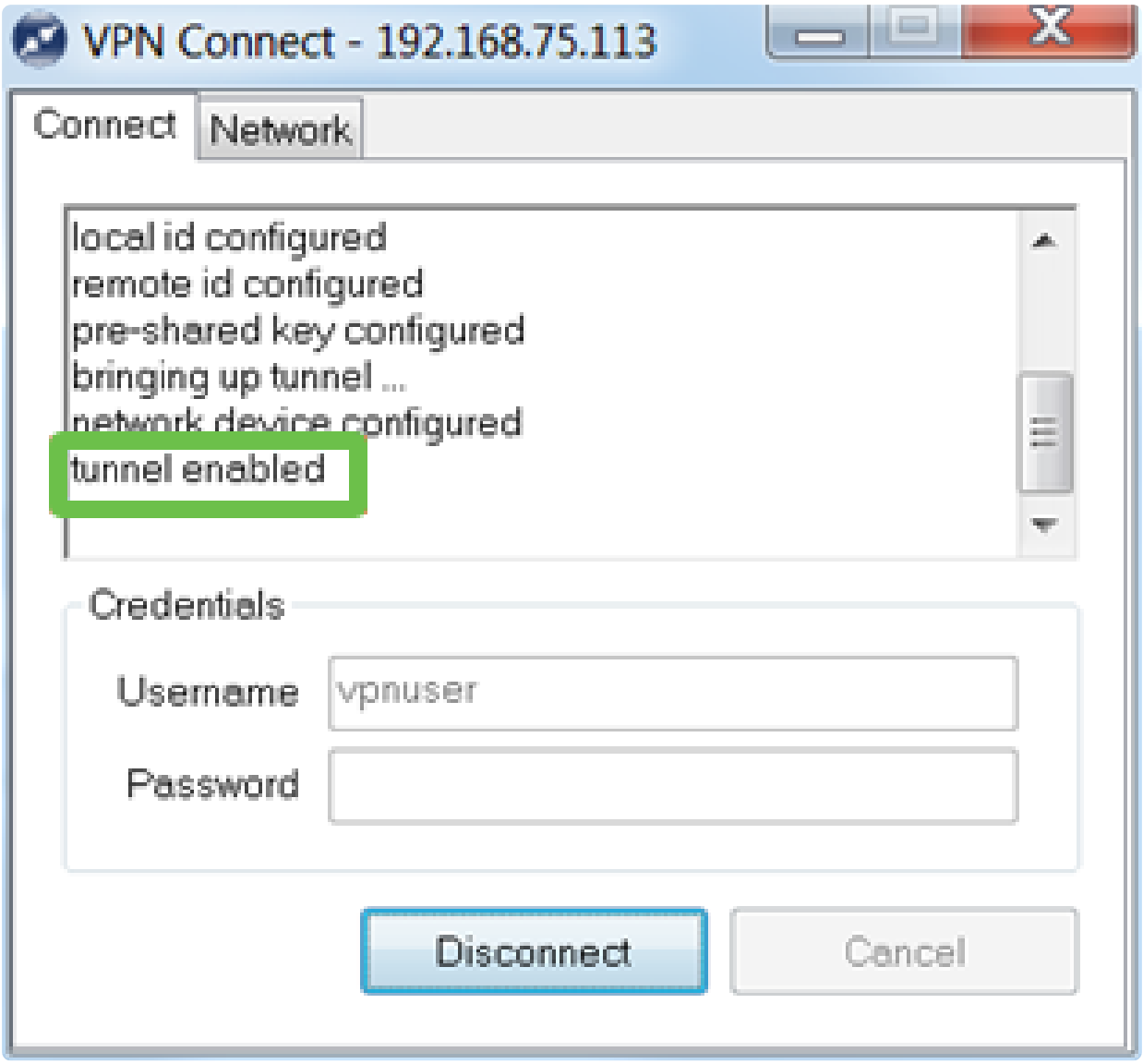
Passaggio 12

Nella finestra VPN Connect che viene visualizzata, immettere il nome utente e la password usando le credenziali per l'account utente creato sull'RV345P (passaggi 13 e 14). Al termine, fare clic su Connetti.



Passaggio 13

Verificare che il tunnel sia collegato. Il tunnel dovrebbe essere abilitato.



ⓘ Note: Shrew Soft è stato utilizzato come esempio in questa configurazione. Poiché Shrew Soft non è un prodotto Cisco, contattare questa terza parte per assistenza tecnica.

Altre opzioni VPN

Ci sono altre opzioni per usare una VPN. Per ulteriori informazioni, fare clic sui seguenti collegamenti:

- Uso del client VPN GreenBow per la connessione con il router serie RV34x

- Configurazione di un client VPN Teleworker sul router serie RV34x
- Configurazione di un server PPTP (Point-to-Point Tunneling Protocol) sul router serie Rv34x
- Configurazione di un profilo Internet Protocol Security (IPsec) su un router serie RV34x
- Configurazione delle impostazioni WAN L2TP sul router RV34x
- Configurazione della VPN da sito a sito sulla RV34x

Configurazioni supplementari sul router RV345P

Configurazione delle VLAN (opzionale)

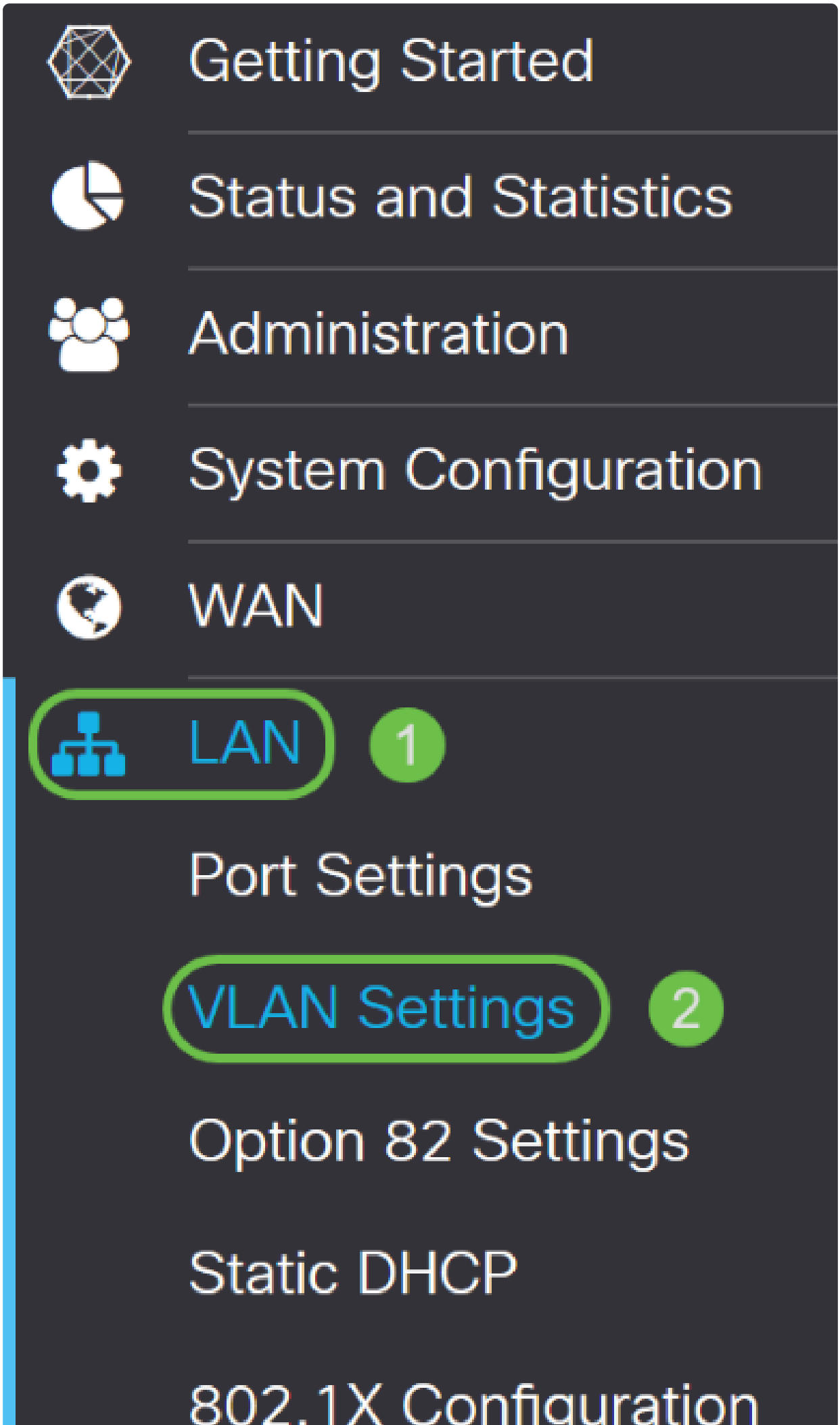
Una LAN virtuale o VLAN (Virtual Local Area Network) consente di segmentare logicamente una LAN (Local Area Network) in più domini di broadcast. Quando sulla rete vengono trasmessi anche dati sensibili, la creazione di VLAN offre una maggiore sicurezza e il traffico viene quindi indirizzato a VLAN specifiche. L'uso delle VLAN inoltre può migliorare le prestazioni in quanto riduce la necessità di inviare pacchetti broadcast e multicast a destinazioni non necessarie. È possibile creare una VLAN, ma questa operazione non ha alcun effetto finché la VLAN non è collegata ad almeno una porta, in modo manuale o dinamico. Le porte devono sempre appartenere a una o più VLAN.

Per ulteriori informazioni, consultare il documento sulle best practice e sui suggerimenti per la sicurezza delle VLAN.

Se non si desidera creare le VLAN, è possibile passare alla sezione successiva.

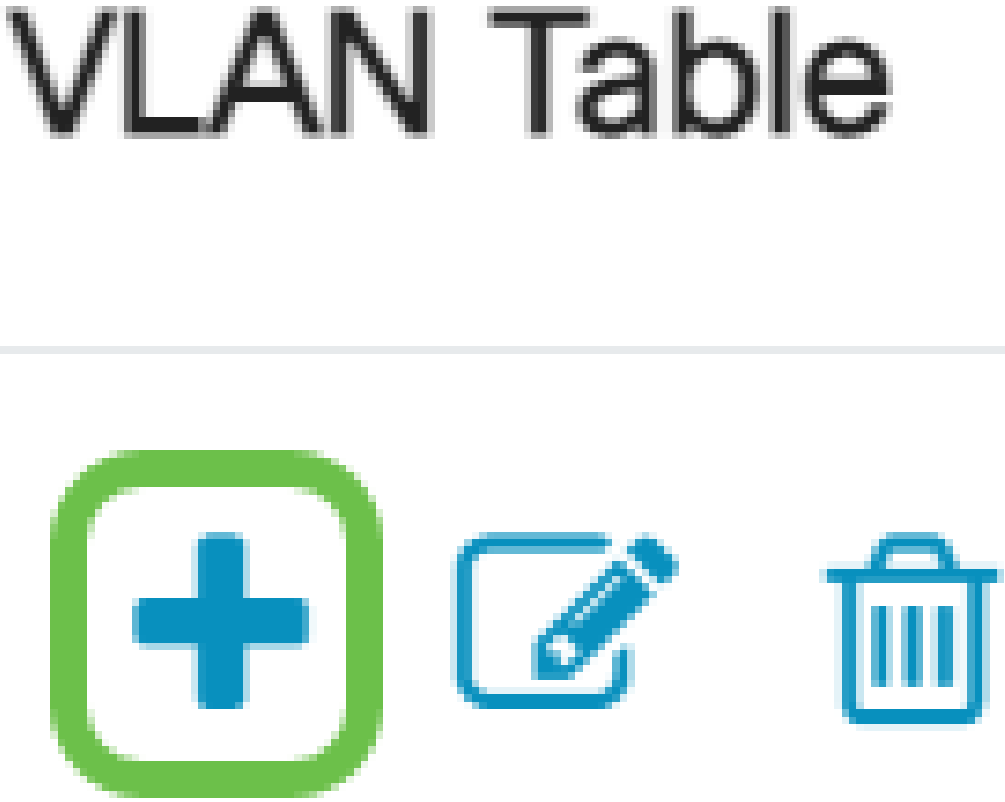
Passaggio 1

Accedere a LAN > VLAN Settings (LAN > Impostazioni VLAN).


Getting Started
Status and Statistics
Administration
System Configuration
WAN
LAN
1
Port Settings
VLAN Settings
2
Option 82 Settings
Static DHCP
802.1X Configuration

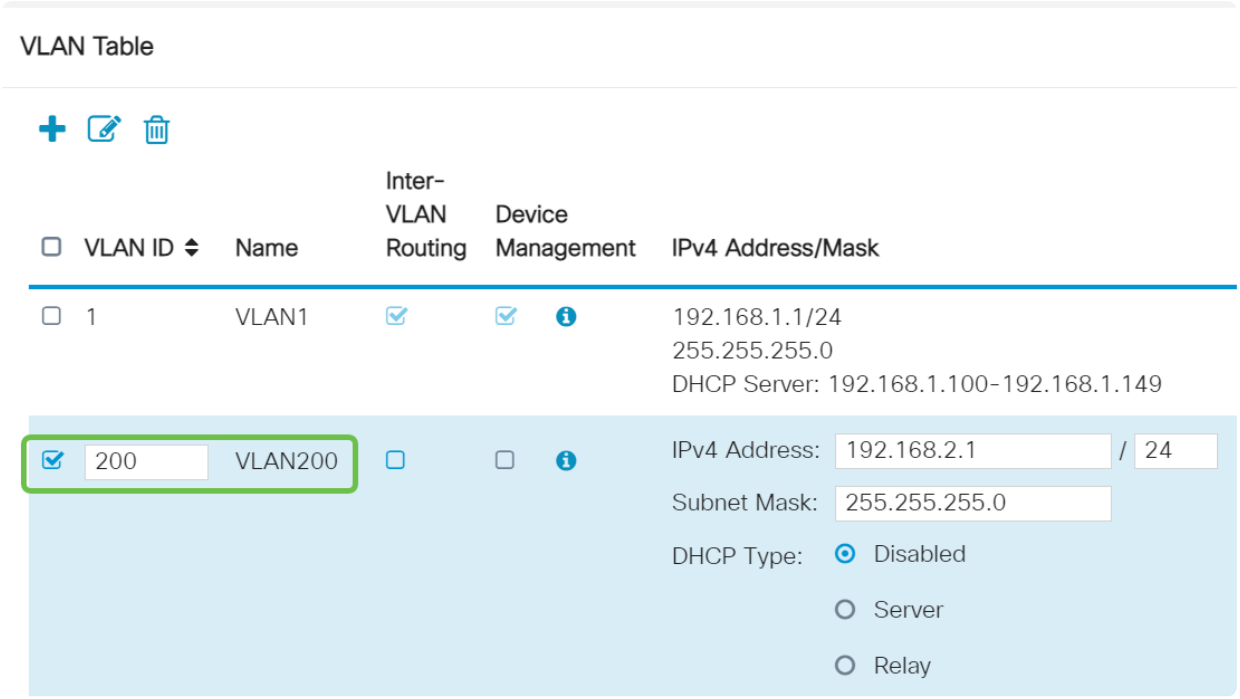
Passaggio 2

Fare clic sull'icona Add per creare una nuova VLAN.



Passaggio 3

Immettere l'ID VLAN che si desidera creare e il relativo nome. L'intervallo degli ID della VLAN è compreso tra 1 e 4093.



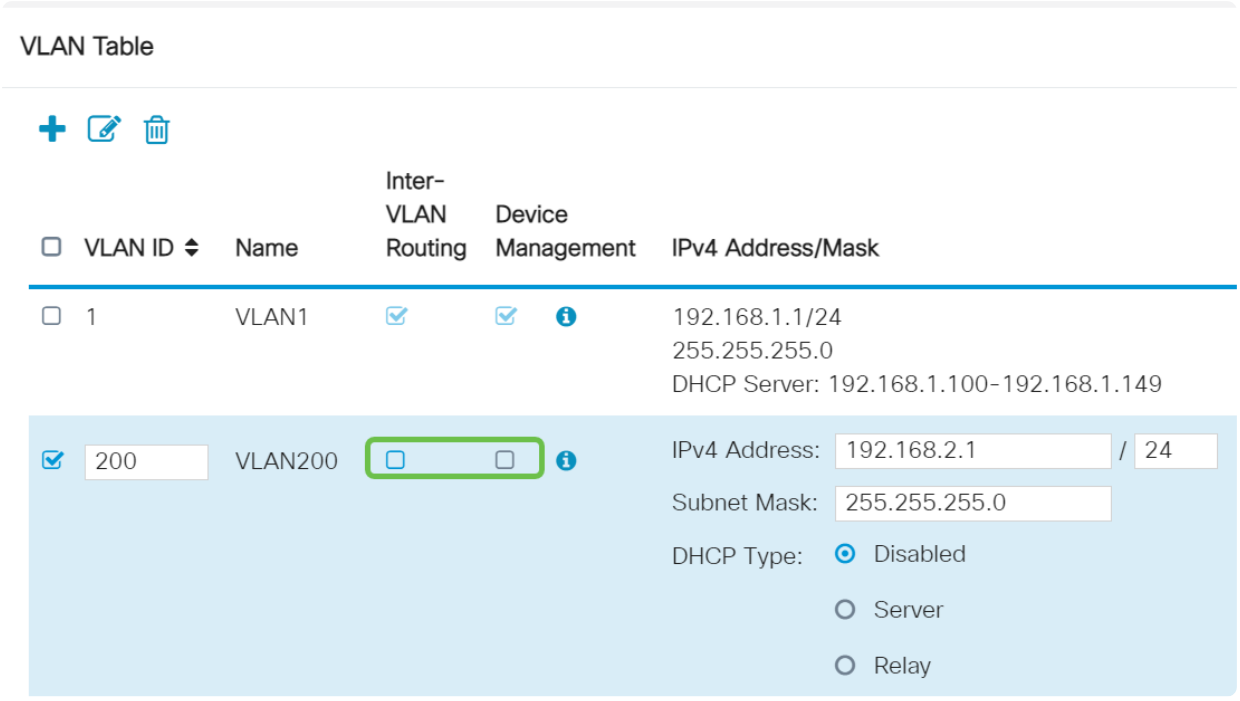
Passaggio 4

Deselezionare la casella Enabled (Abilitato) per il routing tra VLAN e per la gestione dei dispositivi, se si desidera. Il routing tra VLAN viene usato per indirizzare i pacchetti da una VLAN all'altra.

In generale, questa opzione non è consigliata per le reti guest in quanto si desidera isolare gli utenti guest e ridurre la protezione delle VLAN. In alcuni casi può essere necessario che le VLAN eseguano il routing tra loro. In questo caso, controllare il routing tra VLAN su un router RV34x con restrizioni ACL di destinazione per configurare il traffico specifico consentito tra le VLAN.

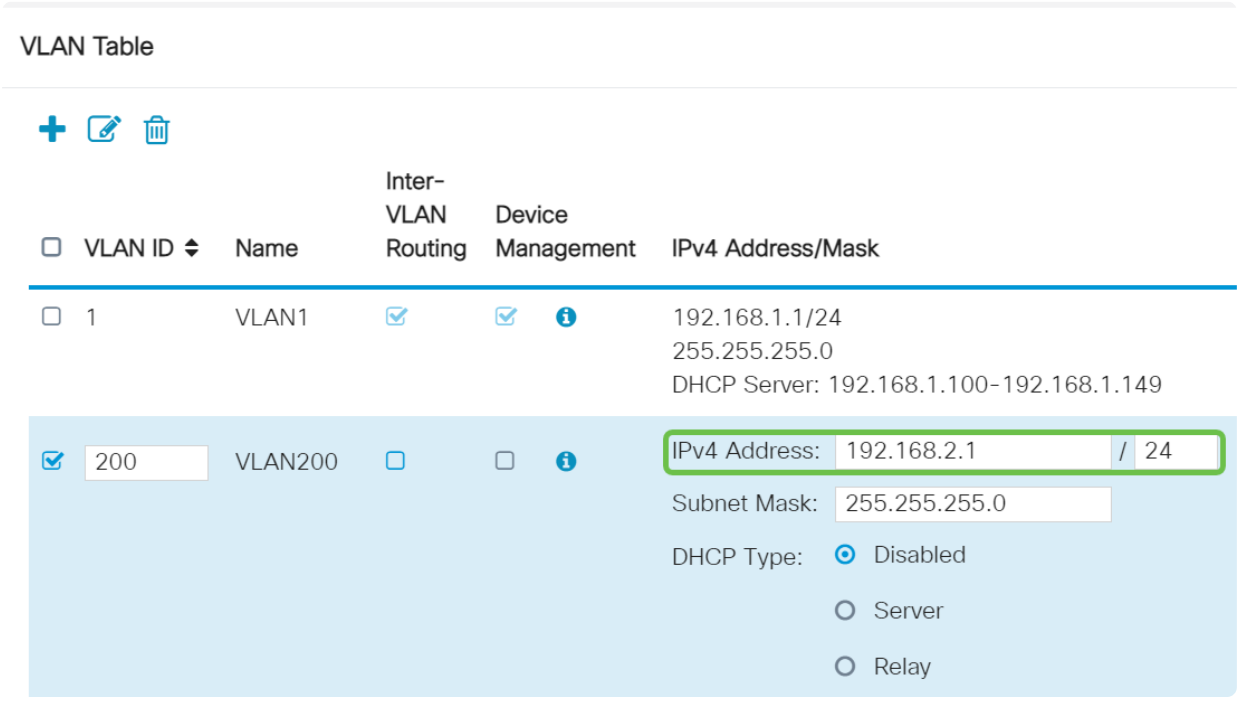
Gestione dispositivi è il software che consente di utilizzare il browser per accedere all'interfaccia Web dell'RV345P dalla VLAN e gestire l'RV345P. Questa opzione deve essere disabilitata anche nelle reti guest.

Nell'esempio, non è stato abilitato né il routing tra VLAN né la gestione dei dispositivi per mantenere la VLAN più sicura.



Passaggio 5

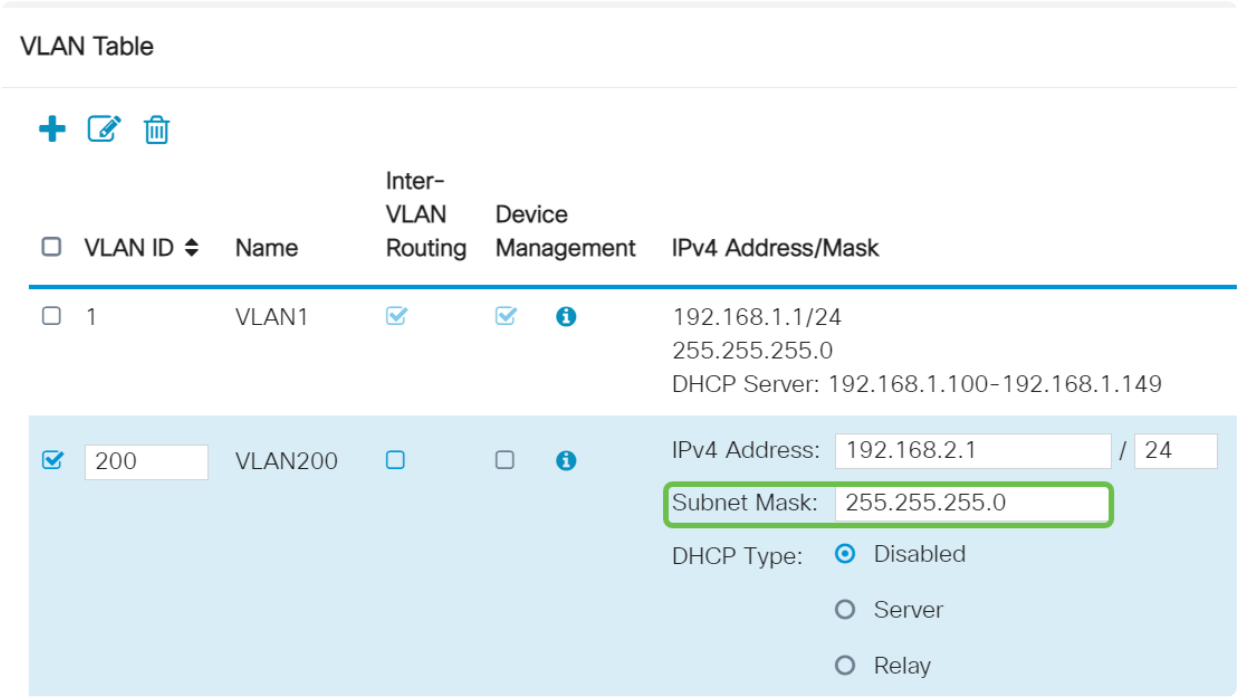
L'indirizzo IPv4 privato verrà popolato automaticamente nel campo Indirizzo IP. È possibile modificare questa impostazione se lo si desidera. Nell'esempio, la subnet ha 192.168.2.100-192.168.2.149 indirizzi IP disponibili per DHCP. 192.168.2.1-192.168.2.99 e 192.168.2.150-192.168.2.254 sono disponibili per gli indirizzi IP statici.



Passaggio 6

La subnet mask in Subnet Mask verrà popolata automaticamente. Se si apportano modifiche, il campo verrà regolato automaticamente.

Per questa dimostrazione, la subnet mask rimarrà impostata su 255.255.255.0 o /24.



Passaggio 7

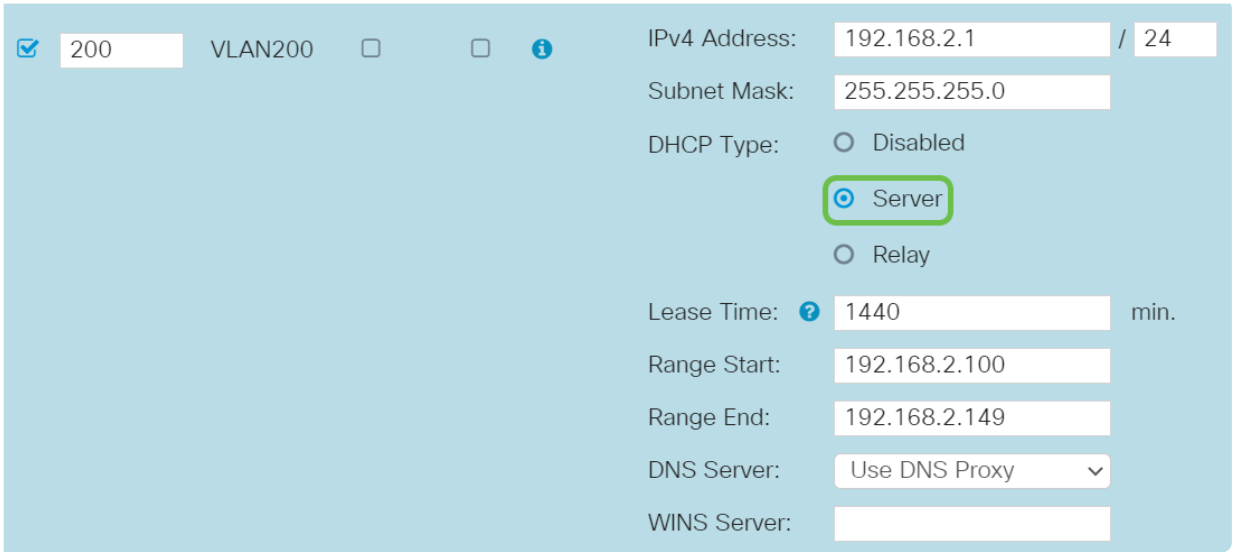
Selezionare un tipo DHCP (Dynamic Host Configuration Protocol). Le opzioni seguenti sono:

Disabled: disabilita il server IPv4 DHCP sulla VLAN. Questa operazione è consigliata in un ambiente di test. In questo scenario, tutti gli indirizzi IP dovranno essere configurati manualmente e tutte le comunicazioni interne.

Server - Opzione utilizzata con maggiore frequenza.

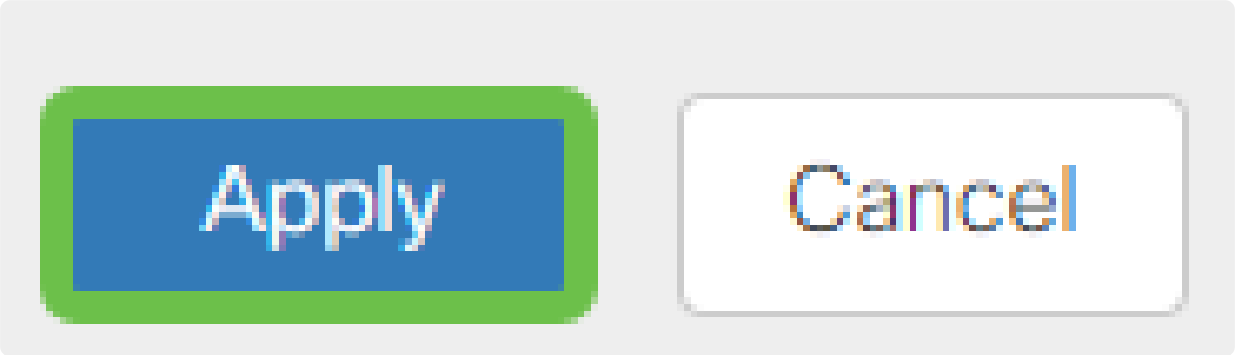
- Durata lease: immettere un valore temporale compreso tra 5 e 43.200 minuti. L'impostazione predefinita è 1440 minuti, ovvero 24 ore.

- Inizio intervallo e Fine intervallo: immettere l'inizio e la fine dell'intervallo di indirizzi IP che è possibile assegnare dinamicamente.
- Server DNS: selezionare questa opzione per utilizzare il server DNS come proxy o dall'elenco a discesa ISP.
- Server WINS - Immettere il nome del server WINS.
- Opzioni DHCP:
    - Opzione 6 - Immettere l'indirizzo IP del server TFTP.
    - Opzione 150: immettere l'indirizzo IP di un elenco di server TFTP.
    - Opzione 67 - Immettere il nome del file di configurazione.
- Inoltro: immettere l'indirizzo IPv4 del server DHCP remoto per configurare l'agente di inoltro DHCP. Si tratta di una configurazione più avanzata.



Passaggio 8

Fare clic su Apply (Applica) per creare la nuova VLAN.



Assegnazione delle VLAN alle porte (facoltativo)

Sull'RV345P è possibile configurare 16 VLAN, con una VLAN per la WAN (Wide Area Network). Le VLAN che non sono su una porta devono essere escluse. In questo modo, il traffico su questa porta viene mantenuto esclusivamente per le VLAN/VLAN specificamente assegnate dall'utente. Questa impostazione è considerata una best practice.

Le porte possono essere impostate come porte di accesso o porte trunk:

- Porta di accesso: assegnata una VLAN. Vengono passati frame senza tag.
- Porta trunk: può trasportare più di una VLAN. 802.1q. il trunking consente di rimuovere il tag da una VLAN nativa. Le VLAN che non si vuole appartengano al trunk devono essere escluse.

A una VLAN è stata assegnata una porta propria:

- Considerata una porta di accesso.
- La VLAN assegnata a questa porta deve essere etichettata come Untagged.
- Tutte le altre VLAN devono essere etichettate come Escluse per quella porta.

Due o più VLAN che condividono una porta:

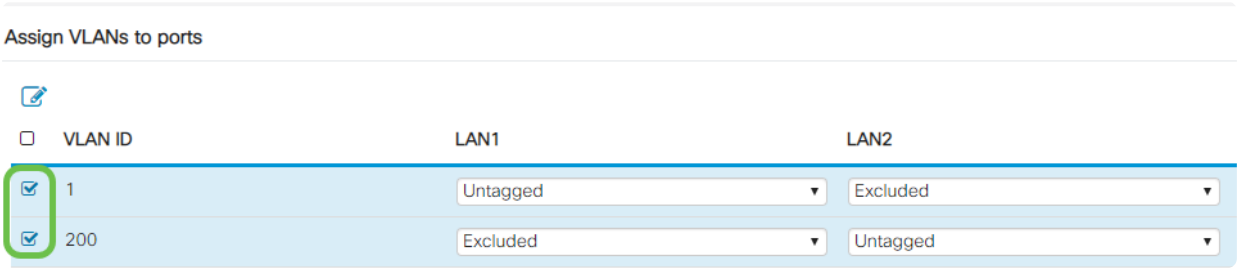
- Considerata una porta trunk.
- Una delle VLAN può essere contrassegnata come Untagged (Senza tag).
- Le altre VLAN che fanno parte della porta trunk devono essere contrassegnate come Tagged (Con tag).
- Le VLAN che non appartengono alla porta trunk devono essere contrassegnate come Excluded (Esclusa) in relazione a tale porta.

> ⓘ Note: In questo esempio non sono presenti trunk.

Passaggio 1

Selezionare gli ID VLAN da modificare.

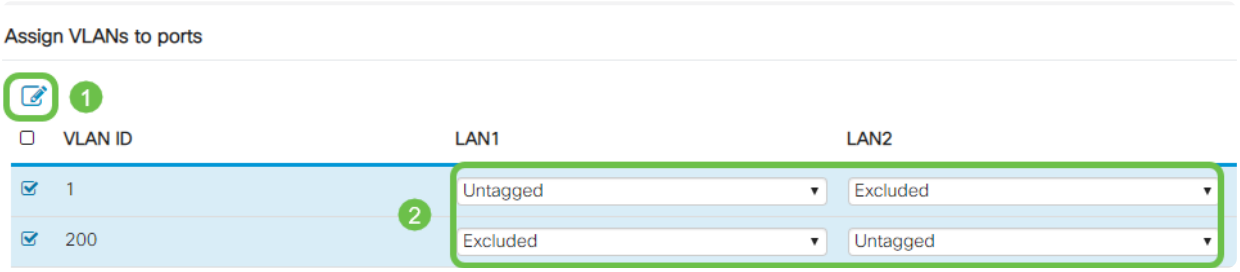
Nell'esempio, sono state selezionate la VLAN 1 e la VLAN 200.



Passaggio 2

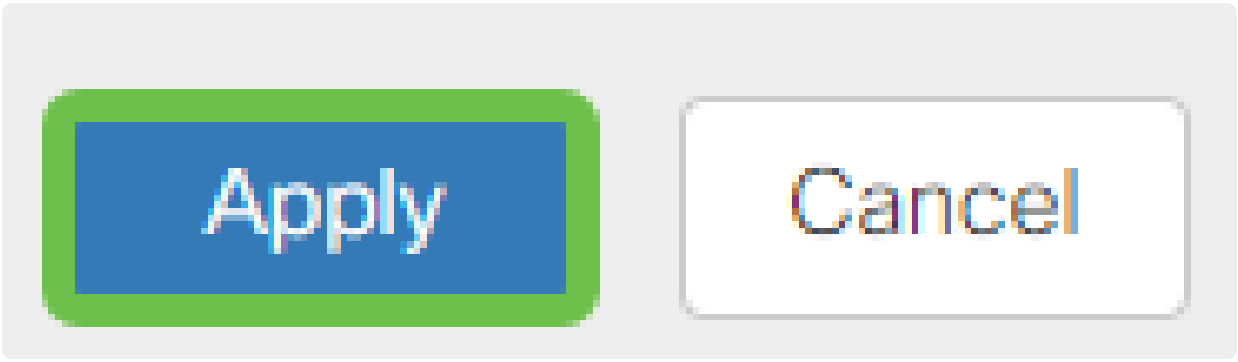
Fare clic su Edit per assegnare una VLAN a una porta LAN e specificare ciascuna impostazione come Tagged, Untagged o Excluded.

Nell'esempio, alla VLAN1 è stato assegnato il valore Untagged per la VLAN 1 e il valore Excluded per la VLAN 200. Alla VLAN 2 è stata assegnata la VLAN 1 come Esclusa e la VLAN 200 come Senza tag.



Passaggio 3

Fare clic su Apply (Applica) per salvare la configurazione.



La creazione di una nuova VLAN e la configurazione delle VLAN sulle porte della RV345P sono state completate. Ripetere la procedura per creare le altre VLAN. Ad esempio, la VLAN300 verrebbe creata per il reparto Marketing con una subnet di 192.168.3.x e la VLAN400 per il reparto Accounting con una subnet di 192.168.4.x.

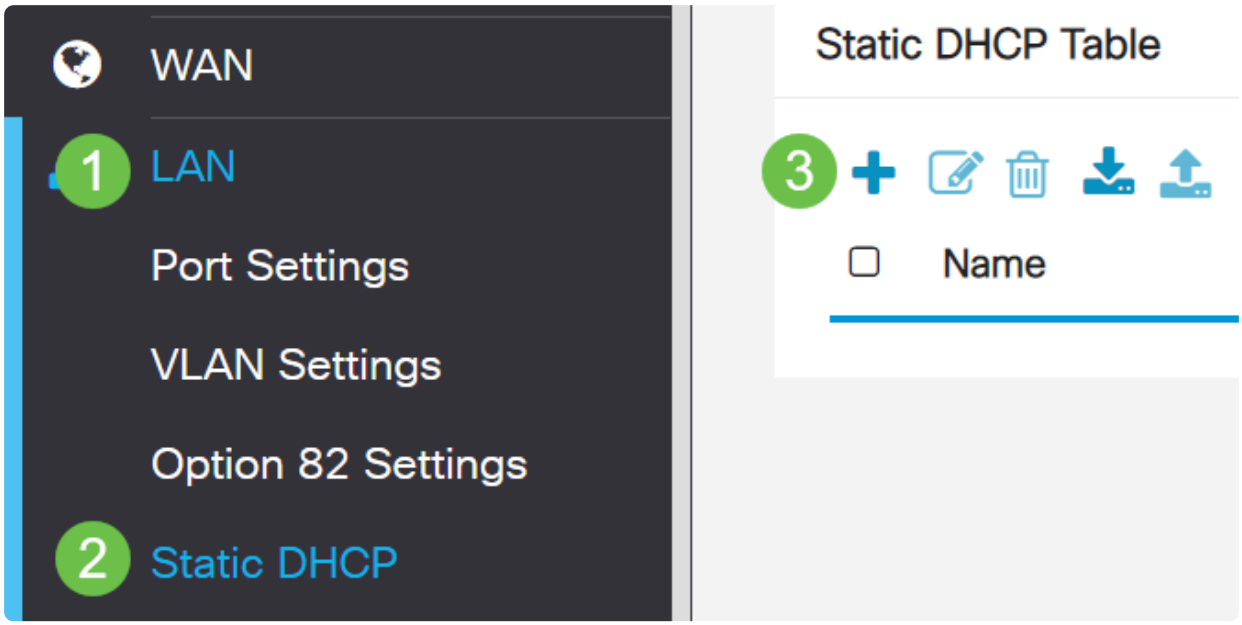
Aggiunta di un indirizzo IP statico (facoltativo)

Se si desidera che un determinato dispositivo sia raggiungibile da altre VLAN, è possibile assegnare a tale dispositivo un indirizzo IP locale statico e creare una regola di accesso per renderlo accessibile. Questa procedura funziona solo se è abilitato il routing tra VLAN. Ci sono altre situazioni in cui un indirizzo IP statico può essere utile. Per ulteriori informazioni sull'impostazione di indirizzi IP statici, vedere Procedure consigliate per l'impostazione di indirizzi IP statici su hardware aziendale Cisco.

Se non è necessario aggiungere un indirizzo IP statico, è possibile passare alla sezione successiva di questo articolo.

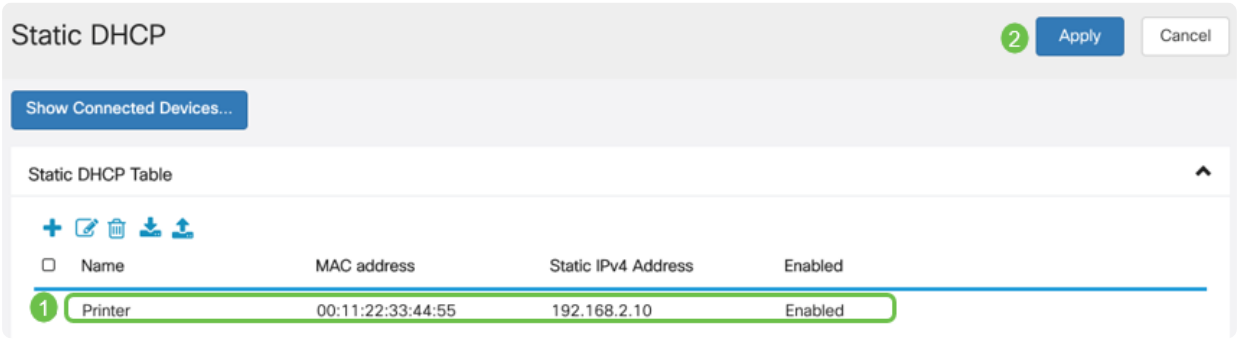
Passaggio 1

Andare a LAN > Static DHCP (LAN > DHCP statico). Fare clic sull'icona più.



Passaggio 2

Aggiungere le informazioni DHCP statiche per il dispositivo. In questo esempio, la periferica è una stampante.



Gestione dei certificati (facoltativo)

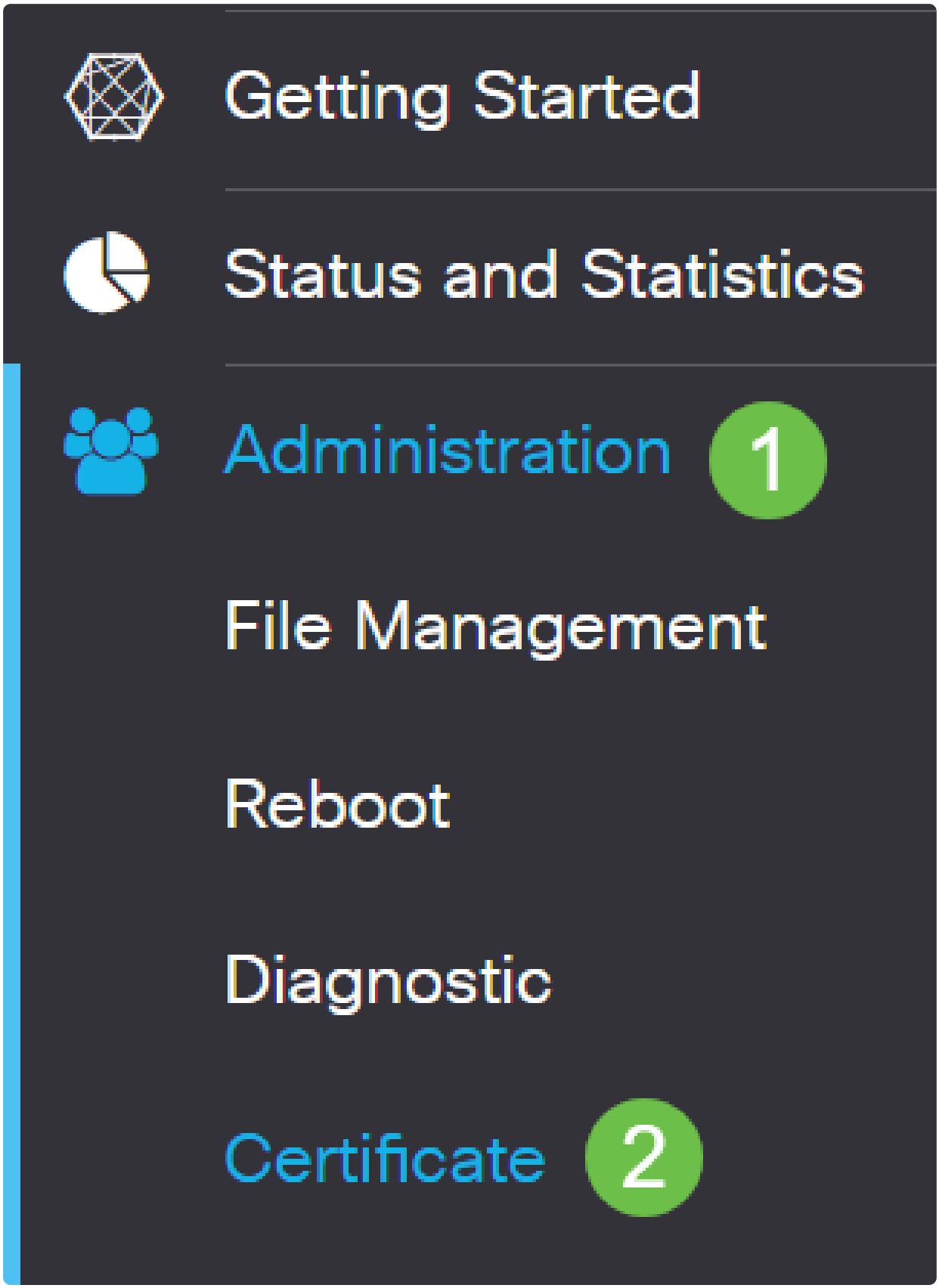
Un certificato digitale certifica la proprietà di una chiave pubblica da parte del soggetto specificato del certificato. In questo modo le relying party possono dipendere da firme o asserzioni effettuate dalla chiave privata corrispondente alla chiave pubblica certificata. Un router può generare un certificato autofirmato, ovvero un certificato creato da un amministratore di rete. Può inoltre inviare richieste alle Autorità di certificazione (CA) per richiedere un certificato di identità digitale. È importante disporre di certificati legittimi provenienti da applicazioni di terze parti.

Per l'autenticazione viene utilizzata un'Autorità di certificazione (CA). I certificati possono essere acquistati da diversi siti di terze parti. È un modo ufficiale per dimostrare che il tuo sito è sicuro. Essenzialmente, la CA è una fonte attendibile che verifica che l'azienda sia legittima e che possa essere considerata attendibile. A seconda delle esigenze, un certificato a un costo minimo. L'utente viene estratto dall'autorità di certificazione e, una volta verificate le informazioni, il certificato verrà rilasciato all'utente. Il certificato può essere scaricato come file nel computer. È quindi possibile accedere al router (o al server VPN) e caricarlo in tale posizione.

Genera CSR/certificato

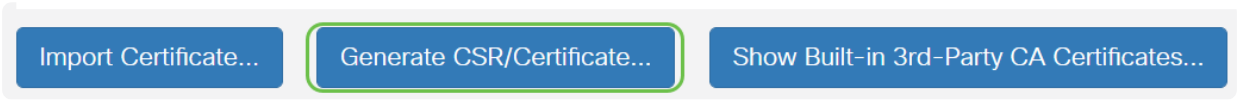
Passaggio 1

Accedere all'utility basata sul Web del router e scegliere Amministrazione > Certificato.


Getting Started
Status and Statistics
Administration
1
File Management
Reboot
Diagnostic
Certificate
2

Passaggio 2

Fare clic su Genera CSR/Certificato. Verrà visualizzata la pagina Genera CSR/certificato.



Passaggio 3

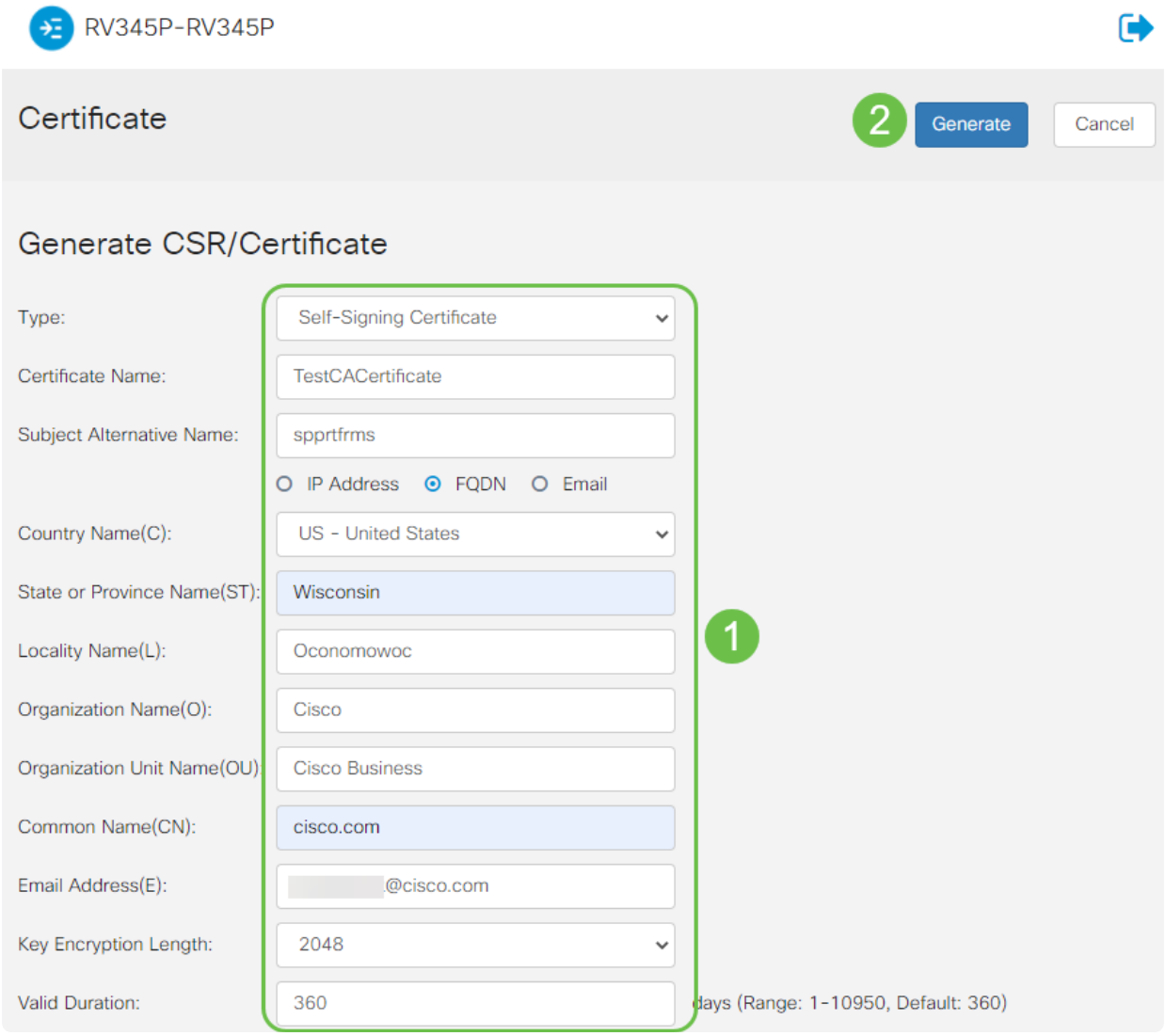
Compilare le caselle con quanto segue:

- Scegliere il tipo di certificato appropriato
    - Certificato con firma automatica - Si tratta di un certificato SSL (Secure Socket Layer) firmato dal proprio creatore. Il certificato è meno attendibile, in quanto non può essere annullato se la chiave privata viene in qualche modo compromessa da un utente non autorizzato.
    - Richiesta di firma certificata - Infrastruttura a chiave pubblica (PKI) inviata all'autorità di certificazione per richiedere un certificato di identità digitale. È più sicuro della firma automatica in quanto la chiave privata viene mantenuta segreta.
- Immettere un nome per il certificato nel campo Nome certificato per identificare la richiesta. Il campo non può essere vuoto né contenere spazi e caratteri speciali.
- (Facoltativo) Nell'area Nome alternativo soggetto fare clic su un pulsante di opzione. Le opzioni sono:
    - Indirizzo IP — Immettere un indirizzo IP (Internet Protocol)
    - FQDN — immettere un nome di dominio completo (FQDN)
    - Posta elettronica - immettere un indirizzo di posta elettronica

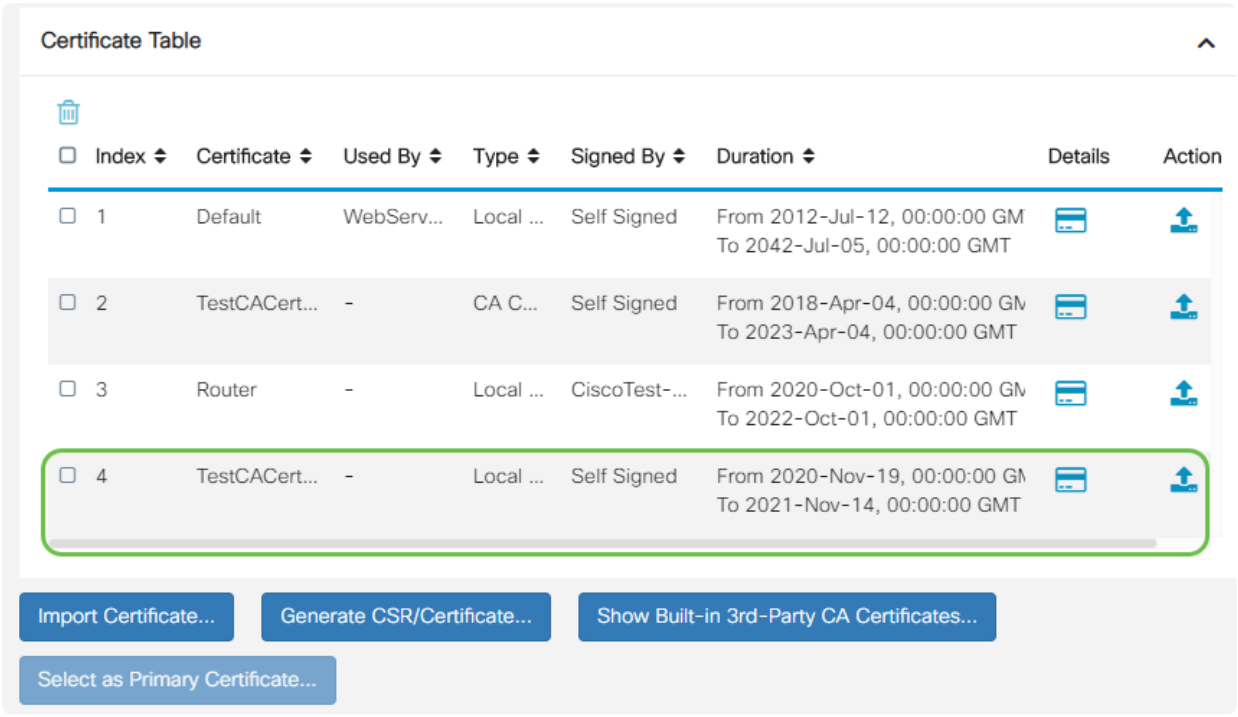
- Nel campo Nome alternativo soggetto immettere il nome di dominio completo.
- Dall'elenco a discesa Country Name (Nome paese), selezionare il nome del paese in cui l'organizzazione è legalmente registrata.
- Inserire il nome o l'abbreviazione dello stato, della provincia, della regione o del territorio in cui si trova l'organizzazione nel campo Nome stato o provincia (ST).
- Nel campo Nome località immettere il nome della località o della città in cui è registrata l'organizzazione.
- Immettere un nome con il quale l'azienda è legalmente registrata. Se ci si iscrive come piccola impresa o come proprietario unico, immettere il nome del richiedente del certificato nel campo Nome organizzazione. Non è possibile utilizzare caratteri speciali.
- Inserire un nome nel campo Nome unità organizzazione per distinguere tra le

divisioni all'interno di un'organizzazione.

- Immettere un nome nel campo Nome comune. Questo nome deve essere il nome di dominio completo del sito Web per il quale si utilizza il certificato.
- Immettere l'indirizzo di posta elettronica della persona che desidera generare il certificato.
- Dall'elenco a discesa Lunghezza crittografia chiave, scegliere la lunghezza della chiave. Le opzioni sono 512, 1024 e 2048. Maggiore è la lunghezza della chiave, più sicuro sarà il certificato.
- Nel campo Durata valida immettere il numero di giorni di validità del certificato. Il valore predefinito è 360.
- Fare clic su Genera.



ⓘ Note: Il certificato generato verrà visualizzato nella tabella Certificati.

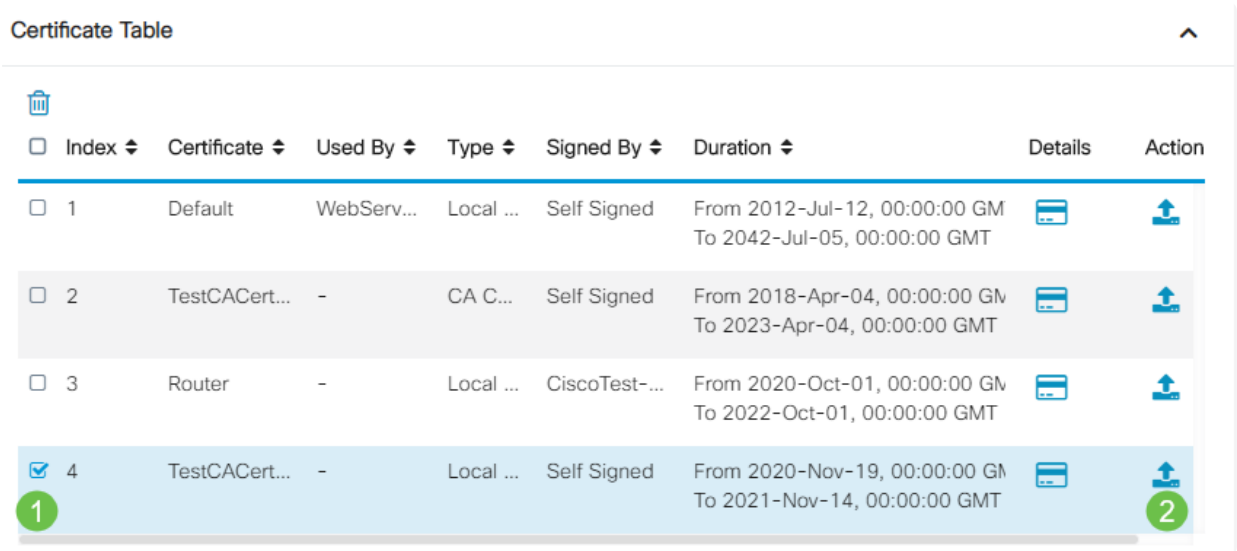


A questo punto, è necessario aver creato correttamente un certificato sul router RV345P.

Esportare un certificato

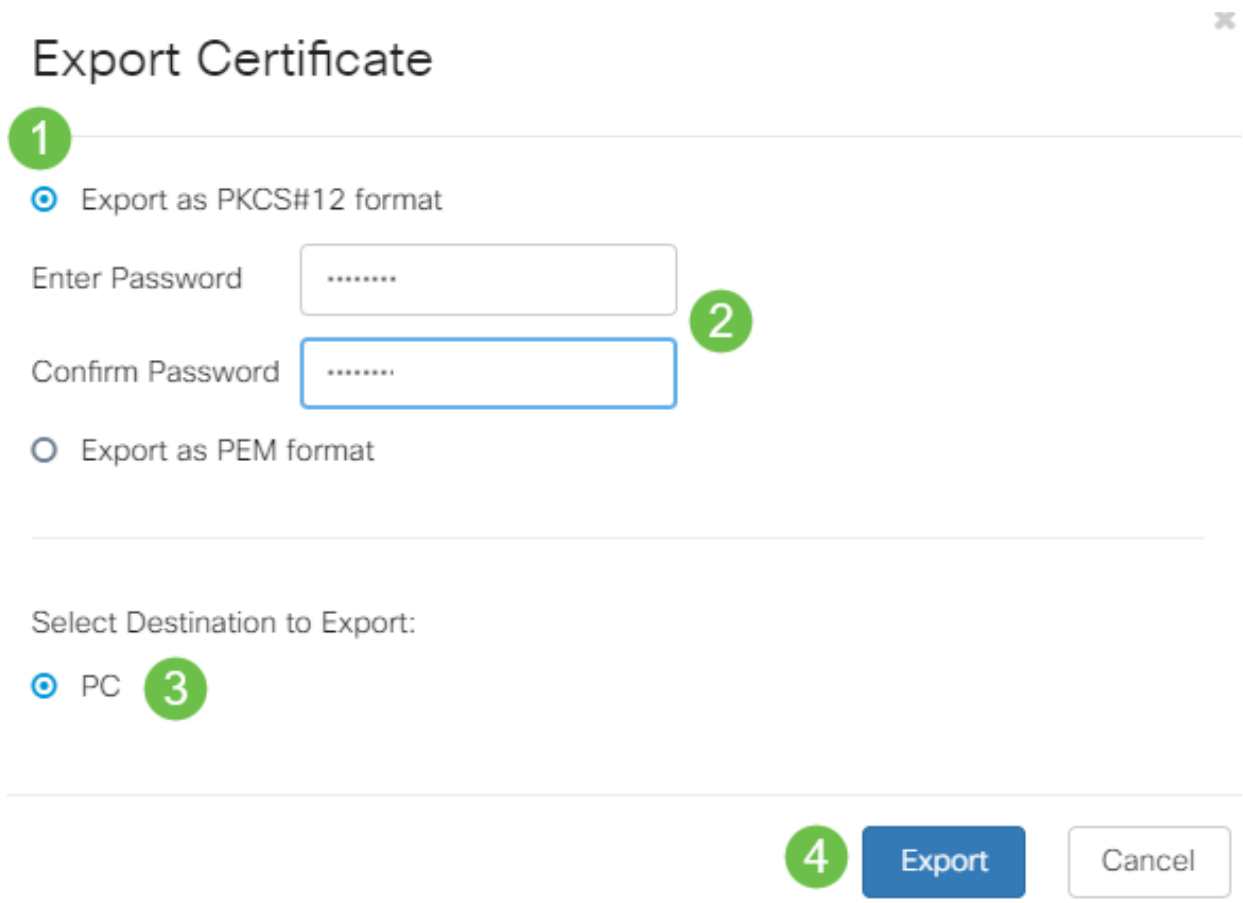
Passaggio 1

Nella tabella Certificati selezionare la casella di controllo del certificato che si desidera esportare e fare clic sull'icona Esporta.



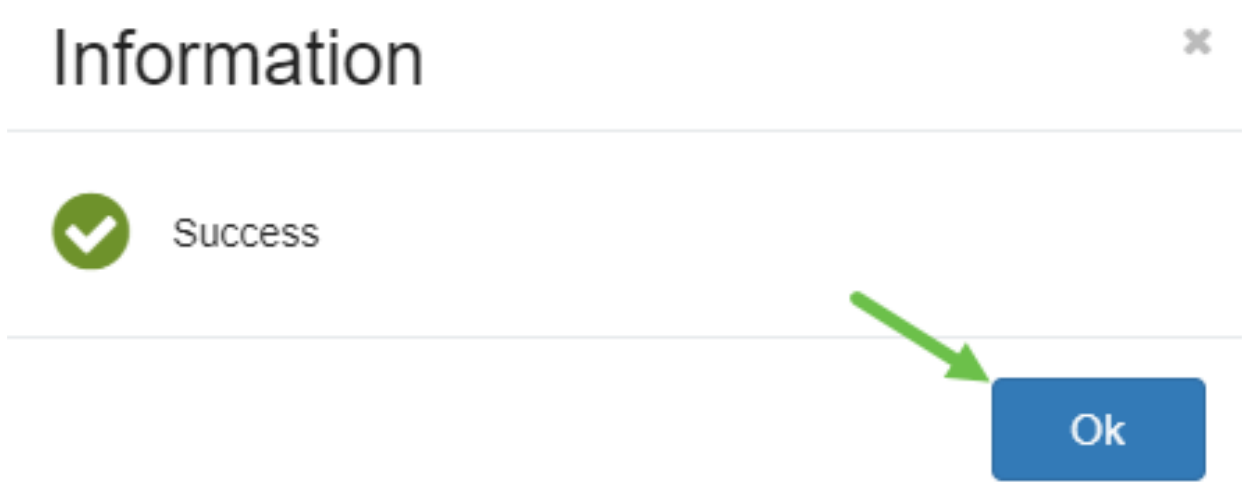
Passaggio 2

- Selezionare un formato per esportare il certificato. Le opzioni sono:
  - PKCS #12 — Public Key Cryptography Standards (PKCS) #12 è un certificato esportato con estensione .p12. Per crittografare il file e proteggerlo durante l'esportazione, l'importazione e l'eliminazione è necessaria una password.
  - PEM — Privacy Enhanced Mail (PEM) è spesso utilizzato per i server Web per la loro capacità di essere facilmente tradotti in dati leggibili utilizzando un semplice editor di testo come il Blocco note.
- Se si sceglie PEM, fare clic su Esporta.
- Immettere una password per proteggere il file da esportare nel campo Immettere password.
- Immettere nuovamente la password nel campo Conferma password.
- Nell'area Seleziona destinazione è stato scelto PC, l'unica opzione attualmente disponibile.
- Fare clic su Esporta.



Passaggio 3

Sotto il pulsante Download viene visualizzato un messaggio che indica che il download è riuscito. Verrà avviato il download di un file nel browser. Fare clic su OK.



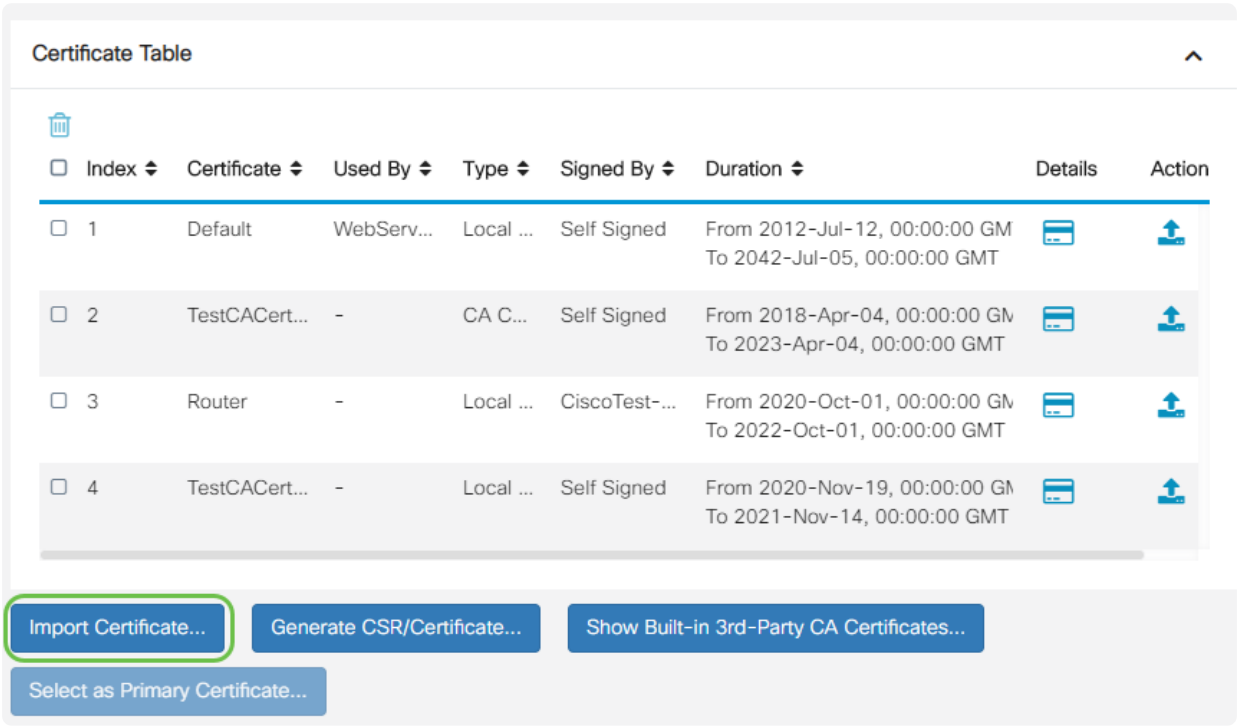
A questo punto, il certificato sul router serie RV345P dovrebbe essere stato esportato

correttamente.

Importa certificato

Passaggio 1

Fare clic su Importa certificato....



Passaggio 2

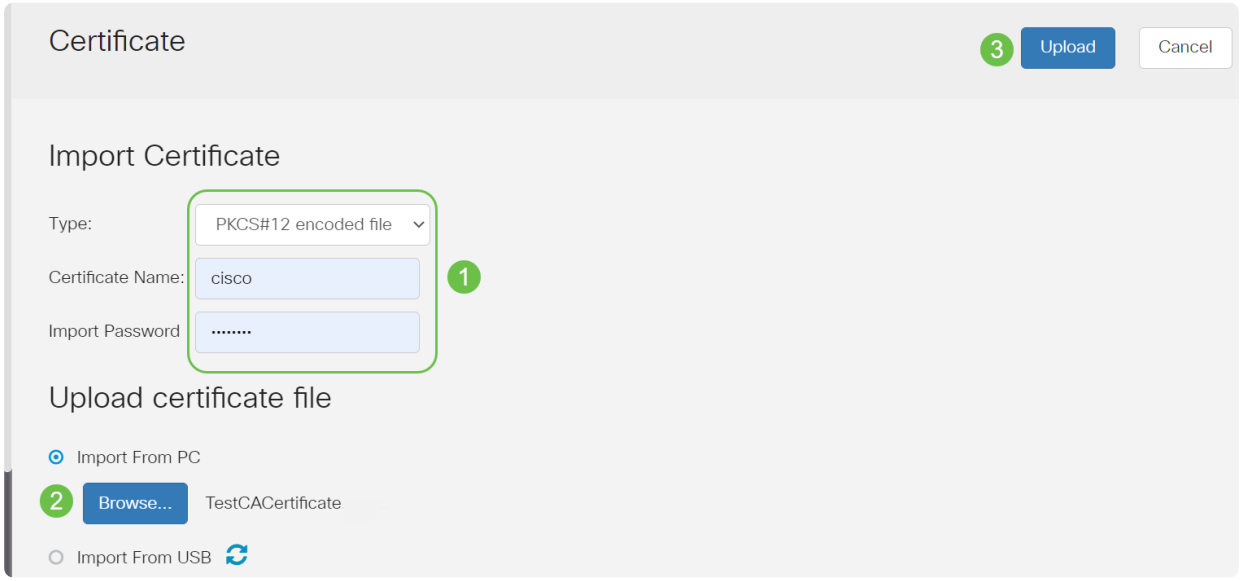
- Selezionare dall'elenco a discesa il tipo di certificato da importare. Le opzioni sono:
  - Certificato locale — Un certificato generato sul router.
  - Certificato CA - Certificato certificato da un'autorità di terze parti attendibile che ha confermato l'accuratezza delle informazioni contenute nel certificato.
  - File codificato PKCS #12 — PKCS (Public Key Cryptography Standards) #12 è un formato di archiviazione di un certificato server.

- Immettere un nome per il certificato nel campo Nome certificato.
- Se è stato scelto PKCS #12, immettere una password per il file nel campo Password

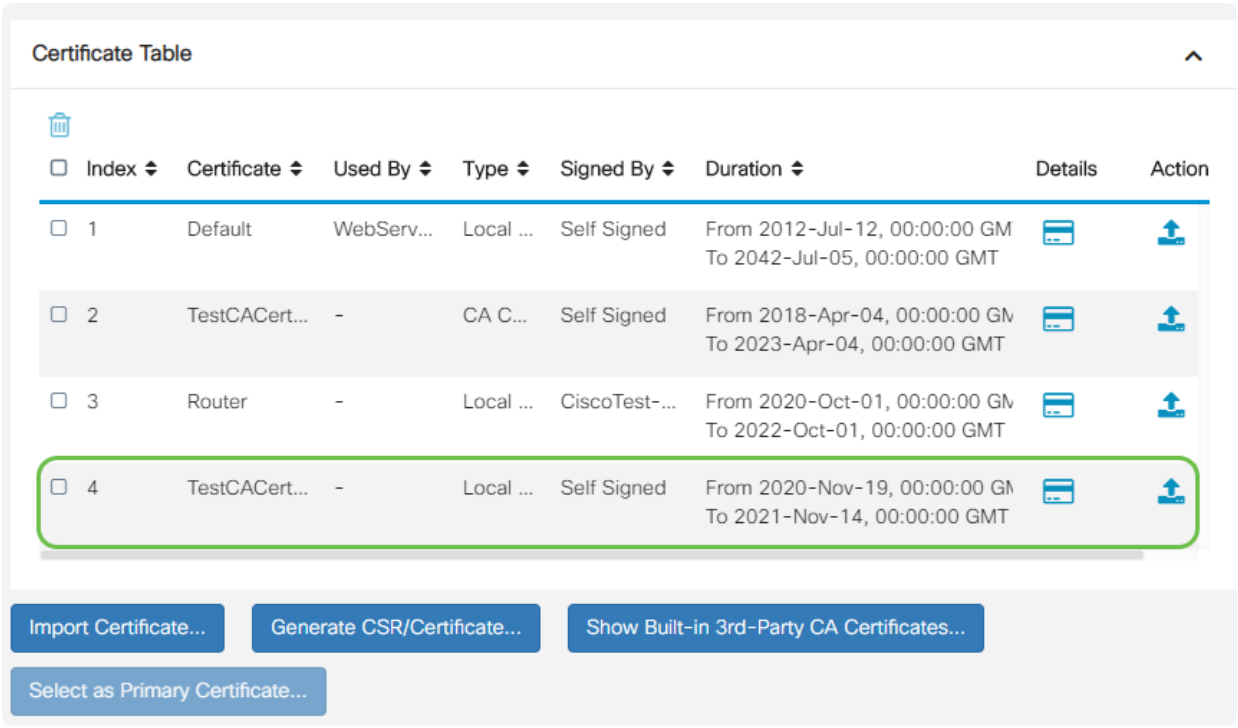
di importazione. In caso contrario, andare al passaggio 3.

- Fare clic su un'origine per importare il certificato. Le opzioni sono:
    - Importa da PC
    - Importa da USB

- Se il router non rileva un'unità USB, l'opzione Import from USB (Importa da USB) non è disponibile.
- Se si sceglie Importa da USB e il dispositivo USB non viene riconosciuto dal router, fare clic su Aggiorna.
- Fare clic sul pulsante Scegli file e scegliere il file appropriato.
- Fare clic su Upload.



Se l'operazione ha esito positivo, verrà visualizzata automaticamente la pagina principale del certificato. Nella tabella dei certificati verrà inserito il certificato importato di recente.



A questo punto, è possibile importare un certificato sul router RV345P.

Configurazione di una rete mobile con un dongle e un router serie RV345P (opzionale)

È possibile configurare una rete mobile di backup utilizzando un dongle e il router RV345P. In questo caso, consultare il documento sulla configurazione di una rete mobile con un dongle e un router serie RV34x.

Congratulazioni, avete completato la configurazione del router RV345P! A questo punto, è possibile configurare i dispositivi Cisco Business Wireless.

Configurazione di CBW140AC

CBW140AC

Innanzitutto, collegare un cavo Ethernet dalla porta PoE del CBW140AC a una porta PoE dell'RV345P. Le prime 4 porte dell'RV345P possono fornire PoE, quindi è possibile utilizzare qualsiasi porta.

Controllare lo stato delle spie. L'avvio del punto di accesso richiede circa 10 minuti. Il LED lampeggerà in verde a più tonalità, alternando rapidamente verde, rosso e giallo prima di tornare verde. L'intensità e la tonalità dei LED possono variare leggermente da un'unità all'altra. Quando la spia LED lampeggia in verde, procedere al passaggio successivo.

La porta uplink PoE Ethernet sull'access point primario può essere utilizzata SOLO per fornire un uplink alla LAN e NON per collegarsi ad altri dispositivi primari compatibili o di estensione mesh.

Se il punto di accesso non è nuovo, accertarsi che sia ripristinato alle impostazioni predefinite di fabbrica per il SSID Cisco Business-Setup da visualizzare nelle opzioni Wi-Fi. Per assistenza, vedere Come riavviare e ripristinare le impostazioni predefinite sui router RV345x.

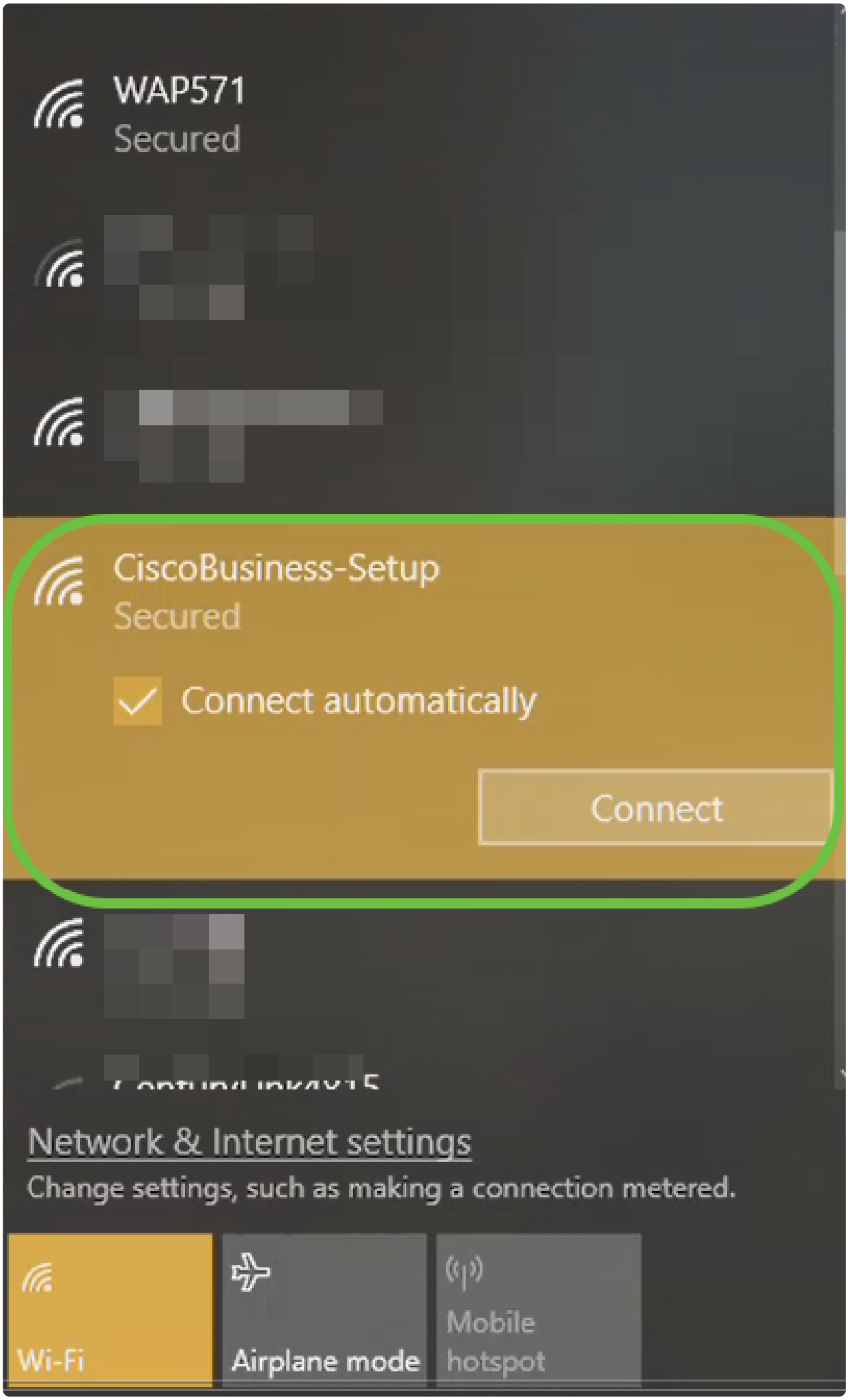
Configurazione del punto di accesso wireless primario 140AC sull'interfaccia utente Web

È possibile configurare il punto di accesso utilizzando l'applicazione mobile o l'interfaccia utente Web. In questo articolo viene utilizzata l'interfaccia utente Web per l'installazione, che offre più opzioni di configurazione ma è un po' più complicata. Se si desidera utilizzare l'applicazione per dispositivi mobili per le sezioni successive, fare clic su per accedere alle istruzioni dell'applicazione per dispositivi mobili.

In caso di problemi di connessione, fare riferimento alla sezione Suggerimenti per la risoluzione dei problemi wireless di questo articolo.

Passaggio 1

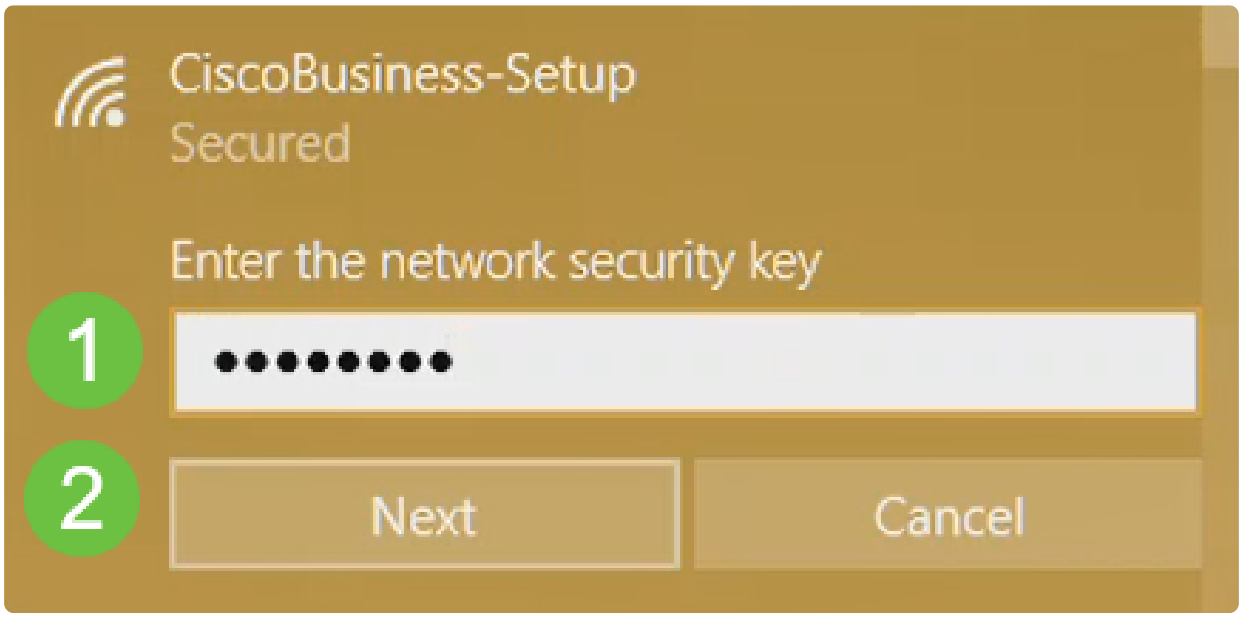
Sul PC, fare clic sull'icona Wi-Fi e scegliere Cisco Business-Setup rete wireless. Fare clic su Connetti.


WAP571
Secured
CiscoBusiness-Setup
Secured
Connect automatically
Connect
Network & Internet settings
Change settings, such as making a connection metered.
Wi-Fi
Airplane mode
Mobile hotspot

Se il punto di accesso non è nuovo, accertarsi che sia ripristinato alle impostazioni predefinite di fabbrica per il SSID Cisco Business-Setup da visualizzare nelle opzioni Wi-Fi.

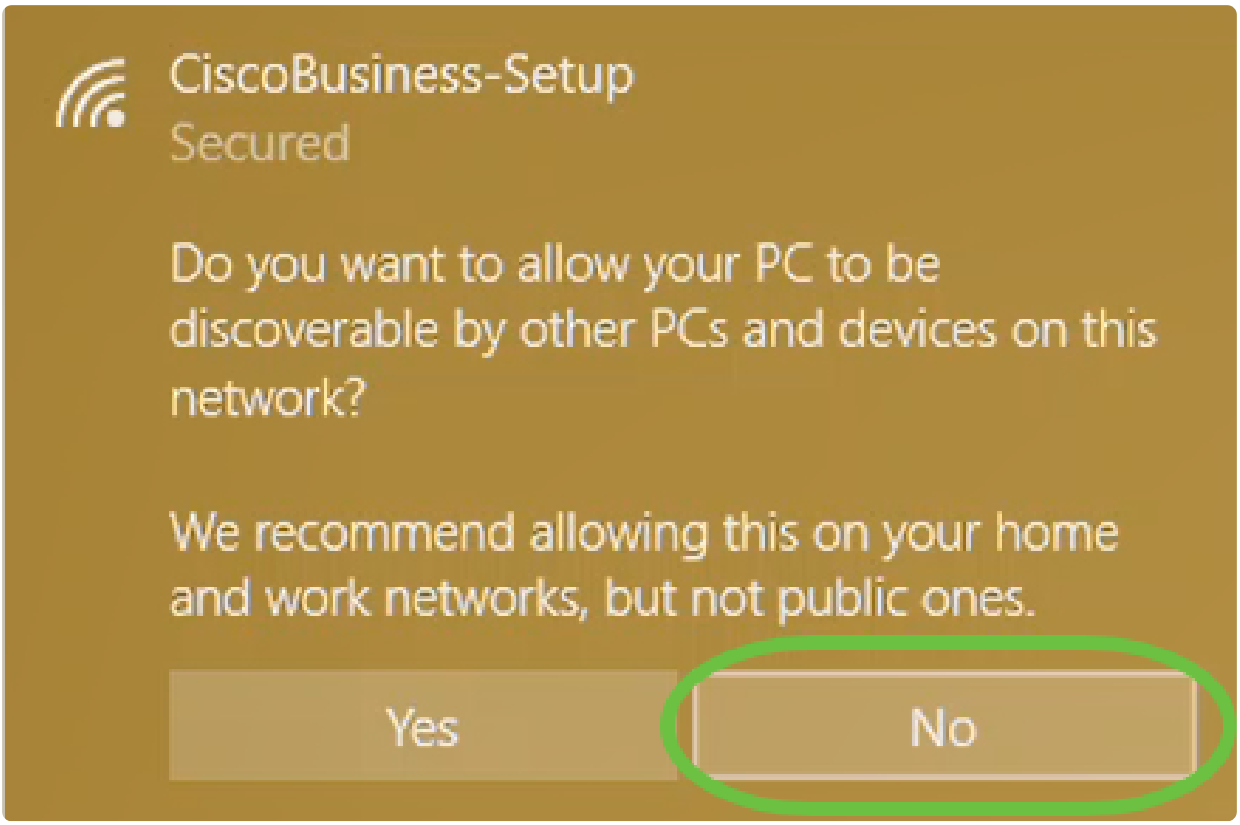
Passaggio 2

Immettere la passphrase cisco123 e fare clic su Avanti.



Passaggio 3

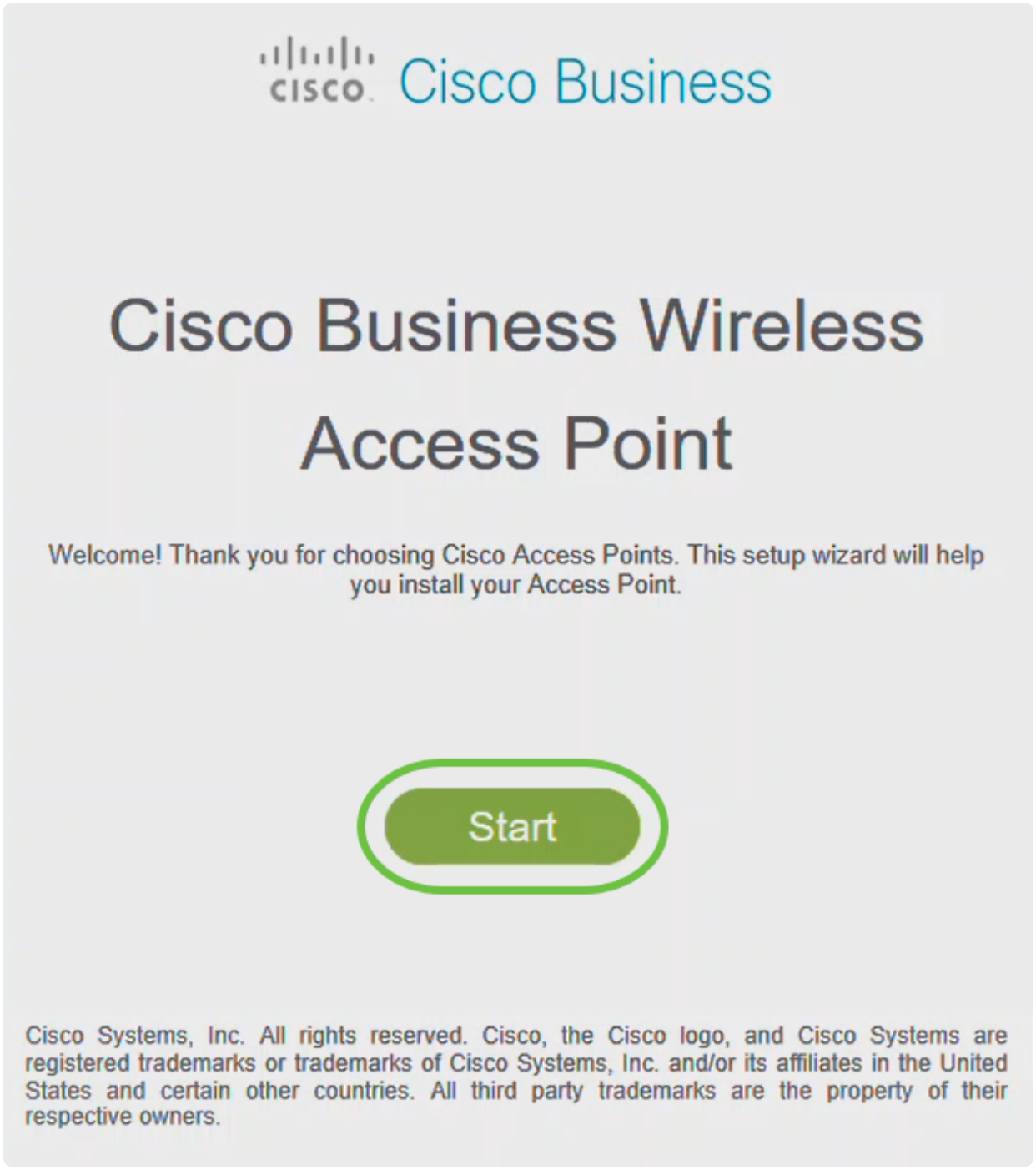
Viene visualizzata la seguente schermata. Poiché è possibile configurare un solo dispositivo alla volta, fare clic su No.



È possibile connettere un solo dispositivo all'SSID Cisco Business-Setup. Se un secondo dispositivo tenta di connettersi, non sarà in grado di connettersi. Se non è possibile connettersi all'SSID ed è stata convalidata la password, è possibile che la connessione sia stata stabilita da un'altra periferica. Riavviare il punto di accesso e riprovare.

Passaggio 4

Una volta connesso, il browser Web deve reindirizzare automaticamente alla procedura guidata CBW AP setup. In caso contrario, aprire un browser Web, ad esempio Internet Explorer, Firefox, Chrome o Safari. Nella barra degli indirizzi, digitare http://ciscobusiness.cisco e premere Invio. Fare clic su Start nella pagina Web.



ⓘ Note: Se la pagina Web non viene visualizzata, attendere qualche minuto o ricaricarla. Dopo questa configurazione iniziale, utilizzare https://ciscobusiness.cisco per eseguire il login. Se il browser Web viene compilato automaticamente con http://, per ottenere l'accesso è necessario digitare manualmente il testo https://.

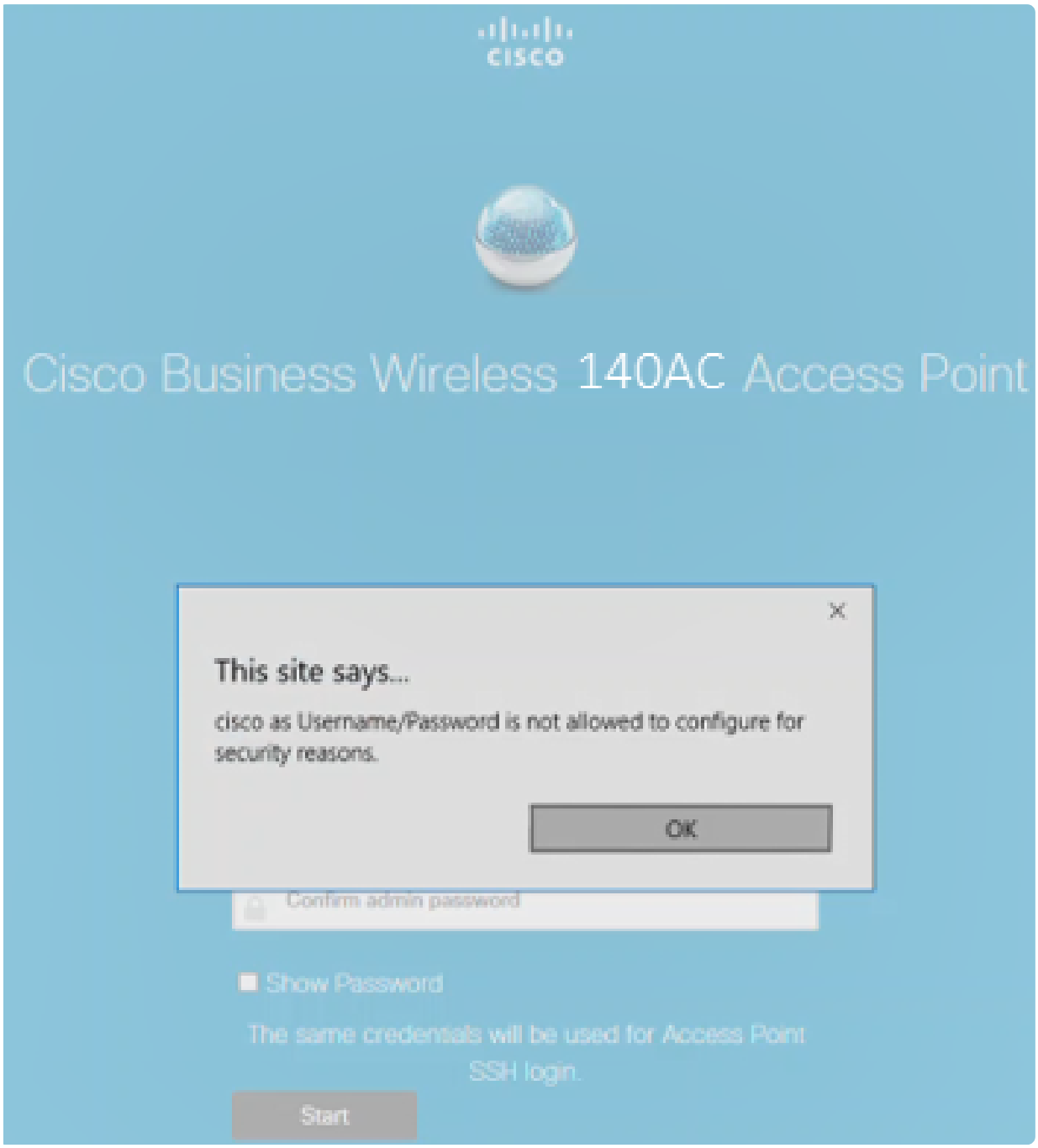
Passaggio 5

Creare un account admin immettendo quanto segue:

- Nome utente amministratore (massimo 24 caratteri)
- Password amministratore
- Conferma password amministratore

È possibile scegliere di visualizzare la password selezionando la casella di controllo accanto a Mostra password. Fare clic su Start.

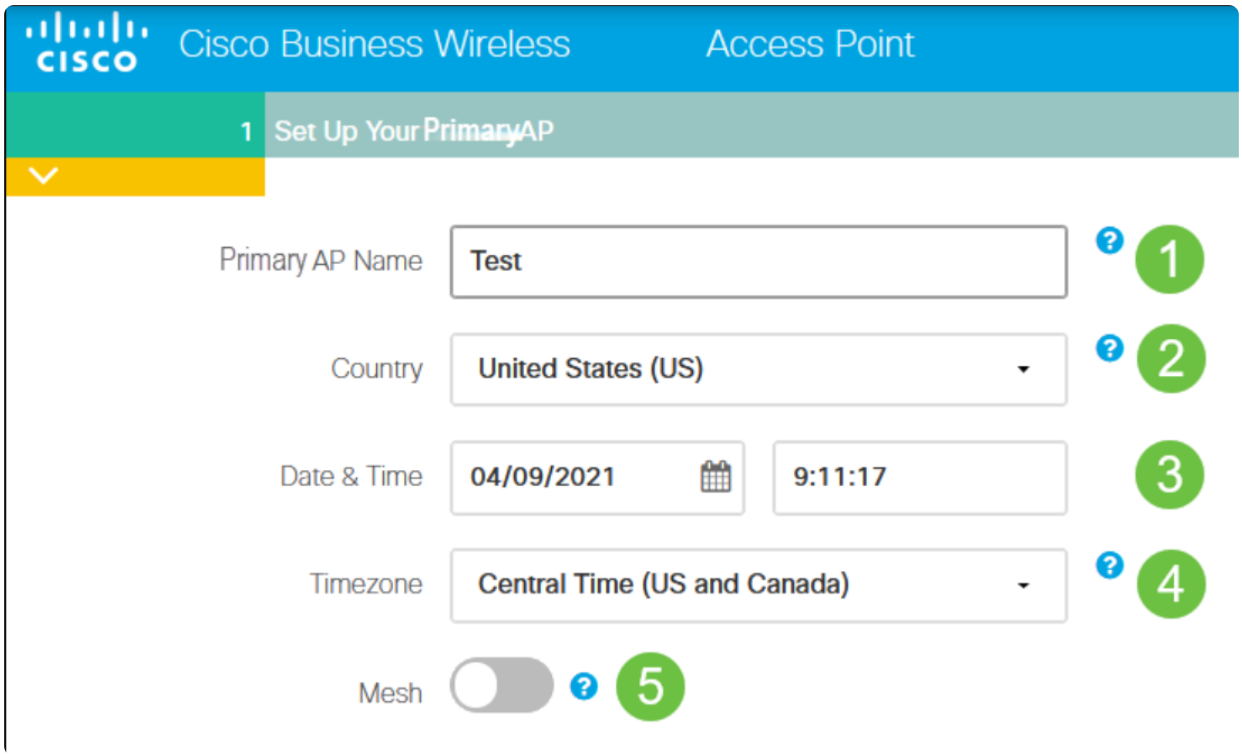
Non utilizzare cisco o sue varianti nei campi del nome utente o della password. In caso contrario, verrà visualizzato un messaggio di errore come illustrato di seguito.



Passaggio 6

Impostare l'access point principale immettendo quanto segue:

- Nome punto di accesso primario
- Paese
- Data e ora
- Fuso orario
- Mesh



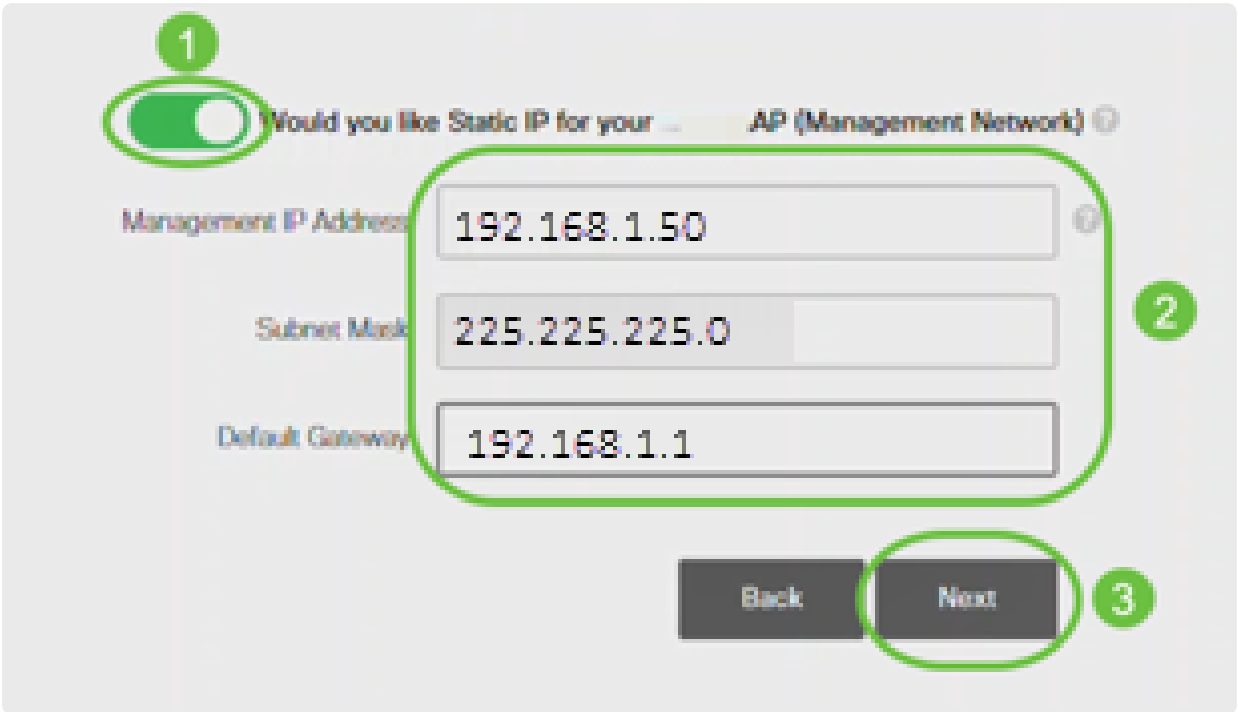
Mesh deve essere abilitato solo se si intende creare una rete mesh. Per impostazione predefinita, è disattivata.

Passaggio 7

(Facoltativo) È possibile abilitare l'indirizzo IP statico per il CBW140AC a scopo di gestione. In caso contrario, l'interfaccia riceve un indirizzo IP dal server DHCP. Per configurare l'IP statico, immettere quanto segue:

- Indirizzo IP di gestione
- Subnet mask
- Gateway predefinito

Fare clic su Next (Avanti).



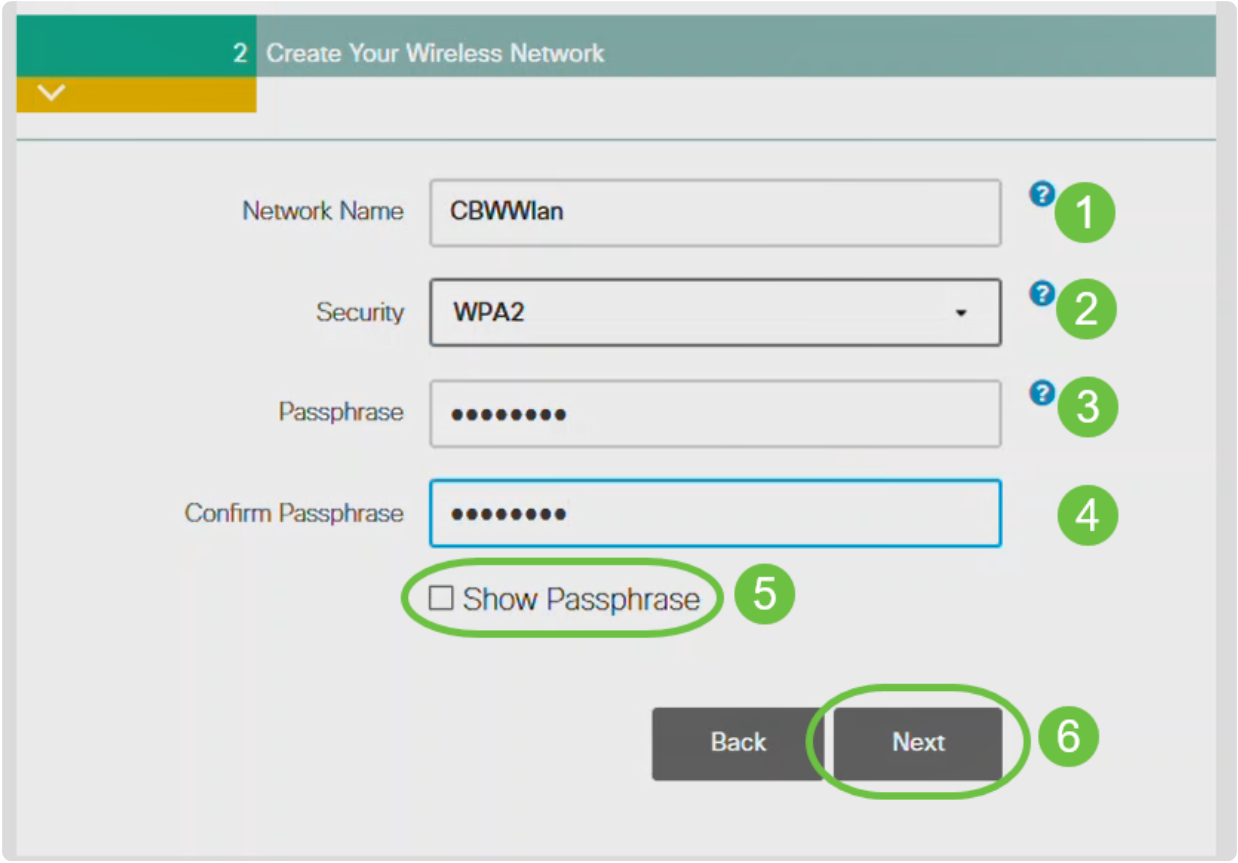
Per impostazione predefinita, questa opzione è disattivata.

Passaggio 8

Creare le reti wireless immettendo quanto segue:

- Nome rete
- Scegli sicurezza
- Passphrase
- Conferma passphrase
- (Facoltativo) Selezionare la casella di controllo Mostra passphrase.

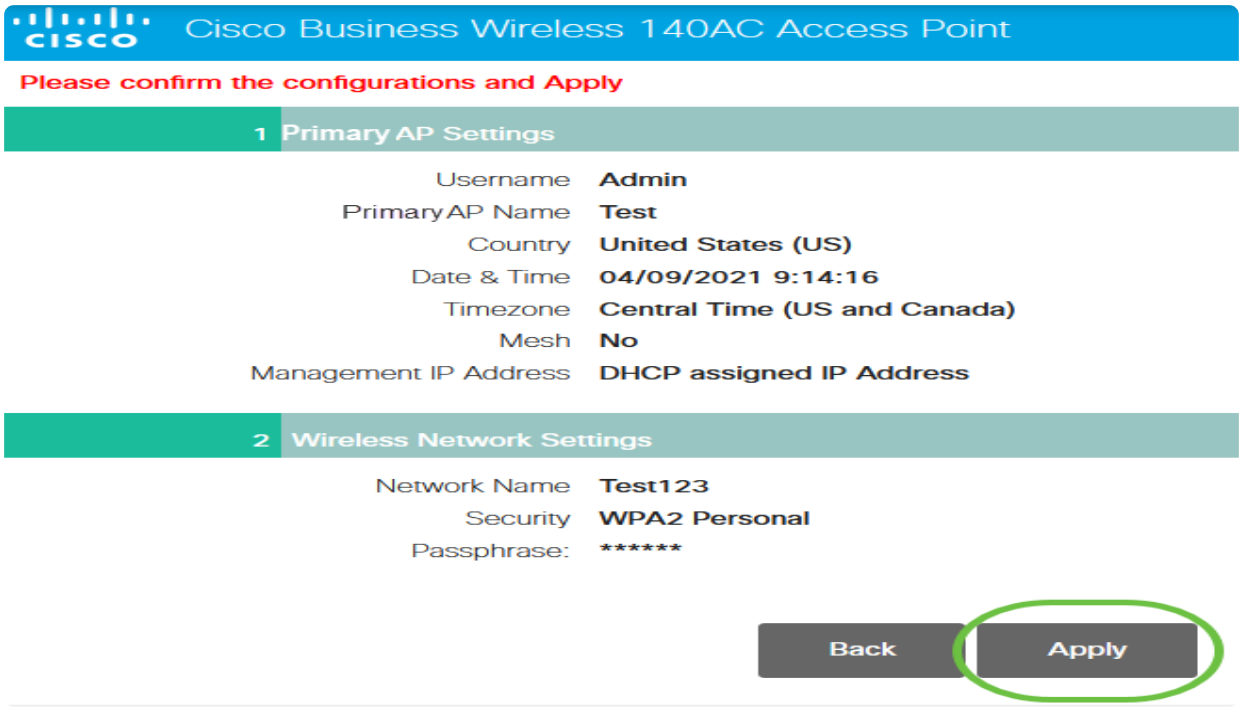
Fare clic su Next (Avanti).



Wi-Fi protected Access (WPA) versione 2 (WPA2) è lo standard corrente per la sicurezza Wi-Fi.

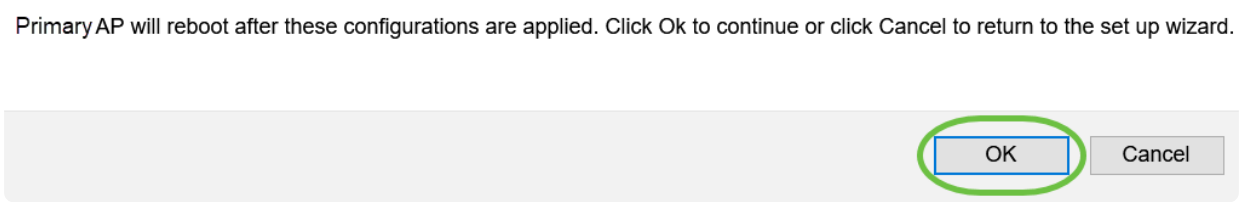
Passaggio 9

Confermare le impostazioni e fare clic su Applica.

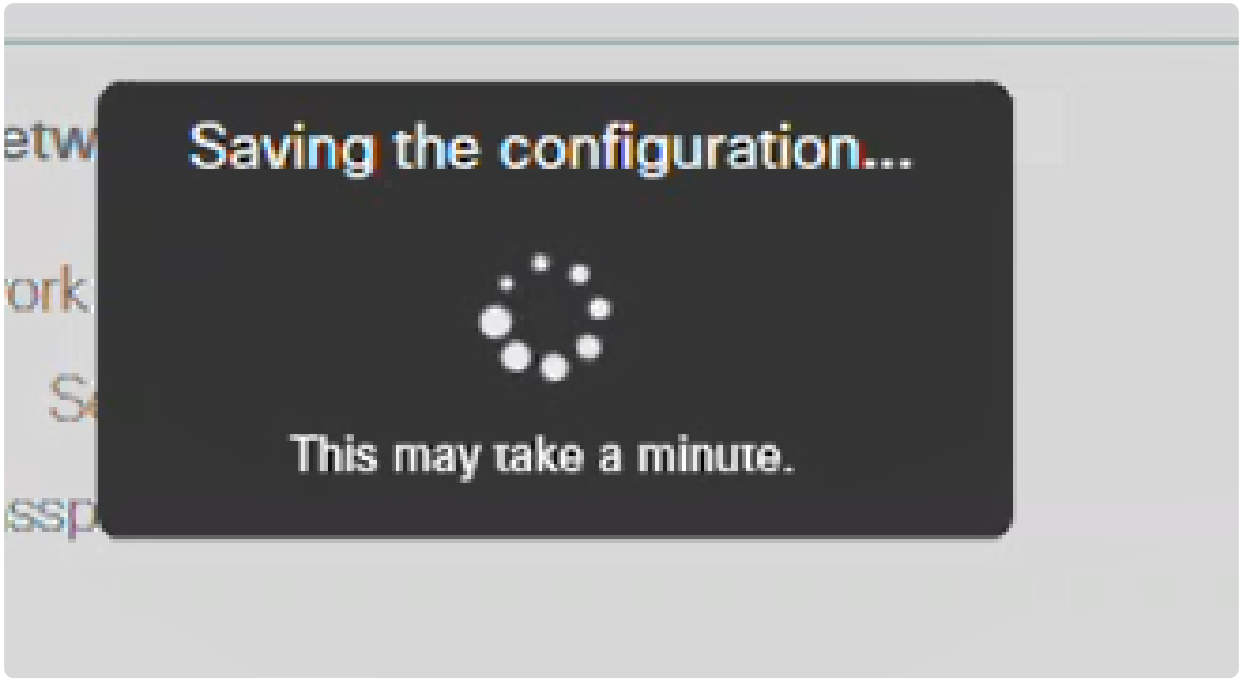


Passaggio 10

Fare clic su OK per applicare le impostazioni.



Durante il salvataggio delle configurazioni e il riavvio del sistema viene visualizzata la seguente schermata. L'operazione potrebbe richiedere 10 minuti.

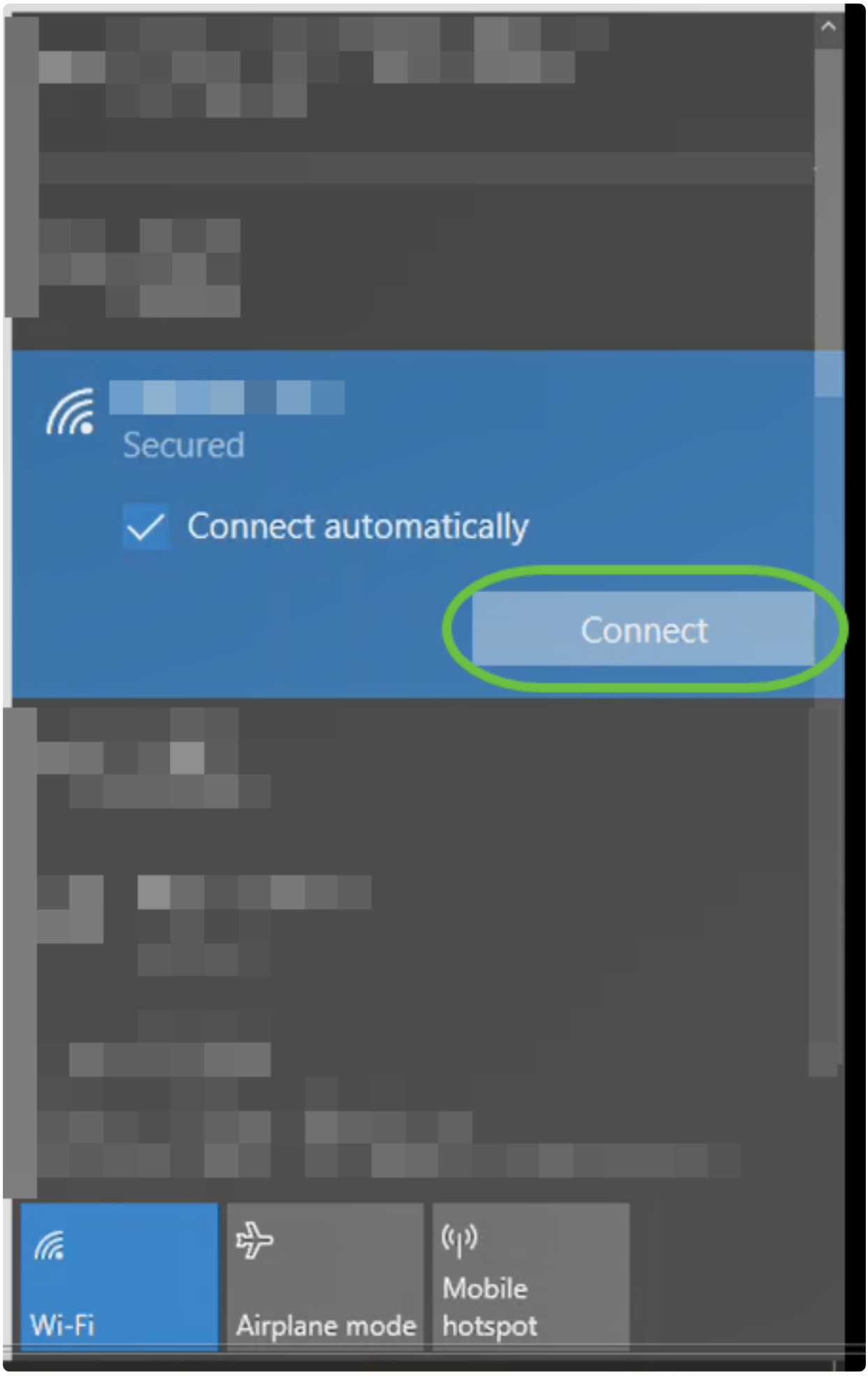


Durante il riavvio, il LED nel punto di accesso passa attraverso diversi modelli di colore. Quando il LED lampeggia in verde, procedere al passaggio successivo. Se il LED non supera il motivo rosso lampeggiante, significa che nella rete non è presente alcun server DHCP. Verificare che l'access point sia collegato a uno switch o a un router con un server DHCP.

Passaggio 11

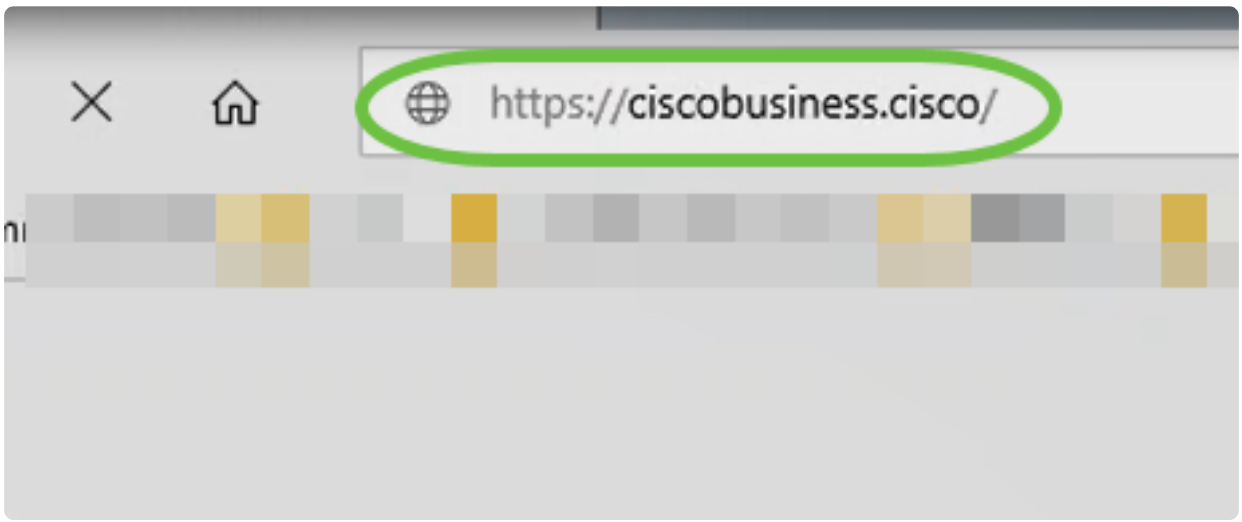
Accedere alle opzioni wireless del PC e scegliere la rete configurata. Fare clic su Connetti.

Il SSID Cisco Business-Setup scompare dopo il riavvio.


Secured
Connect automatically
Connect
Wi-Fi
Airplane mode
Mobile hotspot

Passaggio 12

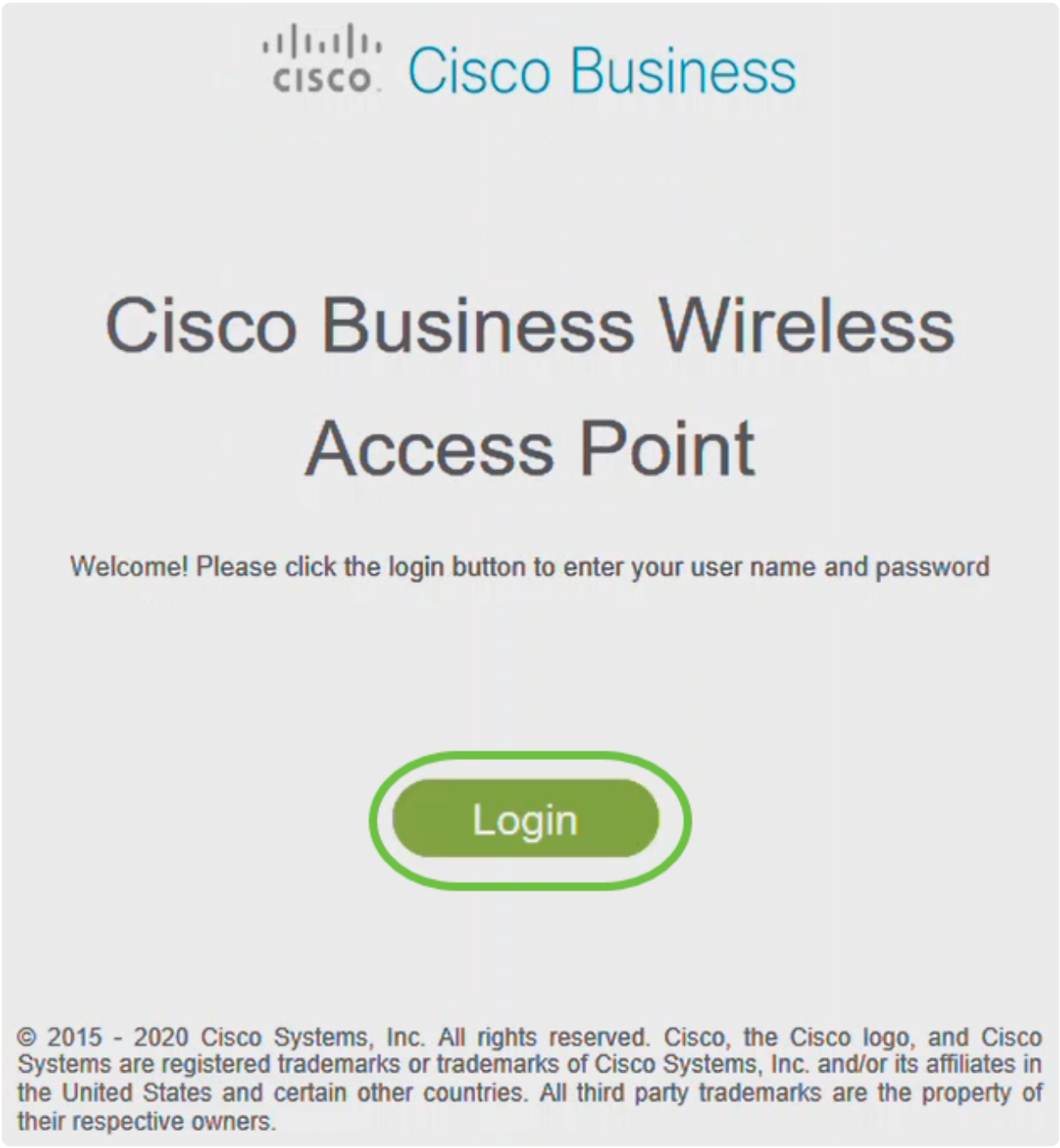
Aprire un browser Web e digitare https://[indirizzo IP dell'access point CBW]. In alternativa, digitare https://ciscobusiness.cisco nella barra degli indirizzi e premere Invio.



ⓘ Note: In questo passaggio, verificare di aver digitato https e non http.

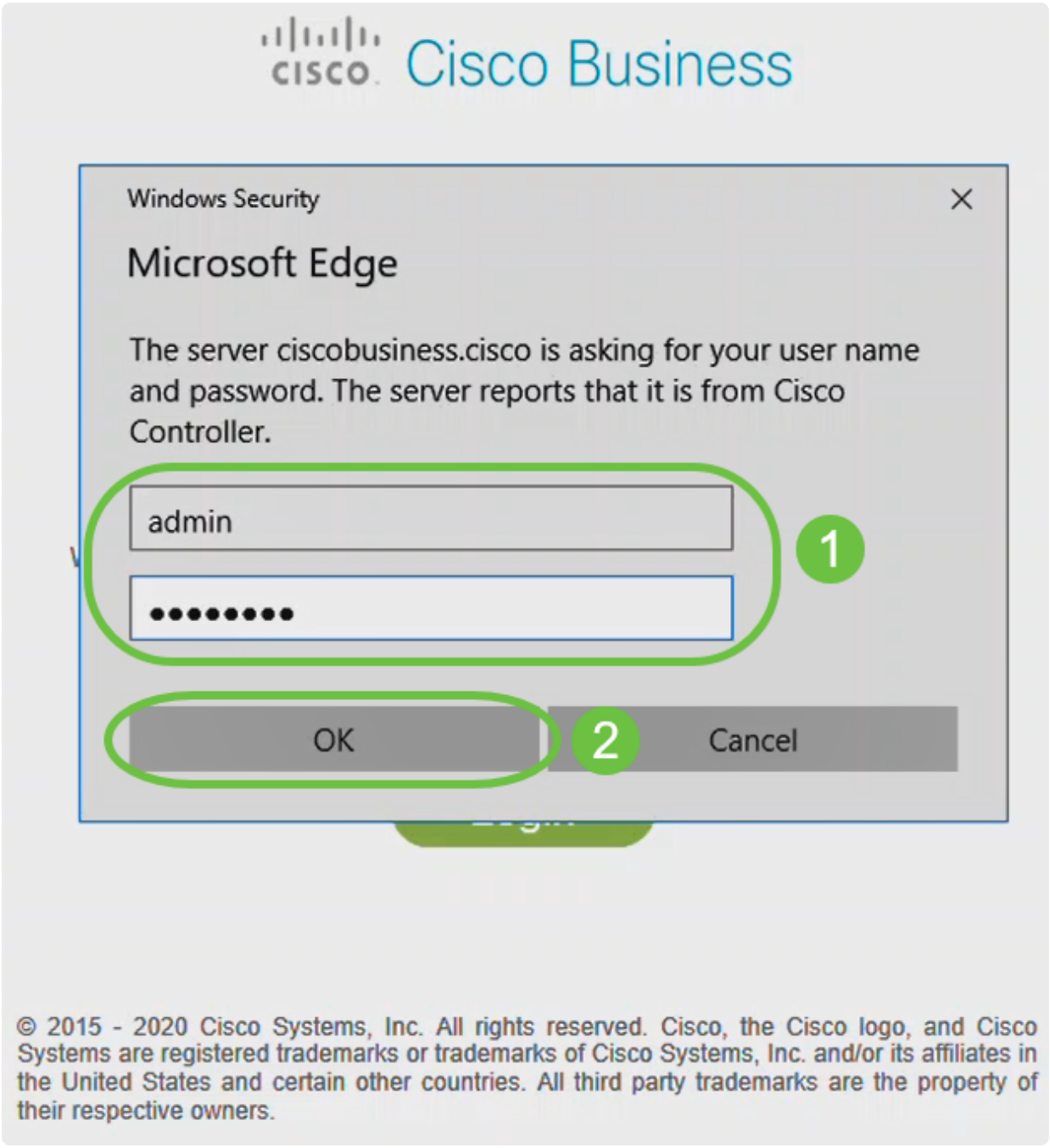
Passaggio 13

Fare clic su Login.



Passaggio 14

Accedere utilizzando le credenziali configurate. Fare clic su OK.



Passaggio 15

Sarà possibile accedere alla pagina dell'interfaccia utente Web dell'access point.

Suggerimenti per la risoluzione dei problemi wireless

In caso di problemi, consultare i seguenti suggerimenti:

- Assicurarsi che sia selezionato l'SSID (Service Set Identifier) corretto. Questo è il nome creato per la rete wireless.
- Disconnetti qualsiasi VPN per l'app per dispositivi mobili o su un laptop. Potresti anche essere connesso a una VPN che il tuo provider di servizi mobili utilizza e che potresti non conoscere. Ad esempio, un telefono Android (Pixel 3) con Google Fi come provider di servizi c'è una VPN integrata che si connette automaticamente senza notifica. Per trovare il punto di accesso primario, è necessario disattivare questa opzione.
- Accedere all'access point primario con https://<indirizzo IP dell'access point primario>.
- Dopo aver eseguito la configurazione iniziale, verificare che il sito https:// is venga utilizzato per accedere a ciscobusiness.cisco o per immettere l'indirizzo IP nel browser Web. A seconda delle impostazioni configurate, è possibile che nel computer sia stato inserito automaticamente http:// since, che corrisponde a quello utilizzato la prima volta che si è effettuato l'accesso.
- Per risolvere i problemi relativi all'accesso all'interfaccia utente Web o al browser durante l'uso dell'access point, nel browser Web (in questo caso Firefox) fare clic sul menu Apri, selezionare? > Informazioni per la risoluzione dei problemi e fare clic su Aggiorna Firefox.

Configurazione dei CBW142ACM Mesh Extender tramite interfaccia utente Web

Sei nella fase iniziale di configurazione di questa rete, è sufficiente aggiungere le tue estensioni mesh!

Passaggio 1

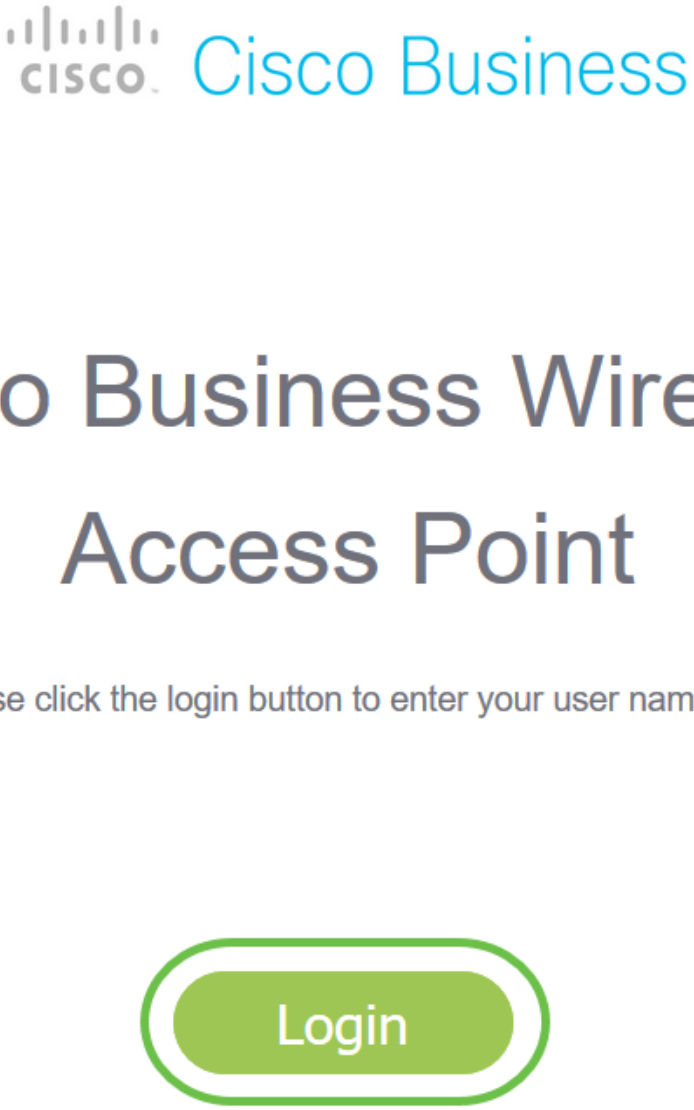
Collegare i due estensori di rete alla parete nelle posizioni selezionate. Prendere nota dell'indirizzo MAC di ciascuna estensione di rete.

Passaggio 2

Attendere circa 10 minuti l'avvio dei dispositivi Mesh Extender.

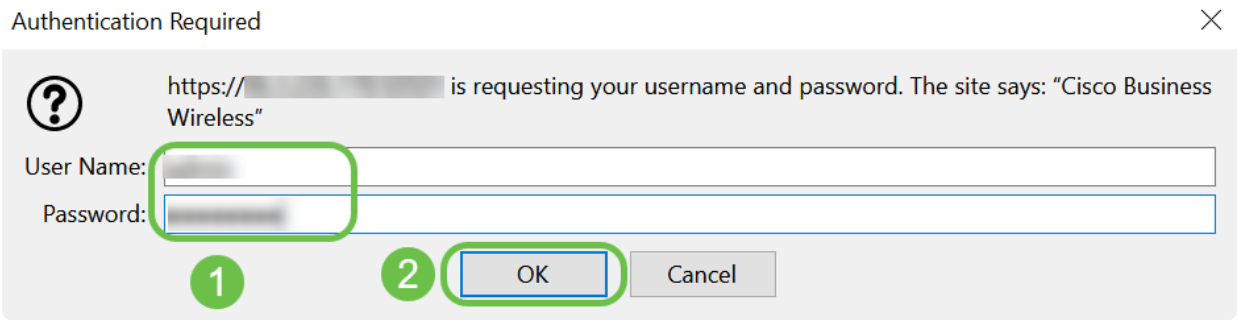
Passaggio 3

Immettere l'indirizzo IP dei punti di accesso principali (AP) sul browser Web. Fare clic su Login per accedere all'access point primario.



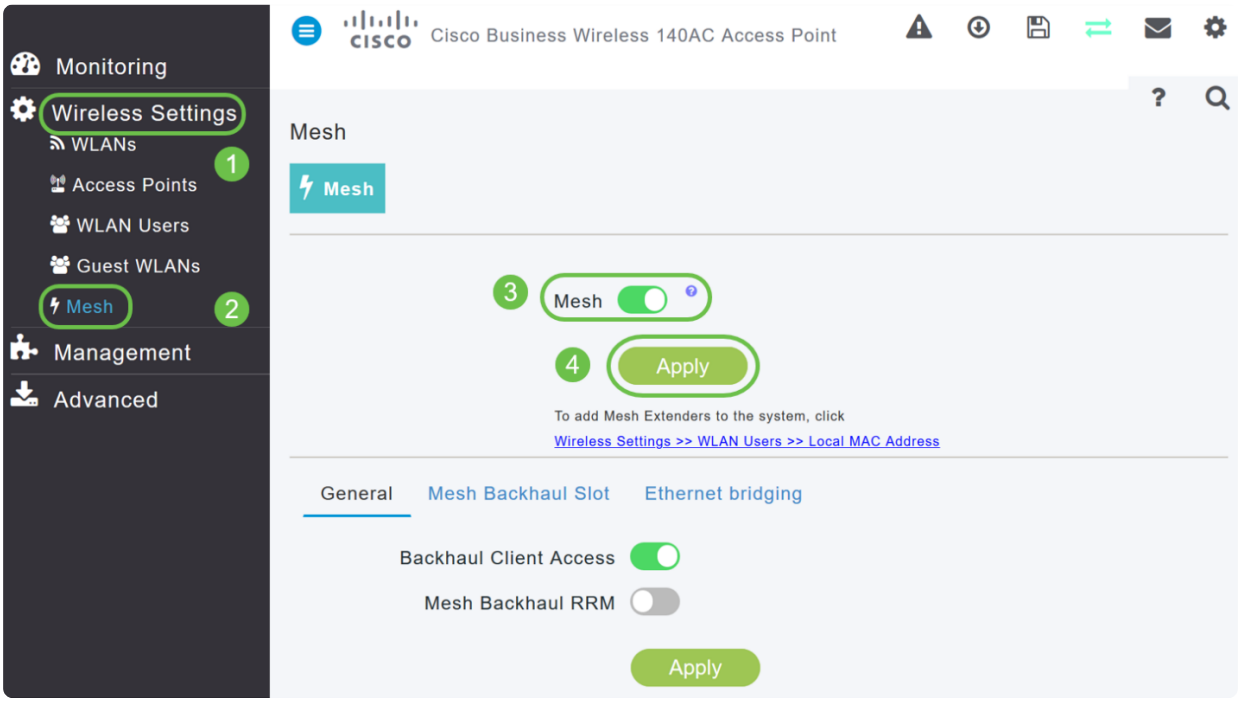
Passaggio 4

Immettere il nome utente e la password per accedere all'access point primario. Fare clic su OK.



Passaggio 5

Selezionare Wireless Settings > Mesh (Impostazioni wireless > Mesh). Accertarsi che la rete sia attivata. Fare clic su Apply (Applica).

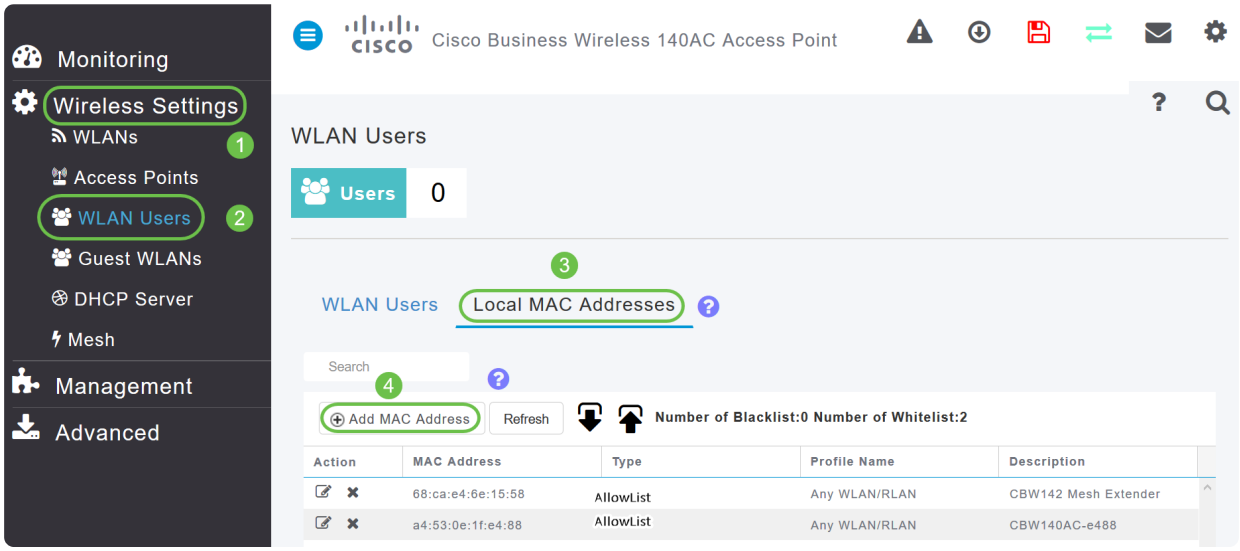


Passaggio 6

Se Mesh non era già stato abilitato, il WAP potrebbe dover eseguire un riavvio. Viene visualizzato un popup per eseguire un riavvio. Conferma. L'operazione richiederà circa 10 minuti. Durante un riavvio, il LED lampeggia in verde in più schemi, alternando rapidamente verde, rosso e ambra prima di tornare verde. L'intensità e la tonalità dei LED possono variare leggermente da un'unità all'altra.

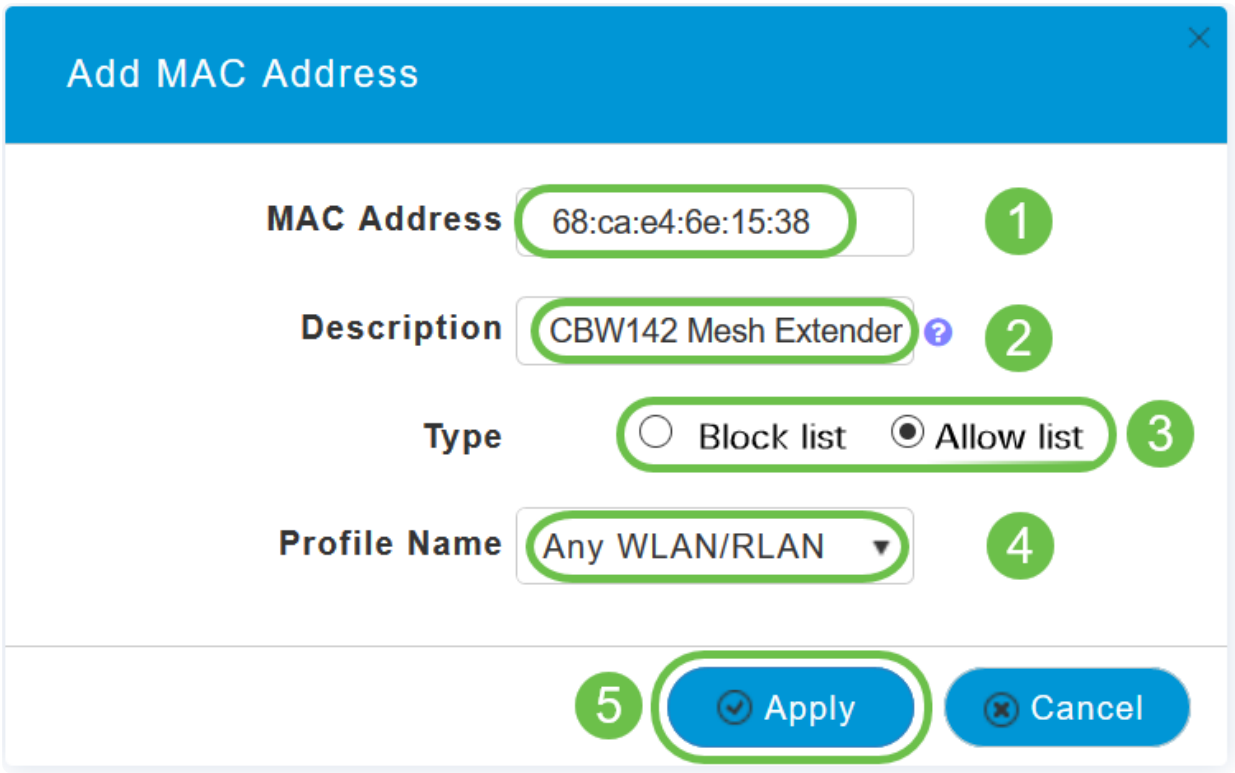
Passaggio 7

Selezionare Impostazioni wireless > Utenti WLAN > Indirizzi MAC locali. Fare clic su Aggiungi indirizzo MAC.



Passaggio 8

Immettere l'indirizzo MAC e la descrizione del dispositivo Mesh Extender. Selezionare l'elenco Tipo consentito. Selezionare Nome profilo dal menu a discesa. Fare clic su Apply (Applica).



Passaggio 9

Accertarsi di salvare tutte le configurazioni premendo l'icona Save (Salva) nel riquadro in alto a destra dello schermo.

Ripetete l'operazione per ogni estensione di mesh.

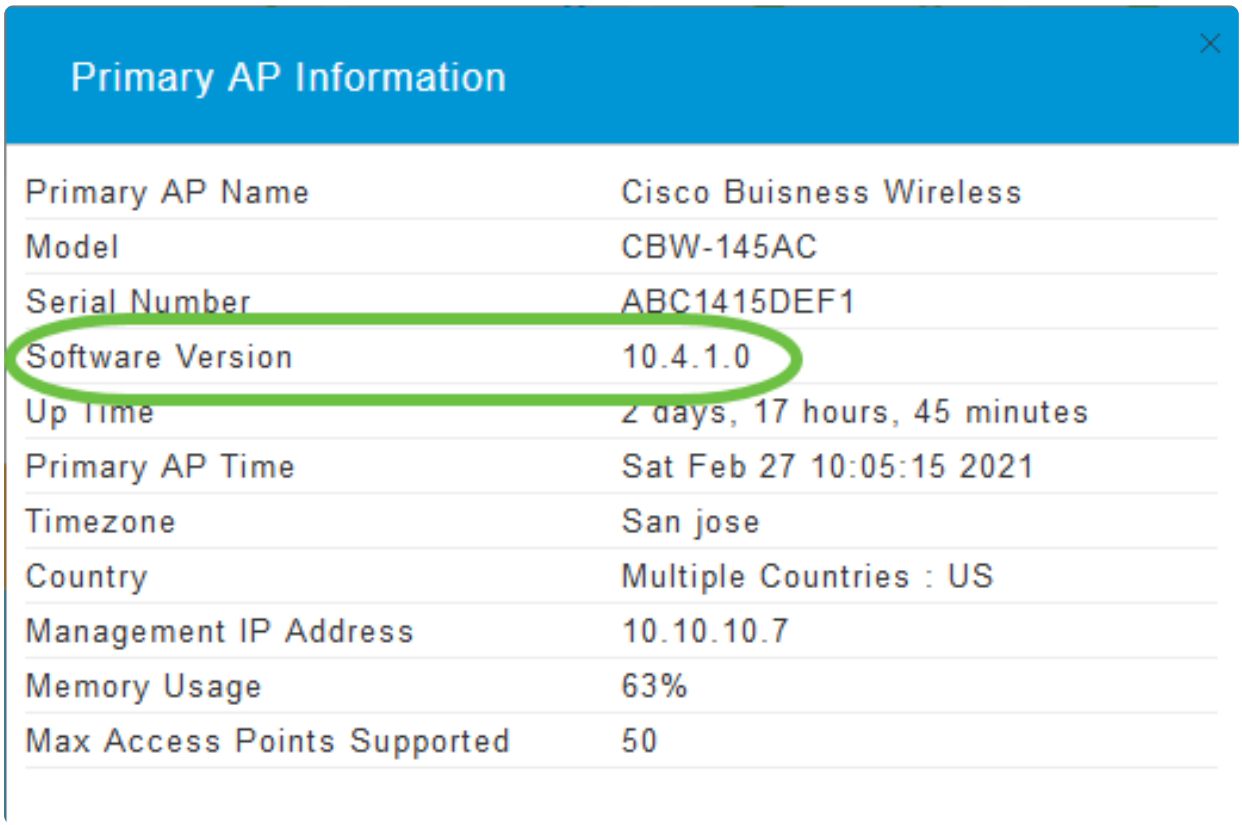
Controllo e aggiornamento del software tramite l'interfaccia utente Web

Non saltare questo passaggio importante! Esistono alcuni modi per aggiornare il software, ma i passaggi elencati di seguito sono consigliati come i più semplici da eseguire quando si utilizza l'interfaccia utente Web.

Per visualizzare e aggiornare la versione software corrente dell'access point principale, effettuare le seguenti operazioni.

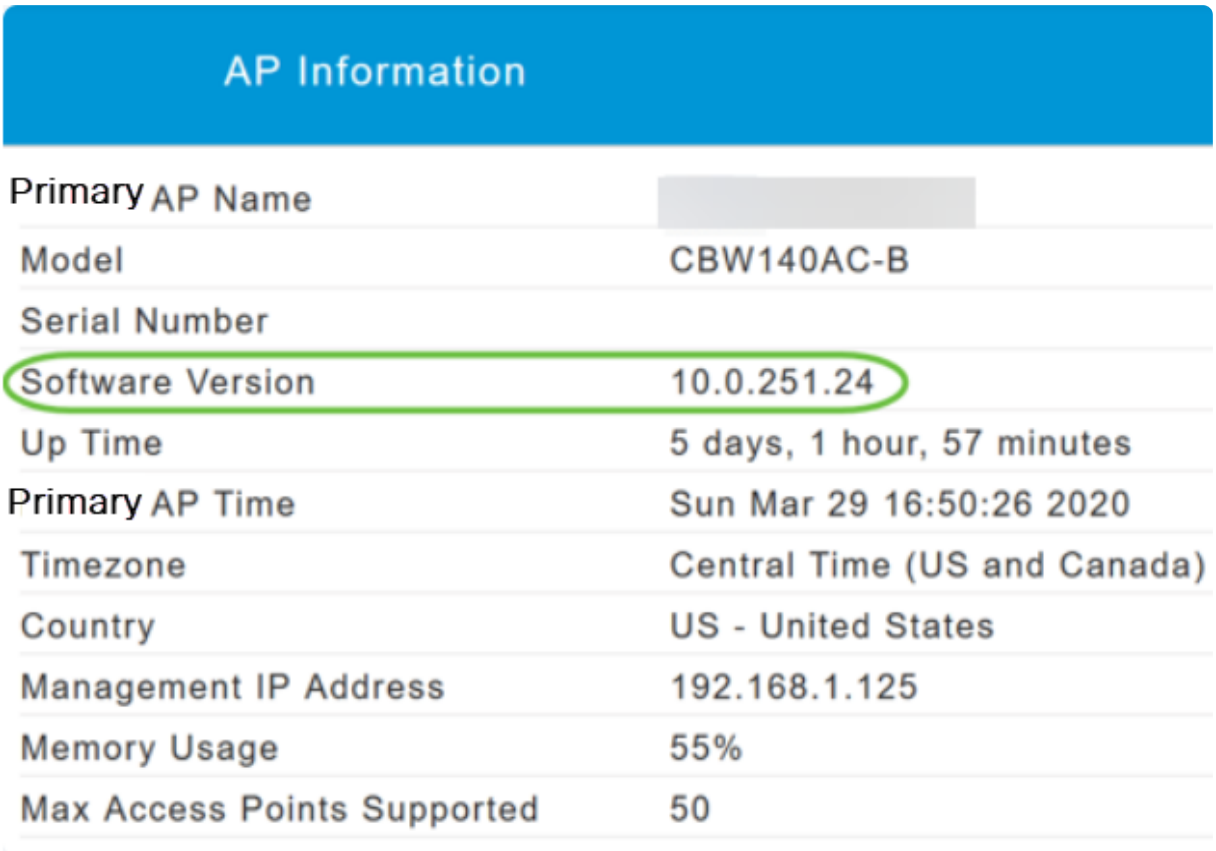
Passaggio 1

Fare clic sull'icona gear nell'angolo superiore destro dell'interfaccia Web e quindi su Primary AP Information.



Passaggio 2

Confrontare la versione in esecuzione con l'ultima versione del software. Chiudere la finestra una volta stabilito se è necessario aggiornare il software.

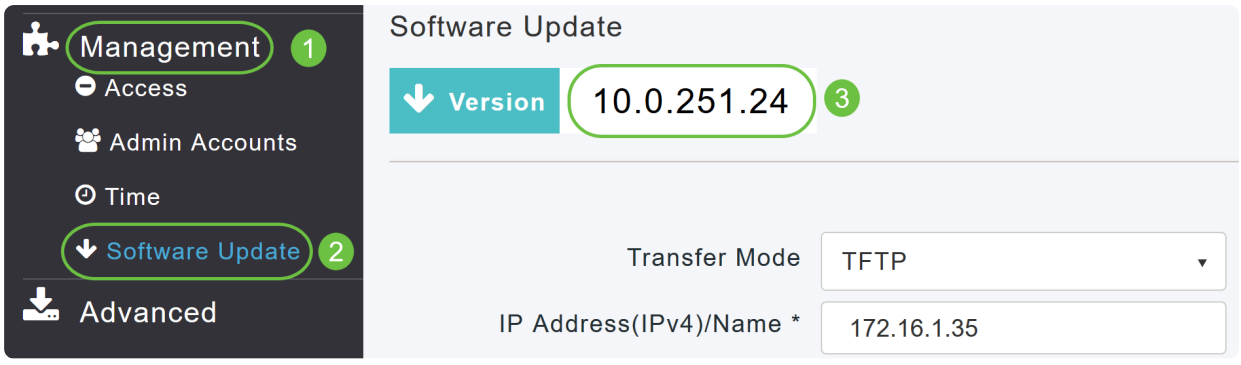


Se si sta eseguendo la versione più recente del software, è possibile passare alla sezione Creazione di WLAN.

Passaggio 3

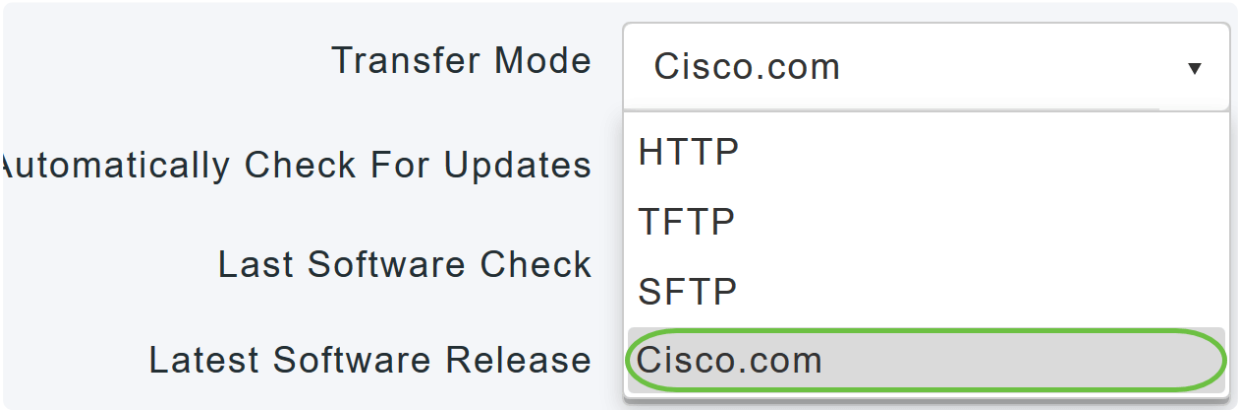
Scegliere Gestione > Aggiornamento software dal menu.

Viene visualizzata la finestra Software Update (Aggiornamento software)con il numero di versione del software corrente riportato nella parte superiore.



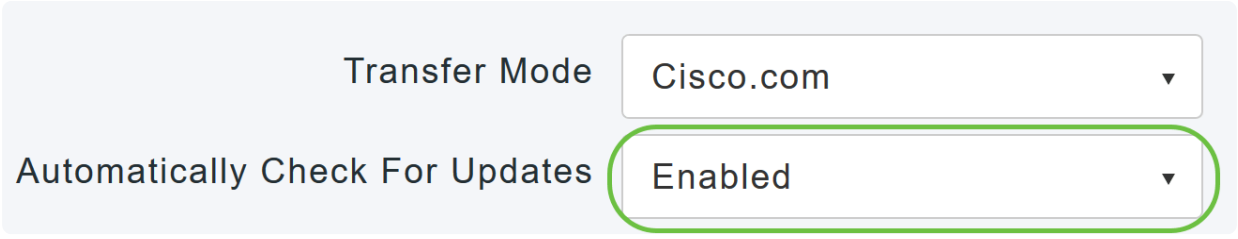
È possibile aggiornare il software CBW AP e le configurazioni correnti sull'access point principale non verranno eliminate.

Dall'elenco a discesa Transfer Mode (Modalità di trasferimento), selezionare Cisco.com.



Passaggio 4

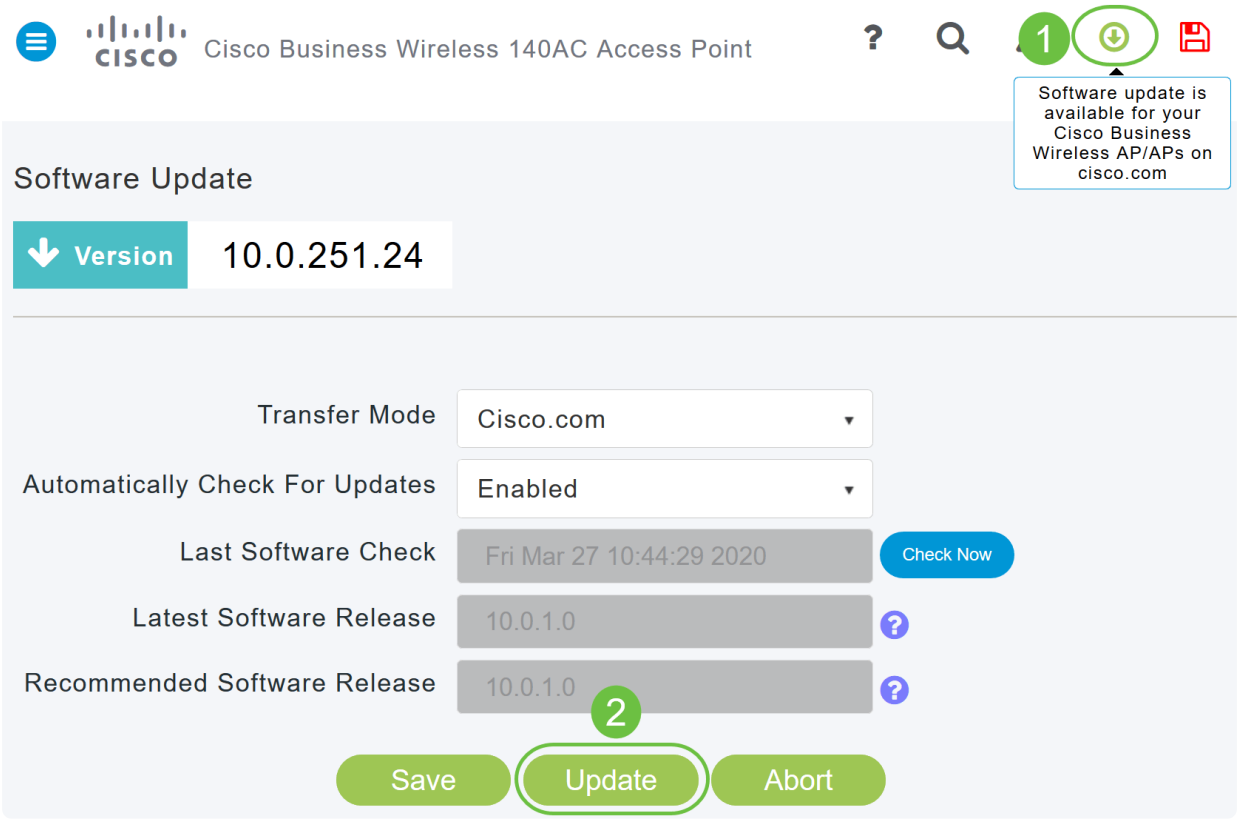
Per impostare l'access point principale in modo che controlli automaticamente la disponibilità di aggiornamenti software, scegliere Abilitato dall'elenco a discesa Controlla automaticamente disponibilità aggiornamenti. L'opzione è abilitata per impostazione predefinita.



Al termine di un controllo software e se è disponibile un aggiornamento software più recente o consigliato sul sito Cisco.com:

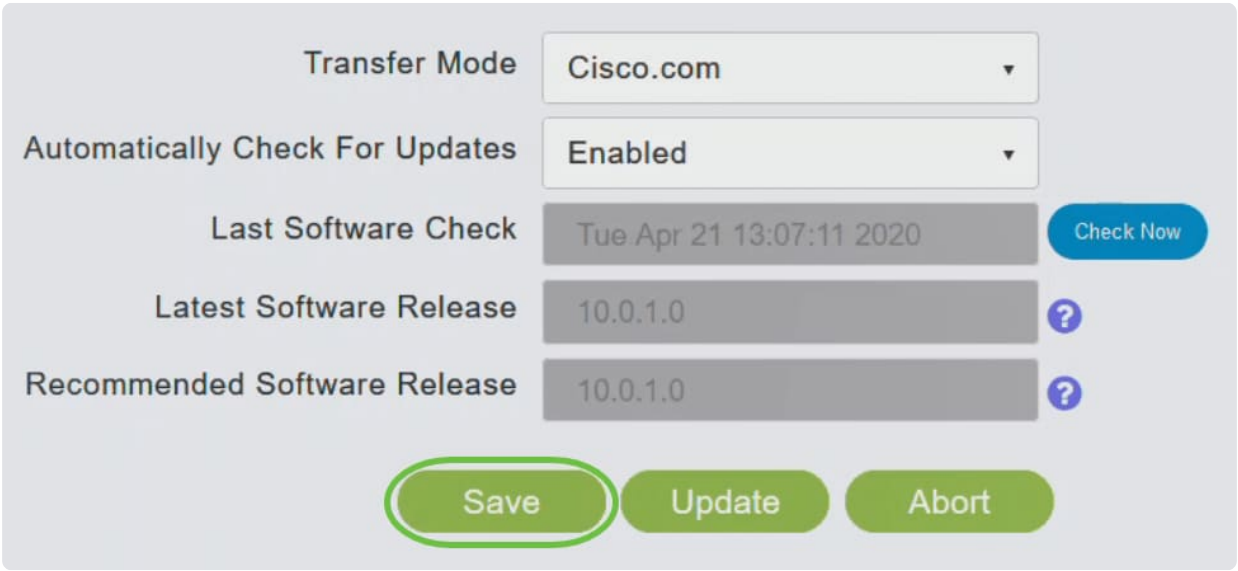
- L'icona dell'avviso di aggiornamento software nell'angolo superiore destro dell'interfaccia utente Web sarà di colore verde (o grigio). Se si fa clic sull'icona, viene visualizzata la pagina Software Update (Aggiornamento software).
- Il pulsante Aggiorna nella parte inferiore della pagina Aggiornamento software è

abilitato.

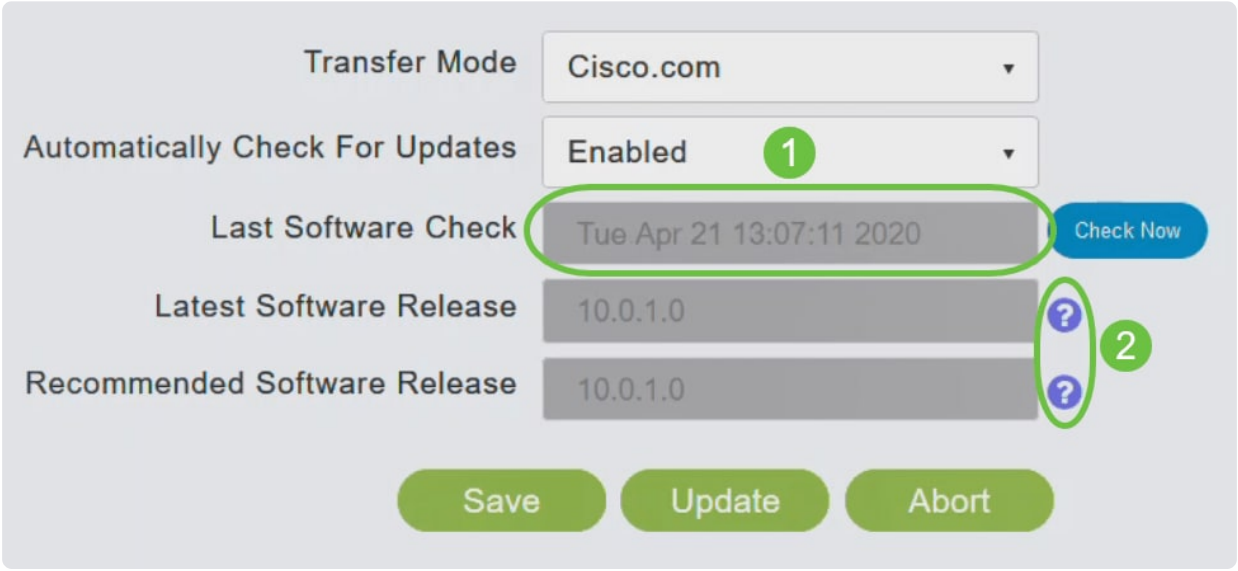


Passaggio 5

Fare clic su Save (Salva). In questo modo vengono salvate le voci o le modifiche apportate sia in modalità di trasferimento che in Controlla automaticamente aggiornamenti.

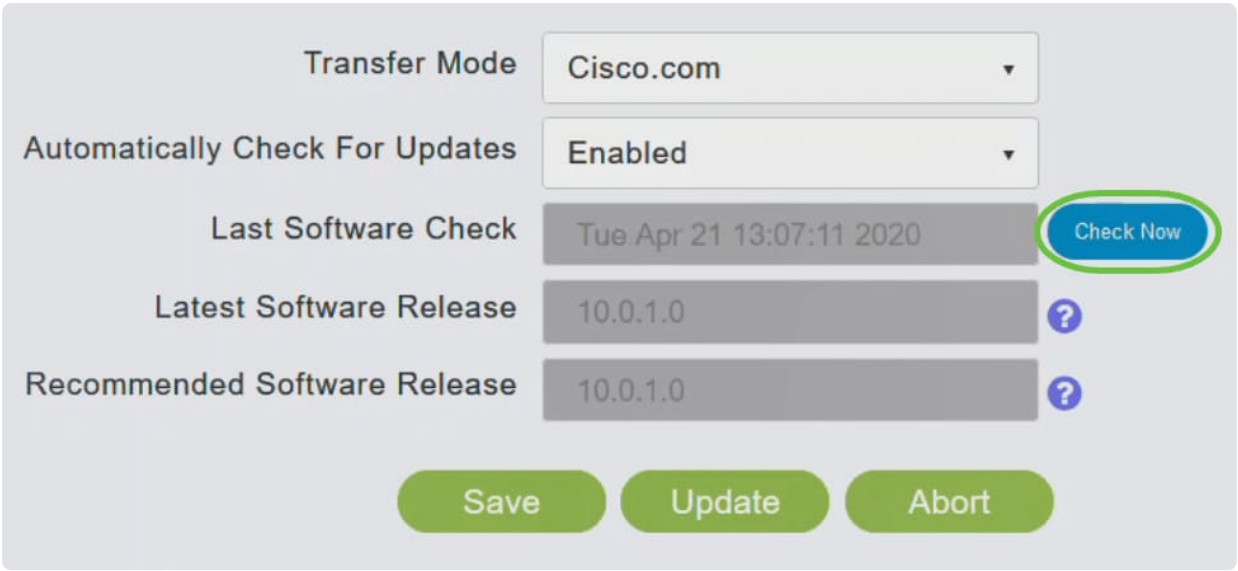


Nel campo Ultimo controllo software viene visualizzato l'indicatore orario dell'ultimo controllo software automatico o manuale. È possibile visualizzare le note delle release visualizzate facendo clic sull'icona del punto interrogativo accanto ad esso.



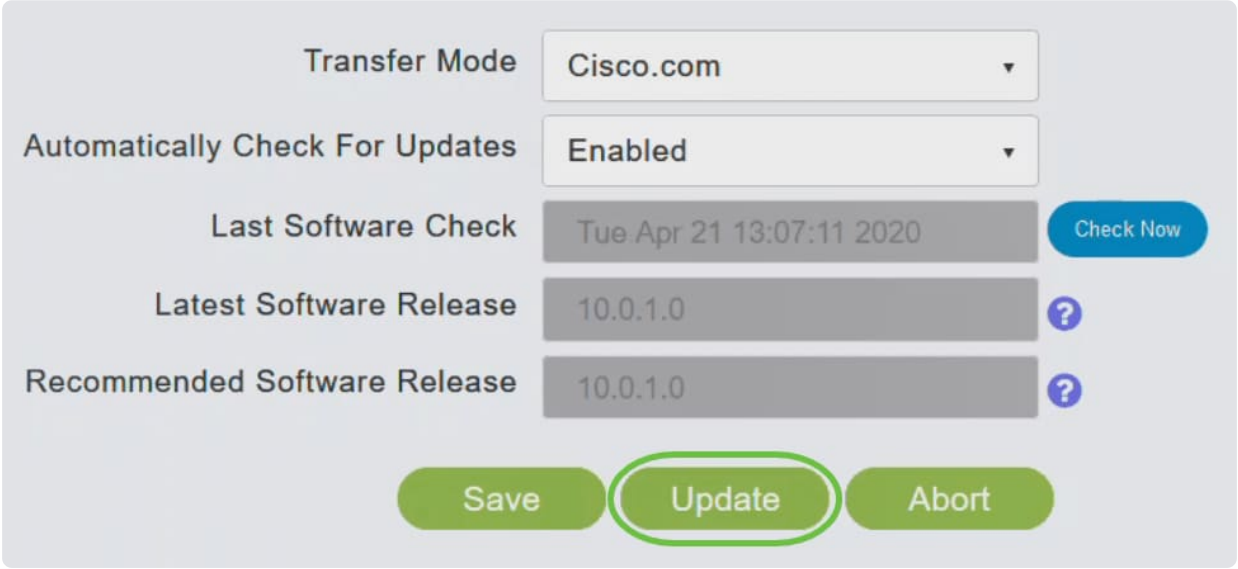
Passaggio 6

È possibile eseguire manualmente un controllo software in qualsiasi momento facendo clic su Esegui controllo.



Passaggio 7

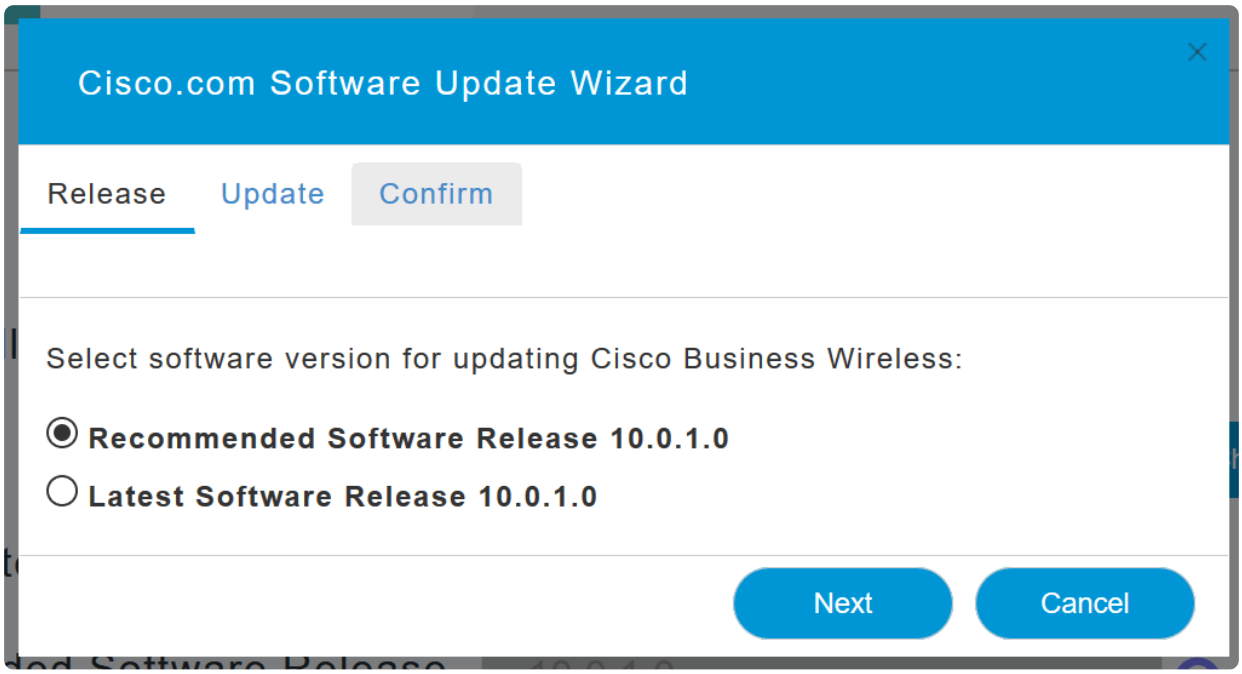
Per procedere con l'aggiornamento del software, fare clic su Aggiorna.



Viene visualizzato l'Aggiornamento guidato software. La procedura guidata consente di visualizzare le tre schede seguenti in sequenza:

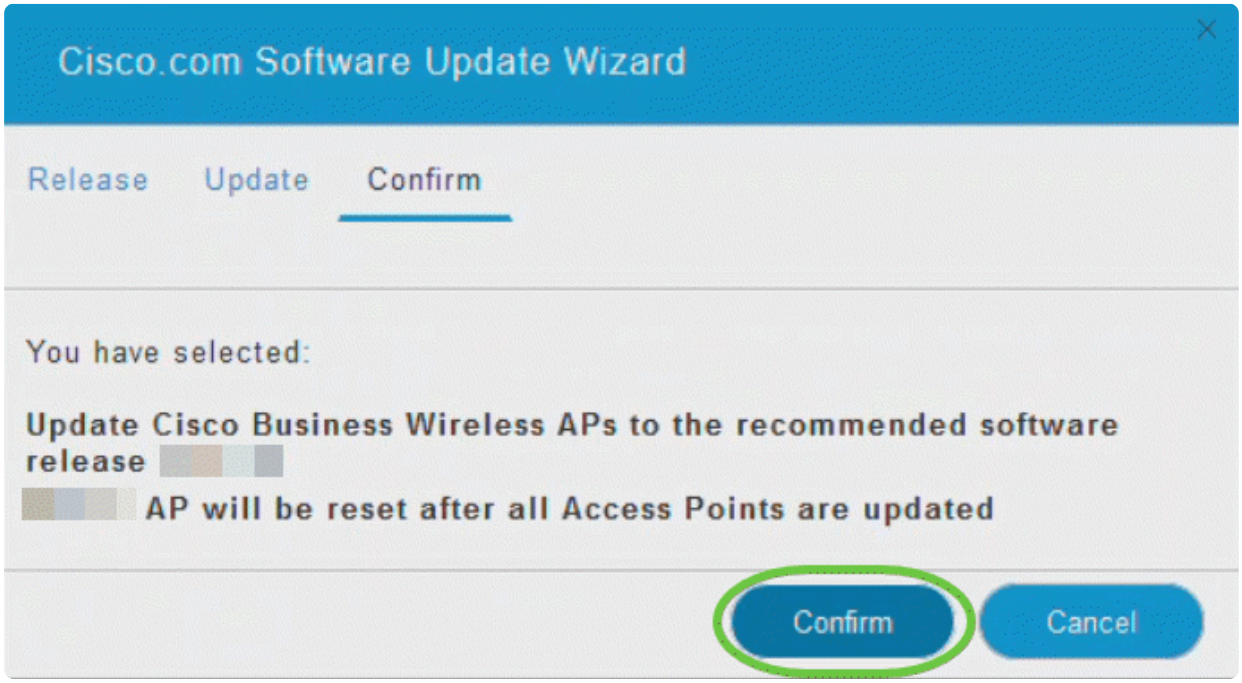
- Scheda Release (Versione) - Consente di specificare se si desidera eseguire l'aggiornamento alla versione software consigliata o alla versione più recente.
- Scheda Aggiorna: specificare quando reimpostare gli access point. È possibile scegliere di eseguirlo immediatamente o pianificarlo per un secondo momento. Per impostare il riavvio automatico dell'access point principale al termine del download preliminare dell'immagine, selezionare la casella di controllo Riavvio automatico.
- Scheda Conferma - Conferma le selezioni.

Seguire le istruzioni della procedura guidata. È possibile tornare a qualsiasi scheda in qualsiasi momento prima di fare clic su Conferma.



Passaggio 8

Fare clic su Conferma.



Creazione di WLAN sull'interfaccia utente Web

In questa sezione è possibile creare reti WLAN (Wireless Local Area Network).

Passaggio 1

Per creare una WLAN, selezionare Wireless Settings > WLAN (Impostazioni wireless > WLAN). Quindi selezionare Add new WLAN/RLAN (Aggiungi nuova WLAN/RLAN).

Passaggio 2

Nella scheda Generale, immettere le seguenti informazioni:

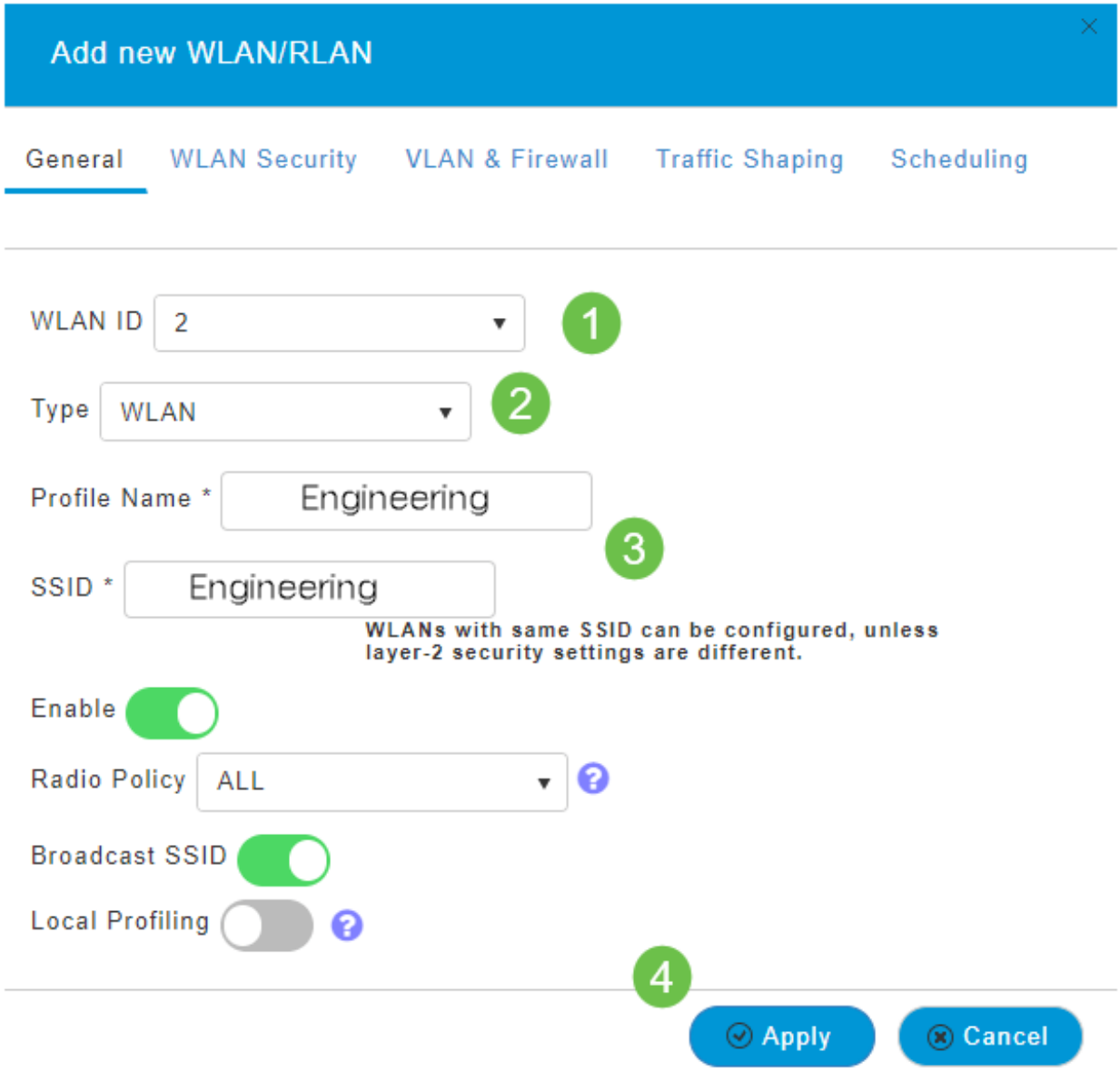
- ID WLAN: selezionare un numero per la WLAN
- Tipo: selezione della WLAN
- Nome profilo: quando si immette un nome, il SSID viene automaticamente compilato con lo stesso nome. Il nome deve essere univoco e non deve superare i 31 caratteri.

I campi seguenti sono stati lasciati come predefiniti in questo esempio, ma sono elencate le spiegazioni nel caso si desideri configurarli diversamente.

- SSID - Il nome del profilo funge anche da SSID. Se lo si desidera, è possibile modificare questa impostazione. Il nome deve essere univoco e non deve superare i 31 caratteri.

- Enable (Abilita) - Questa opzione deve essere lasciata abilitata affinché la WLAN funzioni.
- Criteri radio: in genere si desidera lasciare Tutto questo in modo che i client a 2,4 e 5 GHz possano accedere alla rete.
- SSID di trasmissione: in genere si desidera che l'SSID venga individuato e quindi si desidera lasciarlo abilitato.
- Profilatura locale: si desidera abilitare questa opzione solo per visualizzare il sistema operativo in esecuzione sul client o per visualizzare il nome utente.

Fare clic su Apply (Applica).



Passaggio 3

Viene visualizzata la scheda Sicurezza WLAN.

In questo esempio, le opzioni seguenti sono state lasciate come predefinite:

- La rete guest, l'Assistente rete captive e il filtro MAC sono stati lasciati disattivati. I dettagli per la configurazione di una rete guest sono illustrati nella sezione successiva.
- WPA2 Personal - Wi-Fi Protected Access 2 con formato passphrase PSK (Pre-shared Key) - ASCII. Questa opzione indica Wi-Fi Protected Access 2 con chiave precondivisa (PSK).

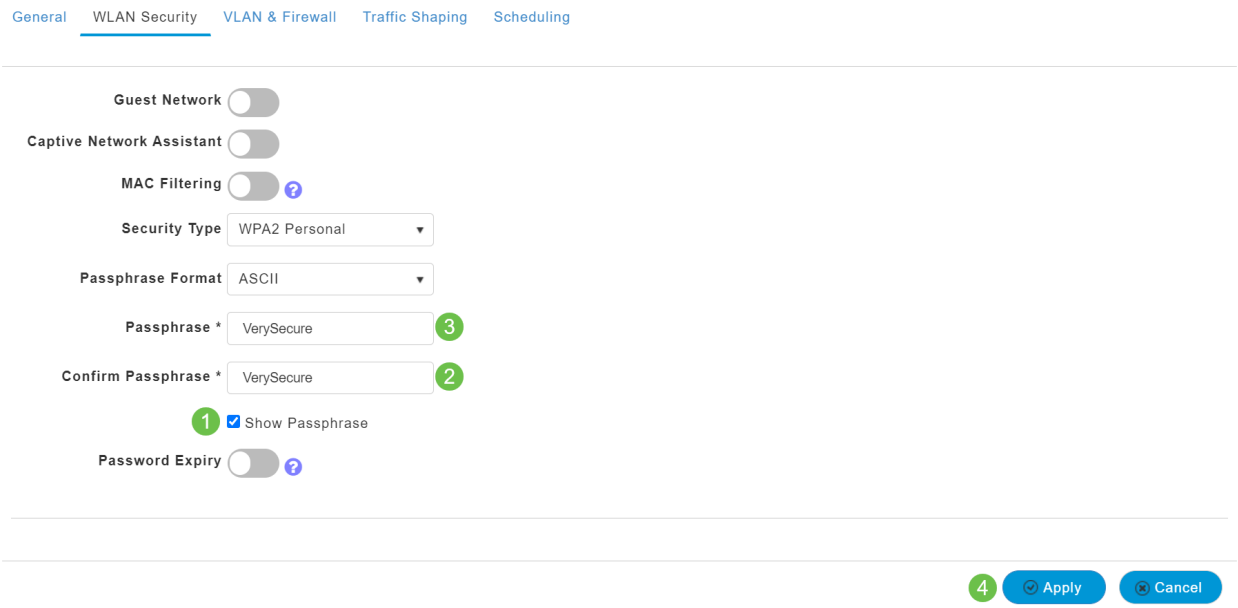
WPA2 Personal è un metodo utilizzato per proteggere la rete tramite l'autenticazione PSK. La chiave PSK viene configurata separatamente sia sull'access point primario, in base ai criteri di sicurezza WLAN, sia sul client. WPA2 Personal non si basa su un server di autenticazione della rete.

- Formato passphrase: ASCII viene lasciato come predefinito.

In questo scenario sono stati immessi i campi seguenti:

- Mostra passphrase: fare clic sulla casella di controllo per visualizzare la passphrase immessa.
- Passphrase: immettere un nome per la passphrase (password).
- Conferma passphrase: immettere di nuovo la password per confermare.

Fare clic su Apply (Applica). La nuova WLAN verrà attivata automaticamente.

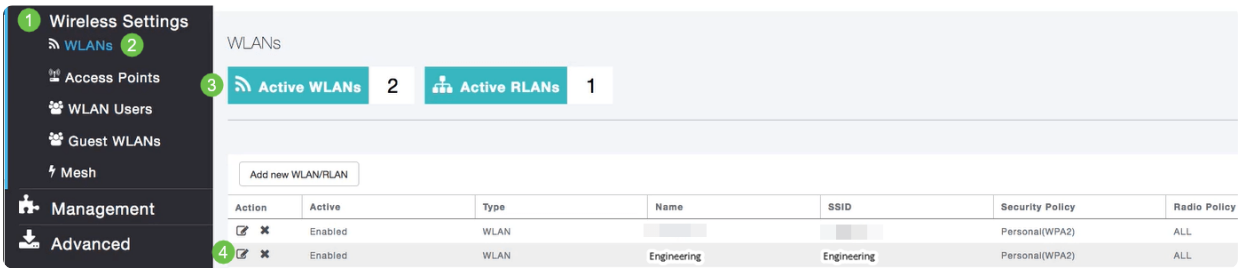


Passaggio 4

Assicurarsi di salvare le configurazioni facendo clic sull'icona Salva nel pannello in alto a destra della schermata dell'interfaccia utente Web.

Passaggio 5

Per visualizzare la WLAN creata, selezionare Impostazioni wireless > WLAN. Il numero di WLAN attive è aumentato a 2 e viene visualizzata la nuova WLAN.



Ripetere questi passaggi per le altre WLAN che si desidera creare.

Configurazioni wireless opzionali

A questo punto sono state impostate tutte le configurazioni di base e si è pronti per l'uso. Sono disponibili alcune opzioni, pertanto è possibile passare a una delle sezioni seguenti:

- Creazione di una WLAN guest mediante l'interfaccia utente Web (facoltativo)
- Creazione profilo applicazione (facoltativo)
- Creazione profilo client (facoltativo)
- Sono pronto per concludere e iniziare a usare la mia rete!

Creazione di una WLAN guest mediante l'interfaccia utente Web (facoltativo)

Una WLAN guest consente l'accesso guest alla rete wireless aziendale Cisco.

Passaggio 1

Accedere all'interfaccia utente Web dell'access point primario. Aprire un browser Web e immettere www.https://ciscobusiness.cisco. È possibile che venga visualizzato un avviso prima di procedere. Immettere le credenziali. È inoltre possibile accedervi immettendo l'indirizzo IP dell'access point primario.

Passaggio 2

Per creare una rete WLAN (Wireless Local Area Network), selezionare Impostazioni wireless > WLAN. Quindi selezionare Add new WLAN/RLAN (Aggiungi nuova WLAN/RLAN).

Passaggio 3

Nella scheda Generale, immettere le seguenti informazioni:

- ID WLAN: selezionare un numero per la WLAN
- Type - Seleziona WLAN
- Nome profilo: quando si immette un nome, il SSID viene popolato automaticamente con lo stesso nome. Il nome deve essere univoco e non deve superare i 31 caratteri.

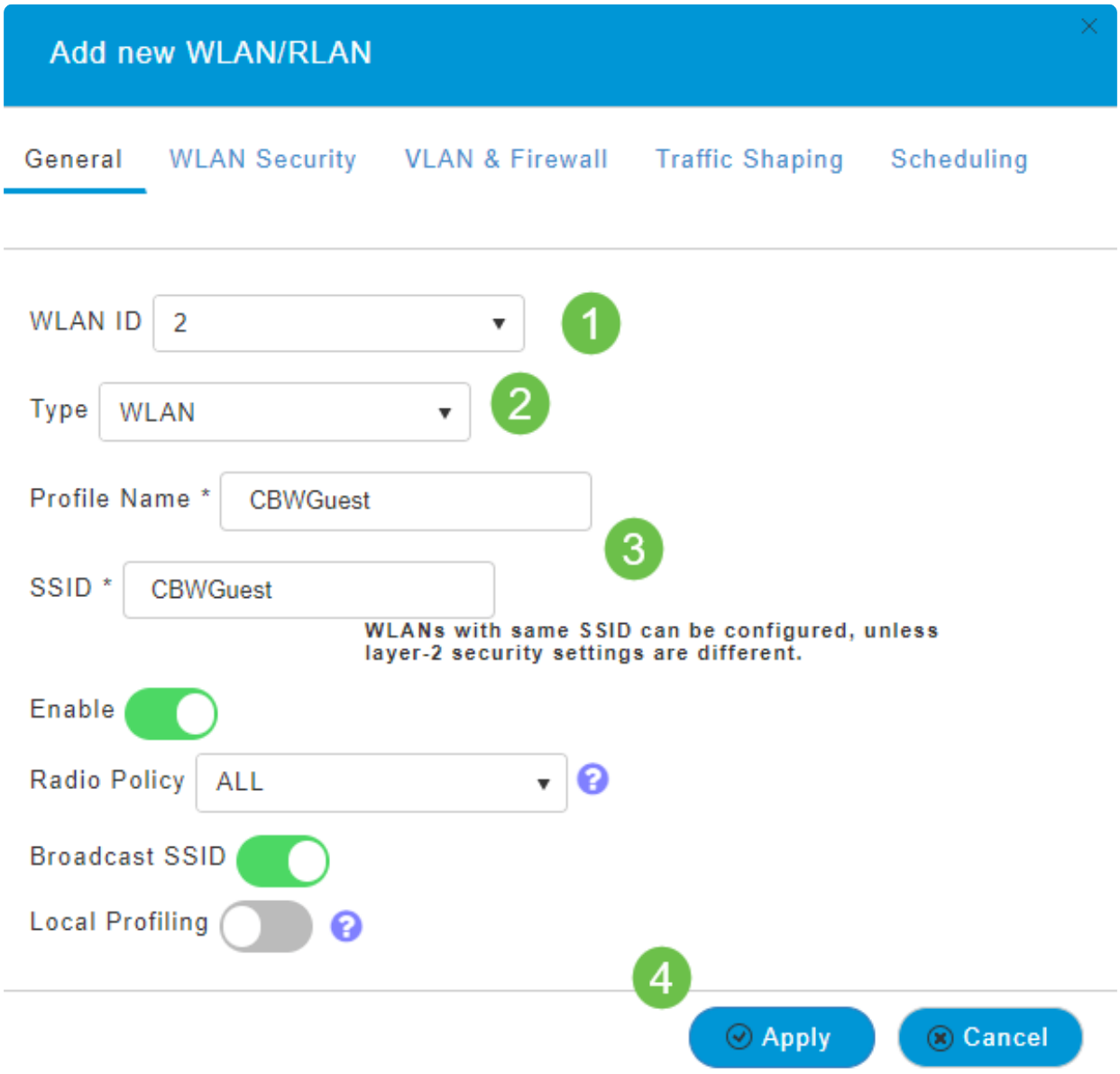
I campi seguenti sono stati lasciati come predefiniti in questo esempio, ma sono elencate le spiegazioni nel caso si desideri configurarli diversamente.

- SSID - Il nome del profilo funge anche da SSID. Se lo si desidera, è possibile modificare questa impostazione. Il nome deve essere univoco e non deve superare i 31 caratteri.
- Enable - Questa opzione deve essere lasciata abilitata affinché la WLAN funzioni.
- Criterio radio - In genere si desidera lasciare Tutto questo in modo che i client 2,4 GHz e 5 GHz possano accedere alla rete.
- SSID trasmissione: in genere si desidera che l'SSID venga individuato e quindi si

desidera lasciarlo abilitato.

- Profilatura locale: si desidera abilitare questa opzione solo per visualizzare il sistema operativo in esecuzione sul client o per visualizzare il nome utente.

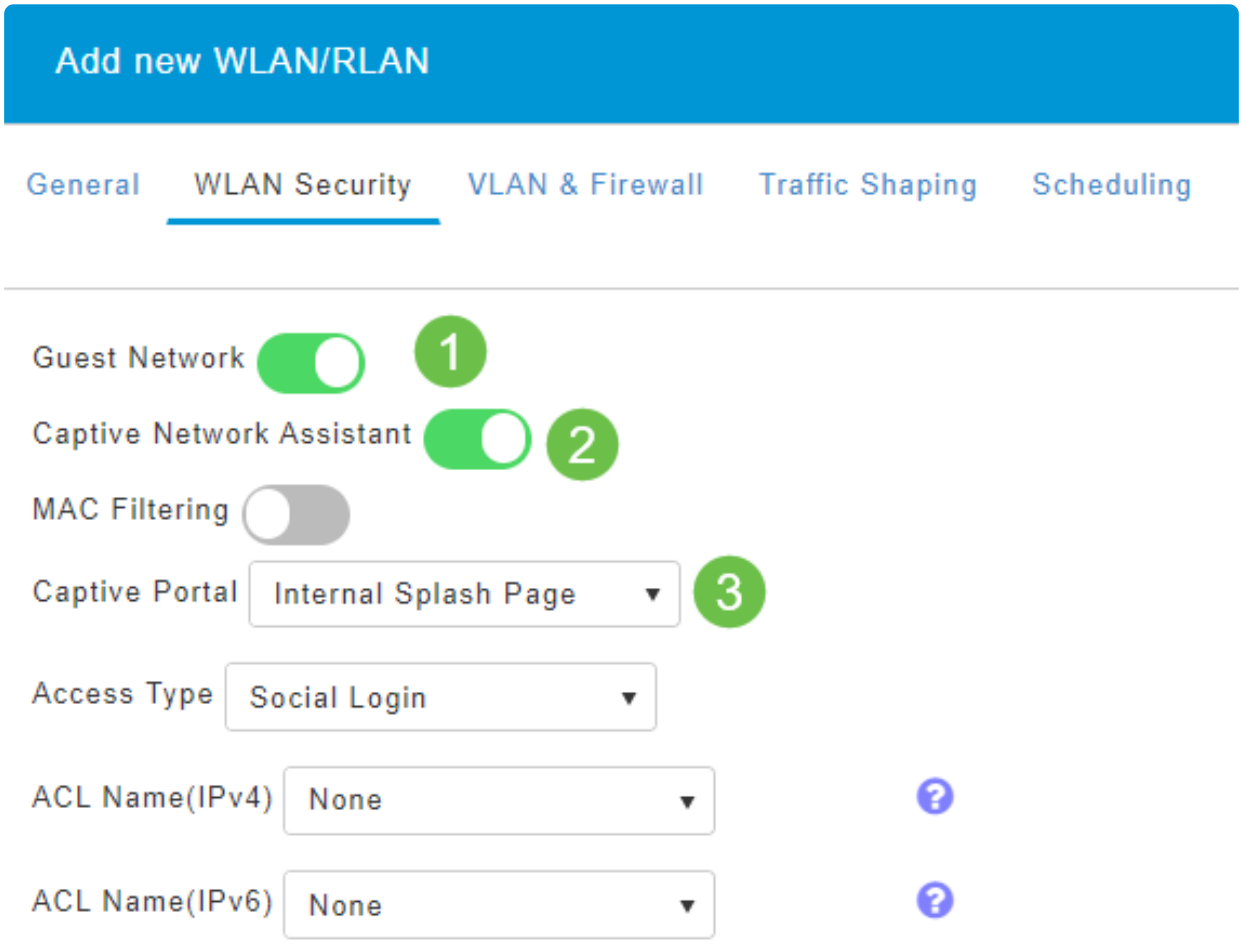
Fare clic su Apply (Applica).



Passaggio 4

Viene visualizzata la scheda Sicurezza WLAN. In questo esempio sono state selezionate le opzioni seguenti.

- Rete guest - Abilita
- Captive Network Assistant - Se si utilizza Mac o IOS, probabilmente si desidera attivare questa funzione. Questa funzionalità rileva la presenza di un portale vincolato inviando una richiesta Web alla connessione a una rete wireless. Questa richiesta viene indirizzata a un URL (Uniform Resource Locator) per i modelli iPhone e, se si riceve una risposta, si presume che l'accesso a Internet sia disponibile e che non siano necessarie ulteriori interazioni. Se non viene ricevuta alcuna risposta, si presume che l'accesso a Internet sia bloccato dal portale in modalità di blocco e che l'Assistente alla rete in modalità di blocco di Apple (CNA) avvii automaticamente lo pseudo-browser per richiedere l'accesso al portale in una finestra controllata. La CNA potrebbe interrompersi durante il reindirizzamento a un portale separato di Identity Services Engine (ISE). L'access point primario impedisce la visualizzazione di questo pseudo-browser.
- Captive Portal - Questo campo è visibile solo quando l'opzione Rete guest è abilitata. Consente di specificare il tipo di portale Web che può essere utilizzato per l'autenticazione. Selezionare Pagina iniziale interna per utilizzare l'autenticazione basata sul portale Web Cisco predefinita. Scegliere Pagina iniziale esterna se si dispone dell'autenticazione del portale vincolato, utilizzando un server Web esterno alla rete. Inoltre, specificare l'URL del server nel campo URL sito.



In questo esempio, verrà creata la WLAN guest con un tipo di accesso di accesso di social networking abilitato. Una volta connesso alla WLAN guest, l'utente verrà reindirizzato alla pagina di accesso predefinita di Cisco, dove potrà trovare i pulsanti di accesso per Google e Facebook. L'utente può accedere utilizzando il proprio account Google o Facebook per ottenere l'accesso a Internet.

Passaggio 5

Nella stessa scheda selezionare un tipo di accesso dal menu a discesa. In questo esempio è stato selezionato Accesso social. Questa è l'opzione che consente agli ospiti di usare le loro credenziali Google o Facebook per autenticarsi e ottenere l'accesso alla rete.

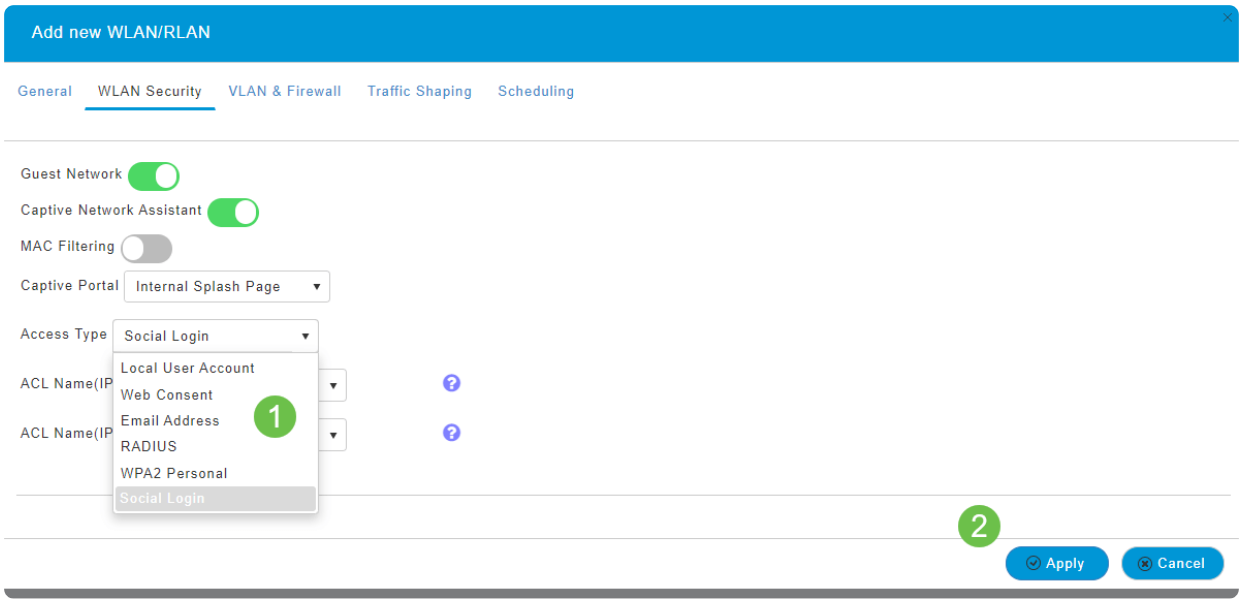
Altre opzioni per Tipo di accesso sono:

- Account utente locale - Opzione predefinita. Scegliere questa opzione per autenticare i guest utilizzando il nome utente e la password che è possibile specificare per gli utenti guest della WLAN, in Impostazioni wireless > Utenti WLAN. Questo è un esempio della pagina iniziale interna predefinita.

È possibile personalizzare questa impostazione selezionando Impostazioni wireless > WLAN guest. Da qui è possibile immettere un titolo e un messaggio di pagina. Fare clic su Apply (Applica). Fare clic su Anteprima.

- Web Consent: consente agli utenti guest di accedere alla WLAN dopo aver accettato i termini e le condizioni visualizzati. Gli utenti guest possono accedere alla WLAN senza immettere un nome utente e una password.
- Indirizzo e-mail - Gli utenti guest devono immettere il proprio indirizzo e-mail per accedere alla rete.
- RADIUS: da utilizzare con un server di autenticazione esterno.
- WPA2 Personal - Accesso protetto Wi-Fi 2 con chiave precondivisa (PSK)

Fare clic su Apply (Applica).



Passaggio 6

Assicurarsi di salvare le configurazioni facendo clic sull'icona Salva nel pannello in alto a destra della schermata dell'interfaccia utente Web.

È stata creata una rete guest disponibile nella rete CBW. I vostri ospiti apprezzeranno la comodità.

Creazione profilo applicazione mediante interfaccia utente Web (facoltativo)

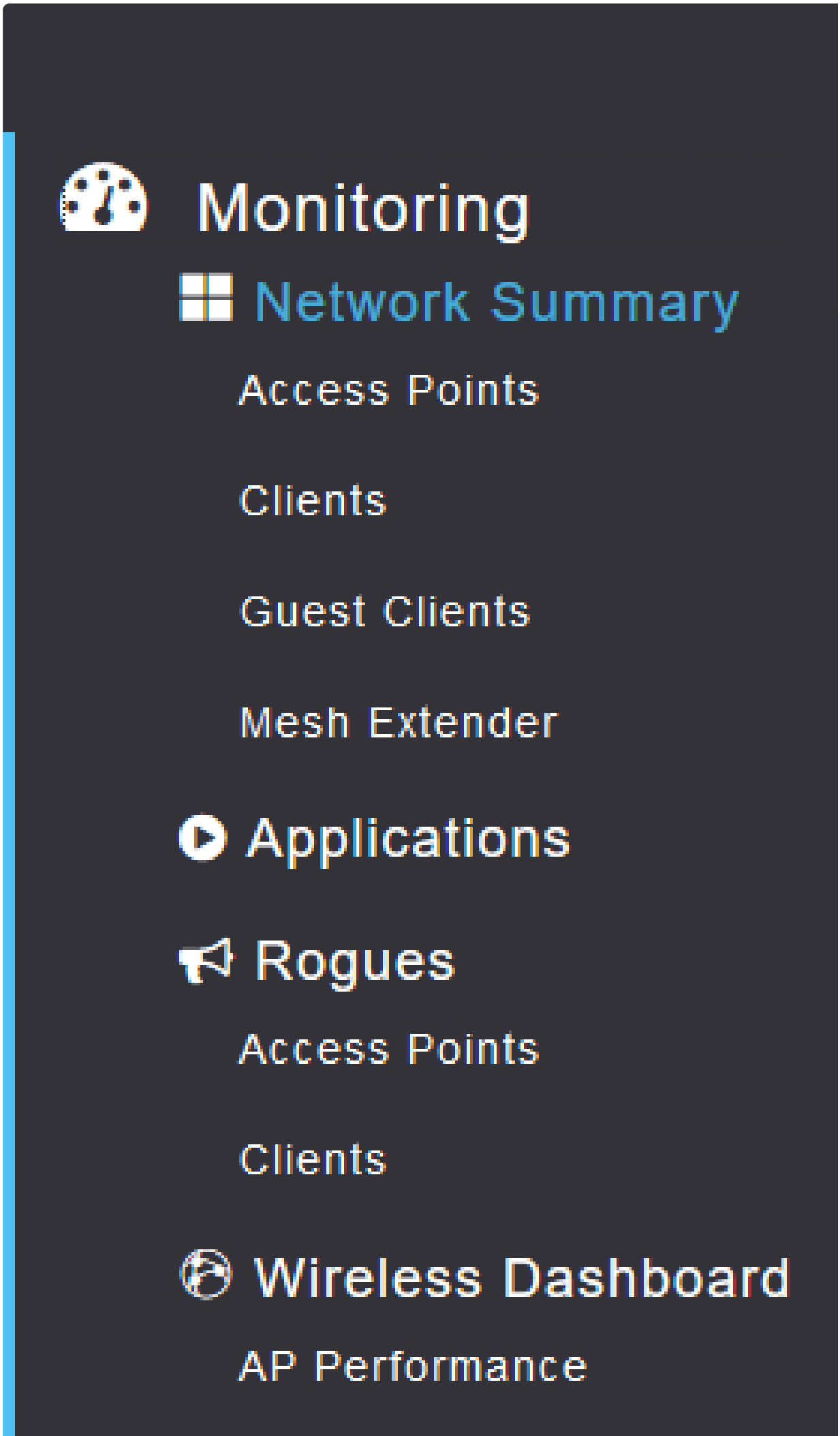
La profilatura è un sottoinsieme di funzionalità che consentono di applicare criteri organizzativi. Permette di associare e assegnare priorità ai tipi di traffico. Come le regole che decidono come classificare o eliminare il traffico. Il sistema Cisco Business Mesh Wireless prevede la profilatura di client e applicazioni. L'accesso a una rete come utente inizia con molti scambi di informazioni, tra cui il tipo di traffico. I criteri interrompono il flusso del traffico per indirizzare il percorso, in modo analogo a un diagramma di flusso. Altri tipi di funzionalità dei criteri includono: accesso guest, elenchi di controllo di accesso e QoS.

Passaggio 1

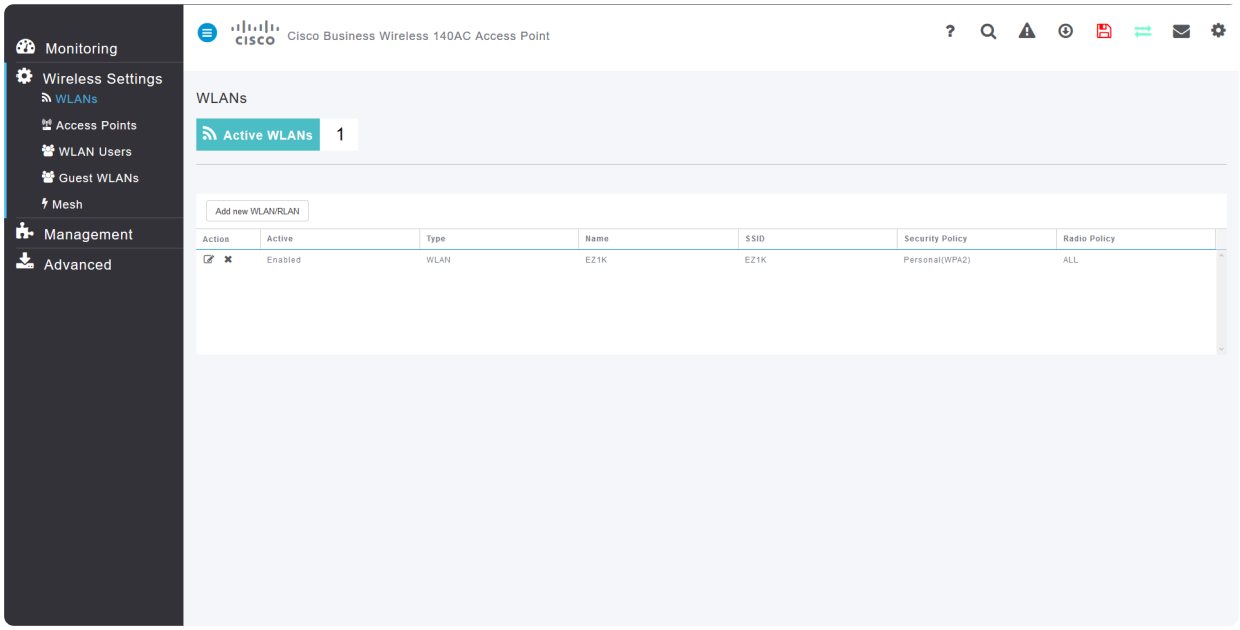
Se la barra dei menu a sinistra non è visibile, spostarsi sul menu sul lato sinistro dello schermo.

Passaggio 2

Il menu Monitoraggio viene caricato per impostazione predefinita quando si accede al dispositivo. Sarà necessario fare clic su Impostazioni wireless.

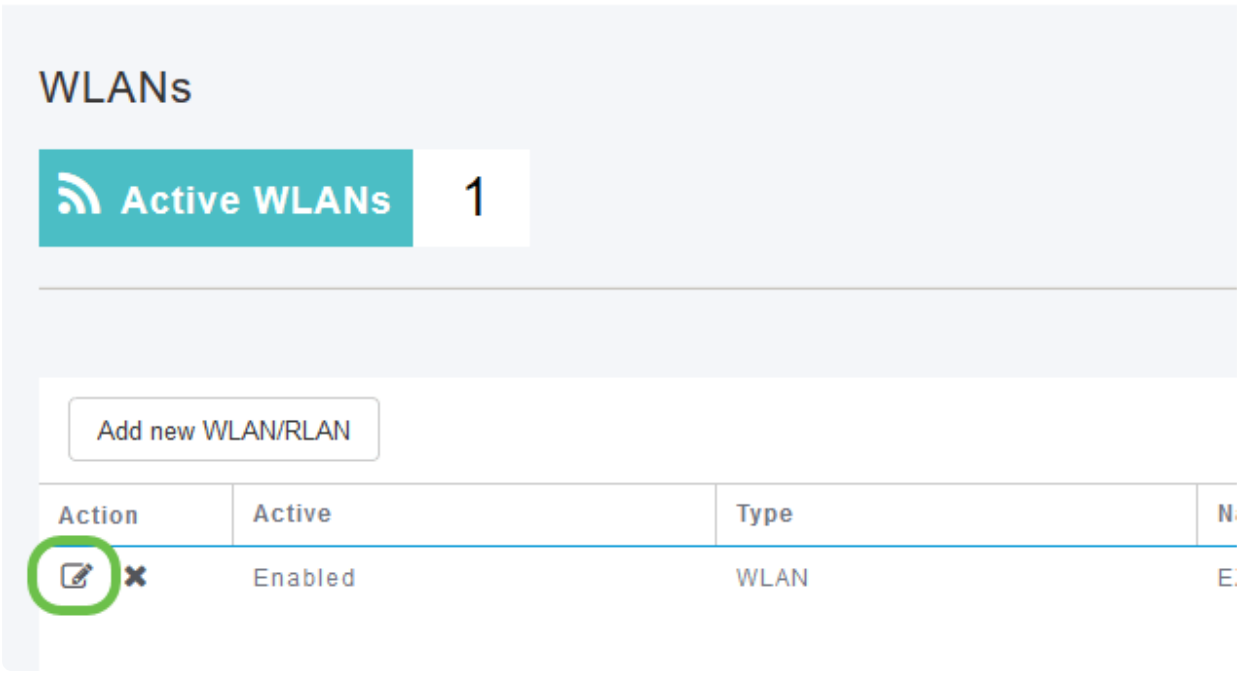

Monitoring
Network Summary
Access Points
Clients
Guest Clients
Mesh Extender
Applications
Rogues
Access Points
Clients
Wireless Dashboard
AP Performance

L'immagine seguente è simile a quella visualizzata quando si fa clic sul collegamento Impostazioni wireless.

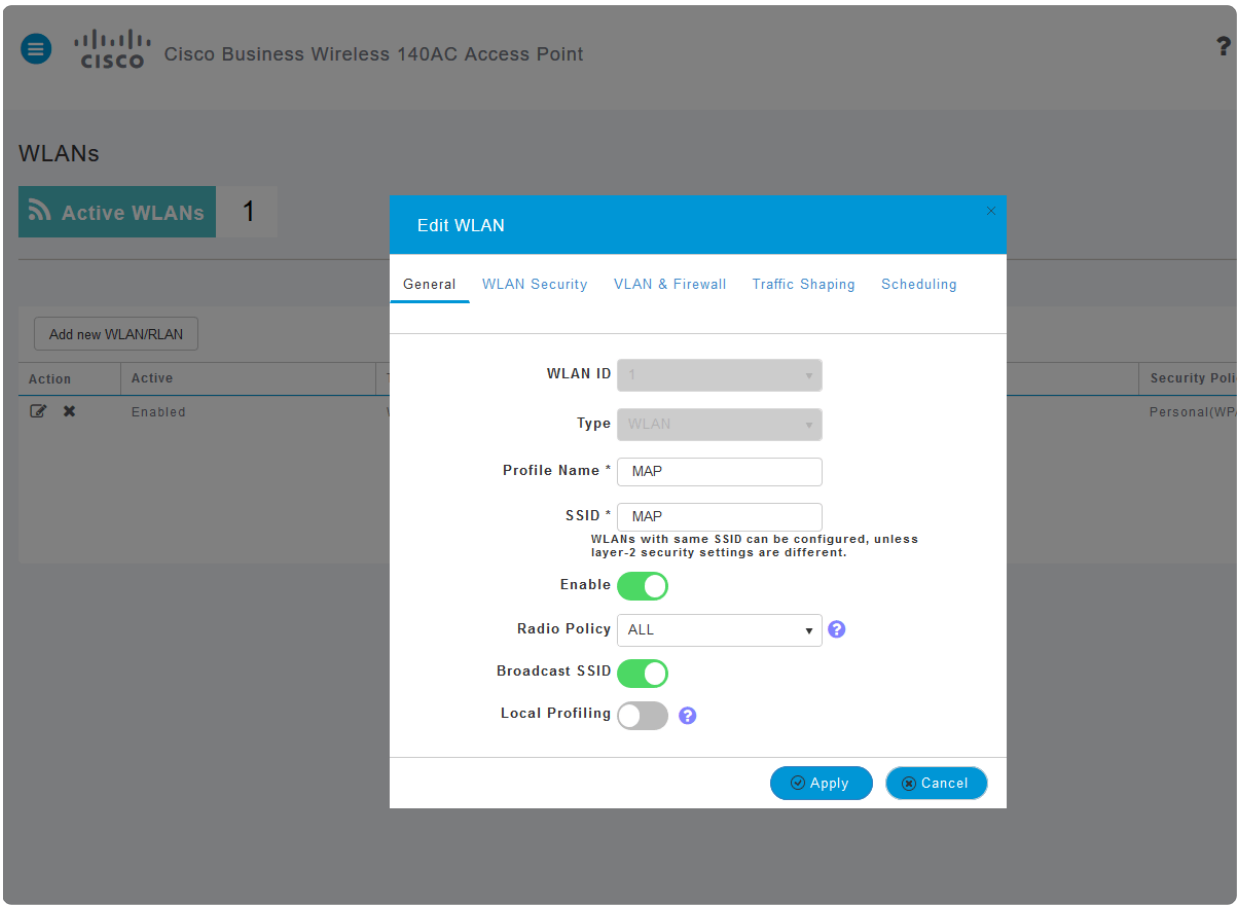


Passaggio 3

Fare clic sull'icona di modifica a sinistra della rete locale senza fili su cui si desidera attivare l'applicazione.

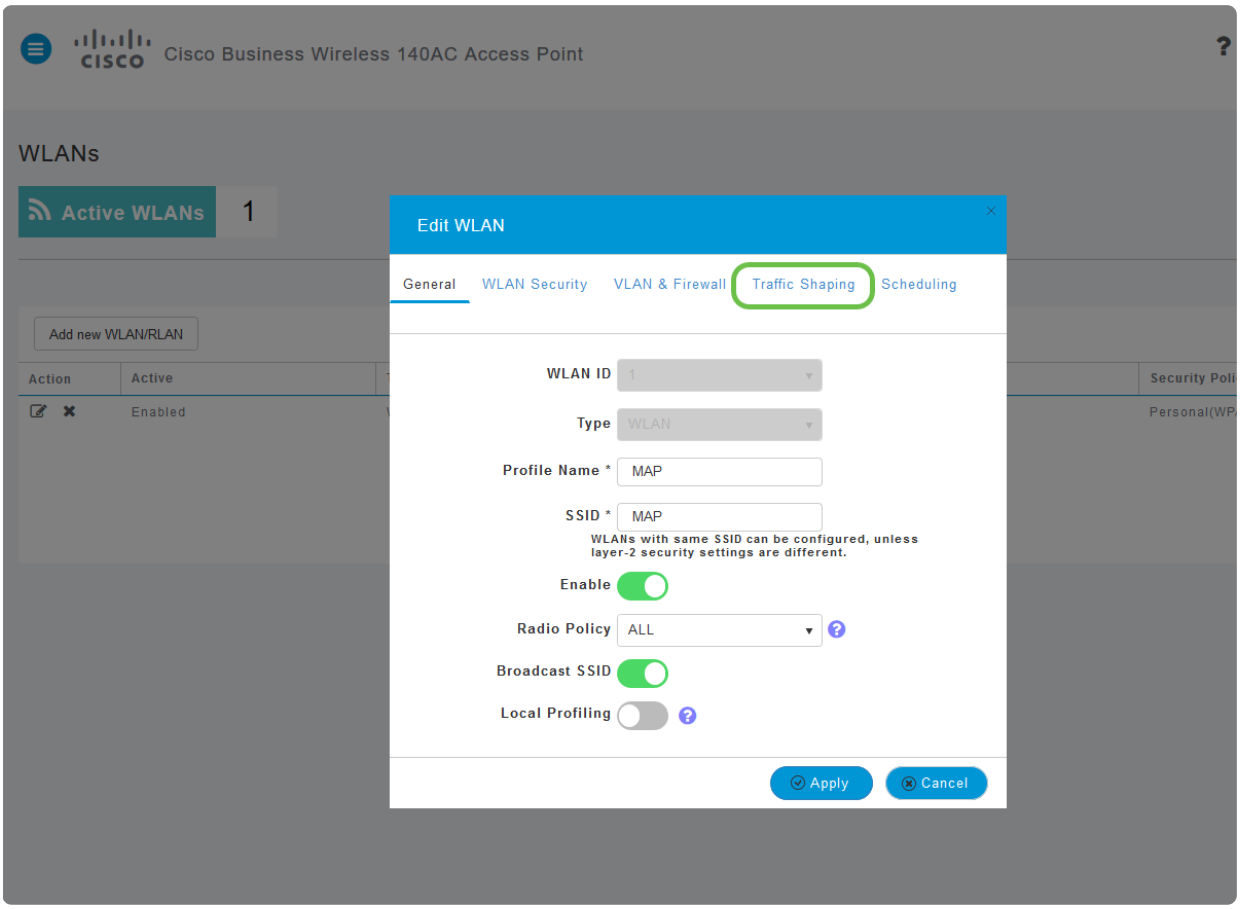


Poiché la WLAN è stata aggiunta di recente, la pagina Modifica WLAN potrebbe essere simile a quella mostrata di seguito:

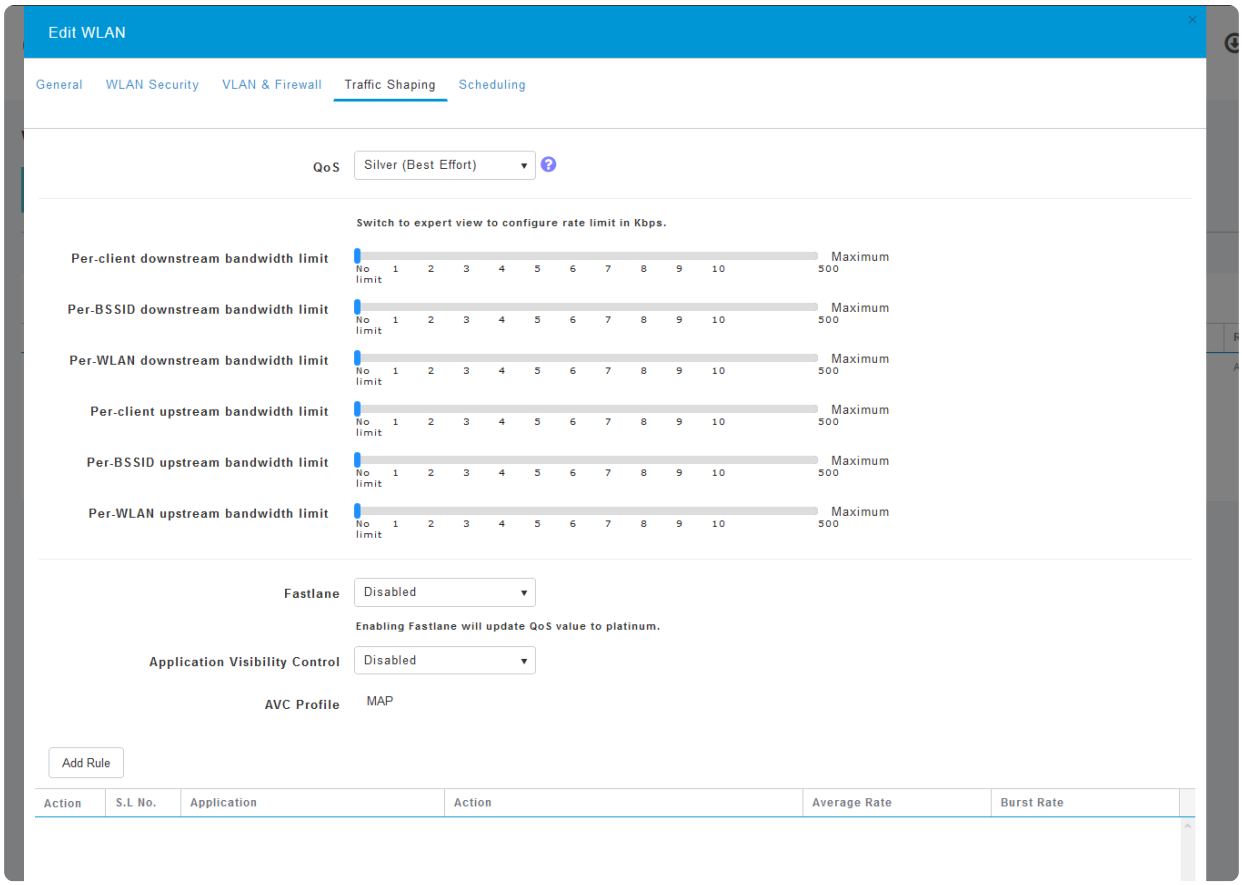


Passaggio 4

Passare alla scheda Traffic Shaping facendo clic su di essa.

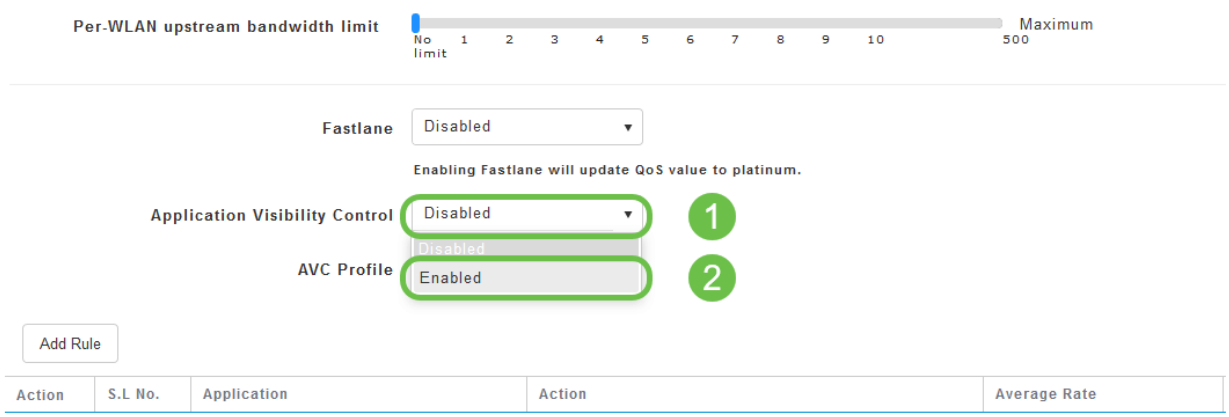


Lo schermo potrebbe apparire come segue:



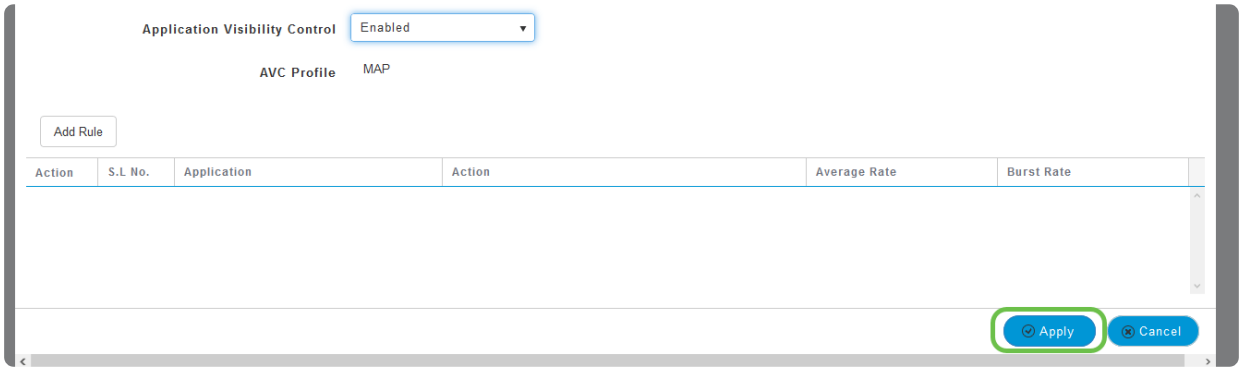
Passaggio 5

Nella parte inferiore della pagina è disponibile la funzionalità Controllo visibilità applicazioni. Questa opzione è disabilitata per impostazione predefinita. Fare clic sull'elenco a discesa e selezionare Abilitato.



Passaggio 6

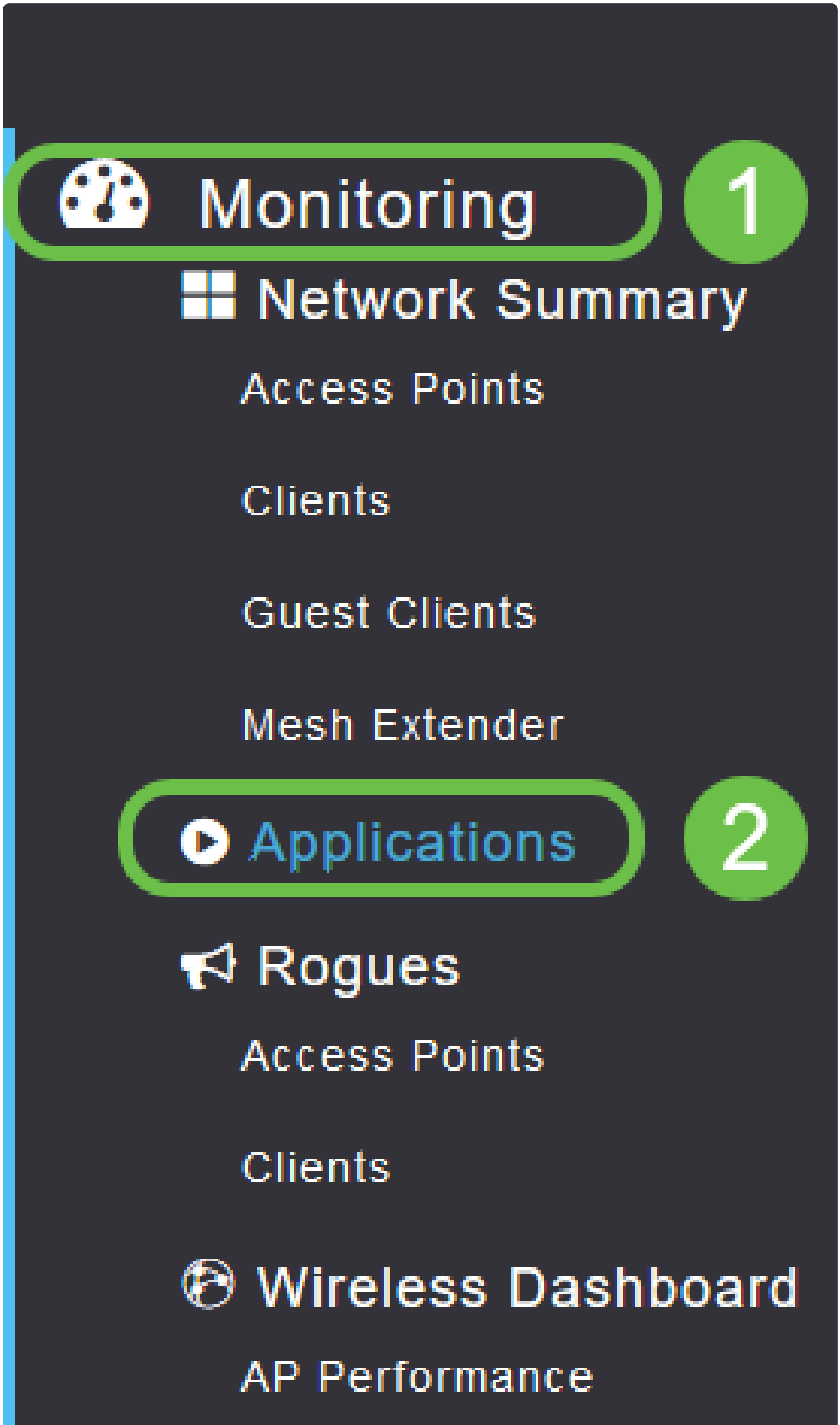
Fare clic sul pulsante Applica.



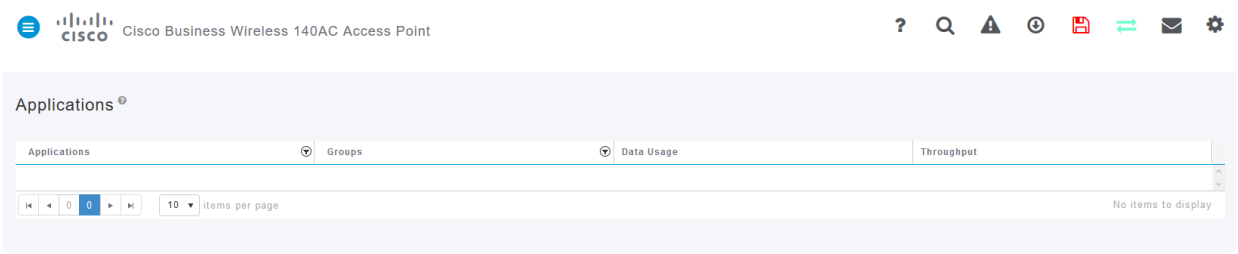
È necessario attivare questa impostazione, altrimenti la funzionalità non funzionerà.

Passaggio 7

Fare clic sul pulsante Annulla per chiudere il sottomenu WLAN. Fare quindi clic sul menu Monitoraggio sulla barra dei menu a sinistra. Una volta completata l'operazione, fare clic sulla voce di menu Applicazioni.


Monitoring
1
Network Summary
Access Points
Clients
Guest Clients
Mesh Extender
Applications
2
Rogues
Access Points
Clients
Wireless Dashboard
AP Performance

Se non hai ricevuto traffico per nessuna fonte, la tua pagina sarà vuota come mostrato di seguito.



In questa pagina verranno visualizzate le informazioni riportate di seguito.

- Applicazione: include molti tipi diversi
- Gruppi: indica il tipo di gruppo di applicazioni per semplificare l'ordinamento
- Uso dati: la quantità di dati utilizzati da questo servizio nel complesso
- Throughput: quantità di larghezza di banda utilizzata dall'applicazione

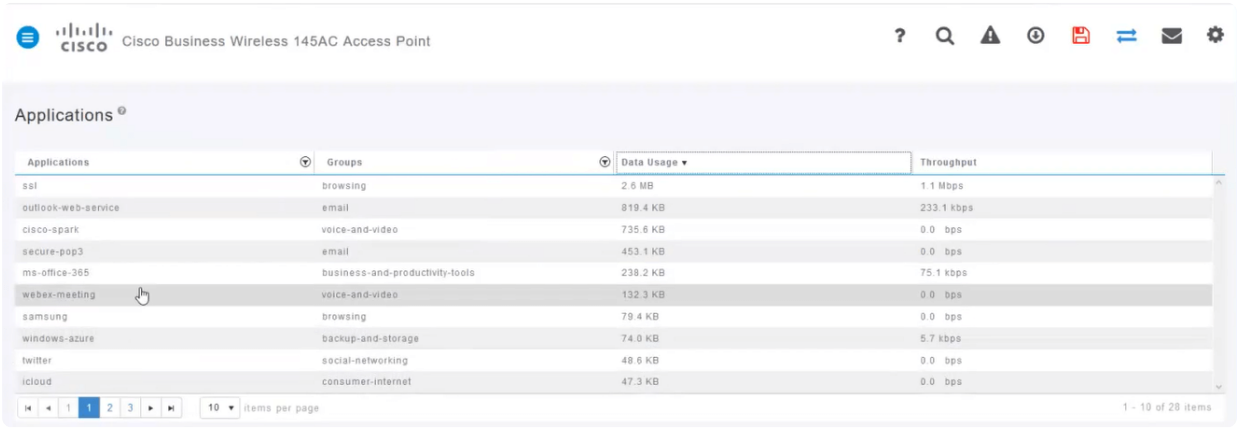
È possibile fare clic sulle schede per eseguire l'ordinamento dal più grande al più piccolo, in modo da identificare gli utenti più grandi delle risorse di rete.

Questa funzionalità è molto potente per la gestione delle risorse WLAN a livello granulare. Di seguito sono riportati alcuni dei gruppi e dei tipi di applicazione più comuni. È probabile che l'elenco ne includa molti altri, inclusi i gruppi e gli esempi seguenti:

- Ricerca
    - ES: Specifico del client, SSL
- Email
    - ES: Outlook, Secure-pop3
- Voce e video
    - ES: WebEx, Cisco Spark,
- Strumenti per il business e la produttività
    - ES: Microsoft Office 365
- Backup e storage
    - ES: Windows-Azure
- Internet consumer
    - iCloud, Google Drive

- Social networking
    - ES: Twitter, Facebook
- Aggiornamenti software
    - ES: Google-Play, IOS
- Messaggistica immediata
    - ES: Hangouts, messaggi

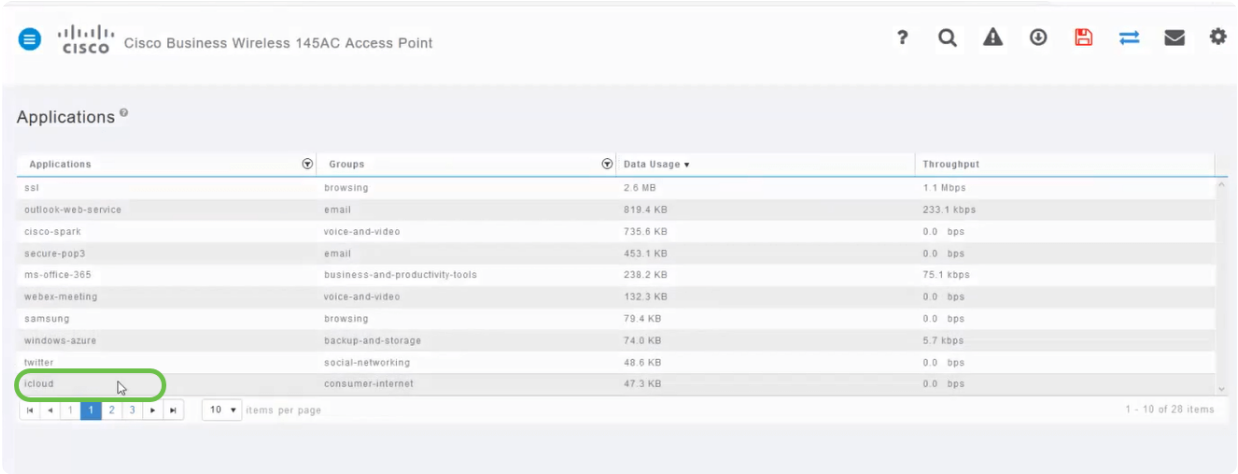
Di seguito è riportato un esempio di come apparirà la pagina quando viene compilata.



Ogni intestazione di tabella è selezionabile per l'ordinamento, il che è particolarmente utile per i campi Uso dati e Throughput.

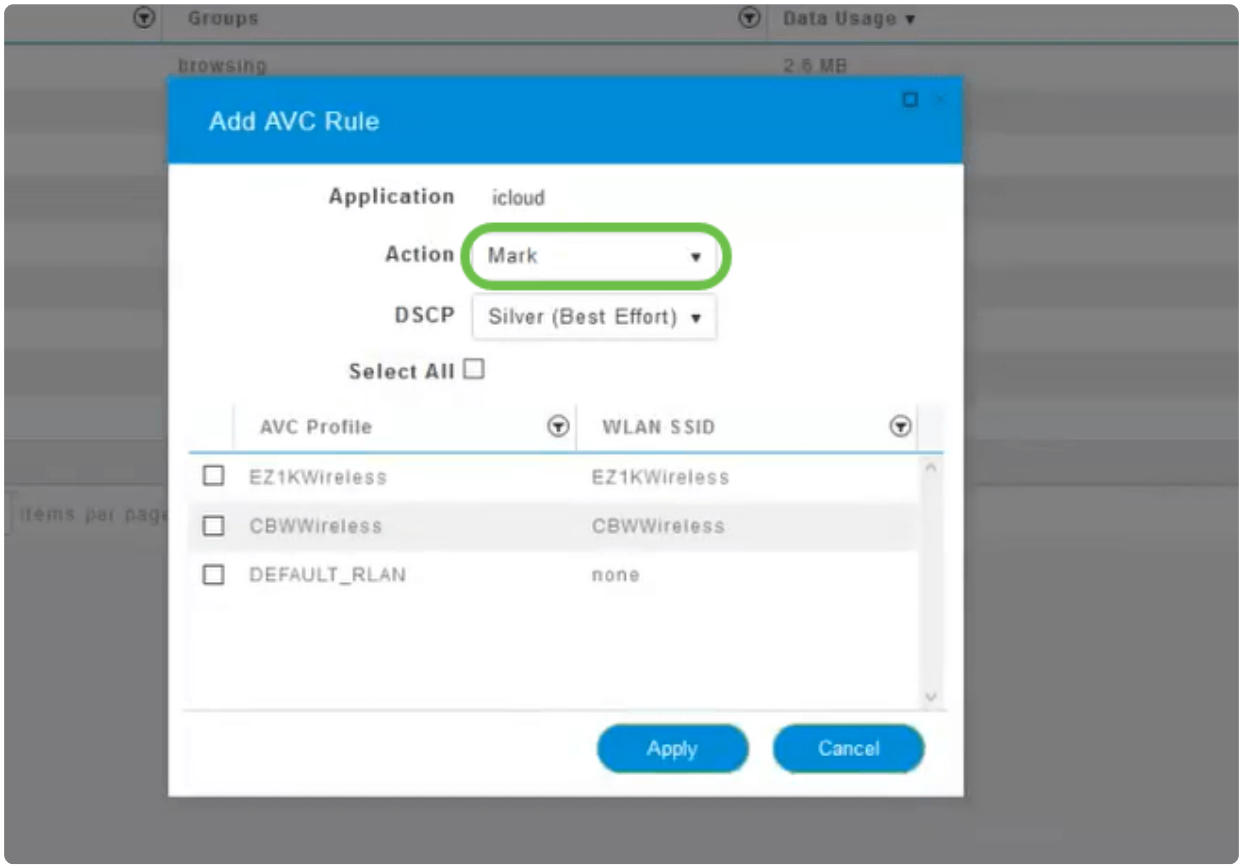
Passaggio 8

Fare clic sulla riga relativa al tipo di traffico che si desidera gestire.



Passaggio 9

Fare clic sulla casella di riepilogo a discesa Azione per selezionare la modalità di gestione del tipo di traffico.



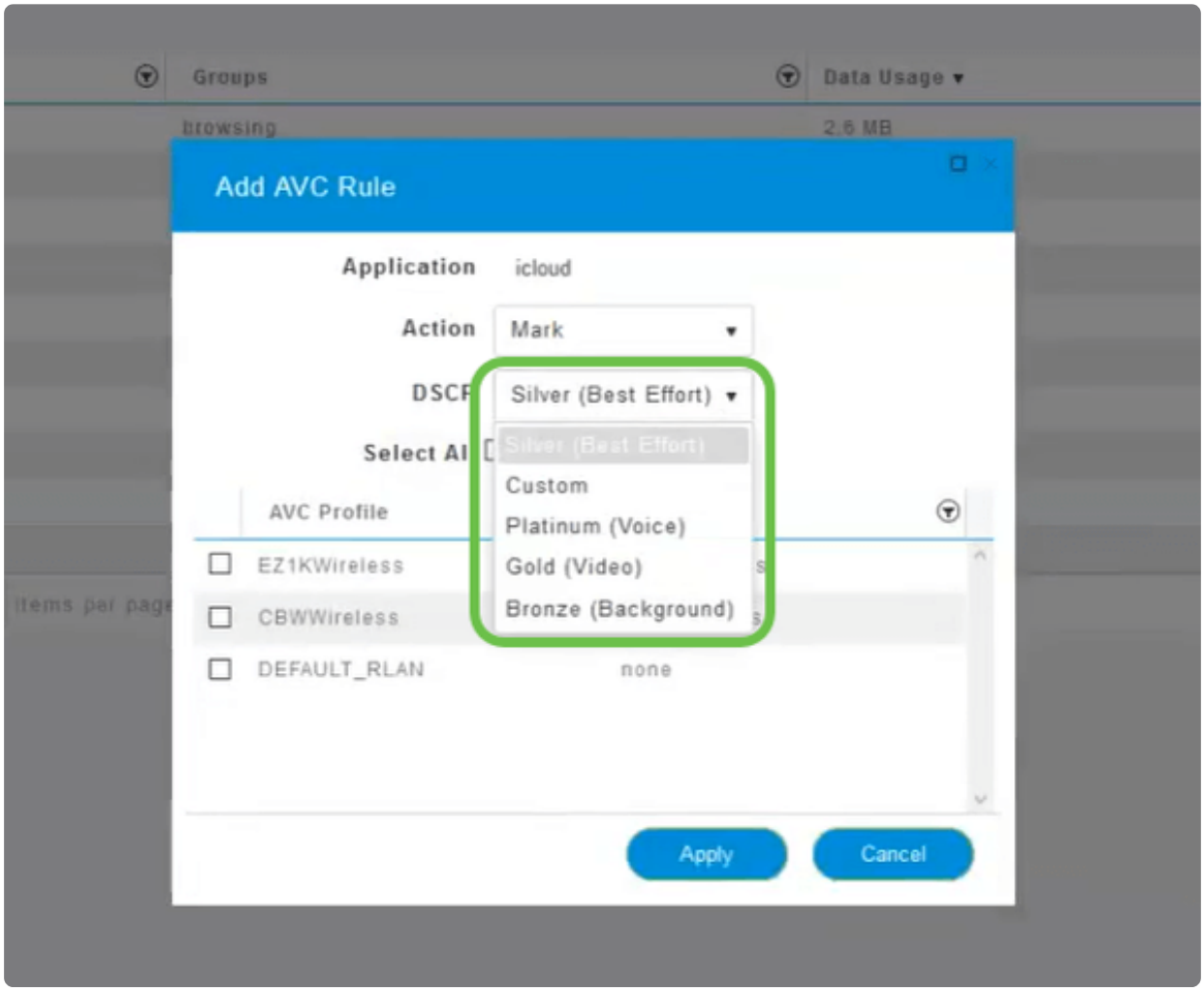
Nell'esempio, questa opzione viene lasciata a Mark.

Azione da intraprendere sul traffico

- Contrassegna: inserisce il tipo di traffico in uno dei 3 livelli DSCP (Differentiated Services Code Point), che definisce il numero di risorse disponibili per il tipo di applicazione
- Drop: non eseguire altre operazioni se non eliminare il traffico
- Limite velocità: consente di impostare la velocità media, burst rate in Kbps

Passaggio 10

Fare clic sulla casella di riepilogo a discesa nel campo DSCP per selezionare una delle opzioni seguenti.



Di seguito sono riportate le opzioni DSCP per il traffico da contrassegnare. Queste opzioni consentono di passare da un numero inferiore di risorse a un numero maggiore di risorse disponibili per il tipo di traffico che si sta modificando.

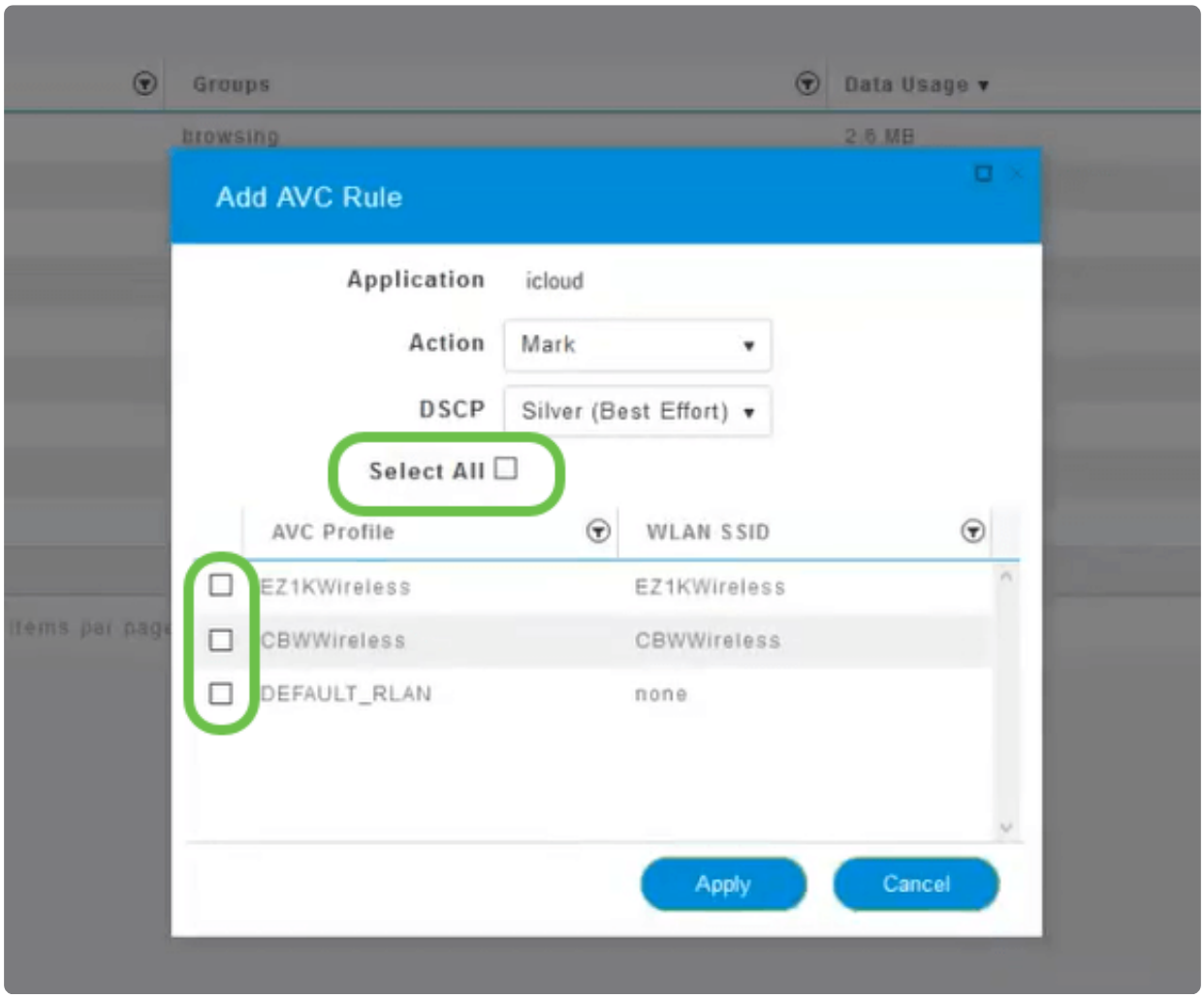
- Bronzo (sfondo) - Meno
- Argento (massimo sforzo)
- Oro (video)
- Platinum (voce) - Altro
- Personalizzato - Set di utenti

Per convenzione Web, il traffico è migrato verso l'esplorazione SSL, che impedisce la visualizzazione degli elementi all'interno dei pacchetti quando questi vengono spostati dalla rete alla WAN. Per questo motivo, la maggior parte del traffico Web utilizza SSL.

L'impostazione del traffico SSL per una priorità inferiore può influire sull'esplorazione.

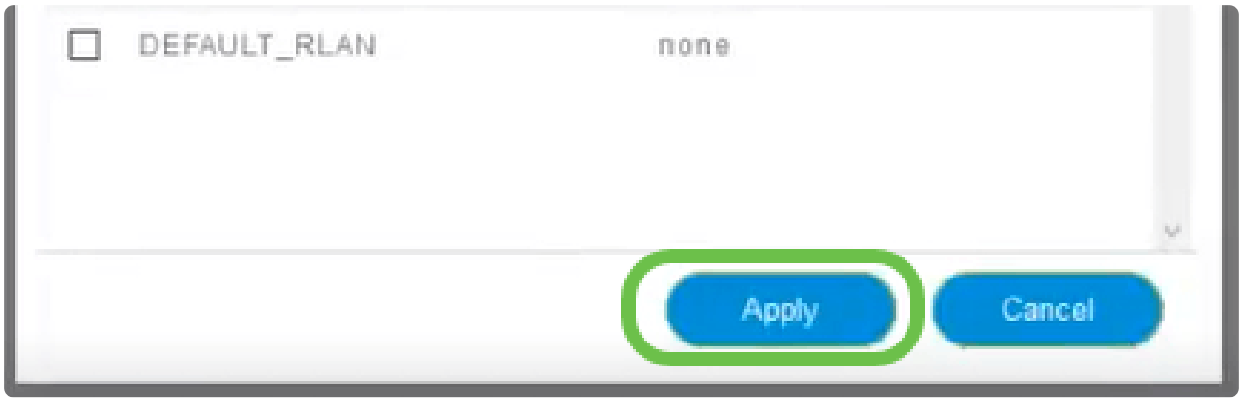
Passaggio 11

Selezionare il singolo SSID che si desidera eseguire con questo criterio oppure fare clic su Seleziona tutto.



Passaggio 12

Fare clic su Applica per iniziare il criterio.



Due casi in cui ciò potrebbe applicarsi:

- Guest/Utenti che gestiscono una grande quantità di traffico impedendo il passaggio del traffico mission-critical. Puoi aumentare la priorità per la voce, abbassare la priorità del traffico Netflix per migliorare le cose.
- Gli aggiornamenti software di grandi dimensioni che vengono scaricati durante l'orario di ufficio possono non essere considerati prioritari o avere una velocità limitata.

Ce l'hai fatta! La profilatura delle applicazioni è uno strumento molto potente che può essere ulteriormente abilitato attivando anche la profilatura dei client, come illustrato nella sezione successiva.

Creazione profilo client tramite interfaccia utente Web (facoltativo)

Al momento della connessione a una rete, i dispositivi scambiano le informazioni di profilatura dei client. Per impostazione predefinita, la profilatura client è disabilitata. Tali informazioni possono includere:

- Nome host - o il nome del dispositivo
- Sistema operativo: il software principale del dispositivo
- Versione del sistema operativo: iterazione del software applicabile

Le statistiche relative a questi client includono la quantità di dati utilizzati e il throughput.

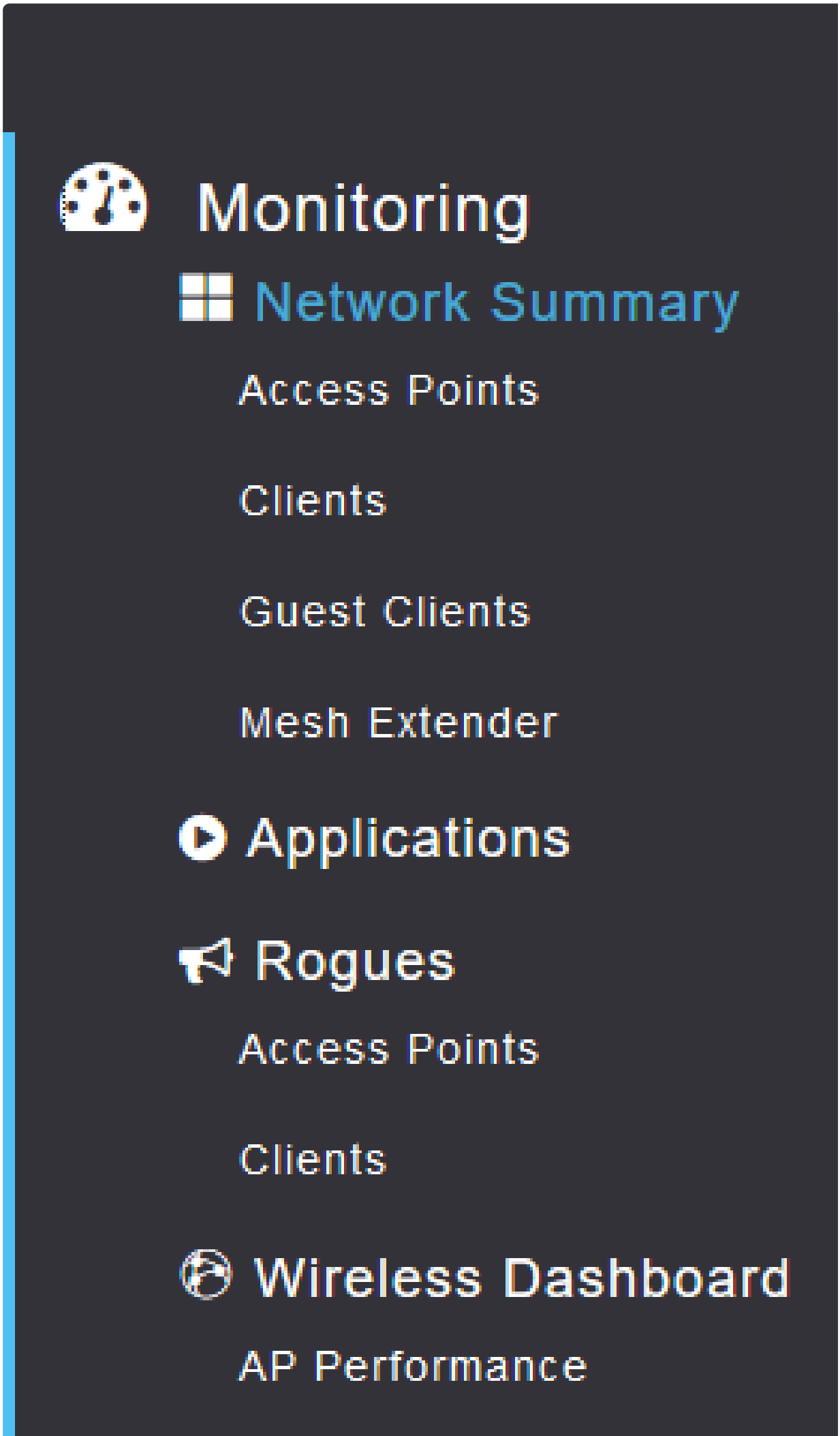
La registrazione dei profili client consente un maggiore controllo sulla rete locale (LAN) wireless. Oppure potreste usarlo come funzione di un'altra feature. Ad esempio,

utilizzando tipi di dispositivi di limitazione delle applicazioni che non trasportano dati mission-critical per l'azienda.

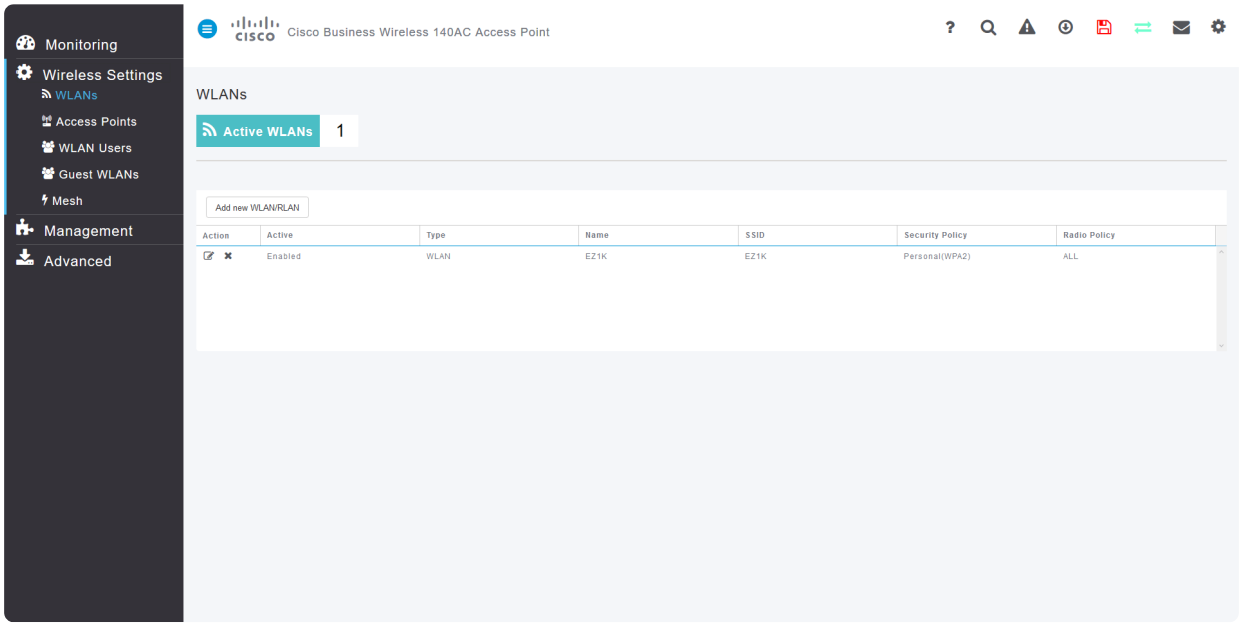
Una volta abilitati, i dettagli client per la rete sono disponibili nella sezione Monitoraggio dell'interfaccia utente Web.

Passaggio 1

Fare clic su Impostazioni wireless.

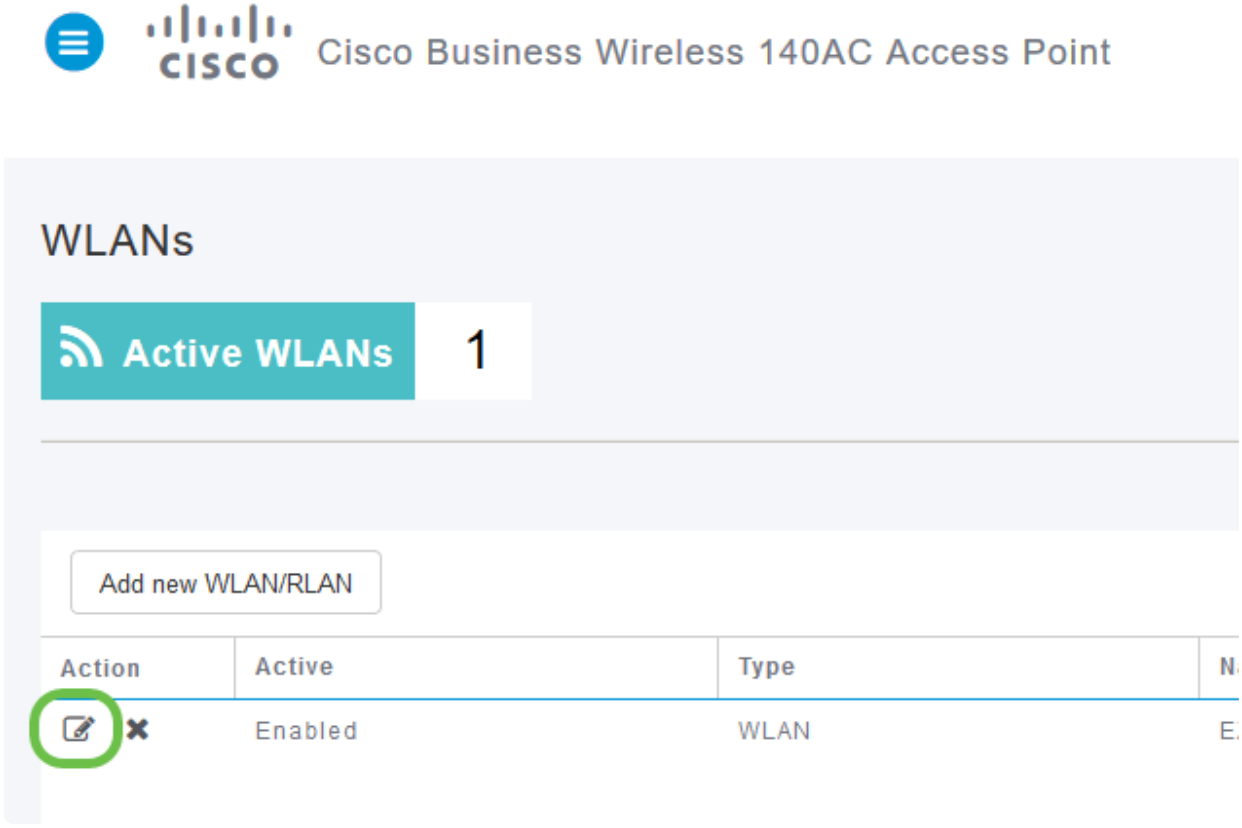

Monitoring
Network Summary
Access Points
Clients
Guest Clients
Mesh Extender
Applications
Rogues
Access Points
Clients
Wireless Dashboard
AP Performance

Le informazioni riportate di seguito sono simili a quelle visualizzate quando si fa clic sul collegamento Impostazioni wireless:



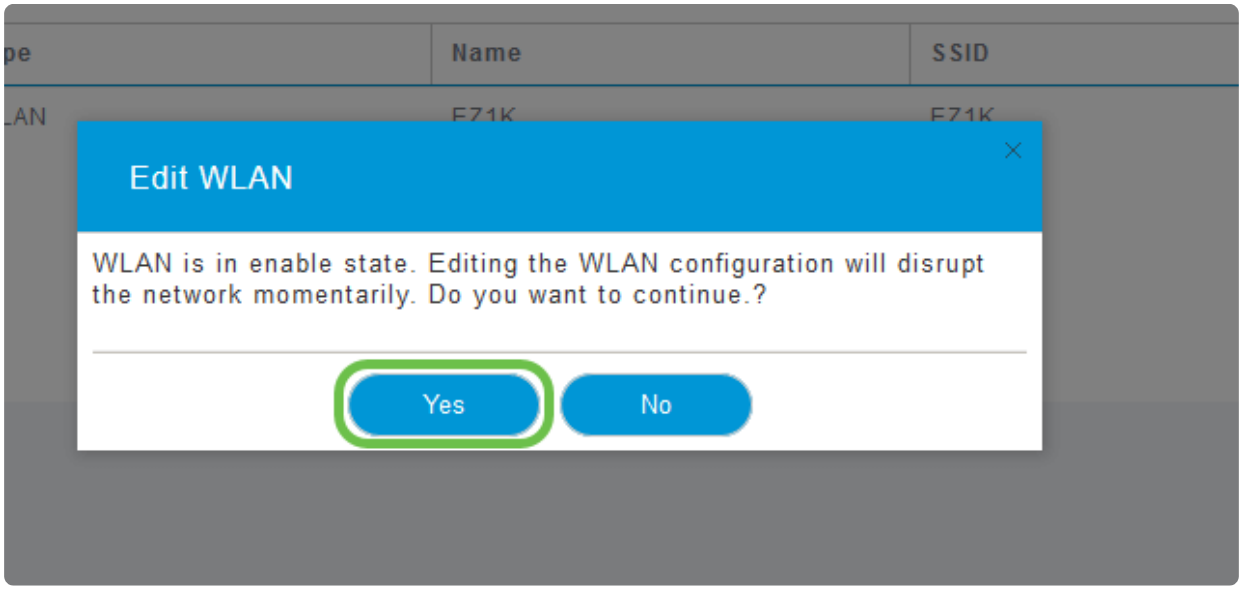
Passaggio 2

Decidere quale WLAN usare per l'applicazione e fare clic sull'icona di modifica a sinistra di essa.



Passaggio 3

È possibile che venga visualizzato un menu a comparsa simile al seguente. Questo messaggio importante può influire temporaneamente sul servizio di rete. Fare clic su Sì per procedere.

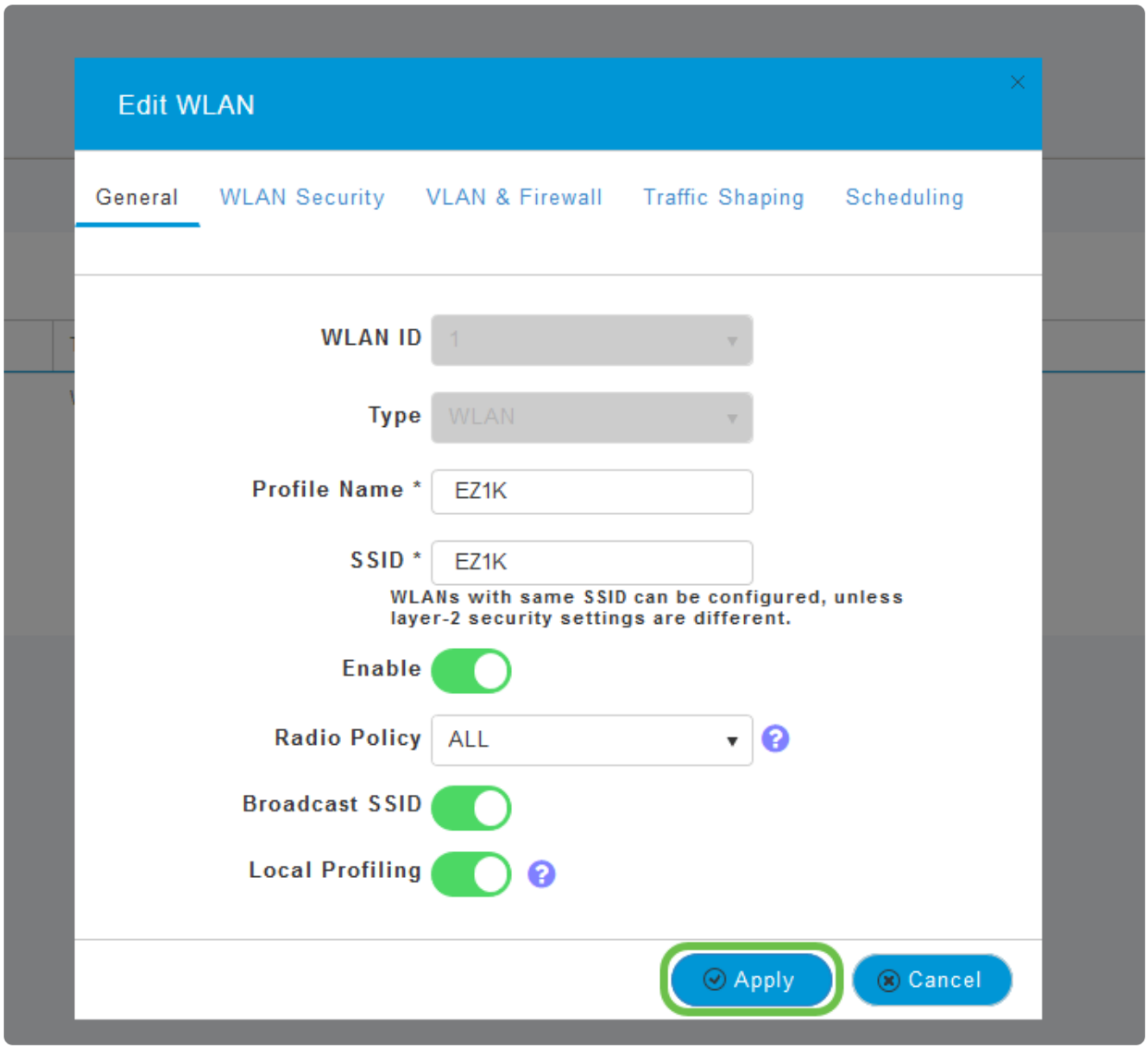


Passaggio 4

Attivare o disattivare la profilatura del client facendo clic sul pulsante Profilatura locale.

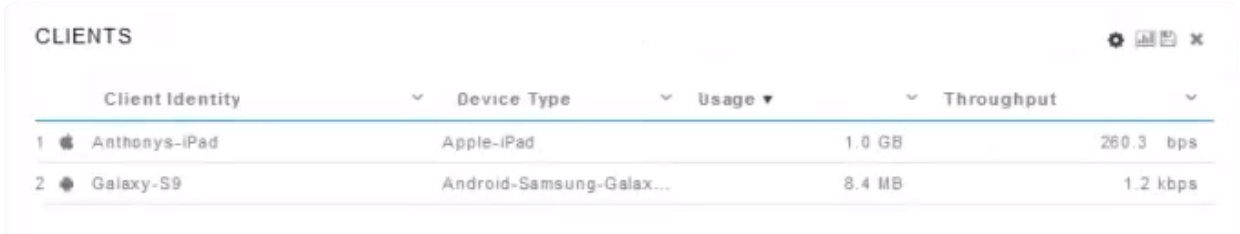
Passaggio 5

Fare clic su Apply (Applica).



Passaggio 6

Fare clic sulla voce di menu della sezione Monitoraggio sul lato sinistro. I dati client verranno visualizzati nel dashboard della scheda Monitoraggio.



Conclusioni

La configurazione della rete protetta è stata completata. Che sensazione fantastica, ora prendi un minuto per festeggiare e poi vai al lavoro!

Vogliamo il meglio per i nostri clienti, quindi se hai commenti o suggerimenti su questo argomento, invia un'e-mail al team Cisco Content.

Per leggere altri articoli e documentazione, consultare le pagine di supporto dell'hardware:

- Cisco RV345P VPN Router con PoE
- Access point Cisco Business 140AC
- Cisco Business 142ACM Mesh Extender

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).