Autenticazione SSH su uno switch Cisco Business 350

Obiettivo

In questo documento viene spiegato come configurare l'autenticazione server su uno switch Cisco Business serie 350.

Introduzione

Secure Shell (SSH) è un protocollo che permette di connettersi in modo sicuro a dispositivi di rete remoti. Questa connessione offre una funzionalità simile a una connessione Telnet, con la differenza che è crittografata. SSH consente all'amministratore di configurare lo switch dalla riga di comando (CLI) con un programma di terze parti. Lo switch funziona come client SSH e fornisce funzionalità SSH agli utenti della rete. Lo switch usa un server SSH per fornire i servizi SSH. Quando l'autenticazione del server SSH è disabilitata, lo switch considera attendibile qualsiasi server SSH, riducendo la sicurezza della rete. Se il servizio SSH è abilitato sullo switch, la sicurezza è migliorata.

Dispositivi interessati | Versione software

- CBS350 (Scheda tecnica) | 3.0.0.69 (scarica la versione più recente)
- CBS350-2X (Scheda tecnica) | 3.0.0.69 (scarica la versione più recente)
- CBS350-4X (Scheda tecnica) | 3.0.0.69 (scarica la versione più recente)

Configurazione delle impostazioni di autenticazione del server SSH

Abilitazione del servizio SSH

Quando l'autenticazione del server SSH è abilitata, il client SSH in esecuzione sul dispositivo autentica il server SSH usando il seguente processo di autenticazione:

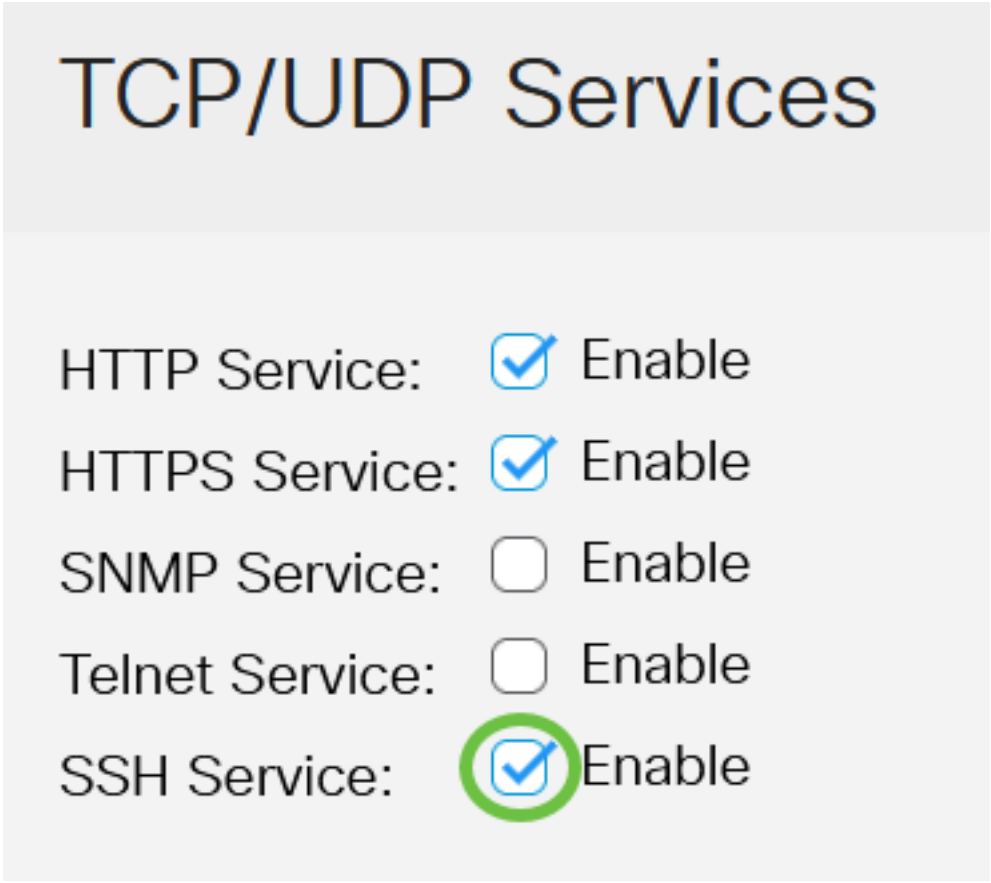
- Il dispositivo calcola l'impronta digitale della chiave pubblica ricevuta del server SSH.
- Il dispositivo cerca nella tabella SSH Trusted Servers l'indirizzo IP e il nome host del server SSH. Si può verificare uno dei tre risultati seguenti:
    1. Se viene trovata una corrispondenza sia per l'indirizzo che per il nome host del server e la relativa impronta digitale, il server viene autenticato.
    2. Se vengono trovati un indirizzo IP e un nome host corrispondenti, ma non vi sono impronte digitali corrispondenti, la ricerca continua. Se non viene trovata alcuna impronta digitale corrispondente, la ricerca viene completata e l'autenticazione non riesce.
    3. Se non vengono trovati indirizzi IP e nomi host corrispondenti, la ricerca viene completata e l'autenticazione ha esito negativo.
    4. Se la voce relativa al server SSH non viene trovata nell'elenco dei server trusted, il processo non riesce.

Per supportare la configurazione automatica di uno switch predefinito con configurazione

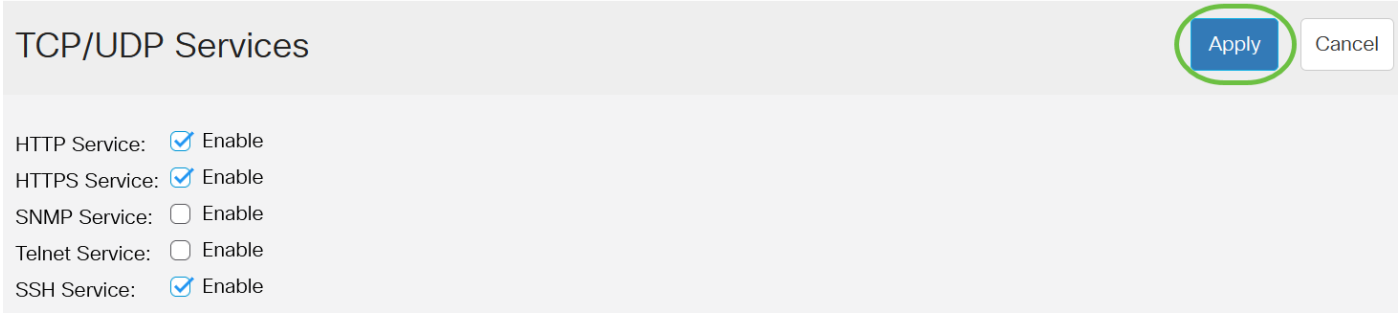
predefinita, l'autenticazione del server SSH è disabilitata per impostazione predefinita.

Passaggio 1. Accedere all'utility basata sul Web e scegliere **Sicurezza > Servizi TCP/UDP**.

Passaggio 2. Selezionare la casella di controllo **Servizio SSH** per abilitare l'accesso del prompt dei comandi degli switch tramite SSH.

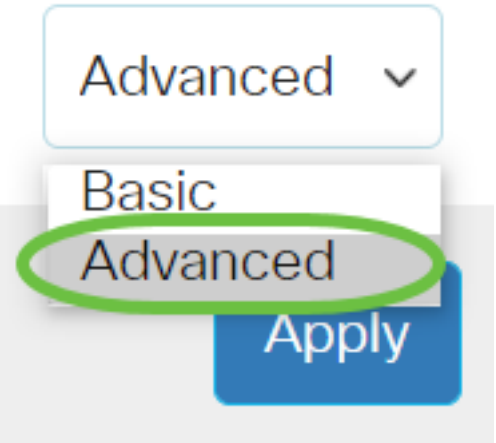


Passaggio 3. Fare clic su **Apply** (Applica) per abilitare il servizio SSH.

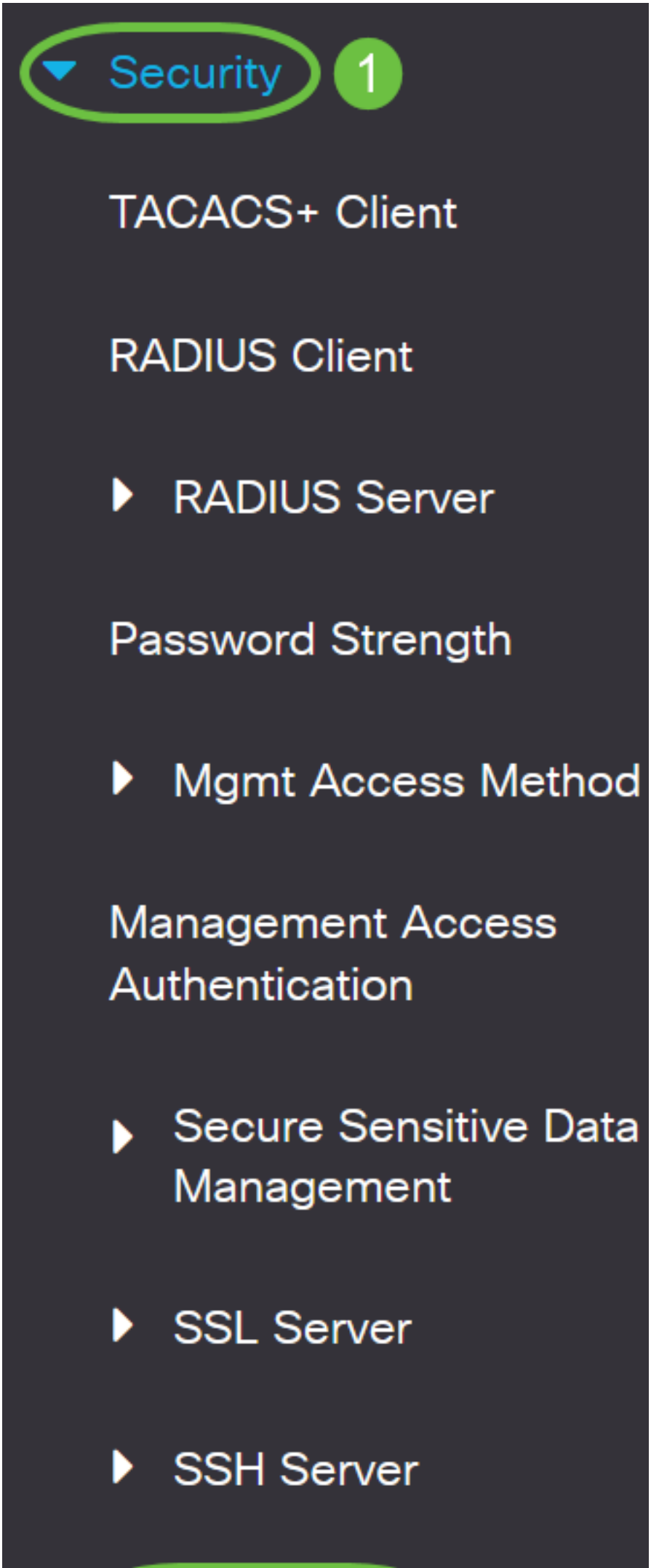


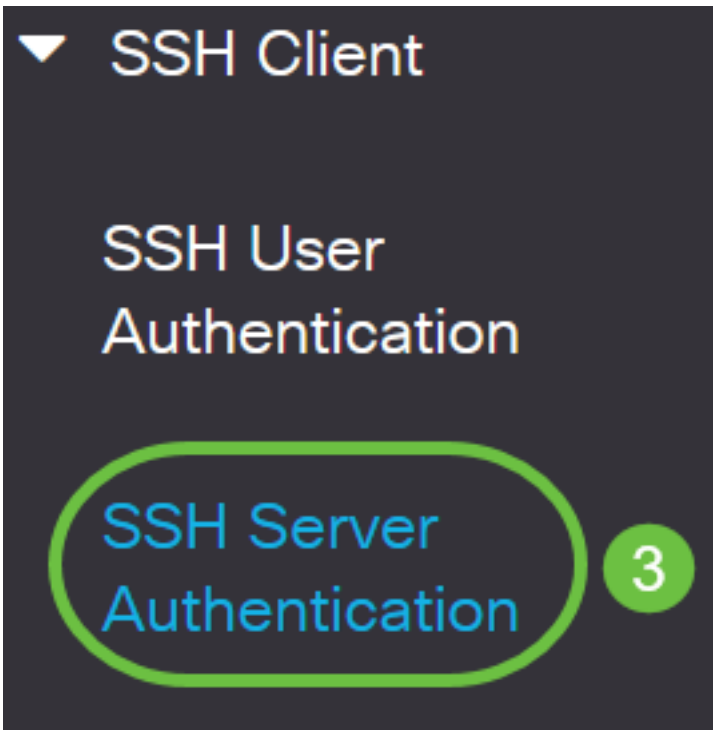
Configurazione delle impostazioni di autenticazione del server SSH

Passaggio 1. Accedere all'utility basata sul Web dello switch, quindi selezionare Advanced nell'elenco a discesa Display Mode (Modalità di visualizzazione).

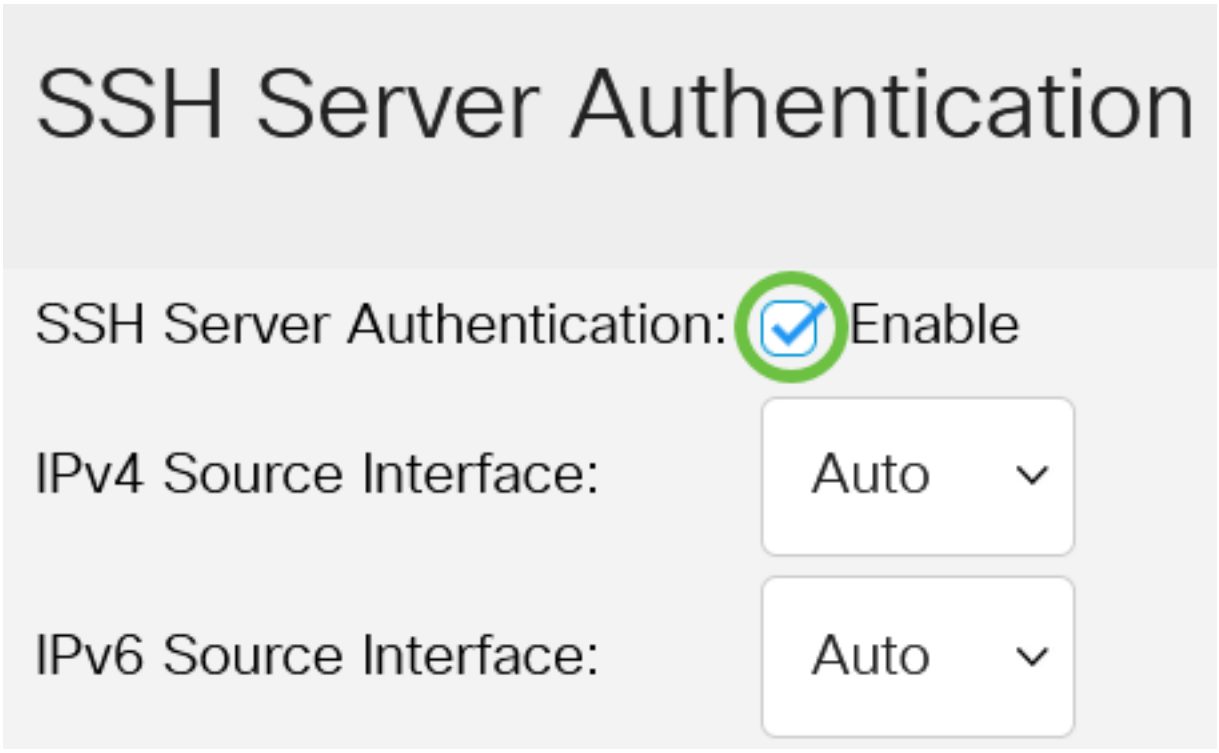


Passaggio 2. Selezionare **Security > SSH Client > SSH Server Authentication** (Sicurezza > Client SSH > Autenticazione server SSH).

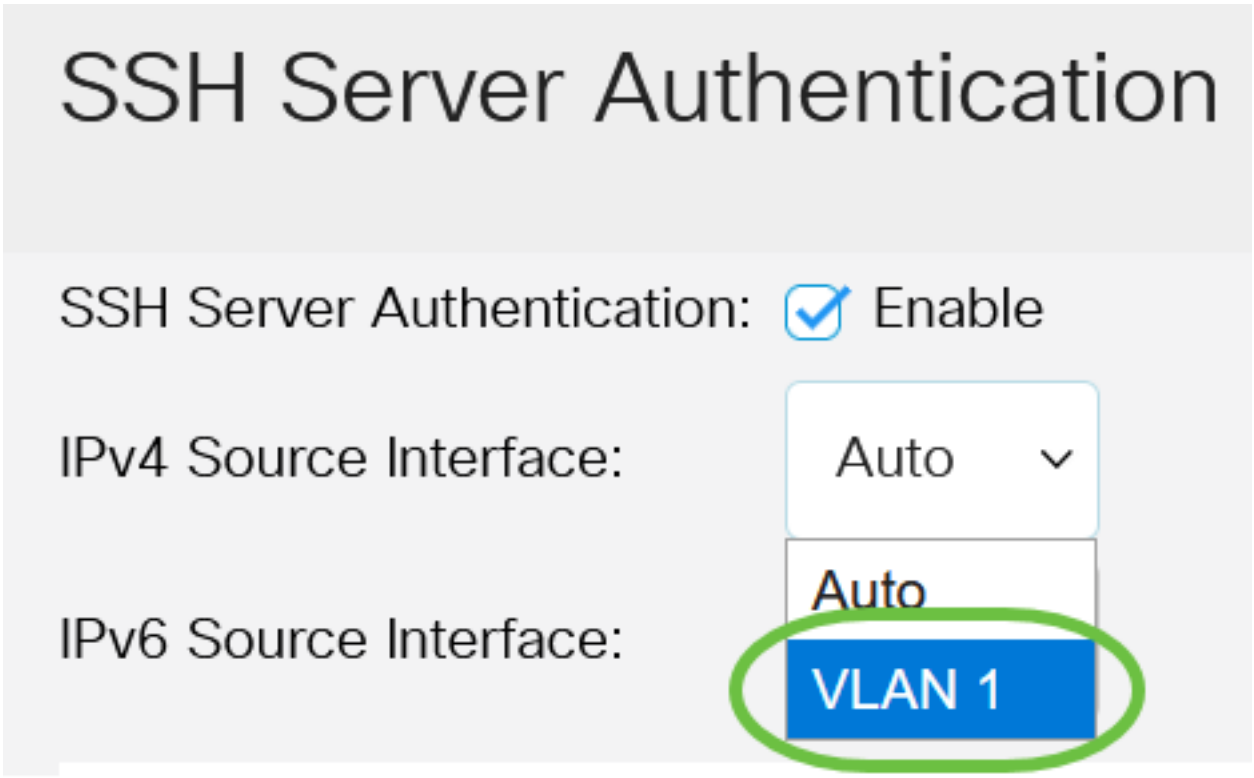

Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Password Strength
Mgmt Access Method
Management Access Authentication
Secure Sensitive Data Management
SSL Server
SSH Server



Passaggio 2. Selezionare la casella di controllo **Abilita** autenticazione server SSH per abilitare l'autenticazione del server SSH.

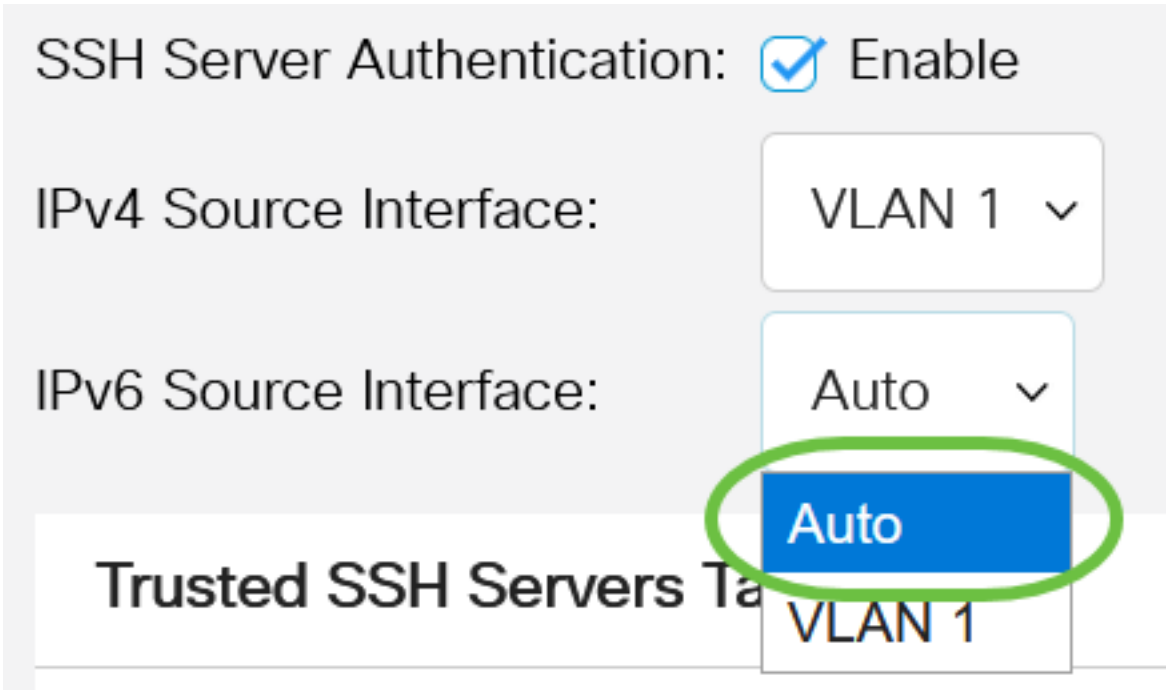


Passaggio 3. (Facoltativo) Nell'elenco a discesa Interfaccia di origine IPv4, scegliere l'interfaccia di origine il cui indirizzo IPv4 verrà utilizzato come indirizzo IPv4 di origine per i messaggi utilizzati nella comunicazione con i server SSH IPv4.



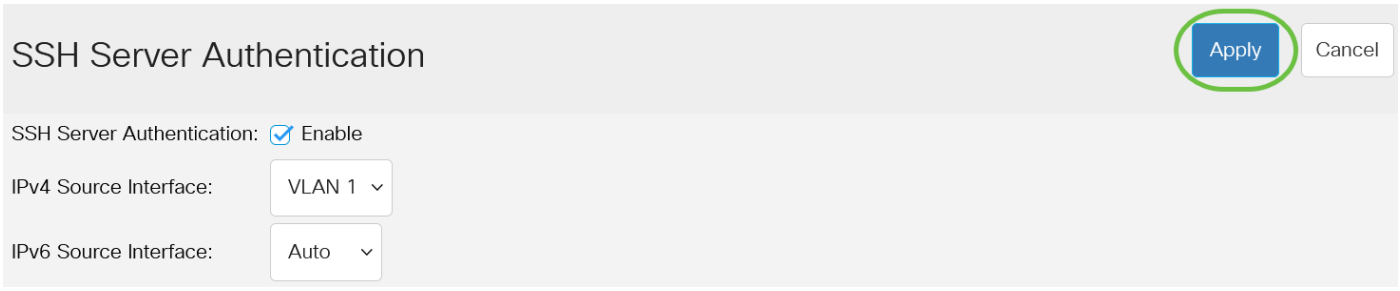
Se si sceglie l'opzione Auto, il sistema recupera l'indirizzo IP di origine dall'indirizzo IP definito sull'interfaccia in uscita. nell'esempio, viene scelta la VLAN1.

Passaggio 4. (Facoltativo) Nell'elenco a discesa Interfaccia di origine IPv6 scegliere l'interfaccia di origine il cui indirizzo IPv6 verrà utilizzato come indirizzo IPv6 di origine per i messaggi utilizzati nella comunicazione con i server SSH IPv6.

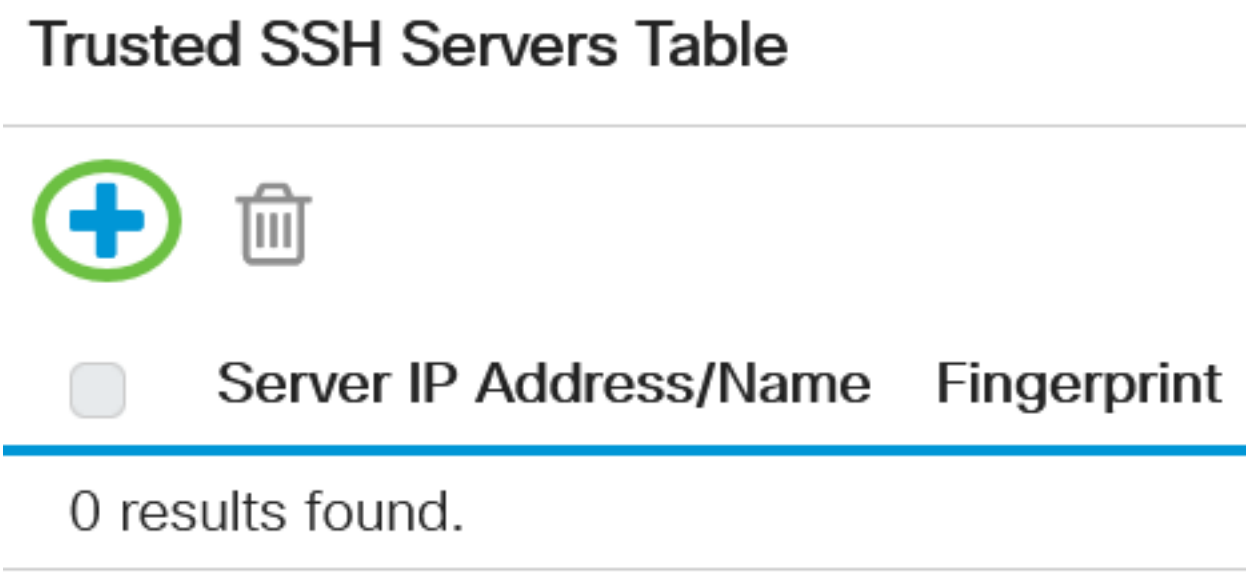


In questo esempio, viene scelta l'opzione Auto. L'indirizzo IP di origine verrà ricavato dall'indirizzo IP definito sull'interfaccia in uscita.

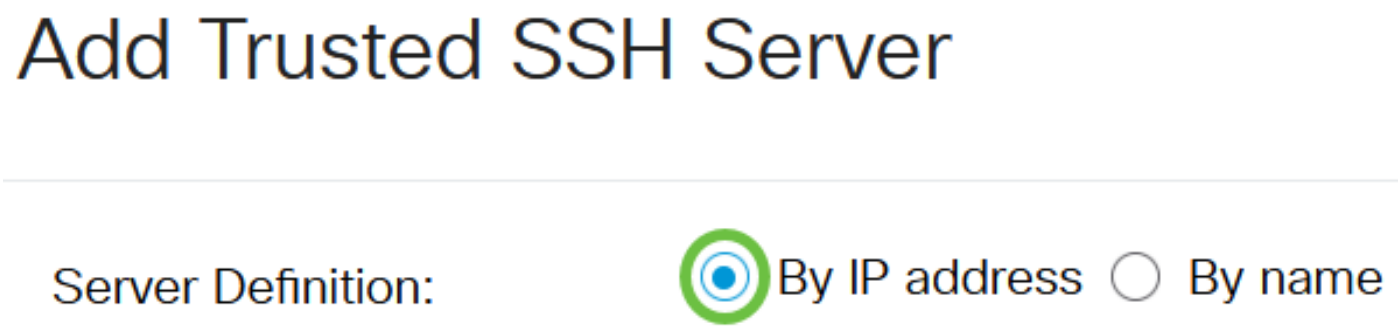
Passaggio 5. Fare clic su **Applica**.



Passaggio 6. Per aggiungere un server trusted, fare clic su **Add** (Aggiungi) nella tabella Trusted SSH Servers (Server SSH trusted).



Passaggio 7. Nell'area Definizione server, fare clic su uno dei metodi disponibili per definire il server SSH.

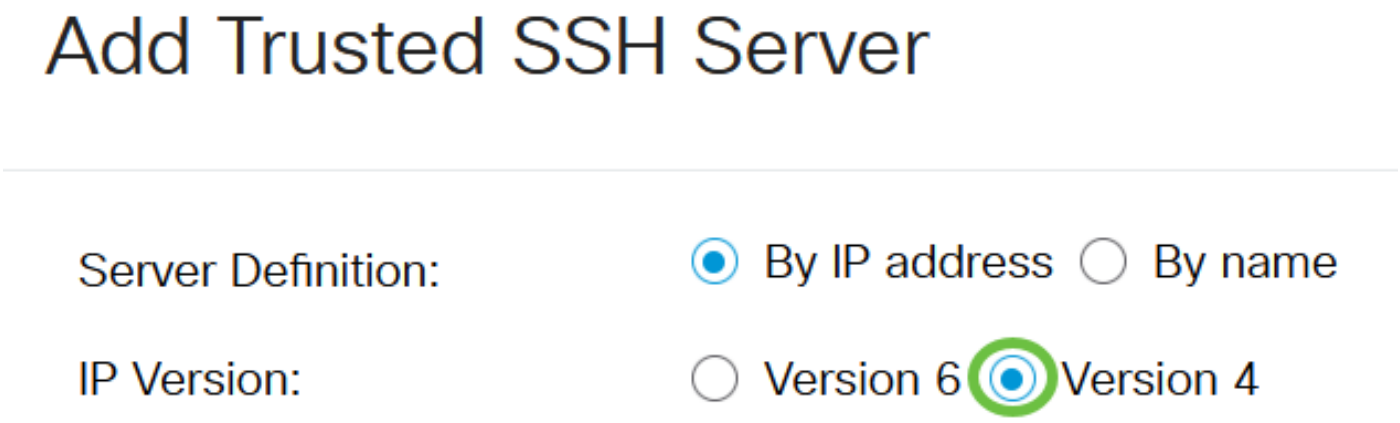


Le opzioni sono:

- Per indirizzo IP: questa opzione consente di definire il server SSH con un indirizzo IP.
- Per nome: questa opzione consente di definire il server SSH con un nome di dominio completo.

Nell'esempio, viene scelto By IP address. Se si sceglie Per nome, andare al passo 11.

Passaggio 8. (Facoltativo) Se si sceglie Per indirizzo IP nel passaggio 6, fare clic sulla versione IP del server SSH nel campo Versione IP.

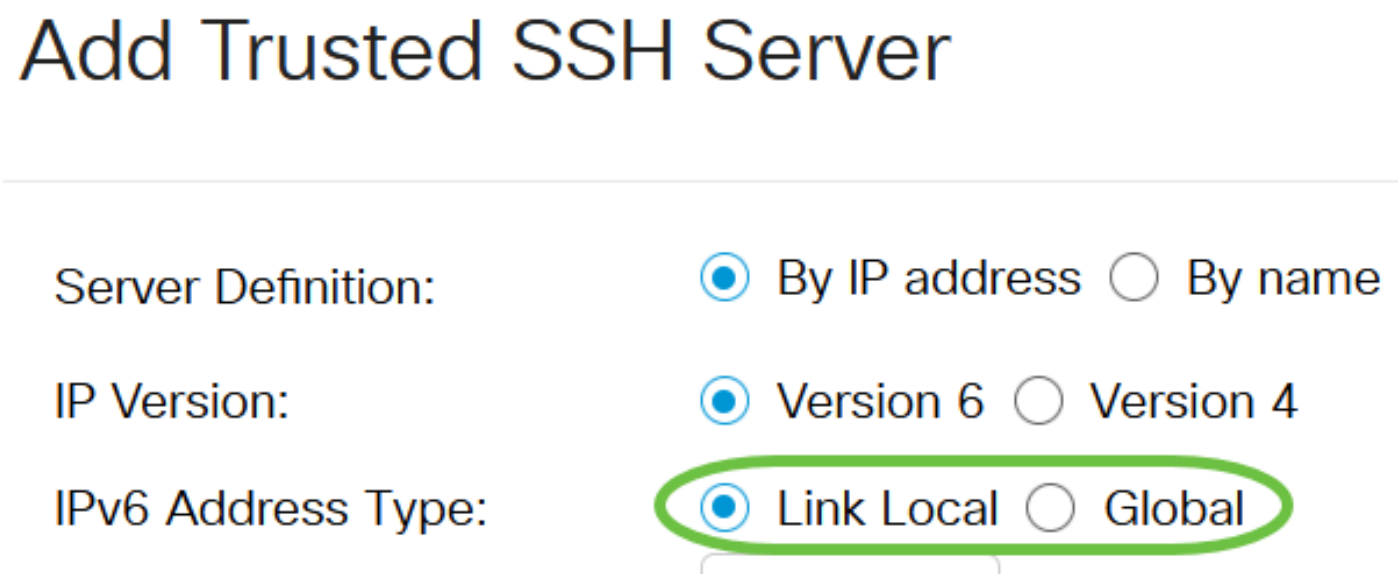


Le opzioni disponibili sono:

- Versione 6 - Questa opzione consente di immettere un indirizzo IPv6.
- Versione 4 - Questa opzione consente di immettere un indirizzo IPv4.

Nell'esempio, è stata scelta la versione 4. Il pulsante di opzione IPv6 è disponibile solo se nello switch è configurato un indirizzo IPv6.

Passaggio 9. (Facoltativo) Se si sceglie la versione 6 come versione dell'indirizzo IP nel passaggio 7, fare clic sul tipo di indirizzo IPv6 in Tipo di indirizzo IPv6.

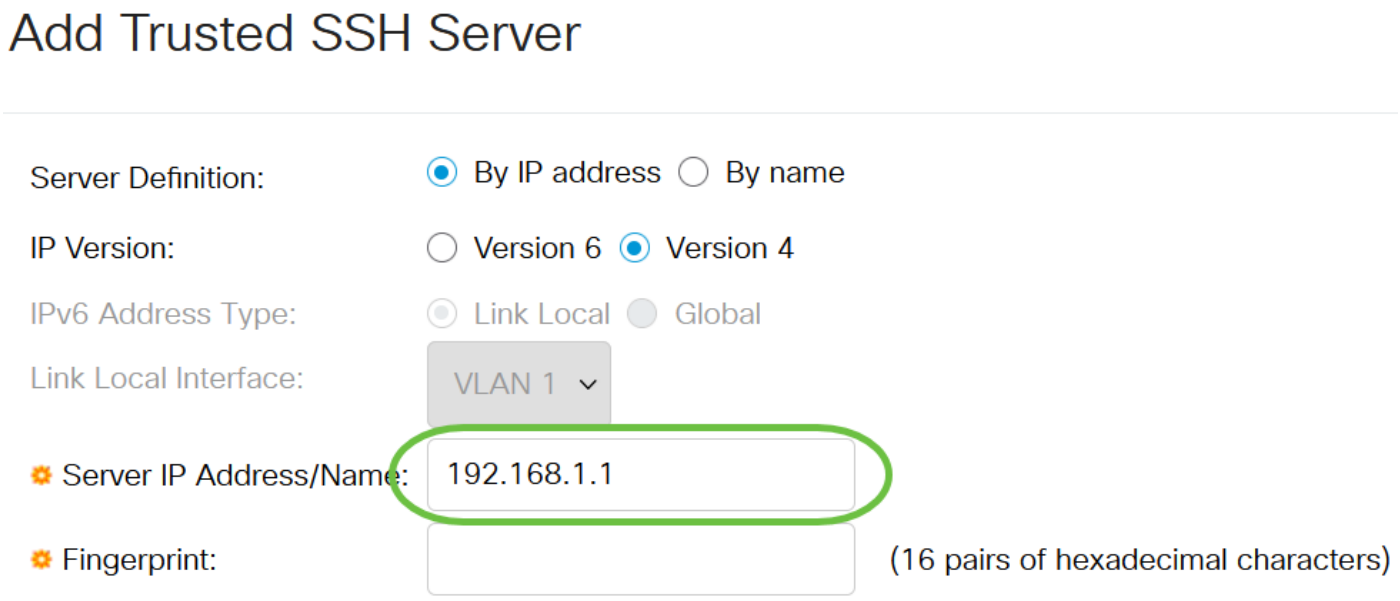


Le opzioni disponibili sono:

- Collegamento locale: l'indirizzo IPv6 identifica in modo univoco gli host su un singolo collegamento di rete. Un indirizzo locale del collegamento ha un prefisso FE80, non è instradabile e può essere utilizzato per la comunicazione solo sulla rete locale. È supportato un solo indirizzo locale del collegamento. Se sull'interfaccia esiste un indirizzo locale del collegamento, questa voce sostituisce l'indirizzo nella configurazione. Questa opzione è selezionata per default.
- Globale - L'indirizzo IPv6 è un unicast globale visibile e raggiungibile da altre reti.

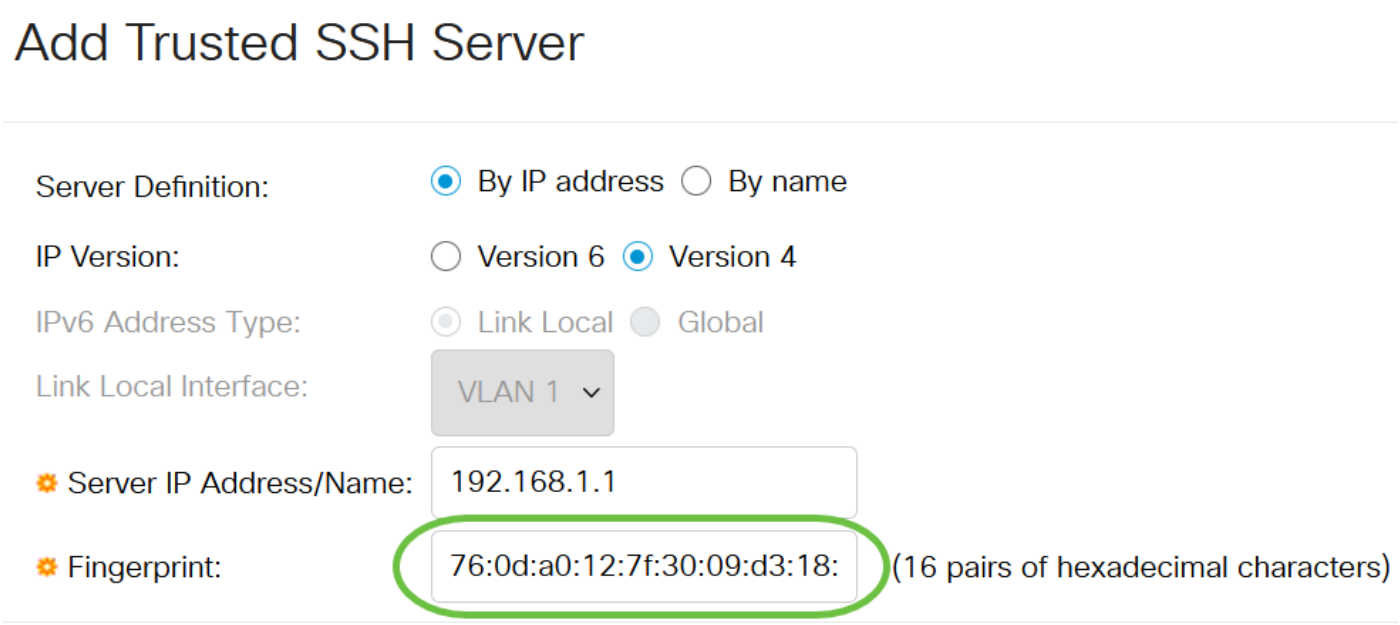
Passaggio 10. (Facoltativo) Se nel passaggio 9 è stato scelto Collega locale come tipo di indirizzo IPv6, scegliere l'interfaccia appropriata nell'elenco a discesa Collega interfaccia locale.

Passaggio 11. Nel campo *Indirizzo IP/Nome server*, immettere l'indirizzo IP o il nome di dominio del server SSH.

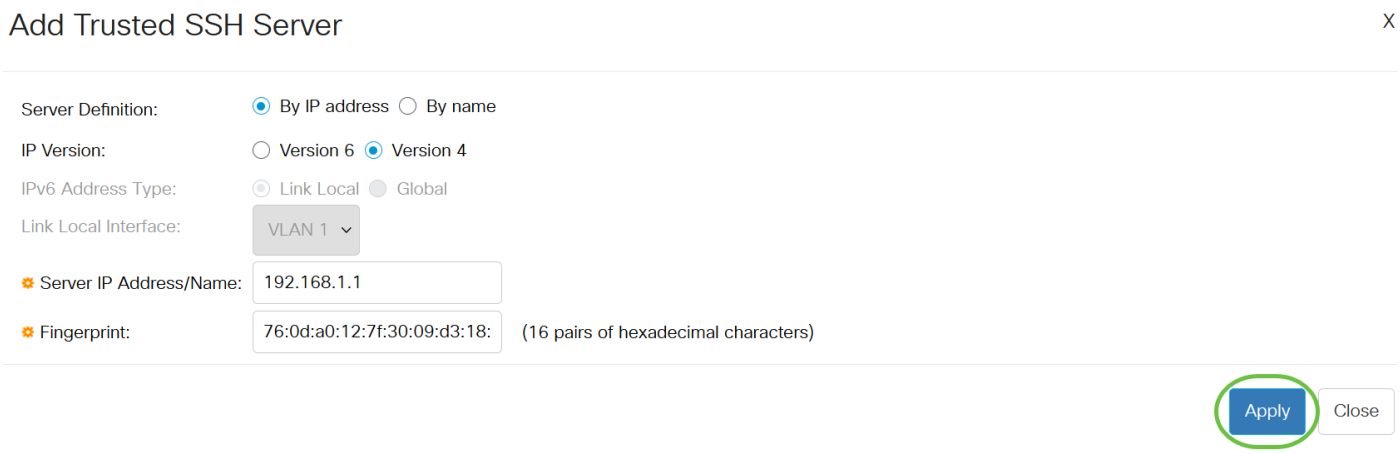


nell'esempio, viene immesso un indirizzo IP.

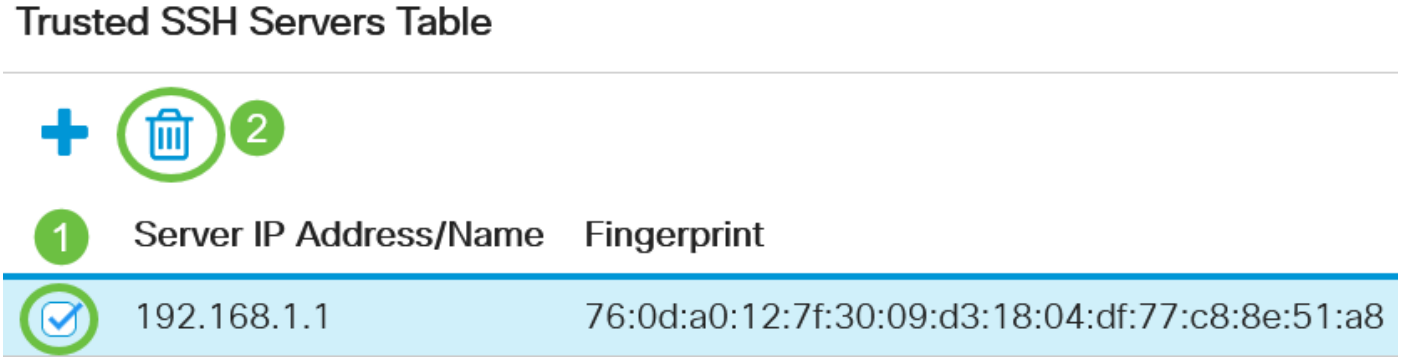
Passaggio 12. Nel campo *Fingerprint* (Impronta digitale), immettere l'impronta digitale del server SSH. Un'impronta digitale è una chiave crittografata utilizzata per l'autenticazione. In questo caso, l'impronta digitale viene utilizzata per autenticare la validità del server SSH. Se esiste una corrispondenza tra l'indirizzo IP/il nome del server e l'impronta digitale, il server SSH viene autenticato.



Passaggio 13. Fare clic su **Apply** (Applica) per salvare la configurazione.



Passaggio 14. (Facoltativo) Per eliminare un server SSH, selezionare la casella di controllo del server che si desidera eliminare, quindi fare clic su **Elimina**.



Passaggio 15. (Facoltativo) Fare clic sul pulsante **Save** nella parte superiore della pagina per salvare le modifiche nel file della configurazione di avvio.

SSH Server Authentication

A questo punto, sono state configurate le impostazioni di autenticazione del server SSH sullo switch Cisco Business serie 350.

Cerchi altri articoli sullo switch CBS350? Per ulteriori informazioni, visitare i seguenti link.

Impostazioni indirizzo IP Impostazioni stack Selettore della modalità di stack Linee guida per lo stack Autenticazione server SSH Recupero password Access CLI con PuTTy Creazione di VLAN Ripristina switch