

Configurazione delle impostazioni di autenticazione utente Secure Shell (SSH) su uno switch Cisco Business serie 350

Obiettivo

In questo documento viene spiegato come configurare l'autenticazione dell'utente client sugli 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.

In modalità CLI tramite SSH, l'amministratore può eseguire configurazioni più avanzate in una connessione protetta. Le connessioni SSH sono utili per risolvere i problemi di una rete in remoto, nei casi in cui l'amministratore di rete non sia fisicamente presente sul sito di rete. Lo switch consente all'amministratore di autenticare e gestire gli utenti per connettersi alla rete tramite SSH. L'autenticazione viene effettuata tramite una chiave pubblica che l'utente può utilizzare per stabilire una connessione SSH a una rete specifica.

La funzionalità client SSH è un'applicazione che viene eseguita sul protocollo SSH per fornire l'autenticazione e la crittografia del dispositivo. Consente a un dispositivo di stabilire una connessione protetta e crittografata a un altro dispositivo che esegue il server SSH. Con l'autenticazione e la crittografia, il client SSH permette una comunicazione sicura su una connessione Telnet non protetta.

Dispositivi interessati | Versione software

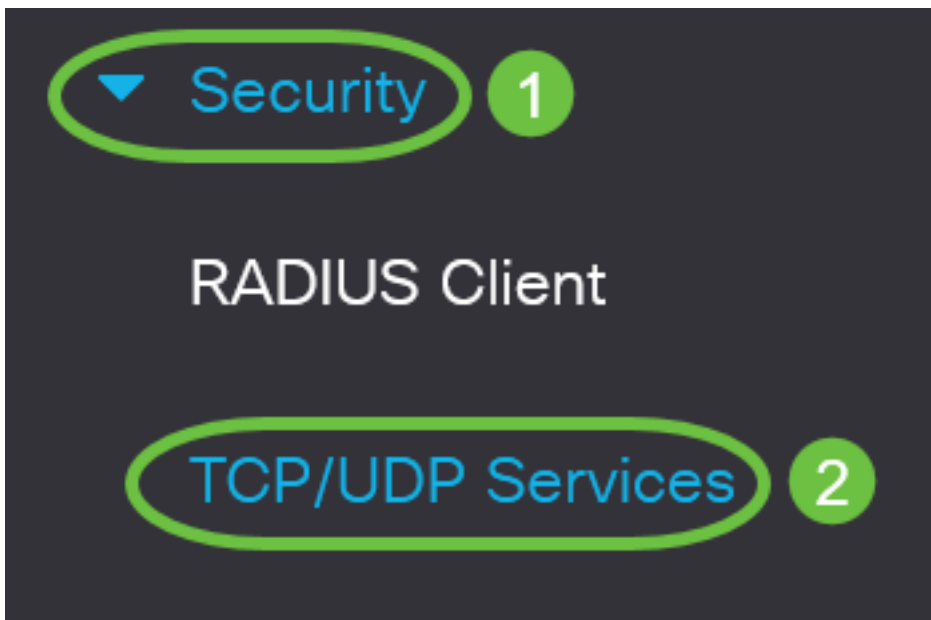
- CBS350 ([Scheda tecnica](#)) | 3.0.0.69 (scarica la versione più recente)
- CBS350-2X ([Scheda tecnica](#)) | 3.0.0.69 (scarica la versione più recente)
- CBS350-4X ([Scheda tecnica](#)) | 3.0.0.69 (scarica la versione più recente)

Configurazione delle impostazioni di autenticazione utente del client SSH

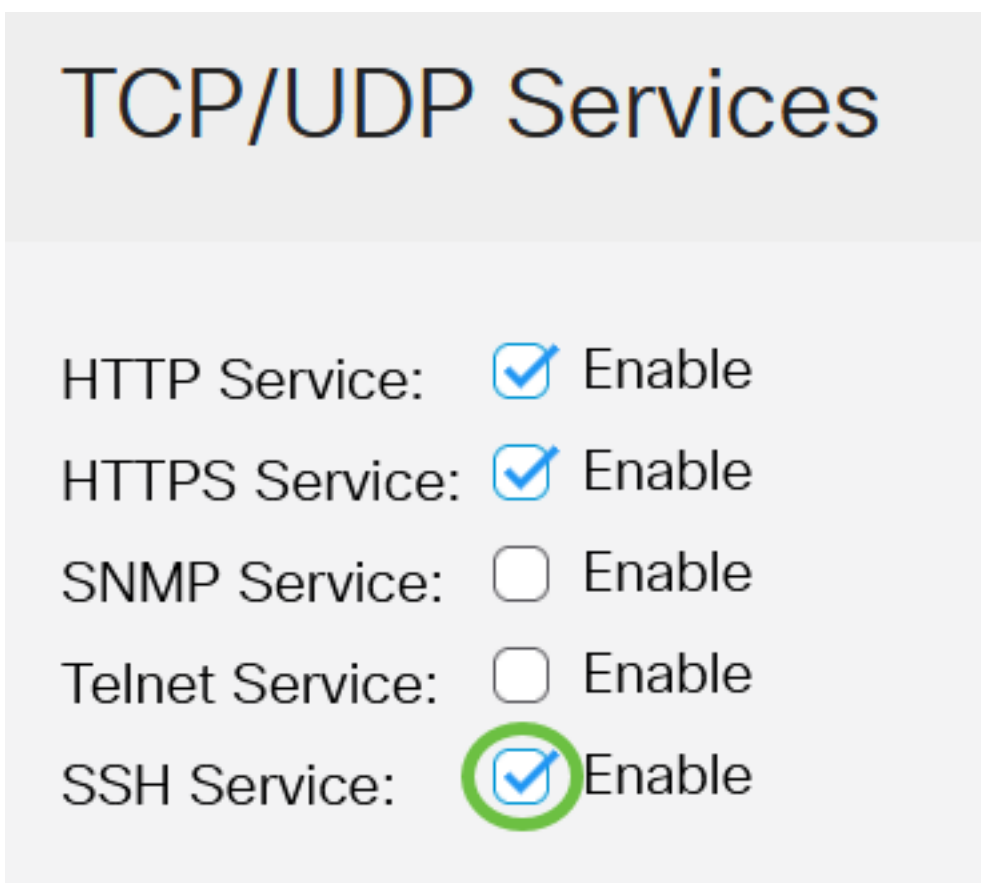
Abilitazione del servizio SSH

Per supportare la configurazione automatica di un dispositivo non incluso (dispositivo con configurazione predefinita), l'autenticazione del server SSH è disabilitata per impostazione predefinita.

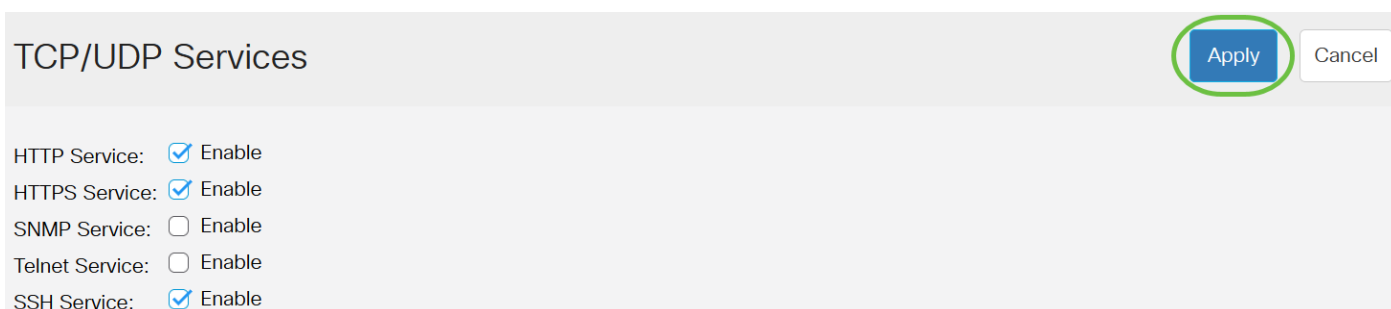
Passaggio 1. Accedere all'utility basata sul Web e scegliere **Sicurezza > Servizi TCP/UDP**



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.

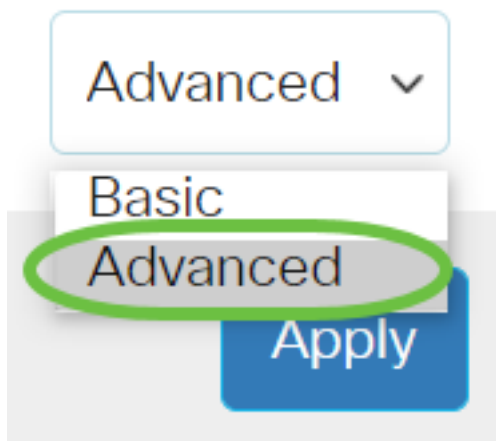


Configurazione delle impostazioni di autenticazione utente SSH

Utilizzare questa pagina per scegliere un metodo di autenticazione utente SSH. È possibile impostare un nome utente e una password sul dispositivo se si sceglie il metodo password. È inoltre possibile generare una chiave Ron Rivest, Adi Shamir e Leonard Adleman (RSA) o Digital Signature Algorithm (DSA) se è selezionato il metodo della chiave pubblica o privata.

Le coppie di chiavi predefinite RSA e DSA vengono generate per il dispositivo all'avvio. Una di queste chiavi è utilizzata per crittografare i dati scaricati dal server SSH. La chiave RSA è utilizzata per impostazione predefinita. Se l'utente elimina una o entrambe queste chiavi, queste vengono rigenerate.

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 User Authentication** dal menu.

▼ Security

1

TACACS+ Client

RADIUS Client

▶ RADIUS Server

Password Strength

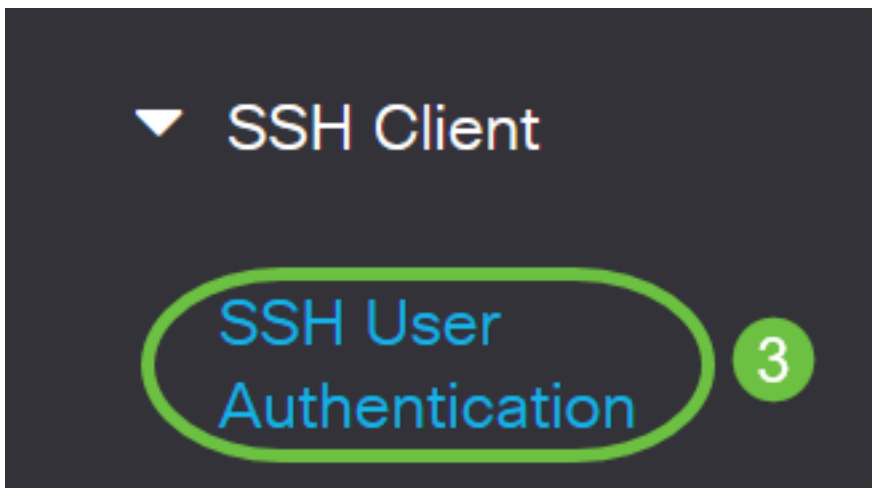
▶ Mgmt Access Method

Management Access
Authentication

▶ Secure Sensitive Data
Management

▶ SSL Server

▶ SSH Server



Passaggio 3. In Configurazione globale, fare clic sul metodo di autenticazione utente SSH desiderato.

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Quando un dispositivo (client SSH) tenta di stabilire una sessione SSH con il server SSH, questo utilizza uno dei seguenti metodi di autenticazione del client:

- Per password: questa opzione consente di configurare una password per l'autenticazione utente. Si tratta dell'impostazione predefinita e la password predefinita è anonima. Se si sceglie questa opzione, verificare che le credenziali di nome utente e password siano state stabilite sul server SSH.
- Per chiave pubblica RSA: questa opzione consente di utilizzare la chiave pubblica RSA per l'autenticazione dell'utente. Una chiave RSA è una chiave crittografata basata sulla fattorizzazione di numeri interi di grandi dimensioni. Questa chiave è la chiave più comune utilizzata per l'autenticazione dell'utente SSH.
- Per chiave pubblica DSA: questa opzione consente di utilizzare una chiave pubblica DSA per l'autenticazione utente. Una chiave DSA è una chiave crittografata basata su un algoritmo discreto ElGamal. Questa chiave non viene in genere utilizzata per l'autenticazione dell'utente SSH in quanto richiede più tempo.

Nell'esempio, viene scelto Per password.

Passaggio 4. Nell'area Credenziali, immettere il nome utente nel campo *Nome utente*.

Credentials

✳ Username: (12/70 characters used)

✳ Password: Encrypted

Plaintext (Default Password: anonymous)

nell'esempio viene usato ciscosbuser1.

Passaggio 5. (Facoltativo) Se si sceglie Per password al passaggio 2, fare clic sul metodo e immettere la password nel campo *Crittografato* o *Testo normale*.

Credentials

✳ Username: (12/70 characters used)

✳ Password: Encrypted

Plaintext (Default Password: anonymous)

Le opzioni sono:

- Crittografata - Questa opzione consente di immettere una versione crittografata della password.
- Testo normale - Questa opzione consente di immettere una password in testo normale.

In questo esempio viene scelto Testo normale e viene immessa una password in testo normale.

Passaggio 6. Fare clic su **Applica** per salvare la configurazione di autenticazione.

SSH User Authentication

Apply

Cancel

By RSA Public Key

By DSA Public Key

Credentials

Username:

ciscosbuser1

(12/70 ch

Password:

Encrypted

AUy3Nne84DHjTuVuzd1Ays

Plaintext

C1\$C0SBSwi+ch

Passaggio 7. (Facoltativo) Fare clic su **Ripristina credenziali predefinite** per ripristinare il nome utente e la password predefiniti, quindi fare clic su **OK** per continuare.

SSH User Authentication

Apply

Cancel

Restore Default Credentials

Global Configuration

Confirm Restore Default Credentials

X



The Username and Password will be restored to the default values (anonymous/anonymous). Do you want to continue?

OK

Cancel

Il nome utente e la password verranno ripristinati ai valori predefiniti: anonimo/anonimo.

Passaggio 8. (Facoltativo) Fare clic su **Visualizza dati sensibili come testo normale** per visualizzare i dati sensibili della pagina in formato testo normale, quindi fare clic su **OK** per continuare.

Confirm Display Method Change



Sensitive data for the current page will be displayed as plaintext. Your HTTP web session is insecure. Do you want to continue?

OK

Cancel

Configurazione della tabella delle chiavi utente SSH

Passaggio 9. Selezionare la casella di controllo della chiave che si desidera gestire.

SSH User Key Table

Generate



Details

Key Type

Key Source

Fingerprint



RSA

Auto Generated

MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2

DSA

Auto Generated

MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

Nell'esempio, viene scelto RSA.

Passaggio 10. (Facoltativo) Fare clic su **Genera** per generare una nuova chiave. La nuova chiave sostituirà la chiave selezionata, quindi fare clic su **OK** per continuare.

SSH User Key Table

Generate



Details

Key Type

Key Source

Fingerprint



RSA

Auto Generated

MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2

DSA

Auto Generated

MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

Confirm Key Generation

X



Generating a new key will overwrite the existing key. Do you want to continue?



Passaggio 11. (Facoltativo) Fare clic su **Modifica** per modificare una chiave corrente.

SSH User Key Table



<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	Auto Generated	MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2
<input type="checkbox"/>	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

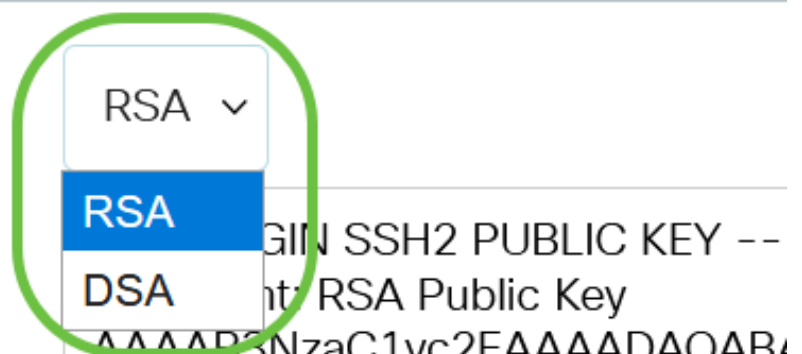
Passaggio 12. (Facoltativo) Scegliere un tipo di chiave dall'elenco a discesa Tipo di chiave.

Edit SSH Client Authentication Settings

When a Key is entered, it should contain the "BEGIN" and "END"

Key Type:

Public Key:



Nell'esempio, viene scelto RSA.

Passaggio 13. (Facoltativo) Immettere la nuova chiave pubblica nel campo *Chiave pubblica*.

Edit SSH Client Authentication Settings

X

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type: RSA ▾

Public Key:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmbp004VvhTXfPqGCzg4/IIFlpm  
hf4ImgpX+XB7aLCi3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXbVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTOwjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

Passaggio 14. (Facoltativo) Immettere la nuova chiave privata nel campo *Chiave privata*.

È possibile modificare la chiave privata e fare clic su *Crittografata* per visualizzare la chiave privata corrente come testo crittografato oppure su *Testo normale* per visualizzare la chiave privata corrente in testo normale.

Passaggio 15. (Facoltativo) Fare clic su **Visualizza dati sensibili come testo normale** per visualizzare i dati crittografati della pagina in formato testo normale, quindi fare clic su **OK** per continuare.

Edit SSH Client Authentication Settings

X

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type: RSA ▾

Public Key:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmbp004VvhTXfPqGCzg4/IIFlpm  
hf4ImgpX+XB7aLCi3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXbVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTOwjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

Confirm Display Method Change

X



Sensitive data for the current page will be displayed as plaintext. Do you want to continue?

Don't show me this again



Passaggio 16. Fare clic su **Apply** per salvare le modifiche, quindi su **Close**.

Edit SSH Client Authentication Settings

X

When a Key is entered, it should contain the "BEGIN" and "END" markers.

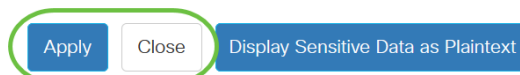
Key Type:

Public Key:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmBp004VvhTXfPqGCzG4/IIFlpm  
hf4ImgpX+XB7aLCI3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjUe1LVZTfrpMSqZ6UB+QtNtvaed46vTOWjgCb4+y+zFYpQjlvZCAuMoaWkljQFsiXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext



Passaggio 17. (Facoltativo) Fare clic su **Elimina** per eliminare la chiave selezionata.

SSH User Key Table



<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	MD5:02:26:b2:5c:56:51:b6:cf:db:fa:f7:b5:1a:26:7e:33
<input type="checkbox"/>	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

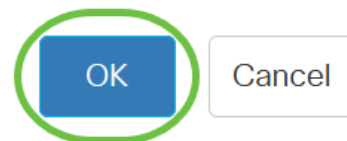
Passaggio 18. (Facoltativo) Quando richiesto da un messaggio di conferma, come mostrato di seguito, fare clic su **OK** per eliminare la chiave.

Delete User Generated Key

X

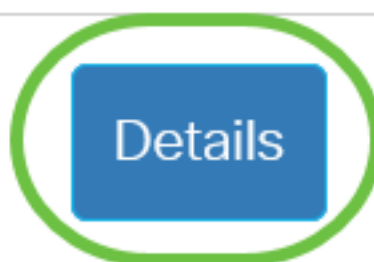


The selected user defined key will be deleted and replaced by an auto generated key. Do you want to continue?



Passaggio 19. (Facoltativo) Fare clic su **Dettagli** per visualizzare i dettagli della chiave selezionata.

SSH User Key Table



Key Type

Key Source

Fingerprint

SSH User Key Details

Back

SSH Server Key Type: RSA

Public Key: ----- BEGIN SSH2 PUBLIC KEY -----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQ=CxBoUggILUWLBwkarVUG9jbM4OQUDsPdr
VmHGNkIRJVg3nxO2wmw10xckYy7YZLPaoriNd/obTuGZ4jOqhSgfQckqhibcSNdlaUrw;
w1v4QBwH8UbGNw1yV/SaECMuFre/VzYdRP
/RvGDNCNOphqMMJyCQ3D+WG2136l+li+U3Kn9BOBoOsSn+gz7c1OvNoXQ9t+NvtJDF
3MfMhmvwx0XIEKgMZgV+ennjipMPja0FP8HGblh
/hOPdhUIPmaRheE3hsDS1S9TJXLu7RnG0TrknL+QUFqZeRT3jSablwZsaGyE8oklpP5E
K9qsLJZlqeMm2gWjziB
----- END SSH2 PUBLIC KEY -----

Private Key (Encrypted): ----- BEGIN SSH2 ENCRYPTED PRIVATE KEY -----
Comment: RSA Private Key
AkNK2himPem2VeoSwyp0U+1FXk81mva9RGX2rBMhCDlj/79rYDLBnYKdSHk3A7Hqg0
aDjeLKVROxyRccQ0UivFp70SYz6mmjfrvwAXgCnZoNkhv8WO+Ktz0tLliHAj2gWaXerYB
D5suzX+RQnl R0Δ0zI I05G663mEMVcOT

Passaggio 20. (Facoltativo) Fare clic sul pulsante **Save** nella parte superiore della pagina per salvare le modifiche nel file della configurazione di avvio.



SSH User Authentication

Apply

Cancel

Res

A questo punto, sono state configurate le impostazioni di autenticazione dell'utente client sullo switch Cisco Business serie 350.