

Autenticazione utente Client Secure Shell (SSH) per gli switch SG350XG e SG550XG

Obiettivo

Secure Shell (SSH) è un protocollo che permette di connettersi in modo sicuro a un dispositivo specifico. Gli switch gestiti serie 350XG e 550XG consentono di autenticare e gestire gli utenti per la connessione al dispositivo tramite SSH. L'autenticazione viene effettuata tramite una chiave pubblica, quindi l'utente può utilizzare questa chiave per stabilire una connessione SSH a un dispositivo specifico. Le connessioni SSH sono utili per risolvere i problemi di una rete in remoto, nel caso in cui l'amministratore di rete non si trovi nel sito di rete.

In questo documento viene spiegato come configurare l'autenticazione dell'utente client sugli switch gestiti serie SG350XG e SG550XG.

Dispositivi interessati

- SG350XG
- SG550XG

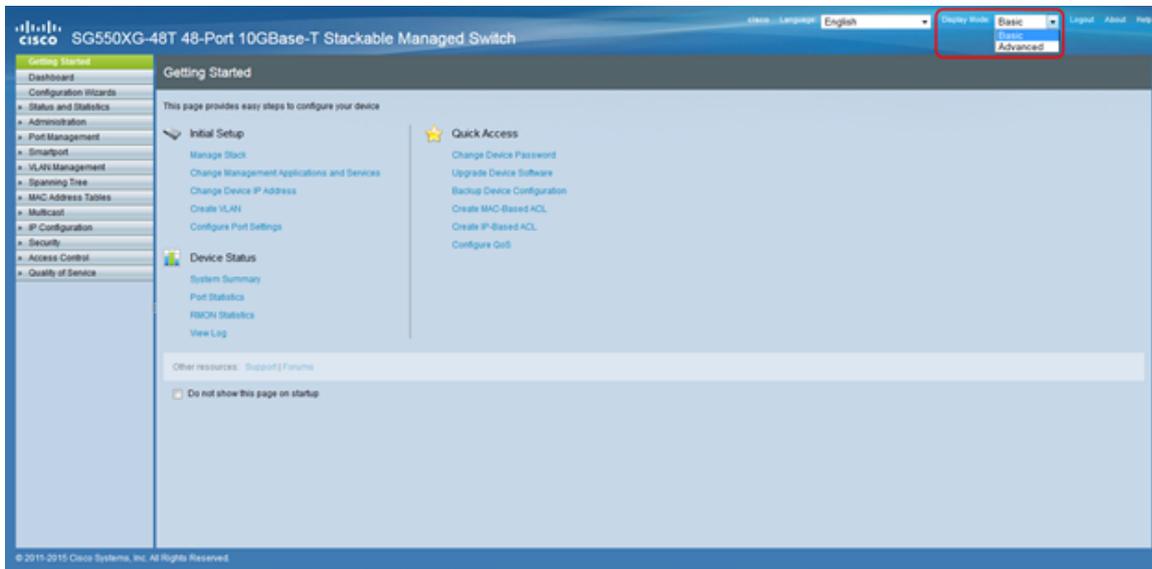
Versione del software

- v2.0.0.73

Configurazione del protocollo SSH Cliente Autenticazione

Configurazione globale

Nota: Le seguenti schermate sono tratte da Advanced Display. È possibile alternare la visualizzazione facendo clic sull'elenco a discesa *Display Mode (Modalità di visualizzazione)* nella parte superiore destra dello schermo



Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Security > SSH Client > SSH User Authentication**. Viene visualizzata la pagina *SSH User Authentication*:

SSH User Authentication

Global Configuration

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

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input type="checkbox"/>	RSA	Auto Generated	6f:bf:d8:12:60:74:ea:4c:68:a1:76:91:e5:8f:a4:d1
<input type="checkbox"/>	DSA	Auto Generated	24:31:b0:3c:5c:94:74:35:ba:d1:ce:c6:f7:16:84:48

Passaggio 2. Nel campo *Metodo di autenticazione utente SSH*, fare clic sul pulsante di opzione corrispondente al metodo di autenticazione globale desiderato.

SSH User Authentication

Global Configuration

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

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Le opzioni disponibili sono le seguenti:

- Per password: questa opzione consente di configurare una password per l'autenticazione utente. Immettere una password o mantenere l'impostazione predefinita "anonimo".
- Per chiave pubblica RSA: questa opzione consente di utilizzare una chiave pubblica RSA per l'autenticazione dell'utente. RSA viene utilizzato per la crittografia e la firma. Se questa opzione è selezionata, creare una chiave pubblica e privata RSA nel blocco della tabella della chiave utente SSH.
- Per chiave pubblica DSA: questa opzione consente di utilizzare una chiave pubblica DSA per l'autenticazione utente. DSA viene utilizzato solo per la firma. Se questa opzione è selezionata, creare una chiave DSA pubblica/privata nel blocco della tabella della chiave utente SSH.

Passaggio 3. Individuare l'area *Credenziali*. Nel campo *Username* (Nome utente), immettere il nome utente.

SSH User Authentication

Global Configuration

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

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

Passaggio 4. Se nel [Passaggio 2](#) è stata selezionata l'opzione **Per password**, fare clic sul pulsante di opzione relativo al metodo di password desiderato nel campo *Password*. La password predefinita è "anonimo".

SSH User Authentication

Global Configuration

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

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

Le opzioni disponibili sono descritte come segue:

- Encrypted - Immettere una password crittografata.
- Testo normale - Immettere una password come testo normale.

Passaggio 5. Fare clic su **Apply** (Applica) per salvare la configurazione dell'autenticazione.

SSH User Authentication

Global Configuration

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

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

Passaggio 6. (Facoltativo) Per ripristinare il nome utente e la password predefiniti, fare clic su **Ripristina credenziali predefinite**. La password predefinita è "anonima".

SSH User Authentication

Global Configuration

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

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply Cancel **Restore Default Credentials** Display Sensitive Data as Plaintext

Passaggio 7. (Facoltativo) Per visualizzare i dati sensibili come testo normale o crittografato, fare clic su **Visualizza dati sensibili come testo normale/crittografato**.

SSH User Authentication

Global Configuration

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

Credentials

Username: (0/70 characters used)

Password: Encrypted
 Plaintext (Default Password: anonymous)

Apply Cancel Restore Default Credentials **Display Sensitive Data as Plaintext**

Nota: Il nome del pulsante cambia a seconda dell'impostazione corrente. Il pulsante consente di attivare e disattivare sempre la visualizzazione dei dati.

Tabella chiavi utente SSH

Questa sezione spiega come gestire la tabella utenti SSH.

Passaggio 1. Passare alla *tabella della chiave utente SSH*. Nell'elenco visualizzato selezionare le caselle di controllo a sinistra della chiave che si desidera gestire.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

Generate Edit... Delete Details

Passaggio 2. (Facoltativo) Fare clic su **Genera** per generare una nuova chiave. La nuova chiave sostituisce la chiave selezionata. Viene visualizzata una finestra di conferma. Fare clic su **OK** per continuare.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

Generate Edit... Delete Details

Passaggio 3. (Facoltativo) Fare clic su **Elimina** per eliminare la chiave selezionata. Viene visualizzata una finestra di conferma. Fare clic su **OK** per continuare.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

Generate Edit... Delete Details

Passaggio 4. (Facoltativo) Fare clic su **Dettagli** per visualizzare i dettagli della chiave selezionata.

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

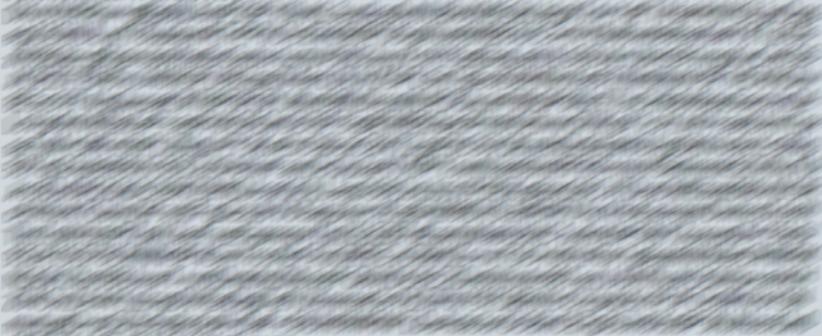
Generate Edit... Delete Details

Viene visualizzata la pagina SSH User Key Details (Dettagli chiave utente SSH). Fare clic su **Indietro** per tornare alla tabella delle chiavi utente SSH.

SSH User Key Details

SSH Server Key Type: RSA

Public Key: ---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxb
XRqFXeMQ2LNyUTCK8hcu0zVSipsQ8AFRZmpnaVkEgSunFK5YYJ2AckP9NyMikihWfRWm
UXT6SBOK/BJk7GPXhcs0JE6I3uPCyiC50vzGRBGhWSH/oGBxMqkavDGpcToaDyKQ==
---- END SSH2 PUBLIC KEY ----

Private Key (Encrypted): ---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
Comment: RSA Private Key

---- END SSH2 PRIVATE KEY ----

Passaggio 5. Fare clic su **Modifica** per modificare la chiave scelta.

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

Viene visualizzata la finestra *Edit SSH Client Authentication Settings*:

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
---- END SSH2 PUBLIC KEY ----
```

Private Key: Encrypted

Plaintext

Passaggio 6. Selezionare il tipo di chiave desiderato dall'elenco a discesa *Tipo di chiave*.

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
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF'
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

Le opzioni disponibili sono le seguenti:

- RSA - RSA viene utilizzato per la crittografia e la firma.
- DSA: DSA viene utilizzato solo per la firma.

Passaggio 7. Nel campo *Chiave pubblica* è possibile modificare la chiave pubblica corrente.

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
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF'
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

Passaggio 8. Nel campo *Chiave privata* è possibile modificare la chiave privata corrente. Fare clic sul pulsante

Pulsante di opzione **Crittografato** per visualizzare la chiave privata corrente come crittografata. In caso contrario, fare clic sul pulsante di opzione **Testo normale** per visualizzare la chiave privata corrente come testo normale.

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted Plaintext

Passaggio 9. Fare clic su **Apply** (Applica) per salvare le modifiche.

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted Plaintext