

# Guida: Generare e Copiare una Chiave SSH su un Server Remoto

Questa guida illustra la generazione di una chiave pubblica SSH e due metodi per installarla su un server Linux.

## Generazione della Chiave SSH

Generare una nuova coppia di chiavi SSH utilizzando l'algoritmo Ed25519:

```
ssh-keygen -t ed25519 -C "tuo_indirizzo_email@example.com"
```

*Nota: Premere Invio per accettare il percorso predefinito. È possibile inserire una passphrase per maggiore sicurezza oppure lasciare vuoto e premere Invio per non utilizzarla.*

---

## Metodo 1: Utilizzo di ssh-copy-id (Automatico)

Questo metodo richiede che l'autenticazione con password sia abilitata sul server remoto.

**Comando standard:**

```
ssh-copy-id utente@indirizzo_server
```

**Comando con porta SSH personalizzata (es. 2222):**

```
ssh-copy-id -p 2222 utente@indirizzo_server
```

### Comando con file chiave specifico:

```
ssh-copy-id -i ~/.ssh/id_ed25519.pub utente@indirizzo_server
```

*Nota: Alla richiesta, inserire la password dell'utente remoto. I caratteri non verranno visualizzati.*

---

## Metodo 2: Inserimento Manuale (Copia e Incolla)

Utilizzare questo metodo se ssh-copy-id fallisce o se l'autenticazione con password è disabilitata.

### 1. Macchina Locale

Visualizzare il contenuto della chiave pubblica e copiarlo negli appunti:

```
cat ~/.ssh/id_ed25519.pub
```

### 2. Server Remoto

Accedere al server remoto.

Creare la directory SSH e impostare i permessi:

```
mkdir -p ~/.ssh  
chmod 700 ~/.ssh
```

Aprire il file delle chiavi autorizzate:

```
nano ~/.ssh/authorized_keys
```

Incollare il contenuto della chiave copiato in precedenza. Salvare e uscire (In nano: CTRL+O, Invio, CTRL+X).

Impostare i permessi di sicurezza sul file:

```
chmod 600 ~/.ssh/authorized_keys
```

---

Revision #1

Created 2026-03-04 13:03:39 UTC by Pe

Updated 2026-06-04 11:53:14 UTC by Pe