Guida Accesso Sicuro con Chiavi SSH — MikroTik RouterOS 7.x

Configurazione dell'autenticazione a chiave pubblica su RouterOS: più sicura delle password e ideale per automatizzare SCP/SSH verso più router da remoto.

> **Regola d'oro:** non disabilitare mai l'accesso via password PRIMA di aver verificato al 100% che l'accesso con chiave funziona. Altrimenti rischi il lock-out, soprattutto da remoto.

---

1. Genera la coppia di chiavi (sul tuo PC)

```
ssh-keygen -t ed25519 -f ~/.ssh/mikrotik_key
```

- `ed25519` è l'algoritmo moderno consigliato (chiavi corte e robuste).
- Se hai router più vecchi che non lo supportano, usa RSA a 2048+ bit:

  ```
  ssh-keygen -t rsa -b 4096 -f ~/.ssh/mikrotik_key
  ```

- Alla richiesta, imposta una **passphrase**: protegge la chiave privata se qualcuno mette le mani sul file.

Vengono creati due file:

- `mikrotik_key` → chiave **privata** (resta sul tuo PC, NON condividerla)
- `mikrotik_key.pub` → chiave **pubblica** (da caricare sul router)

---

2. Carica la chiave pubblica sul router (via SCP)

```
scp ~/.ssh/mikrotik_key.pub admin@<IP-router>:
```

Se RouterOS 7.x rifiuta la connessione per mismatch di algoritmi, abilita lo strong crypto sul router e riprova (vedi anche passo 5):

```
/ip ssh set strong-crypto=yes
```

Verifica che il file sia arrivato:

```
/file print
```

Deve comparire `mikrotik_key.pub`.

---

3. Importa la chiave su RouterOS

Collegati via SSH al router e associa la chiave pubblica all'utente:

```
/user ssh-keys import public-key-file=mikrotik_key.pub user=admin
```

Verifica che sia stata importata:

```
/user ssh-keys print
```

---

4. Verifica l'accesso con chiave (dal tuo PC)

```
ssh -i ~/.ssh/mikrotik_key admin@<IP-router>
```

Se entri **senza** che il router chieda la password (al massimo ti viene chiesta la passphrase della chiave), l'autenticazione a chiave funziona.

> **Non procedere al passo 5 finché questo test non riesce in modo affidabile.**

---

5. Rafforza la sicurezza (solo DOPO aver validato il passo 4)

5.1 Strong crypto

Forza algoritmi robusti e disabilita quelli deboli/obsoleti:

```
/ip ssh set strong-crypto=yes
```

5.2 Disabilita il login con password

Da qui in poi si entra SOLO con chiave:

```
/ip ssh set password-authentication=no
```

> **ATTENZIONE:** dopo questo comando, chi non ha la chiave non entra più via SSH. Assicurati che:
>
> - la tua chiave privata sia al sicuro e con un backup;
> - resti almeno un canale di recupero (vedi sezione 6).

---

6. Rete di sicurezza (paracadute)

Con la password SSH disabilitata, se perdi la chiave privata o cambi PC senza aver configurato la nuova chiave, non entri più via SSH. Tieni quindi attivi:

- **MAC-Winbox su tutte le interfacce** come accesso di emergenza a Layer 2:

```
/tool mac-server set allowed-interface-list=all
/tool mac-server mac-winbox set allowed-interface-list=all
```

- Un **backup della chiave privata** in luogo sicuro.
- Idealmente, accesso fisico o una persona sul posto per i casi estremi.

Config lato client (comodità)

Nel tuo `~/.ssh/config` puoi definire scorciatoie per non ripetere `-i` ogni volta:

```
Host mikrotik-sedeX
    HostName 172.17.5.116
    User admin
    IdentityFile ~/.ssh/mikrotik_key
```

Poi accedi semplicemente con:

```
ssh mikrotik-sedeX
```

Checklist finale

- ☐ Coppia di chiavi generata con passphrase
- ☐ Chiave pubblica caricata e importata sul router
- ☐ Accesso con chiave testato e funzionante
- ☐ Strong crypto abilitato
- ☐ Login password disabilitato SOLO dopo il test riuscito
- ☐ Paracadute attivo (MAC-Winbox + backup chiave privata)

Revision #1
Created 2026-07-03 10:41:04 UTC by Pe
Updated 2026-07-03 10:46:18 UTC by Pe