Troubleshooting

Symptom-first fixes for login and device problems · Checked against tacctl 0.2.25

Contents

1. First five commands 2
2. A user cannot log in to a device 2
3. tacctl ssh / device connection problems 3
4. Device configuration (pull / plan / apply) 3
5. Nothing reaches the server 4
6. WTI units 4
7. Linux hosts 5
8. tacctl itself 5

Symptom-first troubleshooting for login and device problems. Find the symptom, run the checks, apply the fix. The **Tier** column says who can apply the fix: R = read-only, O = operator, E = engineer, S = superuser.

> **Example names used on this page** Devices: `sw1` (Cisco), `rtr1` (Junos), `pdu1` (WTI) · User: `alice` · Scope: `site-a`

1. First five commands

```
tacctl status                    # services running? errors? (per backend)
tacctl log failures              # failures in the last 24 hours, with reasons
tacctl log search alice          # one user's entries (TACACS+: last 7 days)
tacctl scope lookup 10.10.0.1    # which scope answers this address
tacctl config validate           # configuration problems and drift
```

For a live view while someone retries: `tacctl log tail -f`.

---

2. A user cannot log in to a device

Find the log line, then the row:

Log line / clue	Cause	Fix	Tier
`failed to validate the user [x] using a bcrypt password`	Wrong password (the secret is fine)	`tacctl user verify x`, then `tacctl user passwd x`	S
`bad secret detected for ip [a]`	The device's key doesn't match its scope's secret	`scope lookup a`, then re-paste AAA (`device config plan <n>`). On Junos, delete and re-set the secret.	E
`remote [a] has no secret providers`	No scope covers the address	`tacctl scope prefixes <s> add <cidr>`	S
No line at all	The request never arrived	See §5	E
User shown `disabled` in `user show`	Disabled	`tacctl user enable x`	S
`user show` has a `Password change line`; `user list` says `(change required)`	A password change is required: every device refuses the user until it is made	The user logs in to the tacctl server and changes it (*Getting Started* §2.1); `tacctl user require-password-change x off` lifts it	R / S

Log line / clue	Cause	Fix	Tier
User's scopes don't include the device's	Missing grant	`tacctl user scope x add <s>`	S
Red `EMERGENCY LOCKDOWN` line	Lockdown on the scope	`tacctl emergency lockdown status`	S
Device shows `Break-glass: HELD`	The server is deliberately not answering	`tacctl breakglass list`	S
Junos: TACACS+ accepted, login still fails	Template user missing on the device	Create the template users from `tacctl config juniper`	E
Logged in at the wrong level (RADIUS)	The scope doesn't send that vendor's attribute	`tacctl scope vendor-attrs <s>`, `scope devices <s>`	S
RADIUS `not an enabled user of this scope`	Disabled, or missing the scope	As above	S
RADIUS `Crypt digest does not match`	Wrong password	`user passwd`	S

---

3. `tacctl ssh` / device connection problems

Every refusal of `tacctl ssh` (device not found, changed host key, held device, lockdown, legacy ssh, running as root) is listed with its fix in *Connecting to Devices* §4. A changed host key has its own procedure in §5 of that page.

---

4. Device configuration (pull / plan / apply)

Symptom	Cause	Fix
Plan refused: never pulled / stale / failed	Plans need a recent, good pull	`tacctl device config pull <n>`, or `plan --pull`
`needs pull (syntax unknown)` (Cisco)	Version line not mapped (e.g. IOS 15.0/15.1, ASA, XR)	`tacctl device ios-syntax <n> ios12|modern`
`needs pull (vendor changed)`	The vendor was edited	Pull again
Apply `failed: calls itself '<x>'`	The device's hostname differs from the registry	Check it is the right device. Fix the registry or the hostname.

Symptom	Cause	Fix
Apply `failed: other editors or staged changes`	Another session has uncommitted configuration	Coordinate. Commit or discard on the device.
Apply `PENDING until <time>`	The state could not be read after the commit	**Type nothing on the device until the time passes.** Then run `apply --check`.
Apply `rolled back`	The proof failed (the fresh login or the landed change)	Read the reason on the row and fix the cause
Pull refused: break-glass held	The device does not authenticate you	Release the hold first (*Break Glass*)
Plan says `Not fixable by this login`	Your class can't commit that section	Ask a superuser
A pull or an apply of one device ends `timeout`, or the host-key read finds no key, for a device behind a long round trip or with a slow CPU	The device misses the connect, handshake or per-device times	Ask a superuser for a timing scale: `tacctl device timeout-scale <name> 3` (*Connecting to Devices* §7). A `--timeout` you type wins over it.
A run over many devices is slow, and you do not know which device holds it up	Some devices take much longer than others	Add `--timing` to `device config pull`, `diff --pull`, `plan --pull` or `apply`: it prints each device's phases and names the slowest (*Engineer Guide* §3)

5. Nothing reaches the server

1. From the device: `telnet <server_ip> 49` (TACACS+; the port of the listener, see step 3). RADIUS uses UDP 1812/1813 by default and can't be tested with telnet.
2. `tacctl backend status`: are the services and listeners up?
3. `tacctl server listen show` (add `--backend radius` for RADIUS), or `tacctl server show` for every listener with its port and unit state: is the listener on the right address?
4. A Cisco device may be sending from an unexpected interface. Check `tacctl config cisco source-interface <scope>`. The source must be inside the scope's prefixes.
5. Connection filters: `tacctl config allow` / `config deny`. `deny` wins.

6. WTI units

The WTI settings behind these symptoms are explained in *Vendor Notes* §4.

Symptom	Fix (on the unit unless noted)
Every attempt `failed to validate` though `user verify` accepts the password	Set Default User Access `On` / `ViewOnly`
No authorization request seen	Enable the Account Management Module
Wrong level for every group	Service Name must be `wti`, not `shell`
Wrong level for one user	A local account with the same name on the unit overrides it. Remove it.
Login waits out the Fallback Timer, nothing in the server log	IP Tables drop replies. Add the `ESTABLISHED,RELATED` accept before the final DROP.
Session drops right after login	Turn off the Session Management Module (accounting) until tacquito has been rebuilt with `patches/0002` by `tacctl upgrade`
User level: no ports visible	Grant ports under Default TACACS User Access → Port Access
ssh closes without a password prompt	Invalid Access Lockout. Clear it with `/UL`.
Pull refused / second session refused	Set Multiple Logins `On`

For more detail on the server side, set `tacctl config loglevel debug`, retry, run `tacctl log tail 50`, then set the log level back.

---

7. Linux hosts

Symptom	Fix
A user has no account on one host	A local account with the same name. Rename one of them.
Sync stops on a UID conflict	A local UID is inside tacctl's range. Fix the host.
Nobody can `sudo`	Superuser: `breakglass hold <host>`, fix with the local admin, then release

---

8. tacctl itself

Symptom	Meaning / fix
Exit status **3**, or `DRIFT` in `status`	A rendered file was edited by hand. `config validate` names both ways out (keep the edit or discard it).

Symptom	Meaning / fix
`store not initialised`	Legacy read-only mode (after `store rollback` or a stopped upgrade). See the upgrading docs.
`is locked by another tacctl command`	Wait, then retry
`not permitted` in the shell	Your tier doesn't allow the command. `?` shows the tier it needs.
`[ERROR] Unknown subcommand: '<word>'`, then `Run 'tacctl <command> -h' for usage.`	The word is none of that command's sub-commands. The `Did you mean` line, when there is one, names the commands that have it; `<command> -h` lists the sub-commands. In the shell and the console a verb your tier cannot run is refused as not permitted, not as unknown.
`A password change is required of '<user>'`	Only `passwd`, `version` and `help` run until you change your password: `tacctl passwd`
A user cannot log in to the tacctl server or its console	Every user can, unless disabled or in a group of tier none (`tacctl user show <name>`). The account exists after the next `tacctl host sync <server>`. A name with a period (stored by 0.2.20 or 0.2.21) has no Linux account: `tacctl user rename <name> <new-name>`.
`Username must contain only letters, numbers, underscores and hyphens (a period cannot be part of a Linux account name).`	`user add` or `user rename` was given a name with a period. Use `-` or `_`.
`rename it first: tacctl user rename <name> <new-name>` (from `passwd`, `user passwd`, `user require-password-change`), or `tacctl upgrade` refusing	The store holds a user with a period. Rename it, then repeat the command.
`Scope 'tacctl' is reserved. Rename the scope of that name first` (from `host enroll --local`, the sync of the server or `config validate`)	A scope called `tacctl` from an earlier release blocks the server's own login. `tacctl scope rename tacctl <new-name>`, then `tacctl host enroll --local`.
`This machine's own login was not set up (an upgrade does not ask without a terminal)`	`upgrade` found no login and had no terminal to ask on. Run `tacctl host enroll --local`.
`This machine's own login was not set up (the enrolment stopped, see above; nothing is half applied)`	A safeguard stopped the setup, and the lines above say why. Fix that, then run `tacctl host enroll --local`.

Exit statuses, including 3 (hand edit) and the sudo codes 126 and 127, are explained in *Exit Codes*.

See also: Connecting to Devices · Vendor Notes · Incident Response Runbooks · Troubleshooting (repo, server side) · `man tacctl`