

Troubleshooting

Symptom-first fixes for login and device problems · Checked against tacctl 0.2.22

Contents

- 1. First five commands2
- 2. A user cannot log in to a device2
- 3. tacctl ssh / device connection problems3
- 4. Device configuration (pull / plan / apply)3
- 5. Nothing reaches the server 4
- 6. WTI units 4
- 7. Linux hosts5
- 8. tacctl itself5

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)	<code>tacctl user verify x</code> , then <code>tacctl user passwd x</code>	S
bad secret detected for ip [a]	The device's key doesn't match its scope's secret	<code>scope lookup a</code> , 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	<code>tacctl scope prefixes <s> add <cidr></code>	S
No line at all	The request never arrived	See §5	E
User shown disabled in <code>user show</code>	Disabled	<code>tacctl user enable x</code>	S
<code>user show</code> has a Password change line; <code>user list</code> 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 (<i>Getting Started</i> §2.1); <code>tacctl user require-password-change x off</code> lifts it	R / S

Log line / clue	Cause	Fix	Tier
User's scopes don't include the device's	Missing grant	<code>tacctl user scope x add <s></code>	S
Red EMERGENCY LOCKDOWN line	Lockdown on the scope	<code>tacctl emergency lockdown status</code>	S
Device shows Break-glass: HELD	The server is deliberately not answering	<code>tacctl breakglass list</code>	S
Junos: TACACS+ accepted, login still fails	Template user missing on the device	Create the template users from <code>tacctl config juniper</code>	E
Logged in at the wrong level (RADIUS)	The scope doesn't send that vendor's attribute	<code>tacctl scope vendor-attrs <s></code> , <code>scope devices <s></code>	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	<code>user passwd</code>	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	<code>tacctl device config pull <n></code> , or <code>plan --pull</code>
needs pull (syntax unknown) (Cisco)	Version line not mapped (e.g. IOS 15.0/15.1, ASA, XR)	<code>tacctl device ios-syntax <n> ios12 modern</code>
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 <code>apply --check</code> .
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 (<i>Break Glass</i>)
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: <code>tacctl device timeout-scale <name> 3</code> (<i>Connecting to Devices</i> §7). A <code>--timeout</code> 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 <code>--timing</code> to <code>device config pull</code> , <code>diff --pull</code> , <code>plan --pull</code> or <code>apply</code> : it prints each device's phases and names the slowest (<i>Engineer Guide</i> §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. <code>config validate</code> names both ways out (keep the edit or discard it).

Symptom	Meaning / fix
store not initialised	Legacy read-only mode (after <code>store rollback</code> or a stopped upgrade). See the upgrading docs.
is locked by another <code>tacctl</code> command	Wait, then retry
not permitted in the shell	Your tier doesn't allow the command. <code>?</code> shows the tier it needs.
[ERROR] Unknown subcommand: ' <code><word></code> ', then Run ' <code>tacctl <command> -h</code> ' for usage.	The word is none of that command's sub-commands. The <code>Did you mean</code> line, when there is one, names the commands that have it; <code><command> -h</code> 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 ' <code><user></code> '	Only <code>passwd</code> , <code>version</code> and <code>help</code> run until you change your password: <code>tacctl passwd</code>
A user cannot log in to the <code>tacctl</code> server or its console	Every user can, unless disabled or in a group of tier none (<code>tacctl user show <name></code>). The account exists after the next <code>tacctl host sync <server></code> . A name with a period (stored by 0.2.20 or 0.2.21) has no Linux account: <code>tacctl user rename <name> <new-name></code> .
Username must contain only letters, numbers, underscores and hyphens (a period cannot be part of a Linux account name).	<code>user add</code> or <code>user rename</code> was given a name with a period. Use <code>-</code> or <code>_</code> .
rename it first: <code>tacctl user rename <name> <new-name></code> (from <code>passwd</code> , <code>user passwd</code> , <code>user require-password-change</code>), or <code>tacctl upgrade</code> refusing	The store holds a user with a period. Rename it, then repeat the command.
Scope ' <code>tacctl</code> ' is reserved. Rename the scope of that name first (from <code>host enroll --local</code> , the sync of the server or <code>config validate</code>)	A scope called <code>tacctl</code> from an earlier release blocks the server's own login. <code>tacctl scope rename tacctl <new-name></code> , then <code>tacctl host enroll --local</code> .
This machine's own login was not set up (an upgrade does not ask without a terminal)	<code>upgrade</code> found no login and had no terminal to ask on. Run <code>tacctl host enroll --local</code> .
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 <code>tacctl host enroll --local</code> .

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`