Operator Field Guide

For NOC, help-desk and network support staff · Checked against tacctl 0.2.25

Contents

1. What your tier allows 2
2. Getting on 3
3. Connecting to devices 3
4. Monitoring and first-line checks (operator tier) 3
    - 4.1 Shift start 3
    - 4.2 Is the device alive and healthy? 4
    - 4.3 Watching logins 4
    - 4.4 Unregistered devices 4
    - 4.5 Config drift (read-only view) 4
5. Helping a user who cannot log in 5
6. When to escalate 5
7. Quick reference 6

This guide is for NOC staff, help-desk and tier-1/2 network support people whose tacctl group puts them in the **read-only** or **operator** tier. It covers what you can do, how to do it, and when to hand a problem to an engineer or superuser.

> **Example names used on this page** Server: `tacacs.example.net` · Scopes: `site-a`, `site-b` · Devices: `sw1` (Cisco), `rtr1` (Junos), `pdu1` (WTI) · You: `alice`

1. What your tier allows

You can	Read-only tier	Operator tier
Change your own password (`tacctl passwd`)	✔	✔
See users, groups, scopes and devices (`user`, `group`, `device list` and `show`; `scope list`)	✔	✔
`tacctl ssh` to devices in **your own scopes**	✔	✔
Server health (`status`, `backend status`)	✔	✔
Read logs (`log tail`, `search`, `failures`, `accounting`)		✔
Check devices (`device check`, `scan`, `discover`, `list --probe`)		✔
See config-drift state (`device config list`, CONFIG column)		✔
Run `config validate`, `backup list`, `device export`		✔
Add or change users, scopes, devices; lockdowns; break-glass		

Everything in the last row belongs to engineers and superusers. In the `tacctl shell` and the login console, Tab and `?` list only the commands your tier can run.

On a device, your group decides what you can type:

Group	Cisco	Junos	WTI
`readonly`	priv-lvl 1	`RO-CLASS`	ViewOnly
`operator`	priv-lvl 7: `show`, `ping`, `traceroute`	`OP-CLASS`	User

An operator "changes nothing and interrupts nothing". `clear`, `configure` and similar commands are refused on purpose. If you need them, escalate.

---

2. Getting on

Log in to the tacctl server with ssh. You land in the **tacctl console** (`tacacs>`), where you type commands without the `tacctl` prefix. *Getting Started* covers the console, the shell, the password cache and changing your password.

```
ssh alice@tacacs.example.net                    # the console: Tab, ?, help, history
ssh alice@tacacs.example.net 'device list'      # one tacctl line, no terminal needed
tacctl passwd                                   # change your own password
```

If you forget your password, ask a superuser to reset it. A new or reset password usually has to be changed at your next login to the server, before any device accepts it (*Getting Started* §2.1).

---

3. Connecting to devices

```
tacctl device list                      # the devices of your scopes
tacctl device list site-b               # a bare word matches name, address, vendor or
scope
tacctl device show sw1                  # one device in full
tacctl ssh sw1                          # interactive session as you
tacctl ssh rtr1 -- show chassis alarms   # one command, then back
```

Your own username and tacctl password are used: no keys, no agent.

> **ssh refused, or fingerprints printed?** Don't work around it. *Connecting to Devices* §4 lists every refusal, what it means and who fixes it. A changed host key is always handed to an engineer.

---

4. Monitoring and first-line checks (operator tier)

4.1 Shift start

```
tacctl status                   # services up? errors? password-age warnings?
tacctl device notice list       # open notices for your scopes, each with its fix
tacctl log failures             # authentication failures, last 24 hours
tacctl config validate          # problems in configuration (warnings name their fix)
```

4.2 Is the device alive and healthy?

```
tacctl device check sw1       # scope, vendor, last seen, reachable, host key vs. pin,
SNMP, notices
tacctl device list --probe    # adds REACH: TCP connect to each ssh port (3 s)
tacctl device list --stale    # not seen for 30 days (by default)
tacctl device scan            # refresh "last seen" from the server's logs
tacctl device check sw1 --sources   # also test the addresses the device sends AAA from
```

> `check` and `--probe` connect from the tacctl server. If it has no route to a management port, a timeout is not proof the device is down.

4.3 Watching logins

```
tacctl log tail                  # last 20 entries
tacctl log tail -f               # live, until Ctrl-C
tacctl log search alice          # entries for a user or keyword (TACACS+: last 7 days)
tacctl log accounting 50         # who ran what, most recent 50 records
tacctl log failures --since -1h  # failures in the last hour
tacctl log accounting --user alice --device sw1 --json
```

The filters `--since`, `--until`, `--user`, `--device` (and `--type` for accounting) combine, and `--json` prints one object per line (*Day-to-Day Device Operations* §1.4).

4.4 Unregistered devices

```
tacctl device discover           # addresses that authenticated but are not registered
```

Pass the list to an engineer. Each line comes with the `tacctl device add` command they need.

4.5 Config drift (read-only view)

```
tacctl device config list              # ok / differs / never / failed per device
tacctl device config list --differs
tacctl device list --differs           # the same devices, in the device table
```

Report `differs` and `failed` devices to an engineer. Fixing them is their job.

---

5. Helping a user who cannot log in

1. `tacctl user show <name>`: does the user exist, are they `disabled`, which scopes do they have, and must they change their password (a `Password change` line)?
2. `tacctl device show <device>`: which scope is the device in? Is it held for break-glass?
3. `tacctl log search <name>` (operator): what did the server say?
4. Match the log line:

Log line	Meaning	Who fixes it
`failed to validate the user [x] using a bcrypt password`	Wrong password	The user tries again, or a superuser resets it
`bad secret detected for ip [...]`	The device's TACACS+ key is wrong	Engineer (re-paste AAA config)
`has no secret providers`	No scope covers the device's address	Superuser (scope prefixes)
No line at all	The request never reached the server	Engineer (reachability, device AAA config)
RADIUS `not an enabled user of this scope`	User disabled, or lacks the device's scope	Superuser
`user show` has a `Password change` line	No device accepts the user until the password is changed	The user: log in to the tacctl server and change it (*Getting Started* §2.1)

---

6. When to escalate

Situation	Escalate to
New device to register, wrong address/name in the registry	Engineer
Device config `differs` or `failed`	Engineer
Host key changed	Engineer (verifies on the console)
User needs a password reset, scope, or role change	Superuser
Suspected compromised account or shared secret	Superuser, **immediately** (lockdown)
Device locked out after a bad change	Superuser (break-glass hold)

When you escalate, include the device name, the user, the time, and the `tacctl log search` lines that show the problem.

---

7. Quick reference

Task	Command
Change my password	`tacctl passwd`
List my devices	`tacctl device list`
Connect	`tacctl ssh <name>`
One command on a device	`tacctl ssh <name> -- <command>`
Device detail	`tacctl device show <name>`
Device health	`tacctl device check <name>`
Server health	`tacctl status`
Live logins	`tacctl log tail -f`
User's recent activity	`tacctl log search <user>`
Failures today	`tacctl log failures`
Notices	`tacctl device notice list`
Help on any command	`tacctl <command> --help`, or `?` in the console
The manual page at a command	`tacctl man <command>`

See also: Getting Started · Day-to-Day Device Operations · Troubleshooting · Quick Reference · `man tacctl`