What's New for Operators

The changes in each tacctl release that people on shift will notice · Checked against tacctl 0.2.25

Contents

1. tacctl 0.2.25 2
2. tacctl 0.2.24 3
3. tacctl 0.2.23 4
4. tacctl 0.2.22 6
5. tacctl 0.2.21 8
6. tacctl 0.2.20 9
7. tacctl 0.2.19 10
8. tacctl 0.2.18 10
9. tacctl 0.2.17 11
9. Older releases 11

Release notes describe every change in depth. This page lists only what changes day-to-day work: renamed commands, new commands and changed behavior. Each release links to its full notes. The newest release comes first.

> **Scripts break on renames.** tacctl does not keep aliases for renamed commands. Check your scripts against every release you skip.

1. tacctl 0.2.25

Released 2026-11-05 · Full release notes

Change	What it means on shift	Page
`device config shapes` stays narrow	The `NOW` column holds a count (`49 devices`, `1 device`, `-`), and a block headed `At a shape now (last check or apply):` below the table lists the devices of each shape, wrapped at 80 columns. A shape one line from a confirmed one says `1 line differs`	*Engineer Guide* §5.3
Shape, canary and confirmed explained	The planning pages open with a rollout in five steps and say what a shape, a canary and the states `new`, `confirmed` and `seeded` allow. At the default `--max-failures 1` a failed canary stops the whole run. No behavior changed	*Engineer Guide* §5
Junos NETCONF hello in the XML-namespace spelling	A device that names its capabilities `urn:ietf:params:xml:ns:netconf:base:1.0` is read as `hello ok` (it was recorded as `no hello`, and an apply that enabled NETCONF was rolled back). A hello that is none says why on the pull line, in `--json` and in the apply message	*Vendor Notes* §3.2
Slow devices no longer fail with `open: configure exclusive`	A late answer to the empty line the ssh client types is dropped instead of arriving in front of the first command's echo	*Vendor Notes* §3.2
Virtual chassis whose master prints its own label	A two-member chassis whose members both print `fpc0:` and `fpc1:` is applied to; before, every apply on it was rolled back. A refused commit answer shows up to 40 lines	*Vendor Notes* §3.2
Device text is cleaned further	C1 controls, the bidirectional overrides and line separators in text a device sends show as `?`, in the terminal and in `--json`	—
`tacctl rollback 0.2.24`	The release before this one is a target; it converts nothing, removes no key and needs no `--yes`	*Backups and Undo* §5

Before upgrading from 0.2.24:

- Nothing is converted; no stored file changed.

> - A Junos device recorded as `no hello` because of the namespace prefix shows `hello ok` after a new `tacctl device config pull`; `tacctl device check` shows it.
> - After `tacctl rollback 0.2.24` and the install of 0.2.24, those two Junos failures (the `no hello` record and the labelled-master chassis rolled back) return.

---

2. tacctl 0.2.24

Released 2026-11-05 · Full release notes

Change	What it means on shift	Page
Break-glass firewall	A held address can no longer complete a TCP handshake with the server, so a device that falls back to its local accounts only when the server is unreachable (WTI *Fallback Local* `On (Transport Failure)`, Junos `authentication-order [ tacplus password ]`) does fall back. `tacctl config breakglass-firewall reject|drop|off` sets it (`reject` is the default; `off` is the 0.2.23 behavior). The report of a hold and a release has a `Firewall:` line	*Break Glass* §2.1
A missing `nft`	The hold stands but the command exits 1 and the report says in red what the server still does, with the fix (`sudo apt-get install nftables`, then `tacctl config breakglass-firewall <setting>`). With the setting `off`, or nothing held, it is no failure	*Break Glass* §2.1, *Exit Codes* §1
Log filters and `--json`	`log tail`, `search`, `failures` and `accounting` take `--since`, `--until`, `--user`, `--device`, `--type login|change|command` (accounting) and `--json` (one object per line). They combine and apply before a count	*Day-to-Day Device Operations* §1.4, *Audit and Compliance* §1
Accounting names the device	Each record carries `"Device"`, the address it came from; `log accounting` shows the registered name (`"Device":"sw1"`). `<`, `>` and `&` show as typed	*Day-to-Day Device Operations* §1.4
No forwarding while a password change is due	While anyone is held to a password change, the console's sshd drop-in closes every kind of forwarding for them, in every tier. A connection already open keeps its forwardings until it closes (`loginctl terminate-user <name>`)	*Access Lifecycle* §5.1
No `single-connection`	The walkthroughs no longer set it (tacquito closes a connection idle for 15 seconds). `device config plan` and `apply` delete it from tacctl's server on a device that has it; `diff` and `plan` list it as an extra	*Engineer Guide* §4
tacquito from the project's fork	`install` and `upgrade` build tacquito from `rett/tacquito`. git asks for no password, user name or key passphrase and drops a stalled transfer	—

Change	What it means on shift	Page
`tacctl rollback 0.2.23`	The release before this one is a target; it converts nothing and removes the firewall	*Backups and Undo* §5

Before upgrading from 0.2.23:

- Expect one brief interruption of TACACS+. The upgrade rebuilds tacquito once for the patch that adds `"Device"` to accounting records, and restarts it.
- The upgrade installs the `nftables` package and, with holds standing, loads the firewall table for them: from then on the server refuses the TCP connections of every held address. That is the fix. To keep the 0.2.23 behavior, run `tacctl config breakglass-firewall off`. `nftables.service` is never enabled or touched.
- git asks for nothing. A remote that needs a password fails: use a key, the agent or a credential helper. An ssh remote's host key must be in `known_hosts` already. Your own `GIT_SSH_COMMAND` or `GIT_SSH` is replaced: choose a key with `core.sshCommand` in the clone.
- No stored file is rewritten. An installed per-tier sudoers drop-in gains the operator's `log failures *`, so an operator can pass the log filters to `log failures` through sudo.
- The upgrade changes no device. On a device whose configuration still sets `single-connection`, run `tacctl device config plan` and `apply`.
- The way back is `tacctl rollback 0.2.23`. It removes the setting, the table, the rules file and the boot unit of the firewall (the `nftables` package stays) and converts nothing else; it needs no `--yes`. A hold that stands stays, without the firewall. Until the older release is installed, run no verb that changes the holds, the listeners or the setting. On a device whose `single-connection` was removed, 0.2.23's `diff` and `plan` show the line as missing, and applying that plan types it again.

3. tacctl 0.2.23

Released 2026-10-31 · Full release notes

Change	What it means on shift	Page
`device clone`	Registers a copy of a device (registry, SNMP, NETCONF, timing scale, configuration blocks) at a bench address with `--staging`. Engineers may clone within their own scopes	*Engineer Guide* §2.5
`device rename --replace`	Removes the original with its files after a snapshot and one confirmation (`--yes` skips it), moves the replacement to its address and ends the bench address. An original with a break-glass hold needs a superuser	*Engineer Guide* §2.5

Change	What it means on shift	Page
Emergency lockdown reaches the hosts	`enable` and `disable` also close SSH key logins and forwarding on the scope's enrolled hosts, through `host sync`, and ask `Sync these hosts now? [y/N]` (`--yes` answers it). A host that is unreachable stays on a pending list that `status` shows	*Emergency Lockdown* §3.1
SNMPv3 user pools	At each level (server, scope, device) the v3 users are a pool with one default: `v3-user add|remove|default|list`, `--default`, `--none`. A device uses its own default, else its scope's, else the server's. `config snmp version` sets the version	*Superuser Daily Operations* §4.10
`device check --sources`, `device scan --sources`	Connect to the source addresses a device sends AAA from and warn when one is unreachable or presents another host key	*Engineer Guide* §3.1
AAA source address	A source that no interface of the device holds is a difference and a plan item. The settings a device keeps for its own AAA server (a source address, a routing instance) are no longer listed as differences	*Engineer Guide* §3.1
Email address of a user	`user add --email`, `user email <name> [<address>|clear]`: optional, one per user, set by a superuser, shown by `user show`, never logged. No mail is sent	*Access Lifecycle* §2
Users and this server's accounts	A `user` change that touches an account on this server syncs the server's own accounts at once, so a new user can log in to change the password. Other enrolled hosts get one warning and, on a terminal, the question	*Access Lifecycle* §2
`backup keep`, `unkeep`, `recover`	`keep` copies a snapshot beyond the retention; `recover <snapshot> [--only email,snmp-users]` puts back only what a rollback dropped	*Backups and Undo* §4.2, §4.3
`device rename`, `host rename`	Carry the bench address that was staged under the old name	*Engineer Guide* §2.5
`tacctl rollback 0.2.22`	The release before this one is a target; it removes the email addresses and writes the SNMP credential files in version 1 again	*Backups and Undo* §5

Before upgrading from 0.2.22:

- No file is rewritten at the upgrade. The per-tier sudoers drop-in gains the engineers' rule for `device clone`.
- Scripts that call `emergency lockdown` and expect no question: with a terminal, `enable` and `disable` now ask whether to sync the hosts. Answer with `--yes`, or run `tacctl host sync <hosts>` yourself; without a terminal nothing runs and a notice names the hosts.
- The way back is `tacctl rollback 0.2.22`. It removes the users' email addresses and writes the SNMP credential files in version 1 again (one v3 user per level, the default), after a snapshot it keeps, and needs `--yes` when it drops anything. Afterwards the older release reports the rendered config as out of date until its first render. `tacctl backup recover`

> `<snapshot>` returns what was dropped once 0.2.23 or later is installed again. The rollback is refused while an emergency lockdown has enrolled hosts: lift it and sync the hosts first.

4. tacctl 0.2.22

Released 2026-10-29 · Full release notes

Renamed commands, no aliases. The old forms are now unknown sub-commands, and the one-letter form of `--yes` is refused:

Up to 0.2.21	From 0.2.22
`config listen ...`	`server listen ...`
`config metrics ...`	`server metrics ...`
The one-letter form of `--yes`, on any command	`--yes`
`device list` (and `--json`) with the enrolled hosts	`host list` (and `--json`) for the hosts; `device list` has devices only

Change	What it means on shift	Page
`host list`	Shows state, last seen, by and open notices as `device list` does, with the filters `--name`, `--ip`, `--scope` and `--stale`	*Linux Host Operations* §1
`device list --differs`	The devices whose last pull differs from what is rendered now, with no login (operator tier)	*Superuser Daily Operations* §4.1
`tacctl server`	`server show` is this server at a glance (address, name, default method, metrics exporter, backends and listeners); `server name` sets the name the console shows; `server listen` and `server metrics` are the old `config listen` and `config metrics`	*Superuser Daily Operations* §11.3
Timing scale	For a device behind a long round trip or with a slow CPU, one whole number from 1 to 10 multiplies the host-key scan, session, SNMP and per-device pull times: `device timeout-scale <name>`, `scope timeout-scale <scope>`, `config devices timeout-scale` (superuser); engineers read it in `device show` and `scope show`. 1, the default, changes nothing	*Connecting to Devices* §7, *Superuser Daily Operations* §4.9
`--timing`	`device config pull`, `diff --pull`, `plan --pull` and `apply` print, per device, the time of each phase and name the slowest device; `timings` in `--json`	*Engineer Guide* §3

Change	What it means on shift	Page
`host sync` and `host check` take `--concurrency <n>`	Several hosts at once, output in the order typed; nothing is asked, so a key or agent and a root or passwordless-sudo login are needed	*Linux Host Operations* §2.1
Unknown sub-command	One error line, a `Did you mean` hint and a pointer to `-h`; below the first word it is answered before `sudo` asks for a password	*Getting Started* §5
User names	A period is refused again; a user stored with one stays readable and is renamed with `user rename`	*Access Lifecycle* §2
Host keys of slow devices	A device `ssh-keyscan` reads nothing from is read by tacctl's own ssh client	*Connecting to Devices* §6
Junos virtual chassis	The master answers without a label, and the apply reads it	*Engineer Guide* §5.1
Teal command names	The console's lists show command names in teal like the other fixed words	*Superuser Daily Operations* §10.2
Generated tacquito drop-in	Its comment, and the shipped unit comments, name `server listen` and `server metrics`; the first render restarts tacquito once (see below)	*Backups and Undo* §5
`tacctl rollback 0.2.21`	The release before this one is a target; it removes `server.name` and the timing scale and converts nothing else	*Backups and Undo* §5

Before upgrading from 0.2.21:

- Rename every user whose name has a period (`tacctl user list` shows them; `tacctl user rename <name> <new-name>`). If one is left, 0.2.20 or 0.2.21 has already replaced `tacctl` and the tacquito build when the new `tacctl` refuses; the store, the configuration and the services are not changed, and `tacctl upgrade` run again after the rename finishes it.
- Change scripts, runbooks and notes: `config listen` and `config metrics` become `server listen` and `server metrics`, the one-letter form of `--yes` is spelled out, and a script that reads hosts from `device list` reads `host list`.
- No sudoers rule and no stored setting needs to change: the `server` family is the superuser's, as `config listen` and `config metrics` were, and writes the same keys. The timing scale needs no conversion either: it is 1 until a superuser sets it, and every timing is as before.
- Expect one brief interruption of TACACS+. The comment at the top of the generated tacquito drop-in names the current commands, so the first render after the upgrade (the upgrade's own, else the first `config render` or change of a listener, `loglevel` or exporter) rewrites the drop-in, reloads systemd and restarts tacquito once. The upgrade restarts tacquito once at its end for any changed unit file or drop-in, and that is this restart. RADIUS is not touched. A drop-in you edited by hand is saved aside before it is replaced.

- The way back is `tacctl rollback 0.2.21`. It removes `server.name` and the timing scale (the two `tacctl.yaml` keys and each device's `timeout_scale`), with a note in the plan and no `--yes`. After it the older release's `config validate` reports the rendered config as out of date until its first render writes its own comment, which restarts tacquito once; the rollback itself restarts nothing.

5. tacctl 0.2.21

Released 2026-10-28 · Full release notes

Change	What it means on shift	Page
Every user logs in to the server	Every user can log in to the tacctl server and its console, whatever their scopes, unless disabled or in a group of tier none. The login is a scope called `tacctl` that tacctl manages: reserved, in no listing, edited by no command. Device logins keep the user's own scopes.	*Superuser Daily Operations* §10, §11.1
`install` and `upgrade` set the login up	`install` asks once (`--yes` answers, `--server <ip>` sets the address); `upgrade` asks on a terminal only. `host enroll --local` stays the way to rebuild, move or repair it.	*Superuser Daily Operations* §11.1
`tacctl server addresses`	The address devices and hosts reach the server at is a setting of its own. The device walkthroughs, `config linux script` and `host enroll` default to it.	*Superuser Daily Operations* §11.2
`ssh` asks for the password first	With the password cache on and empty, `ssh` and `device ssh` ask for the password once, before they connect; the next `ssh` asks nothing.	*Getting Started* §1.3
Walkthroughs follow the listener port	A TACACS+ listener that is not on 49 adds its `port` to the Cisco and Junos walkthroughs and the WTI Authentication Port item.	*Engineer Guide* §4.1
Junos chassis of one member	`device config apply` treats it like a single device	*Engineer Guide* §5.1
`tacctl rollback 0.2.20`	The release before this one is a target; every target keeps the users' server login	*Backups and Undo* §5

Before the upgrade, rename a scope of your own that is called `tacctl` (`tacctl scope rename tacctl <new-name>`): it is never taken over, and while it exists `host enroll --local`, the sync of the server and `config validate` stop with one line. **After it,** check the line about the machine's own login, and run `tacctl host sync <server>` as before.

6. tacctl 0.2.20

Released 2026-10-28 · Full release notes

Removed console commands, no aliases. The old forms are now unknown sub-commands:

Up to 0.2.19	From 0.2.20
`console tiers`, `console user` (who gets the console)	Nothing to set: the console is the login shell of every tacctl user
`console system-shell tiers <csv>|none`	`console system-shell <tier> enable|disable`

Change	What it means on shift	Page
Required password change	A new user, and a user whose password a superuser reset, must change it at the next login to the tacctl server before any device accepts them. `--no-change-required` skips it; `user require-password-change` sets or lifts it.	*Getting Started* §2.1, *Access Lifecycle* §5.1
The console for everyone	Every tacctl user, of every tier, logs in to the server's console. The system shell is opened by a superuser per tier or per user; engineers never have it.	*Superuser Daily Operations* §10
Password cache is your choice	`console password-cache on` turns it on for you, where your tier is allowed it; it is off until you do	*Getting Started* §1.3
`--help`, `-h` and `tacctl man`	`--help` after a command prints what `?` prints; `man <command>` opens the manual page there, in the console too. In bash, `?` after `tacctl …` prints help.	*Getting Started* §1
`console color`, `console list-max`	The console's list colours and the longest list it shows without asking	*Superuser Daily Operations* §10.2
Strict Junos management filter	`scope mgmt-acl <scope> mode strict` makes the Junos filter deny by default; engineers can read the mode of their scopes	*Vendor Notes* §3.4
Junos `root` as break-glass	`scope breakglass <scope> add root`; the walkthrough renders the root password and `root-login allow` as comments to fill in	*Break Glass* §1.1
`Kept:` and `Secrets:` in plans	A device's own SNMP, system and NETCONF statements are no irregularity any more; the secrets line is information	*Engineer Guide* §4
Apply on a virtual chassis	The check and the commits must answer for every member; `PENDING until` is the device's own clock	*Engineer Guide* §5.1
Host keys read one type at a time	A device that gives no key to the scan is asked again, and the refusal says how to pin a key by hand	*Connecting to Devices* §6
User names with a period	0.2.20 and 0.2.21 accept a period between the parts of a user name; such a user has no Linux account. 0.2.22 refuses a period	*Access Lifecycle* §2

Change	What it means on shift	Page
`tacctl rollback 0.2.19`	Goes back to the previous release, with warnings for what it undoes	*Backups and Undo* §5

> **After the upgrade,** run `tacctl host sync <server>` for the server's own host entry: the console becomes the login shell of every tacctl user then, and not before. No existing user must change their password until a superuser says so.

7. tacctl 0.2.19

Full release notes

Change	What it means on shift	Page
Emergency lockdown (`tacctl emergency lockdown`)	Superusers can refuse the logins of chosen groups on a scope at once. A red notice appears on every command that names a locked scope.	*Emergency Lockdown*
Engineers work their own scopes	Engineers can enroll, collect, onboard, sync and apply for the devices of their own scopes	*Engineer Guide*
`tacctl device support-bundle`	Collects a scrubbed, read-only bundle of what a developer needs from one device	Device commands (repo)
Wider `system` blocks	Junos and IOS `system` blocks now cover syslog, login banners, login retry and password policy, ssh settings and timestamps; plans can remove a service a scope requires to be off	*Engineer Guide* §3
Host names may contain dots	`tacctl host rename web1 web1.example.net` works	*Linux Host Operations*
Unknown commands answered first	A mistyped command is answered before `sudo` asks for a password	—

8. tacctl 0.2.18

Full release notes

Renamed commands, no aliases. The old names are now unknown commands:

Up to 0.2.17	From 0.2.18
`device config-syntax <name> [auto|ios12|modern]`	`device ios-syntax <name> [auto|ios12|modern]`

Up to 0.2.17	From 0.2.18
`device add --config-syntax <syntax>`	`device add --ios-syntax <syntax>`
`device notices [<name>] [--all]`	`device notice list [<name>] [--all]`
`device ssh-config`	`device client-config`

Also: Tab now completes these names with a space, `?` describes every command and flag from its own usage, and a mistyped command suggests what you may have meant (`tacctl enroll` suggests `device enroll` and `host enroll`). Every tier can run `device notice list` and `device client-config`.

9. tacctl 0.2.17

Full release notes

Change	What it means on shift	Page
`tacctl device enroll`	One attended command from a new address to its plan: key, vendor, registration, pull, plan	*Engineer Guide* §2.2
Apply review asks per device	Approve each Junos device by typing its name. Typing a count no longer works; scripts use `--confirmed --yes`.	*Engineer Guide* §5.1
Host keys accepted one device at a time	`enroll`, `collect` and `onboard` show the one key they will pin; you accept it by typing the name back	*Connecting to Devices* §6
Audit session id	Every audit line ends in `sid=<id>`, so one `grep` finds a whole command. Log filters that anchor the end of a line (`$`) need updating.	*Audit and Compliance* §2
`cmd start` / `cmd end` lines	Every change writes a start and an end line, with the result and the snapshot taken	*Audit and Compliance*
Vendor read by SNMP	`device add` and `device check` say which vendor the device reports; `device vendor <name> --from-device` sets it	*Engineer Guide* §2.4
New selectors	`device config pull`, `diff`, `plan` and `apply` take `--differs`, `--name` and `--ip`; `apply --pull` reads fresh first	*Engineer Guide* §5.1

9. Older releases

Releases 0.2.0 to 0.2.16 are listed on the releases page, and every change is numbered in `CHANGELOG.md`.

See also: About These Docs (which release each page was checked against) · `tacctl version`