Concepts

Users, groups, scopes and tiers, and the other words tacctl uses · Checked against tacctl 0.2.25

Contents

1. The access model 2
2. Groups and tiers 2
3. Scopes 3
4. Devices and hosts 4
5. Notices 4
6. Pull, diff, plan, apply 4
7. Snapshots and the audit trail 5
8. The two emergency controls 5

tacctl decides three things for every login: **whether** a person may log in, **where**, and with **what** privileges. This page explains the model behind those decisions, and the objects you meet in daily work: devices, hosts, notices, plans and snapshots.

> **Example names used on this page** Scopes: `lab`, `site-a`, `site-b` · Devices: `sw1` (Cisco), `rtr1` (Junos), `pdu1` (WTI) · Host: `web1` · User: `alice`

1. The access model

Element	Decides	Set with
Group	*What* a person can do: device privilege (Cisco priv-lvl, Junos class, WTI level) and their tacctl tier	`tacctl user add <name> <group>`, `tacctl user move`
Scopes	*Where* a person can log in: which devices and hosts, by address range	`tacctl user add --scopes`, `tacctl user scope`
Status	*Whether* a person can log in at all	`tacctl user disable` / `enable`

> **An empty scope list means no access anywhere.** It never means everywhere. A new user created without `--scopes` is placed in the default scope only (`tacctl scope default` shows which one).

The tacctl server and its console are the exception: every user can log in there, whatever their scopes, unless disabled or in a group of tier none.

---

2. Groups and tiers

Each group maps to a privilege on every vendor, and to a **tier** for tacctl itself:

Group	Cisco priv-lvl	Junos class	WTI level	tacctl tier	Suits
`readonly`	1	`RO-CLASS`	ViewOnly	read-only	Monitoring, NCM and backup service accounts
`operator`	7	`OP-CLASS`	User	operator	NOC, tier 1–2 troubleshooting
`engineer*`	15	`EN-CLASS`	SuperUser	engineer	Day-to-day change engineers
`superuser`	15	`RW-CLASS`	Administrator	superuser	Platform owners

* Optional. It exists only after a superuser has run `tacctl group preset roles`. Check with `tacctl group list`.

The tiers build on each other: **read-only < operator < engineer < superuser**. Each tier can run everything the tiers below it can.

Tier	Adds
Read-only	Lists and shows of users, groups and devices, `scope list`, `ssh` to devices in your scopes, `status`, `passwd`, `device notice list`, `device client-config`, `man`
Operator	Logs, `config validate`, `device check`, `scan`, `discover`, `device config list`, `backup list`, `device export`; `console show` and the console's system-shell settings (read only); turning their own password cache on or off
Engineer	For the devices of **your own scopes only**: registry changes, pull, diff, plan, Junos apply, enroll, onboard, host keys; listing break-glass holds; listing and showing hosts; `scope show`; reading the Junos management filter mode
Superuser	Everything else: users, groups, scopes, secrets, hosts, lockdowns, break-glass holds, restores

On a device, an operator "changes nothing and interrupts nothing": `clear`, `configure` and similar commands are refused on purpose.

The full verb-by-verb table is in the repository's Tiered access page, and every command's entry in `man tacctl` ends with its `Requires: <tier>` line.

---

3. Scopes

A **scope** bundles client address prefixes with a **shared secret** (the TACACS+ or RADIUS key the devices use). A device or host belongs to the scope whose prefixes cover its address.

```
tacctl scope list                    # one row per scope
tacctl scope lookup 10.10.0.1        # which scope answers this address
tacctl scope show site-a             # prefixes, users, secret length, settings
```

- Every prefix belongs to exactly one scope. Adding a prefix another scope already claims is refused with the owner's name.
- A device whose address no scope covers is **unconfigured**: nobody can log in to it.
- Changing a scope's secret takes effect on the server **at once**. Every device in the scope fails until it has the new key.
- The name `tacctl` is reserved. A scope of that name, managed by tacctl, is this server's own login: it is in no listing and no command edits it.

---

4. Devices and hosts

Object	What it is	Where it is managed
Device	A Cisco, Junos or WTI unit in the **device registry**, by name, with its address, vendor and pinned ssh host keys	*Engineer Guide: Device Changes*, *Superuser Daily Operations*
Linux host	A server **enrolled** so that logins and `sudo` authenticate against tacctl, with accounts tacctl creates	*Linux Host Operations*

Devices and hosts share one namespace, so `tacctl ssh <name>` works for both. `tacctl device list` lists the devices and `tacctl host list` the hosts. A registered device is **configured** when a scope's prefixes cover its address. Only configured devices authenticate users.

> **Hosts follow users only when you sync.** A user change reaches the Linux hosts at the next `tacctl host sync --all`.

---

5. Notices

A **notice** flags something that needs attention on a device or host, such as an unpinned or changed host key, a vendor that differs from what the device reports, or a name mismatch. Each comes with the command that fixes it.

```
tacctl device notice list           # open notices for your scopes
```

Some notices can be acknowledged by a superuser. A changed host key cannot.

---

6. Pull, diff, plan, apply

tacctl knows what each device's AAA configuration should be. It compares that with what the device runs in a fixed set of **managed sections** (`aaa`, `roles`, `mgmt-acl`, `snmp`, `netconf`, `breakglass`, and in some scopes `system`).

Step	What it does	Touches the device?
Pull	Logs in as you and reads the managed sections	Read only
Diff	Shows what differs, section by section	No (uses the last pull)

Step	What it does	Touches the device?
Plan	Prints the exact lines to paste, the checks and the back-out	No (uses the last pull)
Apply	Junos only: commits under `commit confirmed`, proves it with a fresh login as you, then confirms	Yes

When an apply covers several devices, devices that need the same change share a **shape**; the first device of each shape goes alone (the canary), and a shape that an earlier apply proved is **confirmed**. Cisco plans are pasted by hand; WTI plans are a menu checklist. The whole workflow is in *Engineer Guide: Device Changes*, and the vendor differences in *Vendor Notes*.

---

7. Snapshots and the audit trail

- Every change takes a **snapshot** of tacctl's configuration first. A superuser can compare, restore and keep them: *Backups and Undo*.
- Every change writes **audit lines** to syslog (tags `tacctl` and `tacctl-console`): who, what, the result and the snapshot taken. *Audit and Compliance* explains how to read them.

---

8. The two emergency controls

Control	What it does	Page
Emergency lockdown	The server **refuses** the logins of chosen groups on a scope. Devices do not fall back to local accounts. On enrolled Linux hosts it also closes key logins, through `host sync`. Superusers keep access.	*Emergency Lockdown*
Break-glass hold	The server **stops answering** one device or host (a firewall rule refuses its TCP connections), so its local accounts work while the server stays up for everyone else	*Break Glass*

Neither one expires. A superuser lifts each one by hand.

See also: Getting Started · Glossary · Access Lifecycle · `man tacctl`