Vendor Notes

What differs between Cisco, Junos and WTI for operations staff · Checked against tacctl 0.2.25

Contents

1. At a glance 2

2. Cisco IOS / IOS-XE 3

- 2.1 The standard block 3
- 2.2 Command authorization is held back on purpose 3
- 2.3 enable and the console 3
- 2.4 ssh algorithms and configuration syntax are separate 3
- 2.5 Other Cisco points 4

3. Juniper Junos 4

- 3.1 Template users 4
- 3.2 Applying: commit confirmed and the proof 4
- 3.3 Other Junos points 5
- 3.4 The management filter: ssh-only or strict 5

4. WTI console servers 7

- 4.1 A menu walkthrough, not a paste 7
- 4.2 Levels 7
- 4.3 Limits and settings that bite 7

5. Break-glass by vendor 8

tacctl serves the same users to every vendor, but each vendor takes its configuration, its privileges and its emergencies differently. This page puts those differences side by side. The step-by-step procedures stay in *Engineer Guide: Device Changes*; this page links to them.

> **Example names used on this page** Scope: `site-a` · Devices: `sw1` (Cisco IOS-XE), `sw7` (IOS 12.4), `rtr1` (Junos), `pdu1` (WTI)

1. At a glance

	Cisco IOS / IOS-XE	Juniper Junos	WTI console servers
How a fix lands	You paste the plan's region	tacctl applies it (`device config apply`)	You type a menu checklist
Safety net	Second session; optional restore point; back-out region	`commit confirmed`, proven by a fresh login as you, rolled back if the proof fails	None: values take effect at once, no rollback
Groups map to	priv-lvl 1 / 7 / 15	Classes `RO-CLASS`, `OP-CLASS`, `EN-CLASS`, `RW-CLASS`	ViewOnly / User / SuperUser / Administrator
`enable`	Local enable secret only	—	—
Host key on the console	`show ip ssh`	`file show /etc/ssh/ssh_host_ed25519_key.pub`	—
Break-glass login	Local account after the server timeout; console list is local	Local `system login user`, or `root` when the scope records it; `root` on the console is always local	Only if *Fallback Local* is `On`
Steps	Engineer Guide §5.5	Engineer Guide §5.1	Engineer Guide §5.6

Junos is the only vendor tacctl writes to. For Cisco and WTI it reads, compares and plans; a person makes the change.

---

2. Cisco IOS / IOS-XE

2.1 The standard block

Every Cisco device gets the same lines in the same order, so a pull can say exactly what differs. The walkthrough and plans have:

- **Step 0**, a commented checklist (hostname, ssh settings, the local enable secret and similar). It is never compared.
- **Step 1**, the AAA standard, in an order that keeps the session you paste from alive.
- **The check, then Step 2**, command authorization.

2.2 Command authorization is held back on purpose

Until the device is proven to use the scope's server, plans leave out `aaa authorization commands` and `config-commands`. Once a commands list names the server, any user the server doesn't know (including the local user your paste session runs as) is denied every command. Paste Step 1, prove the path, **pull again**, and the next plan adds Step 2.

2.3 `enable` and the console

- `enable` always uses the **local** enable secret. Users land at their level directly (superuser 15, operator 7), so nobody needs `enable` day to day.
- The console line has its own login list, `CONSOLE`, which is local only. A local account can always log in there; with the server up it lands at privilege 1, and `enable` with the local enable secret takes it to 15.

2.4 ssh algorithms and configuration syntax are separate

Setting	What it is	Command
`legacy-ssh`	The device offers only SHA-1 key exchange, CBC ciphers and `ssh-rsa`	`tacctl device legacy-ssh sw7 enable`
`ios-syntax`	Which Cisco syntax is compared: `modern` (IOS 15.2+, 16.x, 17.x, IOS-XE) or `ios12` (IOS 12.x)	`tacctl device ios-syntax sw7 ios12`

With `auto` (the default), the version line of the last pull decides the syntax. A device whose version line isn't mapped shows `needs pull (syntax unknown)`: set `ios12` or `modern`, then pull again. A new IOS 15.6 router may need `--legacy-ssh` and still speak `modern`.

2.5 Other Cisco points

- **Source interface.** A device may send AAA from another interface than its registered address. `tacctl config cisco source-interface <scope>` shows or pins it; the source address must be inside the scope's prefixes.
- **Restore point.** `tacctl device config plan sw1 --restore-point=flash:` adds a block to paste first; `configure replace` with that file backs out.
- **Server port.** When the TACACS+ listener is not on 49 (`tacctl server listen`), the walkthrough adds `port <n>` under `tacacs server TACACS`, after `address ipv4` (with `--legacy`, after the address on the `tacacs-server host` line). On 49 it adds nothing.
- **No `single-connection`.** From 0.2.24 the walkthrough and `--legacy` (`tacacs-server host <address> [port <n>] timeout 5 key ...`) leave it out, and `plan` removes it from a device that has it: tacquito closes a connection idle for 15 seconds (*Engineer Guide* §4).
- **Vendor detection** by SNMP does not name IOS 12.x devices (or ASA and IOS XR). Register them with `--vendor cisco`.

---

3. Juniper Junos

3.1 Template users

Junos logs a TACACS+ user in through a local **template user** of the group's class. **Template users must exist before TACACS+ logins work.** If a login fails right after the server accepted it, the template user is missing: create the template users from the walkthrough (`tacctl config juniper`, or `tacctl device config show rtr1`).

3.2 Applying: `commit confirmed` and the proof

`tacctl device config apply` commits under `commit confirmed` (10 minutes by default for an apply), logs in again **as you** through the device's own login path, checks what landed, and only then confirms. If the proof fails, the change rolls back by itself.

A pasted Junos plan region also ends in `commit confirmed` (5 minutes by default); you type `commit` yourself after the check.

> **`PENDING until <time>`** means tacctl could not read the device after the commit. **Type nothing on that device until the time passes** (the device's own clock, in the zone it prints). Any `commit` would confirm the change. The next apply or `--check` settles the record.

On a virtual chassis, two routing engines or a cluster, the apply expects the check and the commits to answer for every member `show version` lists, and fails the step when one does not. The master of a virtual chassis answers without a label, or, on a chassis of two members, with its own label as well, and a chassis of one member is applied to like a single device (*Engineer Guide* §5.1).

3.3 Other Junos points

Situation	What to do
Apply `failed: other editors or staged changes`	Someone has uncommitted configuration on the device. Coordinate; commit or discard on the device.
`bad secret` continues on a Junos device after a re-paste	Delete the secret and set it again, to avoid hidden characters
A blank device with only a local account	`tacctl device onboard` (Engineer Guide §2.3)
The TACACS+ listener is not on 49 (`tacctl server listen`)	The walkthrough adds `set system tacplus-server <address> port <n>`
Break-glass	A local `system login user` works after the tacplus timeout; `root` on the console is always local. Over ssh, `root` needs the scope to record it and `root-login allow` on the device (*Break Glass* §1.1)

3.4 The management filter: `ssh-only` or `strict`

The Junos walkthrough renders a management filter (`MGMT-ACL` unless another name is set) from the scope's permit list (`tacctl scope mgmt-acl <scope> list`, else the global `tacctl config mgmt-acl list`), the same list that drives the Cisco VTY-ACL and the WTI IP Tables list. Each scope chooses one of two modes for it with `tacctl scope mgmt-acl <scope> mode`. Only Junos devices read the mode: the Cisco VTY-ACL and the WTI IP Tables list are the same in both.

	Mode ssh-only (the default)	Mode strict
Restricts	ssh, NETCONF and SNMP	Every protocol
Last term	`default-accept`: everything else is accepted	None: the implicit discard drops whatever the terms do not accept
From the permit list	ssh and NETCONF, from each plain entry and each entry whose services include `tcp/22`	A plain entry: everything from its source. An entry with services: only those services. First comes the address tacctl reaches the device from.
SNMP client terms	Kept	Kept

The authentication server's address in `strict`. When the device authenticates against another address than the one tacctl reaches it from (`--server`, the recorded server address (`tacctl server addresses`), a RADIUS listener bound to another address, or `--source` alone, the device still being told the address detected for the server), that address is not a source of `permit-mgmt`. The device starts

those sessions, so a term of its own, `permit-auth-replies`, last in the filter, accepts from it only the server's answers:

Protocol	What `permit-auth-replies` accepts from the address
TACACS+	tcp from the TACACS+ listener's source port (`tacacs`, 49, by default) with `tcp-established`: established connections only, so a new connection from that port is refused
RADIUS	udp from source ports `radius` and `radacct` (the listener's, 1812 and 1813 by default), after the SNMP terms, so `deny-snmp` decides udp port 161 first

The filter keeps no state and matches the answers by source port, so for RADIUS it cannot tell an answer from another udp packet sent from those ports (a scope with no SNMP clients has no `deny-snmp` term, and udp port 161 from that address and port is accepted too). There is one address and no such term with neither flag and no recorded address, with `--server` equal to the detected address or to `--source`, or when a plain entry of the permit list holds the address (it is then accepted for everything, as any source of the list). An entry with services for the address keeps its services, and the term adds the answers. The address is no way in for ssh: the lock-out check of a plan does not count it (*Engineer Guide* §4.2). Add it to the permit list to accept more from it.

Once a strict filter is applied to `lo0`, these stop reaching the routing engine:

- routing protocols carried over IP from neighbours that are not in the permit list (BGP, OSPF, LDP, VRRP, BFD);
- the replies of servers that are not in the list: TACACS+ and RADIUS (the replies of the server the walkthrough names are accepted: it is in the list or has `permit-auth-replies`), NTP, DNS;
- NTP, syslog and DHCP from hosts that are not in the list;
- SNMP from sources outside the list (the SNMP clients still poll);
- every other protocol (ping, traceroute) from sources outside the list.

IS-IS is not carried over IP, so a `family inet` filter on `lo0` does not see it: the filter neither stops nor permits it.

> **Before a device gets a strict filter:** add every neighbour and server it needs to the permit list the scope renders from (its own list replaces the global one; *Superuser Daily Operations* §8.1), keep a console session open while the change goes in, and commit with `commit confirmed`. An entry with services needs `tcp/22` among them for ssh, and `tcp/830` for NETCONF.

The walkthrough keeps the line that applies the filter to `lo0` commented, and a plan never adds it. A permit list with no IPv4 entry that permits ssh (a plain entry, or one whose services include `tcp/22`) renders no filter in either mode, because the server's address alone would let only tacctl in; the walkthrough then says what each entry permits instead. Setting the mode is the superuser's (*Superuser Daily Operations* §8); engineers can read it for their own scopes and plan the change (*Engineer Guide* §4). The repository's Management ACL page lists the terms each mode renders.

---

4. WTI console servers

4.1 A menu walkthrough, not a paste

WTI units are configured through numbered text menus on the serial SetUp port. `tacctl config wti` and the plans give a walkthrough: `/N`, then the **TACACS** entry, one value per item, then `[Esc]` until the unit saves.

A WTI plan is a **numbered checklist** of menu steps plus one IP-tables block. Values take effect as soon as you enter them, and **there is no rollback**. The plan never types the local accounts or the final IP-tables `DROP`. Before you start:

- check `/H` (firmware) and `/SN` (other administrators logged in);
- keep a serial console or a second session open.

4.2 Levels

The unit asks for the `wti` service and reads the standard `priv-lvl`:

priv-lvl	WTI access level	Shipped group
0–4	ViewOnly (only the ports granted under Default TACACS User Access)	`readonly` (1)
5–9	User (only the ports granted under Default TACACS User Access)	`operator` (7)
10–14	SuperUser (all ports and plugs)	a group with `wti-level superuser`
15	Administrator	`superuser` (15)

4.3 Limits and settings that bite

Item	Rule
Scope secret	At most 32 characters, no whitespace or punctuation. Regenerate a hex-only key with `tacctl scope secret site-a set $(openssl rand -hex 16)` (superuser).
Usernames	WTI's limit is 32 characters
Service Name	Must be `wti`, not `shell`
Fallback Local	Must be `On` for break-glass to work. With `Off`, nobody gets in until the hold is released.
Authentication Port	The TACACS+ listener's (49 by default; `tacctl server listen`)
Multiple Logins	`On`, or pulls and second sessions are refused

WTI symptoms and fixes are in *Troubleshooting* §6.

---

5. Break-glass by vendor

How to get into each vendor while the server is deliberately not answering is in *Break Glass* §3.

See also: Engineer Guide: Device Changes · Troubleshooting · Cisco, Junos and WTI (repo) · `man tacctl`