

Emergency Lockdown

Refusing the logins of chosen groups on a scope, and lifting it again · Checked against tacctl
0.2.22

Contents

1. When to use it	2
2. Preview first	2
3. Lock	2
4. Close the gaps a lockdown cannot close.....	3
5. Monitor	4
6. Lift.....	4
7. Quick reference.....	4

An emergency lockdown makes the tacctl server **refuse** the logins of selected groups on every device and Linux host in a scope. It is the fastest way to shut a team or a tier out during an incident, without touching a single device. Locking and lifting are **superuser** tasks.

Example names used on this page Scopes: `site-a`, `site-b` · Groups: `operator`, `readonly` · Ticket `INC-4821`

1. When to use it

Typical triggers:

- a leaked shared credential, or several users' credentials exposed;
- a suspected compromised account whose group should be frozen;
- an incident that requires an immediate change freeze on a scope;
- a suspicious script running under an operator account.

For a single account, disabling the user is usually enough (*Incident Response Runbooks R1*).

How it works: the locked groups' users are taken out of the scope when the server's configuration is rendered. The server keeps answering, and answers each login and every further command authorization with an explicit refusal (TACACS+ FAIL, RADIUS Reject). Because it refuses rather than staying silent, **devices do not fall back to their local accounts**. Superusers are never locked out.

2. Preview first

`--dry-run` lists who loses access and who keeps it, and changes nothing:

```
tacctl emergency lockdown site-b enable --dry-run
```

3. Lock

Pick one form. Always give a `--reason` with the ticket number (1 to 256 characters); it is stored with the lockdown and written to the audit log.

```
# Every group that is not a superuser's, on one scope
tacctl emergency lockdown site-b enable --reason "INC-4821 credential leak"

# Only the groups named
tacctl emergency lockdown site-b enable operator,readonly --reason "INC-4821 change freeze"

# Every group of one tier (readonly, operator or engineer)
tacctl emergency lockdown site-b enable --tier engineer --reason "INC-4821"

# Every scope, including this server's own logins
tacctl emergency lockdown --all-scopes enable --reason "INC-4821"
```

- At the terminal you confirm by typing the **scope name** back, or the word `all` for `--all-scopes`. There is no `--yes`.
- A further `enable` adds to what is already locked.
- This server's own login (the reserved scope `tacctl`) is locked by `--all-scopes` only, and `--all-scopes disable` lifts it; its lines say this server's own login. `emergency lockdown tacctl ...` is refused.

Never put a secret in a reason. Reasons are logged as typed.

4. Close the gaps a lockdown cannot close

A lockdown blocks only what asks the tacctl server. Check these separately during the incident:

Gap	What to do
Sessions already open (Junos, WTI and Linux keep a session until it logs in again or runs <code>sudo</code>)	Clear them on the devices
Device local accounts: the Cisco console line, Junos <code>root</code> on the console	Check and, if needed, rotate them on the device
Scopes set to <code>local-first</code> (<code>tacctl scope aaa-order <scope></code>)	<code>enable</code> warns about these in red
Local ssh keys on devices	Remove them on the device
Devices that cannot reach the server	Handle on the device
Devices under a break-glass hold	<code>tacctl breakglass list (Break Glass)</code>

`tacctl emergency lockdown status` lists these ways in for the scope.

5. Monitor

```
tacctl emergency lockdown status    # all lockdowns: groups, since, by whom, why, who is
locked out
tacctl emergency lockdown status site-b
tacctl emergency lockdown status --json
```

While a lockdown stands:

- every command that names the scope prints a red **EMERGENCY LOCKDOWN** on scope ... line;
- `tacctl status`, `tacctl config validate` and `tacctl backup restore` show it (engineers see it there for their own scopes);
- locked-out users see the red line too, so expect calls: tell the service desk which superuser to contact.

6. Lift

```
tacctl emergency lockdown site-b disable    # lift everything on the scope
tacctl emergency lockdown site-b disable readonly    # lift for one group only
tacctl emergency lockdown --all-scopes disable
```

The rendered configuration comes back byte for byte.

There is no timer. A lockdown stays until a superuser disables it. Agree at the start of the incident who lifts it, and when.

Verify: `tacctl emergency lockdown status` lists nothing for the scope, and the red line no longer appears on other commands.

7. Quick reference

Task	Command
Preview	<code>tacctl emergency lockdown <scope> enable --dry-run</code>
Lock everyone but superusers	<code>tacctl emergency lockdown <scope> enable --reason "<ticket>"</code>
Lock chosen groups	<code>tacctl emergency lockdown <scope> enable <g1>,<g2> --reason "<ticket>"</code>

Task	Command
Lock one tier	<code>tacctl emergency lockdown <scope> enable --tier <tier> --reason "<ticket>"</code>
Lock every scope	<code>tacctl emergency lockdown --all-scopes enable --reason "<ticket>"</code>
Status	<code>tacctl emergency lockdown status [<scope>]</code>
Lift	<code>tacctl emergency lockdown <scope> disable [<group>]</code>

See also: *Incident Response Runbooks R2 · Break Glass* · [Emergency commands \(repo\)](#) · `man tacctl`