Your Tanium maintenance schedule

Daily, weekly, monthly, and quarterly checks that keep your Tanium deployment reporting accurately at scale. Print it, pin it, and put a name next to every check. The pages that follow show how to run each one.

Daily

Tanium operator

About 10 minutes, first thing

- [ ] **Online Clients vs. expected**
  Online vs. Total Endpoints on the Tanium Home page. Investigate any drop you can't explain.
- [ ] **Failed Connect and integration jobs**
  CMDB feeds, SIEM exports, and ticketing integrations.
- [ ] **Failed deployments**
  Patch and Deploy deployments with errors since yesterday.

Weekly

Endpoint engineer

Pick a fixed day

- [ ] **Client health failures**
  Including tooling left behind by modules you no longer use.
- [ ] **Patch and Deploy tool status**
  Endpoints marked “needs attention” don't receive deployments.
- [ ] **Maintenance window coverage**
  Deploy skips endpoints with no window. In Patch, it depends on your window model.
- [ ] **Release notes**
  Read new Tanium Cloud release notes for fixes and required actions.

Monthly

Tanium administrator

The week of Patch Tuesday

- [ ] **Patch Tuesday scan sync**
  Sync Tanium Scan for Windows on Patch Tuesday evening.
- [ ] **Client version spread and upgrades**
  Version count, upgrade failures, and known-issue builds.
- [ ] **Patch results and scan settings**
  30-day success rate, scan errors, and scan settings.
- [ ] **Third-party coverage**
  Gallery updates needed, and package sync failures.
- [ ] **Scheduled actions**
  Stale, duplicate, or outdated-package actions.
- [ ] **Most expensive Sensors**
  Custom Sensors sorted by runtime. Flag the top few.
- [ ] **API tokens**
  No use in 14+ days, or not restricted by trusted IP.
- [ ] **Atlas AI credit usage**
  Credit pace, user caps, alerts, and background agents.
- [ ] **New OS coverage**
  Comply assessment coverage for new OS versions.

Quarterly

Platform owner, with security

Book it a quarter ahead

- [ ] **Computer groups**
  Manual groups, and negative conditions like not contains.
- [ ] **Admin role assignments**
  Direct Admin assignments, and who still needs Admin.
- [ ] **Custom role review**
  Unused custom roles, and roles missing new permissions.
- [ ] **Custom Sensor review**
  What each one collects, whether it's still needed, and whether its results are still correct.
- [ ] **Orphaned content**
  Content owned by people who have left. Transfer it to an active owner.

Start next week

1. **Pick three daily checks**
   Put them on a dashboard you open every morning.
2. **Calendar the monthly review**
   The week of Patch Tuesday, with a named owner.
3. **Book your first quarterly review**
   Use it as your baseline lap time.

Questions? nathan.forrester@chuco.com // jeff@chuco.com

How to run each check

Each check below says where to look in the Tanium Console, what good looks like, and what to do when it isn't. Menu paths are from Tanium Cloud; on-premises consoles can differ slightly. Links go to Tanium's own documentation, which stays current as the product changes. Links checked November 12, 2026.

Good looks like targets are Chuco best practices, not Tanium requirements. Adjust them to your environment.

Daily — Tanium operator // About 10 minutes, first thing

Online Clients vs. expected

Questions only return answers from endpoints that are online.

WHERE TO LOOK
- On the Tanium Home page, compare **Online Endpoints** to **Total Endpoints** in Environment Status. Total counts every endpoint that registered in the last 30 days.
- On the same panel, **Unmanaged Network Interfaces** shows devices Discover found without a Tanium Client.
- For detail, go to **Administration > Configuration > Client Status** and sort by last registration. Clear **Hide Duplicate Host Names** to see hosts that registered under more than one computer ID; the item count shows the difference.

GOOD LOOKS LIKE Online close to Total, and both steady from day to day. Every endpoint unseen for 14 days or more is one you expect, such as a decommissioned or stored device. Duplicate registrations under 15% of all registrations.

IF IT'S OFF A drop across one site, subnet, or OS usually points to the network or a proxy. For single endpoints, use a Discover label and a recurring Client Management deployment to reinstall the Tanium Client.

TANIUM DOCS
Monitoring Tanium Clients
Maintaining Tanium Clients

Failed Connect and integration jobs

If a Connect job fails, the system it feeds stops getting updated data.

WHERE TO LOOK
- Go to **Modules > Connect > Connections** and turn on the **Failed** toggle.
- Check integrations that call the Tanium API from outside Connect, such as ServiceNow, on their own side.

GOOD LOOKS LIKE Zero failed connections, and nothing flagged as needing attention.

IF IT'S OFF Open the failed run, fix the cause, and run it again. Then set up a failed connections report or a Failed Connection Run notification so the next failure finds you.

TANIUM DOCS
Maintaining Connect
Managing connections

Failed deployments

Failed deployments leave endpoints without the patches or software they need.

WHERE TO LOOK
- Go to **Modules > Patch > Deployments** and open any active deployment with endpoints that need attention.
- Go to **Modules > Deploy > Deployments** and check the status counts on active deployments.

GOOD LOOKS LIKE No active deployment with failed or needs-attention endpoints that nobody has reviewed.

IF IT'S OFF Open the deployment and read the status per endpoint. Closed maintenance windows, download failures, and low disk space are the most common causes.

TANIUM DOCS
Patch: Reviewing deployments
Deploy: Deployment status reference

Weekly Endpoint engineer // Pick a fixed day

Client health failures

An unhealthy Tanium Client can still show as online but return incomplete results.

WHERE TO LOOK
- Go to **Shared Services > Client Management > Client Health**, open the **Deployment** tab, and review the **Health Failures** panel. Click Interact for endpoint detail.
- For leftover tooling, go to **Shared Services > Endpoint Configuration > Tools** and select **Safe to Remove** under Show tools with.

GOOD LOOKS LIKE 100% healthy, and nothing in Safe to Remove except tools a module installs on purpose, such as the Nmap tools that Discover uses.

IF IT'S OFF Follow Tanium's resolution steps for the failing Client Extension. Remove unused tools from Safe to Remove rather than waiting for automatic removal.

TANIUM DOCS
Maintaining Tanium Clients
Managing installed endpoint tools

Patch and Deploy tool status

If the Patch or Deploy tools aren't working on an endpoint, it won't receive deployments.

WHERE TO LOOK
- Go to **Modules > Deploy > Overview**. The **Deploy Coverage** bar splits endpoints into **Optimal** and **Needs Attention**; click Needs Attention for the list.
- Go to **Modules > Patch > Overview**. Under Health, the **Endpoint Readiness** bar shows Optimal, Needs Attention, Initializing, and Unsupported; click Needs Attention.

GOOD LOOKS LIKE Deploy Coverage and Patch Endpoint Readiness at or near 100% Optimal, with Needs Attention at or near zero.

IF IT'S OFF Clicking Needs Attention in either bar gives the reason for each endpoint. In Patch, the usual reasons are scan errors or stale scans, no scan configuration targeting the endpoint, or missing tools. Fix the largest group first; it is usually one shared cause.

TANIUM DOCS
Patch troubleshooting: unhealthy readiness score
Maintaining Deploy

Maintenance window coverage

Deploy never runs outside a maintenance window. Patch depends on which window model your environment uses.

WHERE TO LOOK
- Review **Modules > Deploy > Maintenance Windows** and **Modules > Patch > Maintenance Windows**, and the computer groups each window is enforced on.
- To find endpoints without one, ask: *Get Deploy - Has Enforced Maintenance Window and Patch - Has Enforced Maintenance Window from all machines*.

GOOD LOOKS LIKE At least 90% of endpoints with an enforced window, and every exception deliberate.

IF IT'S OFF In Patch fail-open, an endpoint with no window can be patched at any time; in fail-closed, it is never patched. Tanium is moving environments to fail-closed, so confirm which model you are on.

TANIUM DOCS
Deploy: Managing maintenance windows
Patch: Setting maintenance windows

Release notes

Tanium Cloud updates often, and the release notes call out fixes, behavior changes, and actions you need to take.

WHERE TO LOOK
- Open **Tanium Release Notes** in the Tanium Resource Center and read the Cloud release notes since your last review, starting with the modules you use.
- Look for items marked as needing customer action, API changes, and fixes for issues you have seen.

GOOD LOOKS LIKE Every release since the last review read, and each required action assigned to an owner.

IF IT'S OFF If an update needs action, such as a manual sync or re-testing API scripts, assign it and track it until it is done.

TANIUM DOCS
Tanium Release Notes
Tanium Product Release: Monthly Roll-Up

Monthly Tanium administrator // The week of Patch Tuesday

Patch Tuesday scan sync

Endpoints can't find new patches until Tanium Scan for Windows syncs the updates Microsoft released.

WHERE TO LOOK
- On Patch Tuesday evening, go to **Modules > Patch > Scan Management > Tanium Scan for Windows** and click **Synchronize Now**. Microsoft's publish time varies, and some months it lands mid-afternoon.
- When it finishes, confirm **Last Successful Synchronization** shows that evening.

GOOD LOOKS LIKE A successful sync on Patch Tuesday evening, after Microsoft's release, and no Job failed banner on the Patch Overview.

IF IT'S OFF If the sync fails, retry it from the banner. If new patches still don't show as applicable after endpoints scan, deploy Patch - Reset Windows Update Client and then Patch - Force Start Scan [Windows], starting with a small test group.

TANIUM DOCS Configuring Patch: Tanium Scan for Windows

Client version spread and upgrades

Older Tanium Clients miss fixes, and running many versions makes troubleshooting harder.

WHERE TO LOOK
- Go to **Shared Services > Client Management > Client Health**. The **Deployment** tab summarizes Client versions.
- For upgrade progress, ask: *Get Endpoint Configuration - Tools Status Summary from all machines* and look for **Error**.

GOOD LOOKS LIKE No endpoint more than three releases behind the latest, no builds with known issues in the release notes, and All Computers targeted only by the final upgrade ring.

IF IT'S OFF Turn on Tanium Client upgrades in Endpoint Configuration change management, and work through the endpoints in Error before promoting the next version.

TANIUM DOCS Upgrading Tanium Clients
Managing upgrade rollouts

Patch results and scan settings

Patch results are only accurate if scans run on schedule and are configured correctly.

WHERE TO LOOK
- Go to **Modules > Patch > Overview** and review **Endpoint Compliance for Critical & Important Patches** (released over 30 days ago) and **Top Missing Critical/Important Patches**. Note any Job failed banner at the top of the page.
- Go to **Modules > Patch > Scan Management** and review the **Scan Errors** tab.

GOOD LOOKS LIKE 95% or more compliant on patches older than 30 days, and 90% of endpoints scanned in the last 7 days. Turn on **Enable Managed Compatibility** if SCCM or another WSUS product runs on the same endpoints. Random Scan Delay defaults to 120 minutes; use 480 or more for VDI.

IF IT'S OFF Under 80% compliant is a risk. Check maintenance windows and scan errors before changing deployments.

TANIUM DOCS Maintaining Patch
Enforcing scan configurations

Third-party coverage

Browsers and conferencing apps release updates often, so they fall behind fastest.

WHERE TO LOOK
- Go to **Modules > Deploy > Overview** and review **Top 10 Gallery Package Updates Needed**. Each bar is the number of endpoints eligible for an update.
- For every title, not just the top 10, use the **Updates Needed** column in the **Software Packages** grid on the same page.

GOOD LOOKS LIKE No gallery title with an update pending on five or more endpoints, and no sync errors in the Deploy workbench.

IF IT'S OFF Automate the titles that keep coming back. A Job failed: Sync Software Package Files error that lasts over an hour needs troubleshooting.

TANIUM DOCS Maintaining Deploy
Deploy troubleshooting

Scheduled actions

Scheduled actions keep running until someone changes or removes them.

WHERE TO LOOK
- Go to **Administration > Actions > Scheduled Actions** and set the **Source Package** filter to **Has Updates**.
- Then clear the filter and look for disabled actions, actions with no next run, and two actions sending the same package to the same group.

GOOD LOOKS LIKE Nothing under Has Updates, no duplicates, and an owner for every action.

IF IT'S OFF Click Update Source Package on each action with updates. Remove or consolidate the rest.

TANIUM DOCS Managing scheduled actions and action history

Most expensive Sensors

Sensors run on every endpoint each time a question or dashboard asks for them, so slow ones add load everywhere.

WHERE TO LOOK
- Go to **Administration > Content > Sensors** and select **Show Runtime**. Under Filters, add **Modified By (Persona)** is not equal to **taniumconsole**, then sort **Runtime** descending.
- Check which saved questions and dashboards use the slowest ones, and how often they reissue.

GOOD LOOKS LIKE Tanium's default thresholds are Low above 100 ms, Medium above 500 ms, and High above 1,000 ms. A High Sensor on a short reissue interval is the one to fix first.

IF IT'S OFF Lengthen the reissue interval, replace it with a native Sensor, or rewrite it. PowerShell or Tanium Script Language first; Python only when you need it.

TANIUM DOCS Assessing question impacts through Sensor runtimes
Managing sensors

API tokens

Each token gives access to your environment until it expires or is revoked.

WHERE TO LOOK
- Go to **Administration > Permissions > API Tokens**. Under Filters, add **Notes** does not contain **System Use Only** to hide the tokens Tanium uses itself.
- Sort **Last Time Used** oldest first, then check **User**, **Trusted IP addresses**, and **Expiration** for each token.

GOOD LOOKS LIKE No token unused for more than 14 days, none open to every address, one token per process, and tokens bound to service accounts.

IF IT'S OFF Revoke unused tokens and rotate the rest on a schedule.

TANIUM DOCS Enabling long-lived sessions through API tokens

Atlas AI credit usage

Credits reset monthly and don't roll over. A user or environment that hits its cap is blocked from AI work until the reset.

WHERE TO LOOK
- In the Atlas sidebar, go to **Settings > AI Credit Usage**. Check usage against the monthly allocation, the next reset date, and the top users and groups.
- Go to **Settings > Audit** to see credits per conversation, background agent, and external MCP client.

GOOD LOOKS LIKE Usage on pace to stay within the allocation, caps set for users or groups, email alerts configured, an owner for every background agent, and no MCP clients you don't recognize.

IF IT'S OFF Open the top consumers in Audit. For background agents on a fixed schedule, slow the schedule or switch to a poll trigger so they run only when something changes. Move tasks that don't need AI to an Automate playbook. Then set caps.

TANIUM DOCS Managing AI chat and credit usage

New OS coverage

New operating system versions need to be added to Comply assessments before they can be scanned.

WHERE TO LOOK
- Ask: *Get Operating System and Comply - Last Scan from all machines*. Every OS should show a recent scan.
- Go to **Modules > Comply > Assessments** and check Status for errors.

GOOD LOOKS LIKE Every OS in your fleet scanned by a Comply assessment.

IF IT'S OFF Add the new OS to your Comply assessments, then confirm it shows a recent scan.

TANIUM DOCS Maintaining Comply
Creating compliance assessments

Quarterly Platform owner, with security // Book it a quarter ahead

Computer groups

Computer groups control targeting. Groups that aren't maintained can leave endpoints out or pull in ones you didn't intend.

WHERE TO LOOK
- Go to **Administration > Permissions > Computer Groups**. Under Filters, add **Type** is equal to **Manual** to list manual groups.
- Then clear the filter and check each dynamic group's expression for negative conditions such as *not contains* or *not equals*. An endpoint that returns an error or an unexpected answer can match them and land in the group.

GOOD LOOKS LIKE Manual groups are temporary, and every group expression uses positive matches only.

IF IT'S OFF Rebuild manual groups on a Sensor or custom tag so membership updates itself. Replace negative conditions with a positive match, such as a true or false Sensor set to *contains false*.

TANIUM DOCS
Negative Targeting: Use with Caution (Tanium sign-in)
Controlling management rights through computer groups

Admin role assignments

Admin can do anything in Tanium, so it should go only to people who need it.

WHERE TO LOOK
- Go to **Administration > Permissions > Roles** and open the **Admin** role.
- The **Users** list shows people assigned Admin directly. The **User Groups** list shows groups that grant it; check who is in each group.

GOOD LOOKS LIKE Admin granted through user groups, not directly, and only to people whose job needs it.

IF IT'S OFF Move direct assignments into a user group, and remove Admin from anyone who no longer needs it. Give them a narrower role instead.

TANIUM DOCS
Managing access permissions through roles
Managing user groups

Custom role review

Tanium updates add features and permissions, and a custom role doesn't include them until someone adds them.

WHERE TO LOOK
- Go to **Administration > Permissions > Roles** and set **Category** to **Custom**.
- Use **Total Users** to find roles no one uses. Open each role in use and check it against features added since the last review.

GOOD LOOKS LIKE Every custom role is in use, has a clear purpose, and includes the permissions its users need for current features.

IF IT'S OFF Delete unused roles, and add permissions for new features the role's users should have.

TANIUM DOCS
Managing access permissions through roles

Custom Sensor review

Custom Sensors need an owner, and Tanium may now include a built-in Sensor that does the same job.

WHERE TO LOOK
- Go to **Administration > Content > Sensors**. Under Filters, add **Modified By (Persona)** is not equal to **taniumconsole** to list Sensors your team created or changed.
- For each one, read the script to confirm what it collects, check whether it is still used, and ask it on a few endpoints to confirm the results are still correct.

GOOD LOOKS LIKE Every custom Sensor has an owner, a known purpose, results that are still correct, and no built-in replacement.

IF IT'S OFF Retire Sensors no one uses or that a built-in Sensor replaces. Fix any that return wrong results or collect more than they need to.

TANIUM DOCS
Managing sensors

Orphaned content

Content owned by a deleted or locked-out account keeps running with no one responsible for it.

WHERE TO LOOK	• Go to **Administration > Permissions > Deleted User Content**.
GOOD LOOKS LIKE	An empty list.
IF IT'S OFF	Click Manage Content and transfer it to a persona or active account with the same roles and computer groups, or delete what is no longer needed.
TANIUM DOCS	Managing users: delete content or transfer ownership