Tanium Maintenance User Guide

2026H2 Semiannual Release

November 18, 2026



The information in this document is subject to change without notice. Further, the information provided in this document is provided "as is" and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium's customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Please visit https://help.tanium.com for the most current Tanium product documentation.

This documentation may provide access to or information about content, products (including hardware and software), and servicesprovided by third parties ("Third Party Items"). With respect to such Third Party Items, Tanium Inc. and its affiliates (i) are not responsible for such items, and expressly disclaim all warranties and liability of any kind related to such Third Party Items and (ii) will not be responsible for any loss, costs, or damages incurred due to your access to or use of such Third Party Items unless expressly set forth otherwise in an applicable agreement between you and Tanium.

Further, this documentation does not require or contemplate the use of or combination with Tanium products with any particular Third Party Items and neither Tanium nor its affiliates shall have any responsibility for any infringement of intellectual property rights caused by any such combination. You, and not Tanium, are responsible for determining that any combination of Third Party Items with Tanium products is appropriate and will not cause infringement of any third party intellectual property rights.

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S.Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years. We certify against the WCAG 2.2 / VPAT 2.5 standards for all major product modules. Tanium performs ongoing reassessments as appropriate, given the scope and type of changes to the UI and product features from release to release. In the most recent testing, the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.2 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

As new products and features are continuously delivered, Tanium will conduct testing to identify potential gaps in compliance with accessibility guidelines. Tanium is committed to making commercially reasonable efforts to address any gaps as quickly as is feasible, given the severity of the issue and scope of the changes. Tanium factors these objectives into the ongoing delivery schedule of features and releases with our existing resources.

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are

©2026 Tanium Inc. All Rights Reserved

committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, Tanium Support atsupport@tanium.com, or email accessibility@tanium.com to make further inquiries.

Tanium is a trademark of Tanium, Inc. in the U.S. and other countries. Third-party trademarks mentioned are the property of the irrespective owners.

Kubernetes®, K8s®, and the Kubernetes logo are registered trademarks of The Linux Foundation®.

Android, ChromeOS, and Google are trademarks of Google LLC.

iOS, iPad, iPadOS, iPhone, Mac, and macOS are trademarks of Apple Inc., and registered in the U.S. and other countries and regions.

Patents: https://www.tanium.com/patents

Tanium Open Source Disclosure : https://tanium.github.io/opensource/

© 2026 Tanium Inc. All rights reserved.

Table of contents

Getting started 8
- Back up your deployment 8
- Configure RBAC for maintenance tasks 9
  - Module-specific roles and permissions 9
- Verify TPAN report generation 11
- Configure Tanium™ Appliance monitoring 11
- Automate auditing and remediation of disconnected Clients 12
- Configure a failed connections report 13
- Contact Tanium Support 14

Weekly maintenance 15
- Review and resolve critical and high TPAN findings 15
- Review the Tanium Client deployment 15
  - Check the endpoint leader percentage 16
  - Check the endpoint count 17
  - Review and update tags 17
  - Review and update enhanced tags 17
  - Review and update custom tags 18
- Review and update actions that target No Computers 18
- Perform weekly Deploy maintenance 19

Monthly maintenance 20
- Review Tanium security advisories 20
- Review all TPAN findings 21
- Review Appliance health 22
  - Review the Health Check report 22
  - Monitor Appliance performance (optional) 22
- Review and update global bandwidth throttles 23
- Review and import solution updates 23
- Asset monthly maintenance 24

©2026 Tanium Inc. All Rights Reserved

Review Tanium source imports 24
Review the status of import and export jobs 24
Review reports 24
Review views 25
Automate monthly maintenance 25
Benchmark monthly maintenance 25
Certificate Manager monthly maintenance 26
Client monthly maintenance 26
Review and remediate Tanium Client health and Client Extension issues 26
Review and adjust the distribution of Tanium Client registration traffic 27
Review and update Tanium Client logging levels 28
Review and update Tanium Client settings 29
Review and upgrade Tanium Client versions 29
Review and update Tanium Client subnets 30
Review and update isolated subnets 31
Review and update separated subnets 31
Review and update intentional subnets 32
Comply monthly maintenance 32
Connect monthly maintenance 33
Review and remediate connection issues 33
Review and remediate connection schedules 34
Review and update connection owners 34
Review and remediate destination issues 35
Criticality monthly maintenance 35
Deploy monthly maintenance 35
Review and remediate Deploy coverage 35
Remove unused Deploy software packages 36
Stop unneeded ongoing deployments 36
Direct Connect monthly maintenance 36
Directory Query monthly maintenance 36
Discover monthly maintenance 36
Review and remediate Discover resource usage on the Module Server 37
Review and update discovery methods 37
Monitor and troubleshoot endpoints managed 38
Monitor and troubleshoot mean time to manage 39

©2026 Tanium Inc. All Rights Reserved

Endpoint Configuration monthly maintenance 41
Review and remediate tools deployment 41
Verify whether endpoints have the latest manifest 41
Update the manifest 42
Endpoint Management for Mobile monthly maintenance 43
Endpoint Management for Operational Technology monthly maintenance 43
End-User Notifications monthly maintenance 43
Enforce monthly maintenance 44
Engage monthly maintenance 44
Gateway monthly maintenance 44
Guide monthly maintenance 45
Health Check monthly maintenance 45
Impact monthly maintenance 45
Integrity Monitor monthly maintenance 46
Interact monthly maintenance 46
Investigate monthly maintenance 46
Patch monthly maintenance 46
Review and remediate Patch coverage 47
Review and update scan configurations 47
Review and update deployments 48
Review and update maintenance windows 48
Performance monthly maintenance 49
Provision monthly maintenance 50
Reporting monthly maintenance 50
Reputation monthly maintenance 51
Reveal monthly maintenance 51
Threat Response monthly maintenance 51
Trends monthly maintenance 52
Zero Trust monthly maintenance 53

Quarterly maintenance 54
Review and update backups and the disaster recovery plan 54
Verify the GRUB key backup (physical or virtual Appliance only) 55
Review and update Console user accounts 55
Review and update RBAC permissions and authentication settings 56
Review and update TanOS user accounts (Appliance only) 57

©2026 Tanium Inc. All Rights Reserved

Review and update site bandwidth throttles 58
Delete unnecessary computer groups 59
Review and update scheduled actions 59
Review and update Comply assessments 61
Review and update custom action groups for Deploy 62
Review Jump Gate policies 62
Review access policies 62
Review timeout and data retention policies 63
Review and update custom action groups for Patch 64

Semi-annual maintenance 66
Review and update Deploy self-service profiles 66

Annual maintenance 67
Test a planned failover 67
Test disaster recovery 67

As-needed maintenance 68
Rotate certificates for Tanium Console, Module Server, and API access 68
Review and update Patch block lists 68

©2026 Tanium Inc. All Rights Reserved

Getting started with Tanium maintenance

About this task

After you set up a Tanium deployment, perform regular maintenance tasks to ensure that the deployment uses resources efficiently and provides the best user experience. This guide is intended to provide a baseline of recommended maintenance tasks for all Tanium deployments at various intervals. For example, the recommended tasks alert you to changes in your network, tools deployment, and role-based access control (RBAC) assignments. The specifics of your environment might require different tasks and different intervals, and both might change over time. Contact Tanium Support on page 14 if you need help determining the appropriate maintenance tasks or help troubleshooting issues that you discover during maintenance.

Perform the one-time tasks described in the following sections to facilitate regular maintenance.

Back up your deployment

About this task

Create a disaster recovery plan and back up the Tanium™ Core Platform servers and databases so that you can restore your deployment to a known functional state in case of issues. For example, if a system failure makes the host system of the Tanium™ Server unrecoverable, you can use a backup to quickly restore functionality on a new host.

The backup procedure depends on your Tanium infrastructure:

- Tanium Appliance User Guide: Tanium Appliance redundancy, backup, and recovery
- Tanium Core Platform User Guide for Windows Deployments: Back up Tanium Core Platform servers and databases

©2026 Tanium Inc. All Rights Reserved

Note: Review and update backups and the disaster recovery plan on page 54 during quarterly maintenance.

Test disaster recovery on page 67 during annual maintenance.

Configure RBAC for maintenance tasks

About this task

Decide which users are responsible for performing Tanium maintenance tasks and assign the required roles, user groups, personas, and computer groups. For example, users can apply custom tags only to endpoints in computer groups that are assigned to their user accounts. Users who then configure computer groups with tag-based membership require **Computer Group** write permission, **Interact Module** write permission, and **Sensor** read permission.

To assign Tanium-defined roles or to create and assign custom roles, see Tanium Console User Guide: Managing roles. For the Tanium™ solution-specific role permissions that are required to perform maintenance tasks, see the corresponding user guides:

Module-specific roles and permissions

- Asset
- Automate
- Benchmark
- Certificate Manager
- Client Management
- Cloud Workloads
- Comply
- Connect
- Criticality

©2026 Tanium Inc. All Rights Reserved

- Deploy
- Direct Connect
- Directory Query
- Discover
- Endpoint Configuration
- Endpoint Management for Mobile
- Endpoint Management for Operational Technology
- End-User Notifications
- Enforce
- Engage
- Gateway
- Guide
- Health Check
- Impact
- Integrations Gallery
- Integrity Monitor
- Interact
- Investigate
- Jump Gate
- Patch
- Performance
- Provision

©2026 Tanium Inc. All Rights Reserved

- Reporting
- Reputation
- Reveal
- Threat Response
- Trends
- Zero Trust

Verify TPAN report generation

About this task

The Tanium™ Platform Analyzer (TPAN) report can facilitate future troubleshooting regardless of whether your deployment currently has issues. If your Tanium license includes Tanium™ Health Check, verify that it is configured to generate TPAN reports:

1. From the Main menu, go to **Shared Services** > **Health Check**.
2. Go to the **Reports** section and verify that TPAN reports are generated at the expected cadence.
3. If TPAN reports are not generated as expected, see:
    - Tanium Health Check User Guide: Configuring Health Check
    - Tanium Health Check User Guide: Generating reports

Configure Tanium™ Appliance monitoring

Perform any of the following tasks to facilitate monitoring the health of your Tanium deployment if it uses Appliance infrastructure. For example, if your organization has a syslog server or SNMP manager, you can integrate it with the Appliance for monitoring. If these monitoring solutions reveal issues that require resolution, see Tanium Appliance User Guide: Troubleshooting.

Configure TanOS alerts

TanOS can send alerts to a syslog server or to an email recipient. For optimal results, configure an SMTP email recipient. If the syslog server fails, the SMTP recipient receives a failure notification every

©2026 Tanium Inc. All Rights Reserved

15 minutes until either the failure is resolved or syslog forwarding is disabled. For more information, see Tanium Appliance User Guide: Configure syslog alerts.

Configure syslog forwarding

You can forward Appliance logs to a remote syslog server. The syslog forwarding configuration is separate from the syslog alert configuration. For the differences, and the steps to configure syslog forwarding, see Tanium Appliance User Guide: Configuring syslog forwarding.

Configure SNMP

You can configure integration with an SNMP manager to collect and analyze Appliance information. After you configure credentials, the user `tansnmp` can make a remote SNMP connection to the Appliance or to the Integrated Dell Remote Access Controller (iDRAC) interface of a physical Appliance to conduct SNMP polling from a remote host or SNMP manager. For more information, see Tanium Appliance User Guide: Configuring SNMP.

Automate auditing and remediation of disconnected Clients

About this task

In some cases, users with local administrative rights might be able to uninstall the Tanium Client, stop the Tanium Client service, or tamper with Tanium Client files. Use Tanium Discover to regularly audit endpoints to which you have deployed the Tanium Client, and automatically redeploy the Tanium Client to previously managed endpoints that have become unmanaged.

1. Configure a profile in Discover that scans endpoints to which you have deployed the Tanium Client. For more information, see Tanium Discover User Guide: Scan types.
2. Configure an automatic label in Discover (such as `Disconnected`) with conditions that identify endpoints on which you expect the Tanium Client to be installed. For more information, see Tanium Discover User Guide: Automatically label interfaces.

©2026 Tanium Inc. All Rights Reserved

Note:

Discover labels must have the following settings to be used with Client Management:

- **Type**: Automatic
- **Activity**: Retain
- **Retain Activity**: Label

3. (Optional) Configure a Connect destination to alert you of newly unmanaged endpoints that the label identifies. For more information, see Tanium Discover User Guide: Export interface data to a Connect destination.
4. Configure a recurring deployment in Client Management that targets the Discover label you created. For more information, see Tanium Client Management User Guide: Deploying the Tanium Client using Client Management.

Result

Note: If redeploying the Tanium Client is unsuccessful or does not successfully reconnect the endpoint, other issues might be preventing the Tanium Client from connecting or registering. For troubleshooting information, see Tanium Client Management User Guide: Troubleshoot issues with connection and registration.

Tip: To reduce the likelihood of casual tampering by users with local administrator rights on Windows, you can take measures to harden the Tanium Client on Windows. For more information, see Tanium Client Management User Guide: (Optional) Harden the Tanium Client on Windows. Performing regular audits of unmanaged assets is a best practice regardless of whether you have hardened the Tanium Client on Windows.

Configure a failed connections report

About this task

If you use Tanium Connect, you can configure an HTTP destination to schedule the automatic delivery of reports about failed connections. You can set the report format to CSV, delimiter separated values, HTML, or JSON.

©2026 Tanium Inc. All Rights Reserved

If you have the authority to disable or delete failed connections, configuring the report is optional. You can use the report for reviewing and troubleshooting connections before you decide which to disable or delete. Alternatively, you can manually Connect monthly maintenance on page 33 without a report.

If another team in your organization has the authority to disable or delete failed connections, configure the report with the settings that the team requires.

Configure the report as described in Tanium Connect User Guide: Configuring HTTP destinations. A failed connections report requires the following settings:

HTTP destination for failed connections report

Section	Settings
Configuration	• **Source**: **Event** • **Event Group**: **Connect** • **Failed Connection Run**: select • **Unexpected Process Exit**: select • **Destination**: **HTTP**
Enablement	**Listen for this Event** : select

Contact Tanium Support

To contact Tanium Support for help, sign in to the Tanium Customer Community.

For more information about submitting a support case, see Case Submission Form.

©2026 Tanium Inc. All Rights Reserved

Performing weekly maintenance

Review and resolve critical and high TPAN findings

About this task

Check the TPAN report for critical or high findings:

1. Copy the latest Tanium Platform Analyzer (TPAN) report to wherever you store Tanium files for diagnostics. For more information, see Tanium Health Check User Guide: Download a TPAN report.
2. Open the report and select the **Findings** page to see if **Critical** or **High** findings exist.
3. Troubleshoot any **Critical** or **High** findings. For more information, see Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform.
4. Contact Tanium Support on page 14 for help troubleshooting the findings if necessary.

Result

Note: Review all TPAN findings on page 21, including **Medium** and **Low** findings, during monthly maintenance.

Review the Tanium Client deployment

About this task

Check how many endpoints are running the Tanium Client (managed endpoints), how many Clients function as endpoint leaders in Tanium™ linear chains, and the state of custom or enhanced tags on the Clients.

Note: Client monthly maintenance on page 26 during monthly maintenance.

©2026 Tanium Inc. All Rights Reserved

Check the endpoint leader percentage

About this task

In linear chains of Tanium Clients, minimizing the percentage of endpoints that function as leaders helps to reduce bandwidth usage in communications with Tanium Servers and Tanium™ Zone Servers. The leader percentage varies among networks and no specific percentage is ideal for all networks. However, unexpected changes in the percentage might indicate network issues that your networking team must address. For example, a sharp increase in the percentage might cause excessive wide area network (WAN) traffic. Therefore, monitor changes in the leader percentage over time by recording the percentage at weekly intervals.

Note: For more information about leaders, linear chains, and how the Servers evaluate subnet boundaries, see Client peering.

1. Configure the TPAN report if it is not already configured. For more information, see Configuring Health Check.
2. Open the latest TPAN report and select the **Tuning** page.
3. Check the value of **What's the actual or anticipated leader count percentage?** Typically, this value does not change significantly unless your network changes in ways that affect the number and size of Client subnets.
4. If the leader percentage changes more than expected, investigate the possible causes. The percentage might change if:
    - Subnets join or leave your network. Check the endpoint count on page 17 to see if the number of managed endpoints has changed. If the change is due to new subnets, verify that they are authorized to join your network. If the change is due to subnets no longer registering with Tanium Servers or Tanium Zone Servers, verify whether network disruptions or misconfigurations are responsible.
    - A shift occurs between the number of users who are connecting within your internal network and the number who are connecting through virtual private network (VPN) connections. Typically, VPN endpoints do not peer with each other and therefore each one is effectively a leader. For more information, see Configure isolated subnets.

©2026 Tanium Inc. All Rights Reserved

5. Contact Tanium Support on page 14 for help optimizing the leader count, if necessary.

Check the endpoint count

About this task

The number of managed endpoints might fluctuate as endpoints join or leave your network. View the number of managed endpoints to check for potential anomalies and track changes in the weekly count to project future growth. Contact Tanium Support on page 14 to update your license for a higher number of maximum managed endpoints if necessary.

1. Sign in to Tanium Console with a user account that has **Unrestricted Management Rights** for computer groups. The **Administrator** reserved role provides those management rights and you can also switch to a persona that has them.
2. Go to the Tanium **Home** page to check the **Total Endpoints**. This field displays the most accurate tally of online and offline managed endpoints that have registered with the Tanium Server or Zone Server within the retention period (default is 30 days). For more information, see View environment status.
3. Perform one of the following steps if the endpoint count is:
   - Lower than expected: Investigate whether network disruptions or misconfigurations prevent endpoints from registering.
   - Higher than expected: Verify that the new endpoints are authorized to join your network.

Tip: You can configure an automatic Discover label and a Connect destination to alert you when endpoints become unmanaged. For more information, see Audit and remediate disconnected Tanium Clients.

Review and update tags

If you use computer groups for which membership is based on custom tags or enhanced tags, review which endpoints have which tags. Deploy changes to the tags and configure new computer groups if necessary.

Review and update enhanced tags

©2026 Tanium Inc. All Rights Reserved

For information about reviewing and updating enhanced tags, sign in to the Tanium™ Knowledge Base and see the Enhanced Tags Documentation.

Review and update custom tags

1. Determine which endpoints have which tags. For more information, see Review custom tags.
2. Add or remove custom tags if necessary. For more information, see Manage computer group membership through custom tags.
3. Create or delete computer groups with tag-based membership if necessary. For more information, see Managing computer groups.

   Note: You cannot change the membership definition of existing computer groups. You must delete existing groups and recreate them with the correct definition.
4. Add or edit action groups to target tag-based computer groups if necessary. For more information, see Managing action groups.

Review and update actions that target No Computers

About this task

Actions that target the **Default** action group do not deploy to endpoints because **Default** includes only the **No Computers** computer group. In some cases, **Default** might be targeted to prevent unexpected changes on endpoints. Perform the following steps to review the actions that target **Default**, assess whether your environment is ready for deploying the actions, and assign a different action group if necessary.

Best Practice: If you want actions that target **Default** to deploy to endpoints, assign a different action group instead of reconfiguring **Default** to include other computer groups.

Note: For information about actions that target **Default**, see Tanium Console User Guide: Reconfigure actions that target the Default action group.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration** > **Actions** > **Action Groups**.
2. In the **Name** column, click **Default** to view the configuration of that action group.
3. Verify that the assigned **Computer Groups** include only **No Computers**.
   If other computer groups are assigned, deselect them and click **Save**.
4. From the Main menu, go to **Administration** > **Actions** > **Scheduled Actions**.
5. In the **Action Group** drop-down, select **Default** to list only the actions that target that action group.
6. If you want to deploy any of the listed actions to endpoints, assign the actions to a different action group. For more information, see Tanium Console User Guide: Edit action group assignments for scheduled actions.

Result



Note: Review and update scheduled actions on page 59 during quarterly maintenance.

Perform weekly Deploy maintenance

About this task

Monitor Deploy metrics and update the configurations, if necessary.

1. From the Main menu, go to **Modules** > **Trends** > **Boards**.
2. Click **IT Operations Metrics** to view the **Deploy Coverage**, **Endpoints Missing Software Updates Released Over 30 Days**, **Mean Time to Deploy Software**, and **Software Installed by Self Service User Request** panels in the **Deploy** section.
3. Tanium Deploy User Guide: Monitor and troubleshoot Deploy coverage.
4. Tanium Deploy User Guide: Monitor and troubleshoot endpoints missing software updates released over 30 days.
5. Tanium Deploy User Guide: Monitor and troubleshoot mean time to deploy software.
6. Tanium Deploy User Guide: Monitor and troubleshoot software installed by self service user request.

©2026 Tanium Inc. All Rights Reserved

Performing monthly maintenance

About this task

Monthly maintenance includes reviewing health and performance information for the Tanium Core Platform, Tanium Clients, and Tanium solutions.

Tip: For all tasks that provide the option to issue a question in Tanium™ Interact, you can perform additional investigation or remediation on the **Question Results** page by issuing drill-down questions, opening single endpoint views, or deploying actions. For more information, see Tanium Console User Guide: Managing question results.

For tasks that involve viewing reports, you can perform additional investigation or remediation in the Tanium™ Reporting workbench. For more information, see Tanium Reporting User Guide: Working with reports.

For tasks that involve viewing Tanium™ Trends boards, you can perform additional investigation in the Trends workbench. For more information, see Tanium Trends User Guide: Viewing chart results.

Review Tanium security advisories

About this task

Review the security advisories that Tanium publishes to identify and remediate vulnerabilities in Tanium solutions. A Tanium™ Community account is required to perform this task.

1. In your browser, go to the Tanium Technical Support home page and click **Tanium Vulnerabilities**.
   For each advisory, the page provides a brief description that indicates the affected solution and provides a link to a page with full details about the associated vulnerability, such as its severity level.

2. Click each link for vulnerabilities that apply to your licensed solutions and review the

©2026 Tanium Inc. All Rights Reserved

vulnerability details.

3. Perform one of the following tasks:
    - (Best practice) Import any **Available Updates** that resolve the vulnerabilities. For more information, see Tanium Console User Guide: Import or update specific solutions.
    - Apply any **Workarounds and Mitigations** for the vulnerabilities if solution updates are not available or you plan to delay the updates.

Review all TPAN findings

1. Copy the latest Tanium Platform Analyzer (TPAN) report to wherever you store Tanium files for diagnostics. For more information, see Tanium Health Check User Guide: Download a TPAN report.
2. Open the report and select the **Findings** page.
3. Review any **Critical**, **High**, **Medium**, or **Low** findings to decide whether they require:
    - Resolution: Resolve all **Critical** and **High** findings. For example, if the report indicates that the Tanium™ Module Server is not connected, you must resolve the issue immediately because numerous Tanium operations depend on that server. Resolve the **Medium** and **Low** findings only if appropriate. For example, if the **Medium** findings indicate that some actions target the **Default** action group, which includes only the **No Computers** computer group, those actions do not deploy to endpoints. Reconfiguring the actions to target another action group is required only if deploying them to endpoints is appropriate.
    - Investigation: You might have to see more information about findings before deciding if they require resolution or no action. For example, if the **Low** findings indicate that the Tanium Server is using a self-signed certificate for securing user access to the Tanium™ Console, you might have to consult your network security team before deciding whether to replace that certificate with one that a certificate authority (CA) has signed.
    - No action: Some findings might be known conditions that you regard as acceptable. For example, if the **Low** findings indicate that isolated subnets are not defined but you already know that your network does not require isolated subnets, no action is required.
4. Troubleshoot the findings. For more information, see Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User

©2026 Tanium Inc. All Rights Reserved

Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform.

5. Contact Tanium Support on page 14 for help troubleshooting the findings if necessary.

Review Appliance health

About this task

Perform the following tasks if your Tanium deployment uses Appliance infrastructure. If these tasks reveal issues that require resolution, see Tanium Appliance User Guide: Troubleshooting.

Review the Health Check report

About this task

The Health Check report provides information on the health of the Appliance operating system, hardware, users, network, services, applications, database replication, RAID security, Postgres SSL, and virtual machine (if applicable).

1. Run the report. For more information, see Run the Health Check.
2. Review the output for actionable items, which are summarized at the end of the output. For example, the output might indicate that the End User License Agreement (EULA) is not accepted.

Monitor Appliance performance (optional)

For more information about running commands for viewing Appliance performance information, see the following tasks in the Tanium Appliance User Guide:

- Run a SAR command to view statistical information such as CPU load, memory paging, memory utilization, swap usage, and network input/output (I/O).
- Run the iotop command to view I/O utilization by process.
- Run the perf top command to view CPU usage by function.
- Run the htop command to view detailed information about each running process, such as memory and CPU consumption. The output provides an interface whereby you can navigate among values and tabs by keyboard and mouse.

©2026 Tanium Inc. All Rights Reserved

Review and update global bandwidth throttles

About this task

Global throttles limit the bandwidth and the number of concurrent connections that the Tanium Server and Zone Server use to send data to all Tanium Client subnets. Disruptions to Tanium CloudServer functions might occur if the traffic consumes too much bandwidth or if throttles limit the traffic too much for Tanium operations to perform at a reasonable speed. Review the global throttles and, if necessary, update them.

> **Note:** For more information, see Tanium Console User Guide: Bandwidth throttling overview.

1. Check the delays for global throttles to evaluate the current risk of disruptions to Tanium functions. For more information, see Tanium Console User Guide: Verify throttle delays.
2. Update the global throttles if necessary. For more information, see Tanium Console User Guide: Configure global throttles.

Result

> **Note:** Review and update site bandwidth throttles on page 58 during quarterly maintenance.

Review and import solution updates

About this task

Determine whether updates are available for Tanium solutions (modules, shared services, and content-only solutions), and import the updates if appropriate. The best practice is to import solution updates as soon as they become available. However, in certain cases, you might need to delay updates for some solutions while importing others immediately. For example, your organization might have a policy that mandates testing each update in a lab environment before importing it into a production environment.

To review and import solution updates, see Tanium Console User Guide: Import or update specific solutions.

©2026 Tanium Inc. All Rights Reserved

Asset monthly maintenance

Review Tanium source imports

1. From the Main menu, go to **Modules** > **Asset** > **Overview**.
2. Go to the **Health** dashboard to see load time metrics for source data that Tanium™ Asset imports.
3. To investigate load time issues, click **Load Time** to view the import schedules.
4. For any jobs with failed runs, click Edit, set the **Log Level** to **Trace**, and click **Update**.
5. For more information about how to troubleshoot source imports, see Tanium Asset User Guide: Troubleshoot asset data exports and imports.

Review the status of import and export jobs

1. From the Main menu, go to **Modules** > **Asset** > **Overview** and then go to the **Activity** dashboard.
   The dashboard shows the status of import and export jobs.
2. Select each of the **Recent & Upcoming Jobs** and check the status of finished jobs for both **Yesterday** and **Today**. If all the jobs have success status, no troubleshooting is necessary.
3. From the Main menu, go to **Modules** > **Asset** > **Inventory Management** > **Schedules** to see more information about the last completed run for each job in the **Import Schedules** and **Export Schedules** tabs.
4. For any jobs with failed runs, click Edit, set the **Log Level** to **Trace**, and click **Update**.
5. For more information about how to troubleshoot failed jobs, see Tanium Asset User Guide: Troubleshoot asset data exports and imports.

Review reports

1. From the Main menu, go to **Modules** > **Asset** > **Reports** and check the **Status** of the reports. If all the reports are enabled, no troubleshooting is necessary.
2. For any custom reports that have disabled or missing attributes (columns), click Edit, correct the report configuration as necessary, and click **Submit**.

©2026 Tanium Inc. All Rights Reserved

Result

Tip: For more information about report timeout error messages when viewing a report, see Tanium Asset User Guide: Troubleshoot reports.

Review views

1. From the Main menu, go to **Modules** > **Asset** > **Views** and check the **Status** of the views. If all the views are enabled, no troubleshooting is necessary.
2. For any custom views that have disabled or missing attributes (columns), click Edit, correct the view configuration as necessary, and click **Submit**.

Automate monthly maintenance

1. Review playbook run logs to ensure Tanium™ Automate playbook runs are running successfully and targeting the intended endpoints. For more information, see Tanium Automate User Guide: View playbook run.
2. Review playbook runs to ensure there are no runs that are waiting for manual steps. For more information, see Tanium Automate User Guide: View playbook run.
3. To optimize performance, review playbook runs and playbook run logs to ensure playbooks are not running excessively. For more information, see Tanium Automate User Guide: View playbook run.
4. Ensure that any Tanium solutions used by Automate in your environment are running and updated. For more information, see Tanium Automate User Guide: Solution dependencies.
5. Delete temporary and obsolete playbooks. For more information, see Tanium Automate User Guide: Delete a playbook.
6. Review which users have access to playbooks. For more information, see Tanium Automate User Guide: Set up Automate users.

Benchmark monthly maintenance

1. From the Main menu, go to **Modules** > **Benchmark** > **Metric Health**.

©2026 Tanium Inc. All Rights Reserved

2. Review whether you are getting data for each Tanium™ Benchmark metric. For more information, see Tanium Benchmark User Guide: Monitor and troubleshoot Benchmark metric health.

Certificate Manager monthly maintenance

About this task

Identify and resolve errors that might prevent Tanium™ Certificate Manager from completing certificate audits.

1. From the Main menu, go to **Modules** > **Certificate Manager** > **Overview**.
2. In the **Overview** section, review the **Certificate Manager Endpoint Coverage** panel for endpoints with the **Needs Attention** status.
3. To investigate issues, see Tanium Certificate Manager User Guide: Monitor and troubleshoot Certificate Manager Coverage.
4. To troubleshoot other Certificate Manager issues, see Tanium Certificate Manager User Guide: Troubleshooting Certificate Manager.

Client monthly maintenance

Review and remediate Tanium Client health and Client Extension issues

About this task

Perform the following tasks to review the state of the Tanium Clients running on endpoints, as well as Client communication and registration with Tanium Servers and Zone Servers. If you observe Client issues that require resolution, see Troubleshooting Tanium Clients and Client Management.

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. Go to **Client Health** and click the **Deployment** tab to review the **Health Failures** panel. This panel shows failures associated with Tanium™ Client Extensions. Perform the remaining steps if you need to troubleshoot Client Extension issues.
3. Click Interact in the **Health Failures** panel to display the question results that provide the panel data.

©2026 Tanium Inc. All Rights Reserved

4. Retrieve any additional details from endpoints that you need to diagnose Client Extension issues. For more information, see Managing question results.
5. To resolve Client Extension failures, see the following sections:
    - To resolve Client Index Extension failures, see Reference: Common health check issues.
    - To resolve Client Recorder Extension failures, see Troubleshooting the Client Recorder Extension.
    - To resolve failures associated with Client Extensions for other Tanium solutions, see Troubleshoot solution-specific issues and Identify and resolve issues with endpoint tools or Client Extensions.

Review and adjust the distribution of Tanium Client registration traffic

About this task

Tanium Clients must register with a Tanium Server or Zone Server for the Client hosts to function as managed endpoints. As Clients and Client subnets are added to or removed from your network, you might have to update client-server connections to optimize registration traffic.

Each Tanium Client connects to only one Tanium Server or Zone Server at a time. However, to avoid a single point of failure, you can configure the **ServerNameList** setting with a list of servers to which the Client can attempt a connection.

> **Note:** For more information about client-server connections, see Configuring connections to the Tanium Core Platform.

To determine which servers are processing Client registrations and, if necessary, to rebalance registration traffic among them:

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. Go to **Client Health** and click the **Settings** tab.
3. Review the **ServerNameList** setting to determine whether Clients are connecting to the correct servers.
4. Review the **ServerName** setting to verify that Client connections are balanced among Zone Servers.

©2026 Tanium Inc. All Rights Reserved

5. Deploy actions with packages that reset the **ServerNameList** settings if necessary to connect Clients to different Servers. For more information, see Content for configuring connections to Tanium Core Platform Servers.
6. Add Zone Servers if necessary to rebalance Client registration traffic and then repeat step 5 to connect Clients to those Servers. For more information, see the procedure for your Tanium infrastructure:
    - Installing an Appliance Array: Review the tasks for adding Array members and assigning roles.
    - Installing the Tanium Zone Server

Review and update Tanium Client logging levels

About this task

Tanium Clients generate logs that can help you troubleshoot issues. Higher logging levels record more details about events on Clients but also consume more Client resources. The default logging level is `1`. Review Client logging levels and adjust them if necessary to ensure new endpoints that join your network have optimal logging levels.

Best Practice: Make sure to keep the logging level at `1` to minimize disk writes on Clients that run on sensitive endpoints, endpoints with limited resources, or virtual desktop infrastructure (VDI) endpoints.

Note: For more information about logging levels, see Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform.

For Tanium™ Client Containers, the default logging level is `10` and you cannot change it through actions. Contact Tanium Support on page 14 to change the logging level on Client Containers.

For more information about logs on Tanium Clients, see Troubleshooting Tanium Clients and Client Management.

1. From the Main menu, go to **Shared Services** > **Client Management**.

©2026 Tanium Inc. All Rights Reserved

2. Go to **Client Health** and click the **Settings** tab.
   If the logging level is set to a value other than the default `1` on any Clients, the **LogVerbosityLevel** setting displays the **Count** of Clients for each value. If all Clients have the default value, the page does not display the setting.

   Tip: To verify that the logging level is set to the best practice value of `1` for Clients on VDI endpoints, select **All Virtual Machines** in the **Computer Group** drop-down.

3. To update the logging level on Clients, see Managing Client settings and configurations in Client Management.

Review and update Tanium Client settings

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. Go to **Client Health** and click the **Settings** tab.
3. Verify that the setting values are correct and that the **Count** column indicates they apply to the expected number of Clients.
4. To update settings, see Managing Client settings and configurations in Client Management.

Review and upgrade Tanium Client versions

About this task

The best practice is to run the latest Tanium Client version on all endpoints, and to maintain a supported configuration, you must install at least the version of the Tanium Client that matches the endpoint toolset installed on an endpoint. However, you might occasionally have earlier Client versions installed to temporarily support legacy configurations. Endpoints might also run an earlier Client version if an upgrade process failed.



Note: For more information about Client versions, see Client version and host system requirements.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Enable Client upgrades in the change management feature in Endpoint Configuration to streamline Client upgrades and to more easily maintain a supported configuration. For more information, see Endpoint Configuration: Managing Tanium Client and endpoint tool upgrade rollouts.

Determine which endpoints are running a Client that is not at the latest version and decide whether to accept the earlier versions or upgrade the Clients:

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. Review the **Health** dashboard to see the **Client Version** panel.
3. If any endpoints are running an earlier Client version, click the **Client Version** title and then click Interact in the **Client Version** panel to display the question results that provide the panel data.
4. Retrieve any details from endpoints that you need to determine whether the versions are appropriate, or upgrades are required, or upgrades failed.
   For example, select a **Filter by Computer Group** option (such as **All Windows**) or update the question as needed. For information about retrieving additional details, see Managing question results.

   Tip: You can use the `Upgrade Ring` field in the `Endpoint Configuration - Change Management Status` sensor to filter endpoints according to the earliest upgrade ring with which they are associated. For example, ask the question: `Get OS Platform and Client Health - Tanium Client Version from all machines with Endpoint Configuration - Change Management Status:Upgrade Ring contains 4`.
5. Upgrade the Client on any endpoints that require the latest version. For more information, see Upgrading Tanium Clients.
6. Troubleshoot Client upgrade issues if necessary. For more information, see Troubleshooting Tanium Clients and Client Management.

Review and update Tanium Client subnets

Separated subnets, intentional subnets, and isolated subnets provide methods for modifying the

©2026 Tanium Inc. All Rights Reserved

default peering behavior of Tanium Clients. Default peering settings define the boundaries of Client subnets in the Tanium linear chain architecture. As subnets are added to or removed from your network, you might have to update the Client subnet configurations. For example, add isolated subnets for any new virtual private networks (VPNs).



Note: For more information about Client peering and subnets, see Configuring Tanium Client peering.

REVIEW AND UPDATE ISOLATED SUBNETS

About this task

Configure isolated subnets for Tanium Clients that are in VPNs. VPN Clients have local IP addresses in a special VPN address block, but their host endpoints are actually not close to each other. If VPN Clients are not isolated, they use WAN links for peering and latency is significantly greater than for client-to-server connections.

1. From the Main menu, go to **Administration** > **Configuration** > **Subnets** and review the **Isolated Subnets**. If necessary, consult your networking team to determine if the configurations require updates.
2. Update isolated subnet configurations if necessary. For more information, see Configure isolated subnets.

REVIEW AND UPDATE SEPARATED SUBNETS

About this task

Configure separated subnet configurations to apply more granular subnet boundaries for Tanium linear chains than the default boundaries.

1. From the Main menu, go to **Administration** > **Configuration** > **Subnets** and review the **Separated Subnets**. If necessary, consult your networking team to determine if the configurations require updates.
2. Update separated subnet configurations if necessary. For more information, see Configure separated subnets.

©2026 Tanium Inc. All Rights Reserved

REVIEW AND UPDATE INTENTIONAL SUBNETS

About this task

In a network configuration that uses network address translation (NAT), you might have to configure intentional subnets to ensure that Clients in the same subnet can peer with each other.

1. From the Main menu, go to **Administration** > **Configuration** > **Client Status**.
   The **Network Location (from Client)** values indicate which Clients are in the same subnet based on the **AddressMask** setting. For more information, see Address mask and prefix settings.

   The **Network Location (from Server)** column indicates the NAT IP addresses of Clients.

2. Select the endpoints that are in the same subnet but are not peering because their NAT IP addresses differ.
3. Click Export, set the **Format** to **List of Clients - CSV**, and click **Export**.
4. From the Main menu, go to **Administration** > **Configuration** > **Subnets** and compare the **Intentional Subnets** configurations to the exported list of Clients.
5. Update the intentional subnet configurations if necessary to enable peering among Clients in the same subnets. For more information, see Configure intentional subnets.

Comply monthly maintenance

1. From the Main menu, go to **Modules** > **Comply** > **Overview**.
2. Scroll to the **Health** dashboard to review any Tanium™ Comply health check errors on endpoints.
   The **Comply Health Checks** panel shows a bar graph with the number of affected endpoints for each type of error, such as outdated tools, scan failures, or insufficient disk space.
3. To investigate a health check error, click one of the error bars. The Tanium Server issues a question that returns the computer name, operating system, IP address, coverage status, and client extensions status for the affected endpoints.
4. To troubleshoot health check errors, see Tanium Comply User Guide: Reference: Common errors in Comply.

©2026 Tanium Inc. All Rights Reserved

Result

> **Note:** Review and update Comply assessments when you perform Comply quarterly maintenance on page 61.

Connect monthly maintenance

Review and remediate connection issues

1. Check for connection failures:
   - If you configured a failed connections report with automatic delivery, access the report at the specified destination. For more information, see Configure a failed connections report.

     > **Note:** If you do not have the authority to delete or disable connections that are no longer required, also configure delivery of the report to a team in your organization that has the authority.

   - To manually review connection failures, see Tanium Connect User Guide: View connection status.

     > **Tip:** If the list of connections is long, click the **Failed** toggle to show only failed connections.

2. Review connection throughput metrics to check for issues. For more information, see Tanium Connect User Guide: View connection metrics.
3. Troubleshoot connection issues if necessary. For more information, see Tanium Connect User Guide: Troubleshooting.
4. Edit connections if necessary to resolve failures. For more information, see Tanium Connect User Guide: Edit connections.
5. Delete or disable connections that are no longer required if you have the authority to perform those actions:
   a. From the Main menu, go to **Modules** > **Connect** > **Connections**.
   b. Select the connections that require an action and select **Actions** > **Disable** or **Actions**

©2026 Tanium Inc. All Rights Reserved

> **Delete**.

Review and remediate connection schedules

1. From the Connect menu, go to **Connections**.
   Perform the remaining steps for each connection.
2. Click the connection **Name** to show all its details.
3. Verify that the **Schedule** and **Next Run** show the expected values.
4. If you must change the schedule, click **Edit**, update the **Schedule** settings, and click **Save** or **Save and Run**.

Review and update connection owners

1. From the Connect menu, go to **Connections**.
   Perform the remaining steps for each connection.
2. Click the connection **Name** to show all its details.
3. Verify that the connection **Owner** (user account) and persona (**Run as Persona**) are still valid.

   Note: When you delete a user or persona, connections that the user or persona owns stops running. If this occurs, export and import the scheduled connection to create a new scheduled connection. For more information, see the following tasks in the Tanium Connect User Guide: Export connections and Import connections.

   a. Verify that the user account is active. For more information, see Tanium Console User Guide: View user settings.
   b. If an alternative persona runs the connection, verify that the persona still exists. For more information, see Tanium Console User Guide: View persona details.
   c. Verify that the owner has the role permissions that are required to run the connection:
      - If the default persona runs the connection, verify the user permissions. For more information, see Tanium Console User Guide: View effective role permissions for a user.
      - If an alternative persona runs the connection, verify the persona permissions. For more information, see Tanium Console User Guide: View

©2026 Tanium Inc. All Rights Reserved

effective role permissions for a persona.

4. Verify that the user password is compliant with the password rotation policy of your organization.

Review and remediate destination issues

1. From the Connect menu, go to **Connections**.
   Perform the remaining steps for each connection.
2. Click the connection **Name** to show all its details.
3. Verify that the **Destination** settings are correct.
4. If you must change the settings, click **Edit**, update the settings, and click **Save** or **Save and Run**.
5. Verify that the destination (such as a server) is available and running without issues.
6. Verify that the destination certificates are still valid.

Criticality monthly maintenance

About this task

To monitor and troubleshoot Tanium™ Criticality health issues, see Tanium Criticality User Guide: Troubleshooting Criticality.

Deploy monthly maintenance

Review and remediate Deploy coverage

1. From the Main menu, go to **Modules** > **Deploy** > **Overview**.
2. Go to the **Health** dashboard to verify that the Deploy process is running on all endpoints.
3. To investigate endpoints that are not running the process, click the number above **False** in the **Running Deploy** panel. The Tanium Server opens the **Deploy - Endpoint Deployment Process Running** report for the affected endpoints.
4. To investigate Deploy coverage issues, go to the **Summary** dashboard and click the number

©2026 Tanium Inc. All Rights Reserved

above **Needs Attention** in the **Deploy Coverage** panel. The Tanium Server opens the **Deploy - Coverage Status Details** report for the affected endpoints.

5. To troubleshoot issues related to the Deploy process or coverage, see Tanium Deploy User Guide: Troubleshoot Deploy Process Not Running.

Remove unused Deploy software packages

1. Go to **Modules** > **Deploy** > **Software**.
2. Review the **Software Packages** and delete unused packages.
   For example, delete software packages that are not the latest version or software that you are no longer using. For more information, see Tanium Deploy User Guide: Managing software.

Stop unneeded ongoing deployments

1. Go to **Modules** > **Deploy** > **Deployments** > **Active**.
2. Review the deployments and stop any deployments that are no longer needed.

Direct Connect monthly maintenance

About this task

To troubleshoot connection or screen sharing issues for Tanium™ Direct Connect, see Tanium Direct Connect User Guide: Troubleshooting Direct Connect.

Directory Query monthly maintenance

1. From the Main menu, go to **Shared Services** > **Directory Query**.
2. Review the **Domains** grid for errors. Hover over an Error icon to display a popup with the error message.
3. To troubleshoot errors, see Tanium™ Directory Query User Guide: Troubleshooting satellite configuration.

Discover monthly maintenance

©2026 Tanium Inc. All Rights Reserved

About this task

Perform monthly maintenance tasks to ensure that Discover successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Discover is not performing as expected, you might need to troubleshoot issues or change settings. For more information about how to view related procedures, see Tanium Discover User Guide: Troubleshooting Discover.

Review and remediate Discover resource usage on the Module Server

About this task

Review and remediate the Discover CPU and memory heap usage. High resource consumption might impact Discover performance.

1. From the Main menu, go to **Modules** > **Trends** > **Boards**.
2. Click the **Discover - Module Health** board and review the panels for resource usage issues.
3. For more information about how to troubleshoot resource usage issues, see Tanium Discover User Guide: Troubleshooting Discover.

Next steps

Note: Tanium Trends is deprecated and you can no longer create, import, or edit sources and boards. If **Discover - Module Health** does not appear on the **Boards** page, you cannot review resource usage in Trends. For more information, see Tanium Trends User Guide: Trends overview.

Review and update discovery methods

About this task

Review profile status and configuration to optimize discovery methods.

1. From the Main menu, go to **Modules** > **Discover** > **Profiles**.
   The **Profiles** page opens.
2. Review the **Status** of the profiles for warnings or errors. These conditions are the result of a profile mismatch between the Tanium Server and the Tanium Client.

©2026 Tanium Inc. All Rights Reserved

3. Contact Tanium Support on page 14 if necessary to resolve any warning or error conditions.
4. Review profile configurations to verify that their discovery methods are optimal. For example:
    - Verify that scanning excludes virtual private network (VPN) connections. Clients that connect over a VPN are typically isolated leaders that do not peer with each other. For more information, see Tanium Client Management User Guide: Verify or remediate Tanium Client peering and leader connections.
    - Review unmanaged endpoints to determine if they are eligible for the Tanium Client. For more information, see Tanium Discover User Guide: View interface data.
5. Troubleshoot discovery issues if necessary. For more information, see Tanium Discover User Guide: Troubleshooting Discover.
6. Edit profiles if necessary to resolve discovery issues: go to the **Profiles** page, click the profile **Name** and reconfigure the settings. For detailed steps, see:
    - Tanium Discover User Guide: Configure profile for distributed scan
    - Tanium Discover User Guide: Configure profile for satellite scan
7. Delete or disable profiles that are no longer useful.
    - **Delete profiles**: From the **Profiles** page, select the profiles and click **Delete Profile**.
    - **Disable profiles**: From the **Profiles** page, select the profiles and click **Disable Profile**. Alternatively, to disable a single profile, in the **Action** column of the profile that you want to disable, click Action and select **Disable Profile**.

Monitor and troubleshoot endpoints managed

About this task

The following table lists contributing factors into why the **Endpoints Managed (%)** metric might be lower than expected, and corrective actions you can make.

Factors that contribute to a lower-than-expected Endpoints Managed metric

Contributing factor	Corrective action
Installation Method Gap	• Use existing tools that are already part of the infrastructure. • Use standard tools (might only cover a subset of potential systems in your environment) such as:

©2026 Tanium Inc. All Rights Reserved

Contributing factor	Corrective action
	• SCCM - easy deployment mechanism (Windows only) • Group Policy - with the correct setting can deploy Tanium Client (Windows only) • Salt - a common tool used for installation of software in any environment (cross-platform) • Use a Tanium-provided installation method such as Tanium Client Management.
Credential Gaps	Use of any of the Tanium-provided installation methods involves using credentials to access the systems. Work with various management teams and deployment teams to understand what credentials are available to do installations on systems. Work with server or workstation support teams to understand these areas.
Network Gaps	Installing clients on "protected" networks such as DMZs or other sensitive areas is often a problem. These issues are technical, but the technical hurdles are generally an issue with policies and permissions. Work with the correct stakeholders to understand how Tanium will be used in the environment. Negotiate restrictions to be lessened to allow installation of Tanium Clients in these protected networks.

Monitor and troubleshoot mean time to manage

About this task

The following table lists contributing factors into why the **Mean Time to Managed** metric might be higher than expected, and corrective actions you can make.

Factors that contribute to a higher-than-expected Mean Time to Managed metric

Contributing factor	Corrective action
No automation	Tanium Maintenance can find clients, but with no action, a project can stall. Automating installation with Maintenance labels to target installation with Tanium Client Management is key. Take the human interaction out when possible, or build a workflow around Maintenance labels when items are found to feed into Tanium Connect and create help desk tickets or simple email lists.

©2026 Tanium Inc. All Rights Reserved

Contributing factor	Corrective action
Non-optimized Maintenance settings	• Adjust configuration settings. The key elements are how often to scan, and how often to import data. The Maintenance scans are built to be “low impact” on any network environment. Recommended scanning is once an hour in most environments. Scanning once an hour causes near zero impact and is fast enough to take action on unmanaged interfaces. Recommended importing is every thirty minutes and causes near zero impact to an environment. • Exclude scanning in parts of the network where you do not need scanning. To be successful in any enterprise, exceptions are always required. Maintenance has fine-grained control so you can exclude what you do not want to scan. For more information, see Knowledge Article: Getting Surgical with Endpoint Discovery: Using Targeting and Exclusions in Tanium Maintenance. • Select a discovery method that provides OS details. If installation requirements are governed by operating system (such as different teams are responsible for installation on different operating systems), selecting the right discovery method is key. Nmap with OS Fingerprinting (level 4 distributed scan) are required to effectively understand the operating system. Level 2 ping scans can provide OS in some but not all cases. • Use Maintenance Labels to make better sense of your environment, so you can bring items under management. Use the Tanium label gallery to import common labels to help determine manageability of existing interfaces. For more information, see Knowledge Article: Maintenance Labels - Common labels available for import. • Best practices • Tanium Community discussion: How do I configure Tanium Maintenance so that home networks are not scanned? • Tanium Community discussion: Visibility of discovered assets - Removing Devices from view • Tanium Community discussion: Visibility of discovered assets - Finding likely manageable resources • Tanium Community discussion: I see assets in my Tanium Maintenance data that are no longer online, how do I keep my Tanium Maintenance database clean?
Regional Ownership	Often various regions have different support structures in the larger enterprise. Understanding what systems belong to these regions is key to providing the guidance to the owning team they need to help install. Use locations to export or visualize data.

©2026 Tanium Inc. All Rights Reserved

Contributing factor	Corrective action
Understand your environment	Proper deployment sometimes requires understanding what is working and what is not working. With the data grids and graphs in Maintenance , you have a real-time view the environment. With a high level view over time, you can understand how deployments are working and cross-pollinate various ideas that work across a larger group. To get a high level view, use the Maintenance dashboards in Tanium Reporting. For more information, see Tanium Reporting .

Endpoint Configuration monthly maintenance

Review and remediate tools deployment

1. From the Main menu, go to **Shared Services** > **Endpoint Configuration**.
2. Review the deployment status of tools:
    a. Go to **Tools**. For more information, see Tanium™ Endpoint Configuration User Guide: View deployed endpoint tools.
    b. Go to **Content-Only Solutions**. For more information, see Tanium Endpoint Configuration User Guide: View the status of content-only solutions.
3. To troubleshoot deployment issues for tools, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or Client extensions.

Verify whether endpoints have the latest manifest

About this task

Verify that endpoints have the latest Endpoint Configuration *manifest*, which is a file that determines the versions of solution tools to install on endpoints. If endpoints do not have the latest manifest because of action locks or some other issue, the endpoints do not install the latest tools versions.

1. From the Main menu, go to **Shared Services** > **Endpoint Configuration**.
2. On the Endpoint Configuration **Overview** page, note the **Manifest Revision** (version) in the **Summary** section.
3. Go to the Tanium **Home** page and ask the following question:
   `Get Endpoint Configuration - Manifest Metadata?maxAge=60 and`

©2026 Tanium Inc. All Rights Reserved

```
Action Lock Status from all machines
```

> **Best Practice:** The manifest changes whenever a configuration or tool change occurs. Therefore, use the `maxage=60` option for the **Manifest Metadata** sensor to ensure that you retrieve the latest data from endpoints.

> **Tip:** Sort the **Question Results** grid by **Revision** to list the versions in descending numerical order, which makes it easier to identify endpoints with an earlier manifest version.

4. If the **Question Results** indicate **Action Lock Status** is on for some endpoints that do not have the latest manifest:
    a. Consult whoever turned on the action locks to verify that it is now safe to run actions on those endpoints.
    b. Perform one of the following tasks:
        - Disable action locks on the endpoints that require an updated manifest. For more information, see Tanium Console User Guide: Turn off action locks.
        - Configure Endpoint Configuration to ignore action locks for all endpoints. For more information, see Tanium Endpoint Configuration User Guide: Global Endpoint Configuration settings.
5. Update the manifest on page 42 on any endpoints that require an updated version.

Update the manifest

About this task

Windows and non-Windows endpoints require separate packages to update the manifest. Therefore, perform the following steps for each type of endpoint:

1. Go to the Tanium **Home** page and ask the following question:
   ```
   Get Endpoint Configuration - Manifest Metadata?maxAge=60 from all machines
   ```
2. Select the endpoints that have an outdated manifest and click **Deploy Action**.
3. Select the **Deployment Package** that matches the target endpoints:
    - Windows endpoints: **Endpoint Configuration - Manifest [Windows] (v.**

©2026 Tanium Inc. All Rights Reserved

<latest_manifest_version>)

- Non-windows endpoints: **Endpoint Configuration - Manifest [Non-Windows] (v. <latest_manifest_version>)**

4. Configure the remaining action settings and deploy the action. For more information, see Tanium Console User Guide: Deploying actions.
   If the manifest update fails, investigate environmental factors, such as security exclusions, file locks, CPU usage, RAM usage, and disk failures. Contact Tanium Support for additional help.

Endpoint Management for Mobile monthly maintenance

About this task

To monitor and troubleshoot Tanium™ Endpoint Management for Mobile issues, see Tanium Endpoint Management for Mobile User Guide: Troubleshooting Device Management.

Endpoint Management for Operational Technology monthly maintenance

About this task

To monitor and troubleshoot Tanium™ Endpoint Management for Operational Technology issues, see Tanium Endpoint Management for Operational Technology User Guide: Troubleshooting Endpoint Management for Operational Technology.

End-User Notifications monthly maintenance

1. From the Main menu, go to **Shared Services** > **End-User Notifications**.
2. Go to the **Health** dashboard to verify whether the latest Tanium™ End-User Notifications tools are installed and active on all endpoints.
3. To investigate endpoints that do not have the latest tools installed, click the number above **No** or **Unsupported**. The Tanium Server issues a question that returns the computer name, operating system, IP address, tools installation status, and installed tools version.
4. To troubleshoot installation issues for End-User Notifications tools, see Tanium End-User Notifications User Guide: Problem: End user notifications are not displayed..

©2026 Tanium Inc. All Rights Reserved

Enforce monthly maintenance

1. From the Main menu, go to **Modules** > **Enforce** > **Overview**.
2. Go to the **Health** dashboard and verify whether Tanium™ Enforce tools are installed and active on all endpoints.
3. To investigate endpoints that do not have Enforce tools installed, click the number above **Not Installed**. The Tanium Server issues the following question:
   `Get?forceComputerIdFlag=1 Endpoint Configuration - Tools Status?ignoreCase=0&maxAge=600 contains Enforce from all machines`
4. For more information about troubleshooting installation issues for Enforce tools, see Tanium Enforce User Guide: Monitor and troubleshoot Enforce coverage status (% of total).

Engage monthly maintenance

About this task

To monitor and troubleshoot Tanium™ Engage issues, see Tanium Engage User Guide: Troubleshooting Engage.

Gateway monthly maintenance

1. Verify that API tokens have not expired. For more information, see Tanium Console User Guide: View API token details.
2. Verify whether any API tokens are due for rotation based on the policy of your organization. For more information, see Tanium Console User Guide: Rotate an API token.
3. Revoke any API tokens that are no longer needed. For more information, see Tanium Console User Guide: Revoke API tokens.
4. Check for deprecated fields and, if necessary, update the integration scripts that use them. For more information, see Tanium™ Gateway User Guide: Reference: Deprecated fields.
5. To investigate and remediate Gateway issues, see Tanium Gateway User Guide: Troubleshooting Gateway.

©2026 Tanium Inc. All Rights Reserved

Guide monthly maintenance

About this task

To monitor and troubleshoot Tanium™ Guide health issues, see Tanium Guide User Guide: Troubleshooting Guide.

Health Check monthly maintenance

About this task

To monitor and troubleshoot Tanium™ Health Check issues, see Tanium Health Check User Guide: Troubleshooting Health Check.

Impact monthly maintenance

1. From the Main menu, go to **Modules** > **Trends** > **Boards**.
2. Click the Tanium™ **Impact** board and review the **Impact Coverage Status** panel for endpoints with the following status:
   - **Needs Attention**: Python tools that are required for Impact sensors are not installed.
   - **Unsupported**: Impact does not support the operating system.
3. To investigate endpoints that need attention, click the **Needs Attention** bar in the chart and select **View Current Endpoint Details filtered by Needs Attention**. The Tanium Server issues the following question:
   ```
   Get Computer Name and Operating System and IP Address and Impact - Coverage Status equals Needs Attention from all machines with Impact - Coverage Status equals Needs Attention
   ```
4. To investigate endpoints that do not support Impact, click the **Unsupported** bar in the chart and select **View Current Endpoint Details filtered by Unsupported**. The Tanium Server issues the following question:
   ```
   Get Computer Name and Operating System and IP Address and Impact - Coverage Status equals Unsupported from all machines with Impact - Coverage Status equals Unsupported
   ```

©2026 Tanium Inc. All Rights Reserved

Integrity Monitor monthly maintenance

1. From the Main menu, go to **Modules** > **Integrity Monitor** > **Overview**.
2. Scroll to the **Health** dashboard to review any health check errors.
3. To investigate issues with client extensions that appear in the panel, click **Health Check**. For specific troubleshooting steps, see Tanium™ Integrity Monitor User Guide: Identify and resolve issues with client extensions.
4. To see detailed health information about endpoints that are included in an error category, click the bar for that category in the chart. For specific troubleshooting steps, see Integrity Monitor User Guide: Reference: Endpoint monitoring health check errors.

Interact monthly maintenance

About this task

To troubleshoot Interact or Tanium Data Service (TDS) issues, see Tanium Interact User Guide: Troubleshooting Interact.

Investigate monthly maintenance

About this task

To troubleshoot Tanium™ Investigate issues, see Tanium Investigate User Guide: Troubleshooting Investigate.

Patch monthly maintenance

About this task

Review Tanium™ Patch coverage, scan configurations, deployments, and maintenance windows. Update the configurations if necessary.

©2026 Tanium Inc. All Rights Reserved

Note: Review and update custom action groups for Patch during Patch quarterly maintenance.

Review and update Patch block lists during as-needed maintenance.

Review and remediate Patch coverage

1. From the Main menu, go to **Modules** > **Patch** > **Overview**.
2. Go to the **Health** dashboard to verify that the Patch process is running on all endpoints.
3. To investigate endpoints that are not running the process, click the number above **No** or **Error** in the **Running Patch** panel. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Patch process status for the affected endpoints.
4. To investigate Patch coverage issues, click the number above **Needs Attention** in the **Patch Coverage** panel. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Patch coverage status details for the affected endpoints.

   Tip: You can also see this information in the predefined **Patch Coverage Status** report, which is available in the Tanium Reporting workbench.
5. To troubleshoot issues related to the Patch process or coverage, see Tanium Patch User Guide: Monitor and troubleshoot Patch coverage.

Review and update scan configurations

1. From the Main menu, go to **Modules** > **Patch > Scan Management**.
2. Review the **Scan Configurations** for each operating system (OS) to verify that they conform to the practices of your organization.
3. Select the **Tanium Scan for Windows** tab and click **Edit**.
4. Review the **Products to Include in Scan**, add any products that you want to include, and click **Submit**.
5. From the Main menu, go to **Modules** > **Patch** > **Overview**.

©2026 Tanium Inc. All Rights Reserved

6. Review the **Days Since Last Patch Scan** and **Scan Errors - Last 7 Days** panels for any errors. Click a panel name to see more details.
7. Troubleshoot scan errors if necessary. For more information, see Tanium Patch User Guide: Troubleshooting Patch.
8. Edit scan configurations if necessary to resolve errors. For more information, see Tanium Patch User Guide: Edit a scan configuration.
9. Delete scan configurations if any are no longer useful. For more information, see Tanium Patch User Guide: Delete a scan configuration.

Review and update deployments

1. From the Patch menu, go to **Deployments**.
2. Review the deployments to determine if any are misconfigured, no longer useful, or do not comply with the practices of your organization.
   For example, if the number of targeted endpoints is low relative to the number of deployments, you might be able to make the patching process more efficient by configuring fewer deployments to target more endpoints.
3. Check the deployment summaries for error messages. For more information, see Tanium Patch User Guide: Review deployment summary.
4. From the Main menu, go to **Modules** > **Trends** > **Boards** and click the **Patch** board.
5. Review the panels in the **Summary**, **Missing Patches**, and **SLA Based Compliance Reporting** sections for any errors. Click a panel name to see more details.
6. Troubleshoot deployments if necessary. For more information, see Tanium Patch User Guide: Troubleshooting.
7. Add targets to the deployments if necessary to resolve errors. For more information, see Tanium Patch User Guide: Add targets to an existing deployment.

   

   Note: For an existing deployment, you cannot perform edits other than adding targets.
8. Stop any deployments that are no longer useful. For more information, see Tanium Patch User Guide: Stop a deployment.

Review and update maintenance windows

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Patch > Deployments**.
2. Review the maintenance windows to determine if any are misconfigured or no longer useful. For example, maintenance windows that have end dates in the past are useful only as blocking maintenance windows. For more information, see Tanium Patch User Guide: Setting maintenance windows.

   Important: Deployments can run anytime if no maintenance windows are configured. If you imported Patch with default settings, it provides predefined maintenance windows that are not enforced on any computer groups. For more information, see Tanium Patch User Guide: Configuring Patch.
3. From the Main menu, go to **Modules** > **Trends** > **Boards** and click the **Patch** board.
4. If the **Endpoints Missing Critical or Important Patches Released Over 30 Days Ago** panel shows a higher than expected number, check whether maintenance windows are a contributing factor. For more information, see Tanium Patch User Guide: Monitor and troubleshoot mean time to patch.
5. Edit maintenance windows if necessary to resolve issues. For more information, see Tanium Patch User Guide: Edit a maintenance window.
6. Remove any maintenance windows that are no longer useful. For more information, see Tanium Patch User Guide: Delete a maintenance window.

Performance monthly maintenance

1. From the Main menu, go to **Modules** > **Performance** to open the Tanium™ Performance **Overview** page.
2. Scroll to the **Health** dashboard to verify that Performance tools are installed on all endpoints and to review which profiles are applied to endpoints.
3. To investigate endpoints that do not have Performance tools installed, click the number above **Needs Attention** or **Unsupported** in the **Performance Coverage** panel. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Performance coverage status for the affected endpoints.

©2026 Tanium Inc. All Rights Reserved

> **Tip:** You can also issue the question `Get Performance - Configured from all machines` through the **Ask a Question** field in Interact and then drill down on results to investigate endpoints that have issues with Performance tools or configuration. For more information, see Managing question results.

4. To review the status, priority, and endpoint targeting of all profiles, click **Active Profiles**. For more information, see Managing profiles.
5. To review the entire configuration of a specific profile, click its name in the **Active Profiles** panel.
6. For more information about how to troubleshoot installation issues related to Performance tools or profiles, see Monitor and troubleshoot Performance coverage.

Provision monthly maintenance

1. From the Main menu, go to **Modules** > **Provision** > **Overview**.
2. In the **Health** dashboard, verify that the Tanium™ Provision service is running as expected on Provision endpoints.
3. If the **Health** dashboard indicates that the Provision service is not running on Provision endpoints:
    a. Click Provision Endpoints to see details about the service status and versions for all Provision endpoints.
    b. To see additional details about a particular endpoint, click Additional Data beside that endpoint.
4. To investigate deployment issues, see Tanium Provision User Guide: Monitor a deployment.
5. To troubleshoot other Provision issues, see Tanium Provision User Guide: Troubleshooting Provision.

Reporting monthly maintenance

About this task

To monitor and troubleshoot Tanium™ Reporting health issues, see Tanium Reporting User Guide: Troubleshooting Reporting.

©2026 Tanium Inc. All Rights Reserved

Reputation monthly maintenance

1. From the Main menu, go to **Modules** > **Trends** > **Boards**.
2. Click the Tanium™ **Reputation** board and review the panels for issues that need attention.
3. If the **Failed Outbound API Requests** panel displays failures, verify that the reputation providers are configured correctly. For more information, see Tanium Reputation User Guide: Configuring reputation sources.
4. If data shows up faster in the **Inbound Items** panel than in the **Outbound Items** panel and the **Outbound Processing Queue** panel is consistently high, configure the reputation providers to send fewer hashes by lowering the **Maximum Hashes Processed Per Day** value.
5. To troubleshoot other Reputation issues or collect logs for a support package, see Tanium Reputation User Guide: Troubleshooting Reputation.

Reveal monthly maintenance

1. From the Main menu, go to **Modules** > **Reveal** > **Overview**.
2. Go to the **Health** dashboard to review:
    - **Reveal Coverage**: To investigate endpoints that do not have Tanium™ Reveal tools installed, click the number above **Needs Attention**. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Reveal coverage (installation) status for the affected endpoints. For more information, see Tanium Reveal User Guide: Monitor and troubleshoot Reveal coverage.
    - **Endpoint Status**: To investigate endpoints that have issues related to Reveal operations, click **Attention Needed**. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Reveal tools status for the affected endpoints. For more information, see Tanium Reveal User Guide: Monitor and troubleshoot endpoints with unconfirmed sensitive data.

Threat Response monthly maintenance

1. From the Main menu, go to **Administration** > **Shared Services** > **Client Management**.
2. From the Client Management menu, select **Client Health** and click the **Deployment** tab.
3. Review the **Health Failures** panel for issues that relate to Tanium™ Threat Response

©2026 Tanium Inc. All Rights Reserved

domains:

- `dec` (Direct Connect)
- `index` (Tanium Index)
- `recorder` (Tanium Recorder)
- `stream` (Tanium™ Stream)
- `threatresponse` (Tanium™ Threat Response Client Extension)

4. Investigate health failures and review the status and configurations of endpoint tools for Threat Response, including:
   - Non-default configuration settings on clients
   - Tools versions
   - Client extension versions
   - (Windows only) Tanium™ Driver status and version
   - Berkeley Packet Filter (BPF) support

   For the specific steps, see Tanium Threat Response User Guide: Get Threat Response endpoint tools status and configurations.

5. From the Main menu, go to **Modules** > **Threat Response** > **Overview**.
6. Go to the **Metrics** panel and check the Threat Response **Coverage**.
7. If the **Coverage** is lower than expected, investigate and remediate coverage as described under Tanium Threat Response User Guide: Monitor and troubleshoot Threat Response coverage. If coverage issues might result from missing or misconfigured Threat Response profiles, click the **Coverage** value to open the **Profiles** page and review profile configurations. For more information about profile issues, see Tanium Threat Response User Guide: My device has no profile or the wrong profile.
8. To investigate and remediate other Threat Response issues, see the following sections in the Tanium Threat Response User Guide:
   - Troubleshooting Threat Response
   - Reference: Common health check issues

Trends monthly maintenance

About this task

©2026 Tanium Inc. All Rights Reserved

To troubleshoot Tanium™ Trends issues, see Tanium Trends User Guide: Troubleshooting Trends.

Zero Trust monthly maintenance

1. Verify that the credentials for your Identity and Access Management (IAM) provider are valid. For more information about changing credentials with Tanium™ Zero Trust, see Tanium Zero Trust User Guide: Configure IAM provider settings.
2. Review the audit logs to verify that Zero Trust is sending data to your provider. For more information, see Tanium Zero Trust User Guide: Review data sent to your IAM provider.
3. Review existing rules for outdated, unused, or overlapping rules. Delete obsolete rules as necessary. For more information, see Tanium Zero Trust User Guide: Managing rules.
4. Verify that any Connect jobs that send audit data are running and sending data. For more information, see Tanium Connect User Guide: Managing connections.

©2026 Tanium Inc. All Rights Reserved

Performing quarterly maintenance

Review and update backups and the disaster recovery plan

1. Verify that a backup of your Tanium deployment is stored in a safe location. Create the backup if it does not exist:
    - Tanium Appliance User Guide: Tanium Appliance redundancy, backup, and recovery
    - Tanium Core Platform User Guide for Windows Deployments: Back up the servers and database
2. Review the disaster recovery plan for all your Tanium Core Platform servers. Update the plan if necessary to accommodate changes to the deployment:
    - Tanium Appliance User Guide: Define a disaster recovery plan
    - Tanium Core Platform User Guide for Windows Deployments: Back up Tanium Core Platform servers and databases
3. Generate support bundles for all the Tanium solutions in your Tanium license every 90 days and store each set of bundles for 180 days. For the steps to generate a support bundle for a solution, see the corresponding user guide:
    - API Gateway
    - Asset
    - Client Management
    - Comply
    - Connect
    - Criticality
    - Deploy
    - Direct Connect
    - Discover
    - Endpoint Configuration
    - End-User Notifications
    - Enforce
    - Health Check
    - Impact

©2026 Tanium Inc. All Rights Reserved

- Integrity Monitor
- Interact
- Patch
- Performance
- Provision
- Reporting
- Reputation
- Reveal
- Threat Response
- Trends

Result

> **Note:** Test disaster recovery on page 67 during annual maintenance.

Verify the GRUB key backup (physical or virtual Appliance only)

About this task

You can use the GRUB key during the boot sequence to diagnose and recover from failure conditions. During recovery, you must provide the key to Tanium Support for a technician to extract the GRUB password.

1. Verify that a backup of the latest key resides in a safe location off the Appliance.

   > **Note:** A new backup is required whenever the key password is regenerated. For more information, see Change the GRUB key password.

2. Export the key and save it in a safe location if no backup exists or if the current backup is not the latest. For more information, see Export the GRUB key.

Review and update Console user accounts

About this task

Review user settings, and update them if necessary, to ensure that account configurations reflect personnel changes as users leave, join, or change roles in your organization:

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration** > **Permissions** > **Users**.
2. Review the following settings:

User settings to review

Setting	Details
Name	If the **Users** grid is missing accounts, the steps to add them depend on the type of identity store: • Remote: Work with your identity store administrator to verify that the accounts exist on the Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server and add the accounts if necessary. If the accounts already exist, verify that the LDAP/AD server connection and synchronization settings are correct. For more information, see Tanium Console User Guide: Configure an LDAP server. • Local (Tanium Server): For more information, see Tanium Console User Guide: Create a user. If the **Users** grid lists accounts for users who are no longer active, see Tanium Console User Guide: Delete, un-delete, or lock out a user .
Locked Out	If the **Users** grid indicates that certain accounts are locked out, see Tanium Console User Guide: Locked-out users .
Last Sign In	If the **Users** grid indicates that certain users have not signed in for a long time, verify that their accounts are still required. For example, a user administrator might have created accounts only for temporary testing, or users might have left your organization. If any accounts are no longer required, see Tanium Console User Guide: Delete, un-delete, or lock out a user .
RBAC assignments and authentication	Verify that the appropriate computer groups, user groups, personas, and roles are assigned to user accounts and that they use the appropriate authentication services. For more information, see Review and update RBAC permissions and authentication settings on page 56 .

Result

Note: For more information about user accounts, see Tanium Console User Guide: Managing users.

Review and update RBAC permissions and authentication settings

About this task

©2026 Tanium Inc. All Rights Reserved

RBAC permissions control what individual Tanium Console and Tanium™ API users can see and do with the Tanium Core Platform, and which endpoints they can monitor and manage. The permissions derive from personas, roles, user groups, and computer groups that are assigned to user accounts. To ensure that users can access all the Tanium features they need but without access to sensitive information they do not need, review and, if necessary, update their permissions. Also review how users are configured to authenticate for Tanium Console and API access.

Note: If it is not feasible to review the RBAC permissions of every user on a quarterly basis, review a sample that is representative of the different types of users in your environment.

1. For each user, open the **Preview User** page and review the permissions. For more information, see Tanium Console User Guide: View effective role permissions for a user.
   The page lists all the permissions that are directly assigned to the user account through roles or that are inherited from user groups. The page also lists the personas and computer groups that are assigned to the account.

2. Create, edit, reassign, or delete RBAC configurations if necessary to update user permissions. For the steps, see the following sections in the Tanium Console User Guide:
   - Managing roles
   - Managing user groups
   - Managing personas
   - Managing computer groups

3. Verify whether any users can access Tanium Console through local authentication if your organization allows that.
   For more information and related tasks, see the following sections in the Tanium Console User Guide:

   - User authentication
   - Disable or enable local user access

   Best Practice: If you use an external service for authentication, maintain at least one user account that relies on local authentication and assign the **Administrator** reserved role to that account.

Review and update TanOS user accounts (Appliance only)

©2026 Tanium Inc. All Rights Reserved

1. On each Appliance, review the TanOS system users to ensure that they can access the Appliance operating system and that they have the appropriate authentication settings. For example, users who authenticate through passwords must comply with the password policy of your organization. For more information, see Configure security policy rules.
   The predefined roles for TanOS system users include:

   - `tanadmin`: Users with this role can access all TanOS console menus. It is useful to have more than one `tanadmin` user in case you forget the password for the initial `tanadmin` user that is created during Appliance setup.
   - `tancopy`: Users with this role can copy files to and from the /incoming and /outgoing directories on the Appliance.
   - `tanuser`: Users with this role can access only status menus in the TanOS console.

   For more information, see Managing users.

2. Verify that the predefined `tanremote` user account is present if you configured an Integrated Dell Remote Access Controller (iDRAC) interface on the physical Appliance. The account provides remote access to the iDRAC virtual console. This is useful for diagnosing hardware and network interface issues if the TanOS system becomes unavailable. For more information, see Manage the iDRAC interface.

Review and update site bandwidth throttles

About this task

Site bandwidth throttles are subnet-specific throttles that are more restrictive than the global throttles that apply to the rest of your network. Review the site throttles and, if necessary, update them. Disruptions to Tanium CloudTanium Core Platform functions might occur if they consume too much bandwidth or do not have enough bandwidth to perform operations at a reasonable speed.



Note: For more information, see Tanium Console User Guide: Site throttles.

1. Check the delays for site throttles to evaluate the current risk of disruptions to Tanium functions. For more information, see Tanium Console User Guide: Verify throttle delays.
2. Update the site throttles if necessary. For more information, see Tanium Console User Guide: Configure site throttles.

©2026 Tanium Inc. All Rights Reserved

Delete unnecessary computer groups

About this task

Users might create computer management groups and filter groups for time-limited activities that are no longer relevant. For example, a user might create a group for initial testing of a new feature after a Tanium solution update and then never use the group after testing finishes. In a Tanium deployment with numerous obsolete computer groups, users might struggle to identify the groups that are still relevant for ongoing activities, such as filtering questions and deploying actions.

Note: For more information about computer groups, see Tanium Console User Guide: Computer groups overview.

Review the existing computer groups and delete any that are no longer useful or that have memberships that duplicate other groups:

1. Review computer groups. For more information, see Tanium Console User Guide: View computer group details.
2. Delete computer groups. For more information, see Tanium Console User Guide: Delete computer groups.

Review and update scheduled actions

About this task

You can reduce resource use on Tanium Cloudthe Tanium Server and Tanium Clients by deleting actions that are no longer useful or that duplicate other actions.

CAUTION: Do not delete actions unless you understand the full impact.

Note: For more information, see Tanium Console User Guide: Managing scheduled actions and action history.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration** > **Actions** > **Scheduled Actions**.
2. Expand the **Filters** section and configure a filter based on an attribute that helps you determine whether actions are still useful. The following filters are examples:

   Filters to find actions that are still useful

Attribute	Operator	Value	Explanation
Status	is equal to	Disabled	Assess whether actions that are currently disabled might be enabled for future use. If a user disabled an action because it will never be useful, delete it.
Issuer	is equal to	<user name>	Knowing the action issuer (owner) can help you assess whether an action is still needed. The issuer can be: • taniumconsoleAdministrator (Windows) or tanium (Appliance): This is the account that Tanium solution services use to issue actions. For example, when you save a scan profile in Discover, the module automatically creates a corresponding scheduled action with Administrator as the issuer. **Note:** Scheduled actions that Tanium Cloudthe Tanium Server automatically imports through content-only solutions (such as **Core Content**) also have **taniumconsoleAdministrator** or **tanium** as the issuer. • Tanium solution: Tanium modules and shared services have solution-specific content that might include scheduled actions that the solution runs. For example, Tanium Endpoint Configuration is the issuer for the **Endpoint Configuration - Manifest** actions. To understand the purpose of these actions and the consequences of deleting them, see the user guides for the associated solutions. • Tanium user: Users might create scheduled actions for activities that are no longer relevant. For example, a user might create an action for initial testing of a new feature after a Tanium solution update and then never use the action again after testing finishes.

3. To disable actions that you want to stop deploying now but that you might deploy again in the future, select the actions and select **More** > **Disable Action(s)**.
4. To delete actions that are no longer useful, select the actions and select **More** > **Delete**.

©2026 Tanium Inc. All Rights Reserved

5. To troubleshoot actions, see Tanium Console User Guide: Monitor actions.

Comply quarterly maintenance

1. From the Main menu, go to **Modules** > **Comply > Assessments** and review the **Status** of assessments for errors or warnings. For more information, see Tanium Comply User Guide: Status definitions.
2. Investigate the error for each assessment.

   Tip: To issue a question that returns details about all the endpoints associated with scan errors, click the **Scan Errors** value above the grid.

   a. In the assessment row, click Additional Data, scroll to **Endpoint Statistics**, and click the **Scan Errors** value.
   b. Click the **Endpoints** value to issue a question that returns details about the affected endpoints. You can then review the results and, optionally, issue a drill-down question to investigate the errors. For more information, see Tanium Console User Guide: Managing question results.
3. Troubleshoot assessments if necessary to resolve issues related to endpoint compliance distribution. For more information, see Tanium Comply User Guide: Troubleshooting.
4. Edit assessments if necessary to resolve issues. For more information, see Tanium Comply User Guide: Edit an assessment.
5. Delete outdated assessments and create new assessments if updated versions of configuration compliance standards are released. For more information, see Tanium Comply User Guide: Creating compliance assessments.

   Note: Assessments that you delete on the **Assessments** page are removed from the Tanium Server but not from endpoints. Delete stale assessments from endpoints if retaining the associated data is no longer necessary. Otherwise, delete assessments from endpoints at intervals that preserve the data for a useful period without allowing the assessments to use too much disk space on endpoints. Base the intervals on how often users delete assessments from the server. For more information, see Tanium Comply User Guide: Delete stale assessments from endpoints.

©2026 Tanium Inc. All Rights Reserved

Deploy quarterly maintenance

About this task

If you install Deploy with default settings, it includes the **Tanium Deploy** action group, to which the **All Computers** computer group is assigned. If you changed computer group assignments for the **Tanium Deploy** action group, or if you created custom action groups for Deploy, review those action groups and, if necessary, update them. For example, if you discover that the Deploy tools are not installed on all the necessary endpoints, you might have to change the computer group assignments in the **Tanium Deploy** action group.

1. From the Main menu, go to **Administration** > **Actions** > **Action Groups**.
2. Use the filters to list only the groups that are for Deploy operations. For more information, see Tanium Console User Guide: View action groups.
   For example, if the custom action groups all have the string "Deploy" in their names, enter `Deploy` in the **Filter items** field.
3. Edit, create, or delete action groups if necessary to ensure Deploy targets the correct computer groups. For more information, see Tanium Console User Guide: Managing action groups.

Review Jump Gate policies

Review access policies

About this task

Regularly review the access policies that are in place to determine the available endpoints for jump requests, the users who can jump to those endpoints, and the approvals that are required:

1. From the Main menu, go to **Modules** > **Jump Gate** > **Access Policies**.
2. Click Expand ▶ for each policy to view the details as necessary, or click Expand All ▶ in the list header to expand all policies. For information about managing policies, see Tanium Jump Gate User Guide: Configure access policies.
3. Make sure that policies are arranged in the appropriate priority order. For information about prioritizing policies, see Tanium Jump Gate User Guide: Prioritize access policies.

©2026 Tanium Inc. All Rights Reserved

Review timeout and data retention policies

About this task

Regularly review the timeout and data retention settings that are configured to make sure they align with your organizational guidelines and policies:

1. From the Main menu, go to **Modules** > **Jump Gate**.
2. Click Settings .
3. On the **General** tab, review each setting to make sure it aligns with your organizational guidelines and policies, and make any necessary adjustments:

   #### Maintenance General settings

Setting	Description
Jump Request Expiration	Configure the amount of time after which a jump request expires. The time begins when a user submits a request and includes the time before the request is approved. After a request is approved, the requester can initiate unlimited new jump sessions before the approved request expires. After the request expires, the requester must submit a new request and receive new approval as applicable to open new session.
Maximum Request Scheduling Time	Configure the maximum amount of time in the future that a user can schedule a request.
Maximum Concurrent GUI Sessions	Configure the maximum number of GUI-based jump sessions, such as RDP sessions, that can run at the same time in Maintenance .
Session Inactivity Timeout	Configure the amount of time after which a user is disconnected from a jump session when the user has not performed any actions.
Maximum Session Time	Configure the amount of time after which a user is disconnected from a jump session even if the user is active.

©2026 Tanium Inc. All Rights Reserved

Setting	Description
	Note: • Jump sessions can be interrupted by Tanium Client resets, which typically occur every two to six hours and might occur before the configured maximum session time. For more information, see Troubleshooting disconnected jump sessions. • If the associated jump request expires during an active jump session, that session disconnects, even if it has not reached the maximum session time.
Maximum Command Time	Configure the amount of time that an asynchronous command issued by a user can run on an endpoint before it terminates.
Data Retention	Configure the amount of time to maintain records of Maintenance activity.

4. Click **Save**.

Patch quarterly maintenance

About this task

If you install Patch with default settings, it includes the **Patch** action group, to which the **Patch Supported Systems** computer group is assigned. If you changed computer group assignments for the **Patch** action group, or if you created custom action groups for Patch, review those action groups and, if necessary, update them. For example, if you discover that the Patch process is not starting on all the necessary endpoints, you might have to change the computer group assignments in the action group that is specified for **Patch - Start Patch Process** actions.

1. From the Main menu, go to **Administration** > **Actions** > **Action Groups**.
2. Use the filters to list only the groups that are for Patch operations. For more information, see Tanium Console User Guide: View action groups.
   For example, if the custom action groups all have the string "Patch" in their names, enter `Patch` in the **Filter items** field.
3. Edit, create, or delete action groups if necessary to ensure Patch targets the correct computer

©2026 Tanium Inc. All Rights Reserved

groups. For more information, see Tanium Console User Guide: Managing action groups.

©2026 Tanium Inc. All Rights Reserved

Performing semi-annual maintenance

Deploy semi-annual maintenance

About this task

Review Deploy self-service profiles and, if necessary, update them to ensure that users have access to all the self-service capabilities:

1. From the Main menu, go to **Modules** > **Deploy** > **Self Service Profiles** and review the profiles. Expand each profile and verify that all the operations are successful.
2. From the Deploy menu, go to **Deployments** > **Self Service** and review the **Failures** column.
3. Troubleshoot self-service installations if necessary to resolve issues. For more information, see Tanium Deploy User Guide: Monitor and troubleshoot software installed by self service user request.
4. Edit, create, or delete self-service profiles if necessary to resolve issues. For more information, see Tanium Deploy User Guide: Managing end-user self service.

©2026 Tanium Inc. All Rights Reserved

Performing annual maintenance

Test a planned failover

About this task

If you have an active-active Tanium Server deployment, fail over to your secondary Server and then fail back to verify that the process works as expected. The failover steps depend on your Tanium infrastructure:

- Appliance: Tanium Appliance User Guide: Testing a planned Tanium Server failover
- Windows: Contact Tanium Support on page 14

Test disaster recovery

About this task

Test restoring your Tanium deployment from a backup to verify that your disaster recovery plan works as expected. The restoration steps depend on your Tanium infrastructure:

- Appliance: Tanium Appliance User Guide: Tanium Appliance redundancy, backup, and recovery
- Windows: Contact Tanium Support on page 14

©2026 Tanium Inc. All Rights Reserved

Performing as-needed maintenance

About this task

The following sections describe tasks you must perform at intervals that vary based on conditions in your Tanium environment or based on the policies of your organization.

Rotate certificates for Tanium Console, Module Server, and API access

About this task

Transport Layer Security (TLS) certificates secure connections to the Tanium Server, Module Server, and Tanium solution services for Tanium user and solution operations. For example, the SOAPServer.crt certificate secures user access to the Tanium Server for Tanium Console or API activities. If your organization has a certificate rotation policy, replace the TLS certificates at the intervals that the policy specifies. For more information, see Tanium Console User Guide: Managing SSL/TLS certificates.

Patch as-needed maintenance

About this task

Review Patch block lists and, if necessary, update them:

1. Go to **Modules** > **Patch** > **Block Lists** and review the block lists.
2. Expand ▶ each block list that has one or more **Targets** (computer groups) and verify that the list is **Enforced**. If a list is **Unenforced** on endpoints or some endpoints have an **Old Version**, click the percentage (number) of affected endpoints to analyze the data in Interact.
3. Edit, create, or delete block lists if necessary to resolve issues. For more information, see Tanium Patch User Guide: Managing patches.

©2026 Tanium Inc. All Rights Reserved