This newsletter is sent to Tech Partner Program members and developer.tanium.com users. Thanks for being part of the Tanium Developer Community. If you no longer wish to receive these communications, you may unsubscribe at any time by choosing the unsubscribe option at the bottom of this newsletter.

Tanium API Updates
October 2026

~ Upcoming Events ~

Tanium Developer Summit is Back at Converge 2026!
Join us live in Las Vegas on Thursday, November 19th for exclusive sessions designed for the Tanium Builder Community.
[Register now → https://converge.tanium.com/2026/developer-summit]

~ What's New? ~

Tanium Atlas MCP Server

- **Bring Tanium's live endpoint data into your AI workflows!** Tanium Atlas MCP Server, a first-party Model Context Protocol (MCP) server, is now available for Tanium Cloud customers. An MCP-compatible AI assistant, such as Claude, ChatGPT, Microsoft Copilot Studio, or an internal LLM platform, can pull live Tanium endpoint data directly into a conversation. For example, you can check patch or vulnerability exposure, investigate an incident, or summarize affected devices without leaving the AI tool for a separate console. Access uses OAuth authentication, and every request is limited to the calling user's existing Tanium permissions, so nothing is exposed beyond what that user can already see. Learn more: Announcement · Quick Start Guide

Tanium Gateway GraphQL

- **Automate**
  - **Schedules and runs:** The following fields were added to describe playbook schedules, runs, and notifications.
    - PlaybookSchedule.disabledReason reports why a schedule was disabled, such as consecutive failures, an expired API token, or a user action, so integrations

can tell automatic disables from manual ones without reading event history. Values come from PlaybookScheduleEventType.
        - PlaybookRun.startType and **startDetails** show whether a run was started by a user or a schedule, and PlaybookRunFieldFilter can now filter runs by start type and schedule type.
        - PlaybookNotificationEvent.errorCode reports why an email notification failed.
    - **Ring deployments:** The following fields were added to support ring deployments.
        - Ring deployments can now send Tanium Guide notifications to chosen users for ring events, such as ring started, manual override, and deployment finished. Set notificationSettings when starting a ring deployment with the **PLATFORM_ACTION** action type, and read it from RingDeployment.notificationSettings.
        - New passWhenNoEndpointsEvaluated option on minimum-success-percentage progression criteria sets whether a ring with no applicable endpoints passes or fails. The default, **false**, keeps the current behavior of failing. Read the setting from ProgressionConditionMinimumSuccessPercentage.
    - **Task results:** The following fields were added to Automate task results.
        - Endpoint-execution task results (AutomateTaskResultEndpointPackageExecution, AutomateTaskResultEndpointRestart, and AutomateTaskResultEndpointConditionEvaluation) now include **skippedEndpoints**, the number of endpoints that did not run the task because endpoint-level execution stopped first.
        - AutomateTaskResultWait and AutomateTaskResultVerifyCondition now include **expectedCompletionTime**.

- Full Tanium Gateway Cloud Release Notes: https://help.tanium.com/bundle/z-kb-articles-mediawiki/page/6242.html#cloud_release_starting_on_august_27_2026edit
- Full On-Prem 2026H1 Release Notes: https://help.tanium.com/bundle/2026H1_releasenotes/page/overview.html
- On-Prem Maintenance Releases for Security and Bug Fixes: https://help.tanium.com/bundle/2026H1_releasenotes/page/maintenance.html#ariaid-title5

Tanium Scripting Language

- **Tanium Scripting Language (TSL) for custom sensors and packages is now available in Early Access.** TSL is a secure, high-performance, cross-platform scripting environment built by Tanium. It offers fast startup, read-only execution controls, and a simple syntax based on Python, and it works the same way on Windows, macOS, Linux, AIX, and Solaris. Tanium continues to support the existing runtimes for custom content (Python, Shell, and PowerShell), but all Tanium-managed content will move to TSL. Learn more: TSL Reference Guide

Tanium Connect

- The Cloud Storage destination can now export data to AWS S3, using an AWS S3 storage profile with the bucket name, region, and an access key that can read and write the bucket.
- Tanium Cloud can now export data to on-premises Socket (SIEM) destinations, such as Splunk, through satellites.

- Full Tanium Connect Cloud Release Notes: https://help.tanium.com/bundle/z-kb-articles-mediawiki/page/5330.html#cloud_release_starting_on_august_4_2026edit
- On-Prem Maintenance Releases for Security and Bug Fixes: https://help.tanium.com/bundle/2026H1_releasenotes/page/maintenance.html#ariaid-title5

Module APIs

- **Patch**
  - Automatic deployment configurations can now be managed through the API: create (POST /patch/v1/automatic-deployment-configurations), list (POST /patch/v1/automatic-deployment-configurations/get), update (PUT /patch/v1/automatic-deployment-configurations/{id}), delete (DELETE /patch/v1/automatic-deployment-configurations/{id}), and pause or resume (PUT /patch/v1/automatic-deployment-configurations/{id}/action). List automatic deployments with POST /patch/v1/automatic-deployments/get and trigger one with PUT /patch/v1/automatic-deployments/{id}/action.
  - Cursor pagination for GET /patch/v1/patches. Pass **take** on the first request, then send each response's **nextCursor** back as **cursor** to fetch the next page. Cursor requests are capped at **take=250**. Offset paging with **skip**/**take** still works.
  - Multi-organization (MSP) support. A global-organization caller can now create the following items within a sub-organization by passing the optional **Tanium-Organization-Id**header, and responses include **organizationId**: patch lists, block lists, deployments, deployment templates, automatic deployment configurations, maintenance windows, scan configurations, and scan configuration priorities.
- **Reputation**
  - The PATCH /v3/reputations/custom/{value} endpoint was added. It updates a custom reputation's note without resending the full object.
- **Threat Response**
  - **Alert prioritization:** The following endpoints were added to support prioritizing alerts. They rank where to look first by how many **distinct** intel documents matched, so one noisy detection firing repeatedly doesn't outrank an endpoint matched by many different detections. Every request takes **filter.alertStates** (for example **unresolved** and **inprogress**) and an optional **filter.alertedAtOrAfter** / **filter.alertedAtOrBefore** time window.
    - **Rank:** POST /v1/alert-priorities/endpoints/list, POST /v1/alert-priorities/process-instances/list, and POST /v1/alert-priorities/users/list rank endpoints, process runs, and user accounts.
    - **Drill down:** for one entry in a ranking, pass its **filter.key** to see the alerts and intel documents behind it:
      - Endpoints: POST /v1/alert-priorities/endpoints/alerts/list and POST /v1/alert-priorities/endpoints/intel-docs/list
      - Process runs: POST /v1/alert-priorities/process-instances/alerts/list and POST /v1/alert-priorities/process-instances/intel-docs/list
      - User accounts: POST /v1/alert-priorities/users/alerts/list and POST /v1/alert-priorities/users/intel-docs/list
  - Alerts now always carry process and user attribution, for example in GET /api/v1/alerts.

- **Alerts and reactions:** The following endpoints were added or updated to support alerts, reactions, and suppression rules.
  - The POST /api/v1/alerts/query endpoint was added. It takes the same filters, sorting, and pagination as **GET /api/v1/alerts**, plus **ids**, in a JSON body, and returns the same response. Use it when your filters are too long for a URL.
  - Suppression rules and reactions can now apply to all profiles or only to selected profiles. POST /api/v1/suppression-rules, PUT /api/v1/suppression-rules/{id}, POST /api/v1/reactions, and PUT /api/v1/reactions/{id} accept **scope** (**all_profiles**, the default, or **selected_profiles**) and **profileIds**. GET /api/v1/suppression-rules and GET /api/v1/reactions filter by **scope**, **profileId**, **orphaned**, and **includeAllProfiles**. GET /api/v1/alerts/{id} returns a **bucket** showing which reaction applied. Existing rules and reactions default to **all_profiles**, so current behavior doesn't change.
  - GET /api/v1/alerts/counts accepts **countDistinct=intelDocId**, which ranks each group by how many different intel documents matched instead of by alert volume. For example, **groupBy=computerName&countDistinct=intelDocId** ranks endpoints by how many different intel documents alerted on them.
  - GET /api/v1/reactions accepts **noLimit**, which returns every reaction in one response.
- **Response actions and intel documents:** The following endpoints were added or updated to support retrieving response actions and intel documents.
  - The GET /api/v1/response-actions/{id} endpoint was added. It returns one response action in the same shape as the list endpoint. It returns **404** if the ID doesn't exist, or if the action belongs to another user and you don't have the visibility-bypass privilege.
  - GET /api/v1/intels/{id} accepts **includeContents** (default **true**). Set it to **false** to get the document's metadata without its raw content, which is faster when you don't need the content.
- **Recorder, configuration and filters:** The following endpoints were added or updated to support recorder configuration and filters.
  - The GET /api/v1/configs/recorder/events endpoint was added. It lists the operating system security event types a recorder configuration can collect, which types are on by default, and the OS event codes each type covers. Each entry includes a stable key, a display name and a platform category (Windows Security, Linux Security, Mac Security). Use the keys to fill a recorder configuration's events array.
  - The GET /api/v1/filters/schema and POST /api/v1/filters/validate endpoints were added. Use the first to look up the syntax for recorder and high-priority-path filters, and the second to check a filter without saving it. An invalid filter returns **400** with a message that names the problem.
  - POST /api/v1/configs and PATCH /api/v1/configs/{id} accept optional **options.fileFiltersRegex** and **options.directoryFiltersRegex** on index configs, so you can limit which files are hashed. Existing configs are unchanged. A malformed pattern returns **400**.
  - GET /api/v2/stats reports what fraction of endpoints running the Threat Response client extension have a recorder profile applied (**data**, from 0 to 1). The response now also includes a **meta** section with the endpoint counts behind this figure, the time they were collected, and a state that explains a **null data** value.

- **Live Response and package management:** The following endpoints were updated to support Live Response and package management.
  - Azure Live Response destinations (POST /api/v1/liveresponse/destinations, PATCH /api/v1/liveresponse/destinations/{id}) accept an optional **options.host**, so files can go to an Azure Blob endpoint other than the default. Use a supported Azure Blob suffix for a host-style endpoint, or a non-Azure host for a path-style endpoint. A subdomain of an Azure suffix returns **400**. Existing destinations are unchanged.
  - GET /api/v1/quarantine/generatePackagesInfo and GET /api/v1/liveresponse/generatePackagesForInteractInfo now return a **deleted** list alongside **created** and **updated**. Deleted rules, profiles, destinations, collection configs, file collector sets, and script sets now count as unapplied changes.
- **Threat Navigator:** The following endpoint was updated to support Threat Navigator hypotheses.
  - PUT /v1/threat-navigator/hypotheses/list accepts optional **limit** and **offset** to support pagination. Requests without them behave as before and return up to 10,000 rows.

~ Changes and Fixes ~

API Ingress Infrastructure

- Known issue: on some Tanium Cloud instances, the **/oauth/authorize** redirect does not include the RFC 9207 **iss** parameter, although the server's OAuth metadata advertises it. MCP clients that enforce RFC 9207, such as Claude Code and MCP Inspector, reject the callback, and the authorization-code login fails. The **client_credentials** flow and API token authentication are not affected. A fix is rolling out to all instances in October.
- The API ingress now accepts many more concurrent client connections. Integrations that saw connection resets under heavy parallel load should no longer reach that limit.

Tanium Gateway GraphQL

- **Automate**
  - **BREAKING CHANGE** – When a ring step fails its progression criteria, the playbook run now emits a new INTERRUPT event and its status becomes **INTERRUPTED**instead of **PAUSED**. Integrations that monitor run status should handle the new values; resume the run with playbookRunPerformOperation using **RESUME**.

Module APIs

- **Comply**
  - The Comply API specification has been updated with many changes; unless otherwise noted, these changes do not alter the behavior of the API, but reflect improvements to how the OpenAPI specification is generated so that it accurately describes the API.

- Responses that include a user ID now also return the user's name and a deleted flag (for example, **createdByName** and **createdByDeleted**) for exceptions, settings, assessments, and report exports.
- **BREAKING CHANGE** – The Comply Report Reviewer role no longer includes the platform Read User privilege. Integrations that rely on this role to call platform user APIs, such as GET /api/v2/users, need Read User granted through another role.
- **BREAKING CHANGE** – GET /v1/results/aggregate is deprecated, and support ends October 2027. It returns empty compliance and vulnerability data. Use GET /v1/results/aggregate/{hash} for per-bundle compliance aggregates, or GET /v1/results/cached-aggregate/{hash} for per-report network unauthenticated scan aggregates, instead.
- Deprecated sensors: **Comply - CVE Findings** (including its Absolute First Found, First Found, Last Found, and Last Scan variants) and **Comply - Compliance Findings**(including its First Found and Last Scan variants). Use **Comply - Vulnerability Status** and **Comply - Compliance Status** instead.

- **Deploy**
  - **BREAKING CHANGE** – Creating or updating a maintenance window that does not use endpoint local time now requires a **tzOffset** value. The API returns a 400 error if it is omitted. Previously, such a window could be saved without an offset, which produced inconsistent or **null** timezone data. Windows that use endpoint local time are not affected. Affects POST /v1/maintenance-windows, POST /v2/maintenance-windows, PUT /v1/maintenance-windows/{id}, and PUT /v2/maintenance-windows/{id}.
  - Updating a software package or a software package bundle no longer resets optional fields that are omitted from the request to their default values. Omitted fields are now preserved, so existing data, such as a bundle's package list, is no longer cleared unintentionally. Integrations that relied on omitting a field to reset it must now send the default value explicitly. Affects PUT /v1/software-packages/{id}, PUT /v2/software-packages/{id}, PUT /v3/software-packages/{id}, PUT /v1/software-package-bundles/{id}, and PUT /v2/software-package-bundles/{id}.
  - **Deprecated endpoints:** The following endpoints are deprecated, and support ends September 2027.
    - **BREAKING CHANGE** – GET /v1/deployments, PUT /v1/deployments, GET /v1/deployments/{id}, and PUT /v1/deployments/{id} are deprecated. Use GET /v3/deployments, PUT /v2/deployments, GET /v2/deployments/{id}, and PUT /v2/deployments/{id} instead.
    - **BREAKING CHANGE** – POST /v1/maintenance-windows, PUT /v1/maintenance-windows/{id}, and DELETE /v1/maintenance-windows/{id} are deprecated. Use POST /v2/maintenance-windows, PUT /v2/maintenance-windows/{id}, and DELETE /v2/maintenance-windows/{id} instead.
    - **BREAKING CHANGE** – GET /v1/software-package-gallery, GET /v2/software-package-gallery, GET /v1/software-package-gallery/{id}, and GET

/v2/software-package-gallery/{id} are deprecated. Use GET /v3/software-package-gallery and GET /v3/software-package-gallery/{id} instead.

        - **BREAKING CHANGE** – GET /v1/software-packages, GET /v2/software-packages, GET /v3/software-packages, GET /v1/software-packages/{id}, GET /v2/software-packages/{id}, and GET /v3/software-packages/{id} are deprecated. Use GET /v4/software-packages and GET /v4/software-packages/{id} instead. PUT /v1/software-packages/{id} is deprecated. Use PUT /v3/software-packages/{id} instead.
- **Patch**
    - **BREAKING CHANGE** – Tanium-managed block lists, patch lists, and always-on maintenance windows now belong to the **Patch Service Objects** content set. If your integration uses a custom Patch role to call GET /patch/v1/blacklists, GET /patch/v1/patch-lists, or GET /patch/v1/maintenance-windows, add read permission on **Patch Service Objects** to that role to keep seeing these objects.
- **Platform**
    - **BREAKING CHANGE** – The Tanium Server now validates parameters on parameterized sensors, packages, questions, and actions. Requests with invalid parameter declarations or values, which were previously accepted, are now rejected. Affects POST /api/v2/sensors, PATCH /api/v2/sensors/{id}, PATCH /api/v2/sensors/by-name/{name}, POST /api/v2/packages, PATCH /api/v2/packages/{id}, PATCH /api/v2/packages/by-name/{name}, POST /api/v2/questions, POST /api/v2/actions, and POST /api/v2/saved_actions.
- **Reputation**
    - **Custom reputation upload and import:** The following custom reputation upload and import endpoints were changed.
        - **BREAKING CHANGE** – POST /v3/reputations/custom/upload now appends when **append** is omitted. Pass **append=false** to replace all custom reputations.
        - **BREAKING CHANGE** – Request bodies now have a size limit, and POST /v2/reputations/import and POST /v3/reputations/custom/upload accept fewer than 60,000 rows. Requests with 60,000 or more rows return **413**.
    - **Adding and deleting reputations:** The following endpoints that add or delete reputations were changed.
        - **BREAKING CHANGE** – POST /v3/reputations/whitelist, POST /v3/reputations/blacklist, and DELETE /v3/reputations/custom now return **status: "failed"** when nothing was written. Check for **failed**, not only **success**.
        - **BREAKING CHANGE** – DELETE /v2/reputations/{type} now deletes the hashes passed in **value**; previously it returned **204** without deleting anything. **value** is required.
    - **Settings and support information:** The following settings and support information endpoints were changed.

        - **BREAKING CHANGE** – PUT /v2/settings now returns **400** for zero, negative, or out-of-range values of **removeAfterDays**, **rescanDays**, **rescanNewMinutes**, **maxDbSizeGB**, and **maxDiskCapacity**.
        - **BREAKING CHANGE** – GET /v2/settings and PUT /v2/settings now require the **reputation settings read** and **reputation settings write** privileges instead of the provider-configuration privileges. Add them to roles that use these routes.
        - GET /v3/support/info no longer requires a privilege.
    - **Querying reputations:** The following reputation query and list endpoints were changed.
        - **BREAKING CHANGE** – The **reputation** and **customOnly** query parameters on GET /v2/reputations, GET /v3/reputations, and GET /v3/aggregate-reputations now return **400** for undocumented values, instead of an empty or incorrect result.
        - **BREAKING CHANGE** – Reputation list routes now accept **updatedAfter** as ISO 8601 or epoch milliseconds, honor **limit=0** and **offset=0**, and reject **lastId**combined with a custom **sortKey**. GET /v2/reputations/{type}/{value} no longer lets **search** override the hash in the path.
    - **Deprecated endpoints:** The following endpoints are deprecated.
        - **BREAKING CHANGE** – GET /v2/reputations is deprecated, and support ends September 2027. Use GET /v3/reputations instead.
        - **BREAKING CHANGE** – PUT /v3/reputations/custom is deprecated, and support ends October 2027. Use PATCH /v3/reputations/custom/{value} instead.
        - **BREAKING CHANGE** – GET /v2/configs/reversinglabs_a1000, PUT /v2/configs/reversinglabs_a1000, GET /v2/configs/reversinglabs_titaniumcloud, and PUT /v2/configs/reversinglabs_titaniumcloud are deprecated, and support ends October 2027. Use GET /v2/configs/reversinglabs-a1000, PUT /v2/configs/reversinglabs-a1000, GET /v2/configs/reversinglabs-titaniumcloud, and PUT /v2/configs/reversinglabs-titaniumcloud instead. They are identical except for the hyphenated path.
- **Threat Response**
    - **Reactions:** The following reaction endpoints were changed.
        - **BREAKING CHANGE** – DELETE /api/v1/reactions changed in three ways:
            - It returns **200** with **meta.deletedCount** instead of an empty **204**. If your code checks for **204**, update it.
            - Unknown request body fields now return **400** instead of being ignored.

        - It now applies the **filters** you send, so a filtered "select all" deletes only the matching reactions. Before, it deleted every reaction.
    - **BREAKING CHANGE** – PUT /api/v1/reactions/{id} returns **200** instead of **201**.
    - GET /api/v1/reactions now honors **includeIntelDocs=false**. Before, it was treated as **true**.
- **Alerts and intel status:** The following alert and intel status endpoints were changed.
    - **BREAKING CHANGE** – Bulk PUT /api/v1/alerts and DELETE /api/v1/alerts reject requests that use **selectionMode=exclude** with no **ids** and no filters. A single request can no longer change or delete every alert.
    - GET /api/v1/intel/status returns **200** with **data.ecfUnavailable: true** instead of **500** when the endpoint configuration service can't be reached.
- **Live Response:** The following Live Response endpoints were changed.
    - **BREAKING CHANGE** – POST /api/v1/liveresponse/destinations and PATCH /api/v1/liveresponse/destinations/{id} return **400** for values that break cloud naming rules:
        - Azure **storageAccount** and **container** must follow Azure naming rules.
        - S3 **bucket** must follow AWS bucket naming rules.
        - **region** may contain only lowercase letters, digits, and hyphens.
    - **BREAKING CHANGE** – DELETE /api/v1/liveresponse/scriptSets/{id} now returns **405** if a collection config still uses the script set. Before, the delete succeeded, and the script set silently disappeared from that collection config. Remove the script set from the collection config first.
- **Connections and labels:** The following connection and label endpoints were changed.
    - **BREAKING CHANGE** – POST /api/v1/conns/connect now requires **target.hostname** plus either **target.eid** or all three of **ip**, **clientId**, and **platform**. Invalid requests return a structured **400**. An integer **eid** is now accepted. Before, a connection opened with one never completed.
    - **BREAKING CHANGE** – PUT /api/v1/labels/{id} returns **400** if **name** is missing.
- **Configuration and suppression rules:** The following configuration and suppression rule endpoints were changed.
    - DELETE /api/v1/configs skips IDs that are already deleted instead of failing the whole request, so it's safe to retry. **meta.deletedCount** reports how many configs were actually removed.
    - POST /api/v1/suppression-rules/import/global with **writeToDb=false** no longer starts a real intel deployment, and it leaves **intelDeployment** out of the response. A dry run also reports **meta.droppedProfiles** for profiles it couldn't resolve.
- **Response actions, tasks and paging:** The following response action, task, and list endpoints were changed.

        - POST /api/v1/response-actions accepts a request that identifies the endpoint only by **computerName** again. From Threat Response 4.21.99 until this fix, those requests returned **400 "eid" is required**.
        - GET /api/v1/tasks returns **400** instead of **500** for a malformed **createdAtFrom** or **createdAtTo**.
        - List endpoints that page with an offset no longer repeat or skip rows when you sort by a field that isn't unique. Ties now break on the record ID. This covers filters, tasks, and evidence lists.

Connect

- **BREAKING CHANGE** – The Connect Operator role no longer includes the platform Read User permission; Connect now resolves connection owner names with its service account. Integrations that rely on this role to call platform user APIs, such as GET /api/v2/users, need Read User granted through another role.
- Comply findings exports now include a Data Cache Date column.
- Email (O365 & SMTP) connections now use STARTTLS on ports 25 and 2525, in addition to port 587.
- Email server profiles have a new **dod-graph.microsoft.us** host option for Microsoft 365 DoD tenants.
- The AWS S3 destination has a new option to set the multipart upload part size.
- The AWS S3 destination is deprecated. Existing connections continue to work; for new connections, use the Cloud Storage destination with an AWS S3 profile.

~ Deprecated Features ~

API Ingress Infrastructure

- The legacy API ingress infrastructure will be retired in 2027. If your Tanium Cloud instance still uses the legacy infrastructure, contact Tanium Support to move it to the newer infrastructure.

Module REST APIs

- Support will end for the following endpoints:
    - GET /plugin/products/asset/v1/settings/{name}
    - PUT /plugin/products/asset/v1/settings/{name}
    - POST /plugin/products/comply/v1/exports/{id}
    - POST /plugin/products/deploy/v2/tempfiles
    - PUT /plugin/products/comply/v1/custom-checks/{id}
- Support ends **October 2027** for the following endpoints:
    - GET /plugin/products/comply/v1/results/aggregate
    - GET /plugin/products/reputation/v2/configs/reversinglabs_a1000
    - PUT /plugin/products/reputation/v2/configs/reversinglabs_a1000
    - GET /plugin/products/reputation/v2/configs/reversinglabs_titaniumcloud
    - PUT /plugin/products/reputation/v2/configs/reversinglabs_titaniumcloud
    - PUT /plugin/products/reputation/v3/reputations/custom

- Support ends **September 2027** for the following endpoints:
  - GET /plugin/products/reputation/v2/reputations
  - PUT /plugin/products/deploy/v1/deployments
  - GET /plugin/products/deploy/v1/deployments
  - GET /plugin/products/deploy/v1/deployments/{id}
  - PUT /plugin/products/deploy/v1/deployments/{id}
  - POST /plugin/products/deploy/v1/maintenance-windows
  - PUT /plugin/products/deploy/v1/maintenance-windows/{id}
  - DELETE /plugin/products/deploy/v1/maintenance-windows/{id}
  - GET /plugin/products/deploy/v1/software-package-gallery
  - GET /plugin/products/deploy/v2/software-package-gallery
  - GET /plugin/products/deploy/v1/software-package-gallery/{id}
  - GET /plugin/products/deploy/v2/software-package-gallery/{id}
  - GET /plugin/products/deploy/v1/software-packages
  - GET /plugin/products/deploy/v2/software-packages
  - GET /plugin/products/deploy/v3/software-packages
  - GET /plugin/products/deploy/v1/software-packages/{id}
  - GET /plugin/products/deploy/v2/software-packages/{id}
  - GET /plugin/products/deploy/v3/software-packages/{id}
  - PUT /plugin/products/deploy/v1/software-packages/{id}

Tanium Gateway GraphQL

- Support ends **June 2027** for the following fields:
  - object.PlaybookStepOverride.stepId
- Support ends **May 2027** for the following fields:
  - object.DiscoverInterface.cloudInstances
  - object.DiscoverInterface.cloudTags
- Support ends **April 2027** for the following fields:
  - input.PlaybookStartInput.taskArgumentOverrides
  - input.PlaybookScheduleUpsertInput.taskArgumentOverrides
  - object.PlaybookSchedule.taskArgumentOverrides
  - object.PlaybookStepTaskArgumentOverride
  - query.playbookRuns.edges.node.steps.error
  - query.playbookRun.steps.error
  - query.playbookRuns.filter.isScheduled
- Support ends **March 2027** for the following fields:
  - query.playbookRun.steps.progress.details.actionID
  - query.playbookRuns.edges.node.steps.progress.details.actionID
- Support ends **February 2027** for the following fields:
  - object.PlaybookSchedule.nextRunTime
- Support ends **December 2026** for the following behaviors:
  - EndpointSourceTDS Input allowing namespaces and allNamespaces fields to be included together
- Support ends **December 2026** for the following fields:
  - query.playbookRun.steps.confirmationResult
  - query.playbookRun.steps.progress
  - query.playbookRuns.edges.node.steps.confirmationResult
  - query.playbookRuns.edges.node.steps.progress

- Support ends **November 2026** for the following fields:
  - mutation.playbookUpsert.playbook.canRun
  - mutation.playbookStart.playbookRun.playbook.canRun
  - query.playbookRuns.edges.node.canRun
  - query.playbooks.edges.node.canRun
  - query.playbookSchedules.edges.node.playbook.canRun
  - mutation.playbookStart.playbookRun.steps.playbookStep.currentUserMissingPermissions
  - mutation.playbookUpsert.playbook.runs.edges.node.steps.playbookStep.currentUserMissingPermissions
  - query.playbookRuns.edges.node.steps.currentUserMissingPermissions
  - query.playbooks.edges.node.steps.currentUserMissingPermissions
  - query.playbookSchedules.edges.node.playbook.steps.currentUserMissingPermissions
- Tanium Gateway APIs Deprecation Reference: https://help.tanium.com/bundle/ug_gateway_cloud/page/gateway/deprecated.html
- Tanium Gateway Stability Index Changes: https://help.tanium.com/bundle/ug_gateway_cloud/page/gateway/stability_index.html
- Comply Deprecated Sensors Reference: https://help.tanium.com/bundle/ug_comply_cloud/page/comply/deprecated_sensors.html

©2026 Tanium All rights reserved.
2100 Powell Street, Suite 1600, Emeryville, CA 94608
https://www.tanium.com | Unsubscribe | Manage Preferences