Tanium Asset User Guide

2026H2 Semiannual Release

Version 1.44

November 19, 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

Overview 13
- Sources 13
- Online and offline asset data aggregation 14
- Predefined reports 14
- Summary report 15
- Custom reports 15
- Views 16
- Profiles 16
- Software inventory and usage 16
- Data export 16
- Supported Languages 17
- Interoperability with other Tanium products 17
- REST APIs to manage assets 18

Gaining organizational effectiveness 20

Requirements 26
- Core platform dependencies 26
- Solution dependencies 26
  - Tanium recommended installation 27
  - Import specific solutions 27
  - Required dependencies 27
  - Feature-specific dependencies 27
- Client extensions and endpoint tools 28
- Tanium™ Module Server 28
  - Disk space 28
- Endpoints 29
  - Supported internet protocols 29
  - Supported operating systems 29
- Third-party software 30

©2026 Tanium Inc. All Rights Reserved

Host and network security requirements 31
Ports 31
Security exclusions 32
Asset endpoint exclusions 32
Third-party internet URLs 35
API access 39
User role requirements 39
Optional Asset roles for Guide observations 44

Installing 46
Before you begin 46
Import Asset 46
Manage solution dependencies 47
Upgrade Asset 47
Verify Asset version 47

Configuring 48
Default settings for Asset 48
Enable collection of Active Directory (AD) information 48
Install the Active Directory Query content-only solution 48
Set the targeting for the Tanium Core AD Query action group and create a scheduled action 49
Install and configure Tanium Endpoint Configuration 49
Manage solution configurations with Tanium Endpoint Configuration 49
Configure Asset 51
Configure the Asset action group 51
Import ServiceNow and Flexera content packs 52
Set up Asset users 52
Set user permissions on computers 54

Building reports 56
Work with existing reports 56
View reports 56
Customize columns 57
Filter reports 58
Filter items 58
Create report filters 59

©2026 Tanium Inc. All Rights Reserved

Create a report 60
Specify general report information 60
Select columns 61
Define default filter 62
Filter calculations 63
Finish report 63
Delete report 64
Purge assets 64

Configuring sources 65
Asset reconciliation 65
About the Tanium source 66
Configure the Tanium source 66
What to do next 68
Create an AWS source 68
Create an AWS Access Key and IAM role 68
Create the AWS source 69
Create a Microsoft Azure source 71
Create a Microsoft Azure client ID and secret 71
Create the Microsoft Azure source 71
Create a database source 73
Create a Google Chromebook source 76
Create a Google Cloud service account to use for authentication 76
Create the Google Chromebook source 76
Create a Google Cloud source 78
Configure the Google Cloud source 79
Create the Google Cloud source 86
Create an Import API source 88
Create the Import API source 89
Create a Microsoft Intune source 90
Create a Microsoft Azure client ID and secret 90
Before you begin 96
Create the Microsoft Intune source 96
Monitor compute source import runs 98
Edit source 99
Disable sources 100

©2026 Tanium Inc. All Rights Reserved

Configuring profiles ... 101
Data collected by the file evidence profile ... 101
Create the file evidence profile ... 103
View file evidence data in Asset ... 104
Export file evidence data ... 105
Create an SBOM profile ... 105
View profile status ... 106
Edit a profile ... 107
Delete a profile ... 108

Configuring attributes ... 109
Asset solution content ... 109
View and edit default asset attributes ... 109
Normalized attributes ... 111
Configure additional Tanium entities and attributes ... 111
Important considerations for attributes ... 111
Add attributes ... 111
Configure external attributes ... 114
Configure custom entities ... 115
Virtual sensor creation ... 116
Schedule and run Asset data imports ... 117
View schedule and run import ... 117
View status of imports and exports ... 118
Set user permissions on computers ... 118
Delete attributes ... 120
Asset data types ... 121

Configuring views ... 123
Create custom views ... 123
Specify view details ... 123
Select columns ... 124
Define filter ... 124
Filter calculations ... 125
Finish and test the view ... 126
Create a ServiceNow view ... 126
Create Flexera views ... 127

©2026 Tanium Inc. All Rights Reserved

Export data from views 127

Monitoring software inventory and usage 129
Enable tracking in Asset 130
View software inventory and usage 131
View product inventory and general usage 131
View last used date of a product 134
View usage levels of a product 134
View installed version of product 135
Manage products based on product usage 135
Remove unused products from endpoints 135
Install required products on endpoints 136

Exporting data 138
CSV file 138
Tanium Connect 138
Requirements 138
Create a connection 139
Asset Reports 139
Asset Computers 139
Compatibility 141
Filtering No Results and Errors 141
Examples 142
Example: Enhanced JSON 142
Example: Flattened JSON 142
Flexera 142
Flexera One 143
Before you begin 143
Flexera One IT Visibility 143
Flexera One IT Asset Management 143
Flexera FlexNet Manager Suite: 2019 R2.2 or later 144
FlexNet Manager Suite requirements 144
Tanium requirements 144
Before you begin 145
Integration instructions 145
Flexera FlexNet Manager Suite: 2019 R1 or earlier 145

©2026 Tanium Inc. All Rights Reserved

Requirements 146
Configure Flexera staging database 146
Add Flexera destination 146
Configure Flexera to receive data from Tanium Asset 149
ServiceNow: Tanium Asset integration 149
Requirements 150
Prepare ServiceNow to receive Tanium data 150
Add tables and Update Identification Rules 153
Configure ServiceNow export settings 153
Add ServiceNow as a destination 154
Exclude computers from exported ServiceNow data 155
Edit ServiceNow export mappings 156
Run export 156
Check data in ServiceNow 157
Configure least privilege access in ServiceNow 157
ServiceNow: Service Graph Connector 157

Creating a Software Bill of Materials 159
Overview 159
Requirements 159
Required dependencies 159
Required RBAC permissions 160
Endpoints 160
Supported operating systems 160
Disk space requirements 161
Supported ecosystems 161
Install SBOM 162
Work with SBOM profiles 162
View SBOM results 162
View SBOM results in Asset 162
View SBOM results in Interact 163
Track libraries and vendors 163
Manage tracked components 164
Disable a tracked component 164
Enable a tracked component 165

©2026 Tanium Inc. All Rights Reserved

Stop tracking a component 165
View library details 166
View reports for tracked components 166
Create reports for unlisted libraries 167
Create a report to show all SBOM package details 167
Add the required attributes 167
Create the report 168
Create a report to show SBOM package details for a specific component 169
Add the required attributes 169
Create the report 170
Export SBOM data 170
SBOM Sensors 170

Integrating with Microsoft Azure Migrate 172
Overview 172
Before you begin 172
Step 1. Create a Microsoft Azure account and configure required permissions 173
Step 2. Create a Microsoft Azure Migrate project 173
Step 3: Create an app registration, Microsoft Azure client ID, and secret 174
Register an application 175
Add a client secret 176
Step 4: Grant the necessary permissions to the service principal for the registered app 177
Step 5: Enable assessments in Asset 177
Enable the assessments feature 177
Enable assessments in the Asset settings 178
Step 6: Confirm that the necessary URLs are allowed through your security software 178
Create an assessment in Asset 178
Work with assessments 181
Run an assessment 182
Edit an assessment 182
Open a completed assessment 182
Delete an assessment 183
Add Tanium data to a Microsoft Azure Migrate assessment 183
Prerequisites 184
Steps 184

©2026 Tanium Inc. All Rights Reserved

Viewing containers **188**
View container charts 188
View container images 189
View image SBOM 190
View image details 192
View endpoints that host clusters 193
View Kubernetes clusters 194
View running Kubernetes containers in the environment 196
View image run history 197

Maintaining **199**
Review Tanium source imports 199
Review the status of import and export jobs 199
Review reports 200
Review views 200
Monitor and troubleshoot key vendors with tracked products 200
Monitor and troubleshoot unused tracked software 201

Troubleshooting **202**
Collect logs 202
Update service log level 202
Configure report timeout period 203
Reset differential load 203
Troubleshoot reports 204
Troubleshoot asset data exports and imports 204
View status of imports and exports 204
View import and export logs 205
Disable imports and exports 206
Fix Error: MULTIPLE_DUPLICATE_RECORDS error message in ServiceNow log file 207
Fix missing information in export to ServiceNow with Tanium Asset integration 207
Fix duplicate entries in ServiceNow with Tanium Asset integration 208
Troubleshoot software inventory and usage monitoring 209
Troubleshoot Microsoft Azure assessments 209
Troubleshoot disabled attributes 210
Issue 210
Causes 210

©2026 Tanium Inc. All Rights Reserved

Solution 210
Back up and restore the Asset database 212
Remove unneeded data from the Asset database 213
Purge assets 213
Delete attributes 213
Configure data retention and vacuuming 214
Verify endpoint tools 216
Identify and resolve issues with Client Extensions 216
Review the Extensions log for an endpoint 219
Remove Asset tools from endpoints 219
Uninstall SBOM 221
Use saved questions to populate Asset database 221
Uninstall Asset 222
Contact Tanium Support 222

Reference: Cron syntax for Asset 223

Reference: ServiceNow mappings 224

Reference: Source field mapping options 230

Reference: Gateway examples for Asset 237
Asset query filter syntax 237
Get Asset products 240
Get endpoints based on Asset products 245
Update Asset endpoints based on source 246
Update Asset endpoints based on endpoint ID (EID) 250
Upsert (create or update by ID) Asset endpoint 252
Import assets 258

Reference: Export data through the Asset REST API 262

Reference: SBOM files and file types 272

©2026 Tanium Inc. All Rights Reserved

Asset overview

With Asset, get a complete and up-to-date view of your enterprise inventory. An *asset* is any endpoint that is managed by a Tanium Client, such as a computer, server, or virtual machine. The inventory is an aggregation of live asset data with the most recent data from offline assets.

You can build reports to show an overview of all assets, or you can drill down into specific endpoints or users.

Sources

Sources define where Asset gets data from. By default, Asset collects data from sensors registered with Tanium™ Data Service to populate information about endpoints in the Asset database.

You can augment Asset inventory data with data from an SQL Server database. By importing data that is typically not available on an endpoint into the Asset data store, you can enable filtering and reporting on information such as department, cost center, building, and location.

About Tanium Data Service

Tanium Data Service stores sensor results for endpoints when a question is issued. When you add an attribute in Asset, Tanium Data Service automatically registers the underlying sensor for collection. After the sensor is registered, Tanium Data Service queries all managed endpoints to collect the results of that sensor and stores the data. To keep the results current, Tanium Data Service periodically reissues questions that contain the registered sensors. Asset then periodically retrieves data from Tanium Data Service.

When Asset retrieves data from Tanium Data Service, Asset only retrieves updated endpoint data. If an endpoint has no changes, the data for that endpoint is not updated in Asset:

- For more information about Tanium Data Service, see Tanium Interact User Guide: Managing Tanium Data Service.
- For more information about how to add attributes into Asset, see Configuring attributes on page 109.

©2026 Tanium Inc. All Rights Reserved

Endpoint uniqueness

Asset uses keys to determine if an asset is unique. Asset keys mirror the endpoint identifiers (EIDs) that Tanium Data Service uses to target unique endpoints:

- When Tanium Data Service identifies a duplicate endpoint, Tanium Data Service removes the duplicate endpoint from its database.
- When Asset retrieves new data from Tanium Data Service, Tanium Data Service passes the EID of the duplicate endpoint to Asset. Asset then removes the EID from its database regardless of the Asset purge rules.
- Endpoints that you manually delete from Tanium Data Service still follow the Asset purge rules.

Online and offline asset data aggregation

Asset aggregates data from both online and offline assets into one complete reporting data set. This data is populated from sensors registered with Tanium Data Service. When you add an attribute in Asset, Tanium Data Service automatically registers the underlying sensor for collection. All endpoints that have answered Tanium Data Service queries are visible in Asset reports. You can configure how long to keep data for endpoints that have not responded to Tanium Data Service queries.

Predefined reports

Asset comes with a set of predefined reports to help you prepare for audit and inventory activities.

- Age of Assets
- Age of Assets for Lost Devices
- Age of Assets for New Devices
- All Adobe Software
- All Assets
- All Short-lived Assets

©2026 Tanium Inc. All Rights Reserved

- All Microsoft Software
- All Software
- All Users
- Physical Machine Summary
- Platform Summary
- SIU Endpoints
- SIU Installed Products
- SIU Product Last Used
- SIU Product Usage
- Tanium Support
- Virtual Machine Summary

Summary report

Summary reports group data by attributes that you select and display a count of matching endpoints.

You can drill down on the endpoint count and see a filtered list of computer details, which includes the software and hardware information about the asset.

If the report contains the computer name or user name attributes, you can also drill down for further details, such as operating system and hardware information.

Custom reports

You can build custom reports that are based on any existing report. You can also create your own reports from data collected by Asset. You can create custom reports to show assets by department, location, user group, or other attributes.

©2026 Tanium Inc. All Rights Reserved

Views

You can build an alternative perspective of the Asset data with views. Views specify available attributes and can filter the included data. You can export data from a view to Tanium™ Connect.

Profiles

Configure profiles to identify files and file types on the endpoint. Currently, you can define a profile to collect data for file evidence and you can define profiles to collect data for Software Bill of Materials (SBOM). For more information, see Configuring profiles on page 101.

Software inventory and usage

You can monitor software inventory and usage on endpoints. Enable reporting for a product to view the data in Asset.

SIU stores data in Tanium Data Service (TDS). TDS is a shared service that periodically collects and caches sensor results from endpoints. For more information about Tanium Data Service, see Tanium Interact User Guide: Managing Tanium Data Service.

Data export

Tanium Connect

You can use any predefined reports, custom reports, or views as a connection source and send to destinations such as Email, File, HTTP, Socket Receiver, Splunk, and SQL Server.

Flexera

You can use the existing Tanium Client to populate information in Flexera FlexNet Manager Suite (FNMS).

ServiceNow CMDB

You can define the server, attribute mappings, and schedule for data to be exported to ServiceNow CMDB, ensuring that it has up-to-date information.

©2026 Tanium Inc. All Rights Reserved

Supported languages

You can select one of the languages in the following table for user interface (UI) text in the Asset workbench and Tanium documentation.

The language that you select for the workbench also sets the date and time format:

- Dates: In the table, the letters `dd`, `mm`, and `yyyy` represent the digits for day, month, and year respectively.
- Times: English (United States) times use the 12-hour clock in the format hh:mm:ss [AM|PM] <time zone>, where `hh`, `mm`, and `ss` represent the hour, minute, and second respectively. Other times use the 24-hour clock, where GMT-<#> indicates the offset from Greenwich Mean Time (GMT). For example, `GMT-7` indicates a time zone that is 7 hours ahead of GMT.

Supported languages with associated date and time formats

Language	Locale code	Date and time format
English (United States)	en-US	mm/dd/yyyy [AM|PM] <time zone>
French (France)	fr-FR	dd/mm/yyyy GMT- <#>
German (Germany)	de-DE	dd/mm/yyyy GMT- <#>
Japanese (Japan)	ja-JP	yyyy/mm/dd GMT- <#>
Korean (Korea, Republic of)	ko-KR	yyyy.mm.dd GMT- <#>
Spanish (Latin American)	es-LA	dd/mm/yyyy GMT- <#>

For information about language support, which types of text are translated, and the steps to select a language, see Tanium Console User Guide: Reference: Language support.

Interoperability with other Tanium products

Asset works with other Tanium products to provide additional features and reporting.

Tanium™ Cloud Workloads

When you view unmanaged Kubernetes clusters in Asset, the **Kubernetes Clusters** page contains a link to Cloud Workloads to manage clusters. For more information, see View Kubernetes clusters on page 194.

©2026 Tanium Inc. All Rights Reserved

Tanium™ Comply

When you view endpoints that host clusters in Asset, the **Endpoints Hosting Clusters** page includes a toggle to show endpoints with software vulnerabilities. For more information, see View endpoints that host clusters on page 193.

Tanium Connect

With Tanium Connect, you can send data to destinations, such as email, file, HTTP, Socket Receiver, Splunk, and SQL Server.

Tanium™ Guide

Tanium Guide can generate Asset-related notifications for Tanium operators, which provide insight into anomalous software.

For more information, see Tanium Guide User Guide: Overview.

Tanium™ Gateway

Use Gateway to access the Asset API. For more information, see Create an Import API source on page 88 and Reference: Gateway examples for Asset on page 237.

Tanium™ Reporting

- Asset includes Container charts on the **Asset Overview** page, which you can interact with to view the underlying data in a table format. For more information, see View container charts on page 188.
- Use Reporting to build a report with Tanium data, and then export the data to a Microsoft Azure Migrate project for assessment. For more information, see Add Tanium data to a Microsoft Azure Migrate assessment on page 183.

REST APIs to manage assets

You can use the REST APIs for Asset to manage assets, including viewing asset details in the Asset database, deleting an asset, and managing views.

©2026 Tanium Inc. All Rights Reserved

To view the Asset REST API documentation, from the **Asset Overview** page, click Help ?, and click **Asset API Documentation**.

©2026 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Asset

The four key organizational governance steps to maximizing the value that is delivered by Asset are as follows:

- Develop a dedicated change management process. For more information, see Change management on page 20.
- Define distinct roles and responsibilities. For more information, see RACI chart on page 21.
- Track operational maturity. For more information, see Operational metrics on page 23.
- Validate cross-functional alignment. For more information, see Organizational alignment on page 22.

Change management

Develop a tailored, dedicated change management process for asset management, taking into account the new capabilities provided by Tanium.

- Update SLAs and align activities to key resources for Tanium Asset activities across IT Security, IT Operations, and IT Risk / Compliance.
- Designate change or maintenance windows for various asset discovery scenarios. For example, set up Active Directory Query and integration with CMDBs such as ServiceNow or Flexera.
- Identify internal and external dependencies to your asset discovery process. For example, achieve effective integrations with the CMDB or Active Directory Query.
- Create a Tanium Steering Group (TSG) for asset management activities to expedite reviews and approvals of processes that align with SLAs.
- Determine frequency of reviews for changes and new information.

©2026 Tanium Inc. All Rights Reserved

- Consider conducting at least a quarterly review of change management process.

RACI chart

A RACI chart identifies the team or resource who is **R**esponsible, **A**ccountable, **C**onsulted, and **I**nformed, and serves as a guideline to describe the key activities across the security, risk/compliance, and operations teams. Every organization has specific business processes and IT organization demands. The following table represents Tanium's point of view for how organizations should align functional resources against asset management. Use the following table as a baseline example.

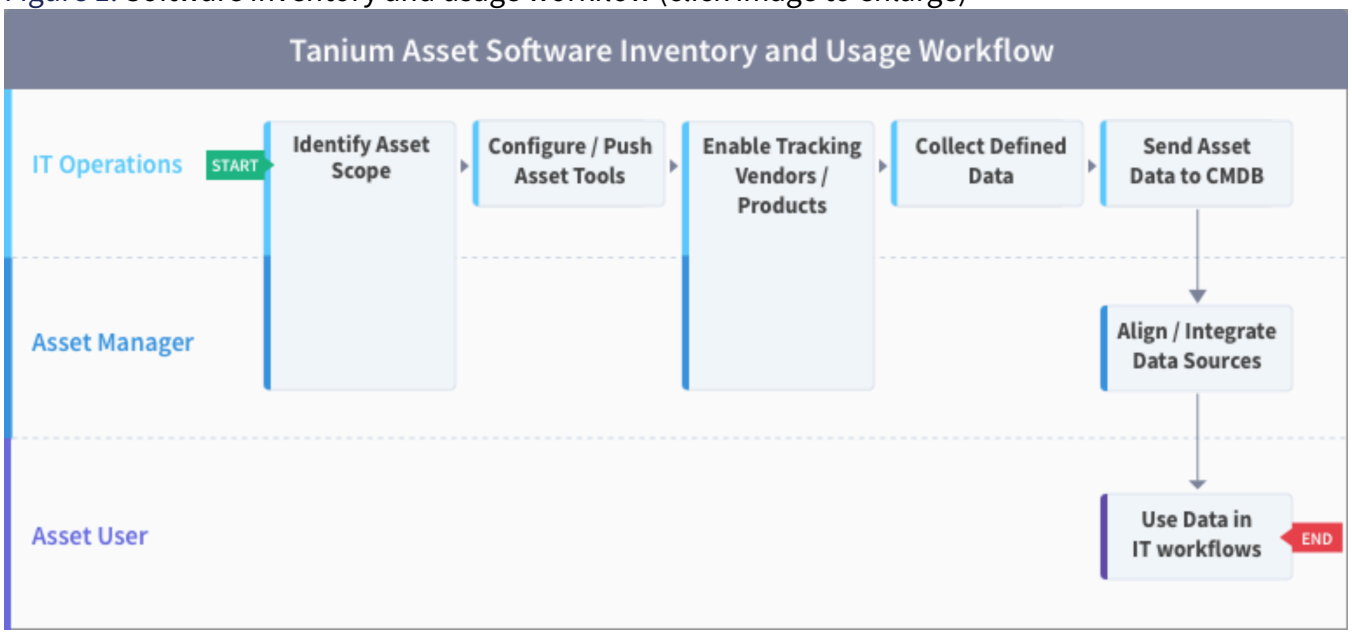
RACI chart for Tanium Asset

Task	IT Operations	Asset manager	Asset user	Rationale
Identify Asset scope	R	C	C	The Tanium platform owner must identify computers that are in scope for Asset . This scope is likely all computers, but a conversation should occur between the CMDB owners and the Tanium platform owners to fully understand scope across both tool sets.
Configure supporting tools	R	-	-	The Tanium platform owner rolls out the required Asset Tools (including Indexing capability) to the determined set of computers. The Tanium platform owner also must continually monitor tool deployment and upgrades.
Create Asset reports	R	R / C	R / C	The Tanium platform owner and business process owner end user must define the report requirements, then build those reports in Asset for viewing by business owners. The platform owner can configure role-based access control (RBAC) to allow users to view reports or to allow business owners to build read-only reports.
Asset RBAC management	R	C	I	The Tanium platform owner must plan and implement appropriate Role Based Access Controls to allow other business units to access and create reports and views.
Enable	C	R	C	If Software Inventory & Usage is configured, the platform owner can

©2026 Tanium Inc. All Rights Reserved

Task	IT Operations	Asset manager	Asset user	Rationale
tracking of products				enable the business owners to align to the identified vendors and products in Asset or the CMDB.
Collect defined data	I	I	I	Tanium Asset collects asset data based on defined requirements and configurations.

Figure 1. Software inventory and usage workflow (click image to enlarge)



Organizational alignment

Successful organizations use Tanium across functional silos as a common platform for high-fidelity endpoint data and unified endpoint management. Tanium provides a common data schema that enables security, operations, and risk/compliance teams to assure that they are acting on a common set of facts that are delivered by a unified platform.

In the absence of cross-functional alignment, functional silos often spend time and effort in litigating data quality instead of making decisions to manage software and hardware assets.

©2026 Tanium Inc. All Rights Reserved

Operational metrics

Asset maturity

Managing an asset management program successfully includes operationalization of the technology and measuring success through key benchmarking metrics. The key processes to measure and guide operational maturity of your Tanium Asset program are as follows:

Processes to measure Tanium Asset maturity

Process	Description
Usage	How and when Tanium Asset is used in your organization
Automation	How automated Tanium Asset is, across endpoints
Reporting	How data from Asset is consumed by people and systems within the organization

Benchmark metrics

In addition to the key asset processes, the key benchmark metrics that align to the operational maturity of the Tanium Asset program to achieve maximum value and success are as follows:

Benchmark metrics for Tanium Asset maturity

Executive Metrics	Key Vendors with Reported Products	Unused Reported Products
Description	The key vendors with reported products	The reported products that are not being used
Instrumentation	**Software Inventory & Usage > All Vendors**	**Software Inventory & Usage > All Products**
Why this metric matters	Key vendors with a cost associated with them that do not have any reported products are a detriment to the value provided by Asset , especially when it comes to software utilization. Cost-significant products should be reported.	The metric demonstrates the usage and effectiveness of software the company has determined is worth reporting on a per user level. Unused software licenses can be reclaimed.

©2026 Tanium Inc. All Rights Reserved

Use the following table to determine the maturity level for Tanium Asset in your organization.

Maturity levels for Tanium Asset

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	• Asset installed • Data retention policies and access established	• Primary user(s) identified on endpoints • Endpoint workflow gap analysis complete	Custom sensors created for use, and new attributes added from custom sensors	ServiceNow , Flexera, or other CMDB integrations are configured, providing enrichment and context to Asset endpoint data	• ServiceNow, Flexera, or other CMDB integrations are configured, providing enrichment and context to Asset endpoint data • All endpoint data flows through Asset, either through imports or exports
	Automation	Import schedule configured, assets are visible	• Integration with Active Directory. Active Directory Query content imported • Data retention rules enabled and aligned with IT policies	• Asset views created to export data • User group permission enabled and aligned with IT policies	• Sending additional attributes to CMDB (ServiceNow or Flexera) • Sending hardware, application, and primary user details to external partners through Connect or	• Sending additional attributes to CMDB (ServiceNow or Flexera) • Sending hardware, application, and primary user details to external partners through Connect or Asset REST APIs.

©2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
					Asset REST APIs.	
	Functional Integration	N/A	• Integration with Active Directory Query • Exporting data from report grid view	Evaluation of ServiceNow or Flexera CMDB for enrichment using Tanium Asset	CMDB enrichment value achieved	• Achieve custom Asset integration with third-party REST endpoint with Tanium Connect • Integration with Tanium Deploy to reclaim unused or underutilized licenses
	Reporting	Manual; Asset workbench and dashboard for Operators only	Manual; Asset reports using integration details	Automated; exporting scheduled reports to file / email / SQL; tracking top ten packaged or paid-for software products	Automated; CMDBs receiving data from Tanium Asset for reporting, including software usage	Automated; CMDBs receiving data from Tanium Asset for reporting, including any third-party products with the Tanium Asset API
Metrics	Key Vendors with Tracked Products	70%	80%	90%	95%	98%
	Unused Tracked Products	50%	40%	30%	20%	5%

©2026 Tanium Inc. All Rights Reserved

Asset requirements

Review the requirements before you use Asset.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Asset. For more information about how to get Asset, see Tanium Solutions & Bundles .
- Tanium™ Core Platform servers
- Tanium™ Client:

  Any supported version of Tanium Client. For more information, see Client version and host system requirements. If you use a Client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed Client versions.
- Tanium Content: (Optional) Asset includes all of the content it needs for base functionality. You can import additional content or sensors into Asset after installation.

Solution dependencies

Other Tanium solutions are required for Asset to function (required dependencies) or for specific Asset features to work (feature-specific dependencies). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.

Note: Some Asset dependencies have their own dependencies, which you can see in the lists of required and feature-specific dependencies below. Where a dependency links to its own user guide, that link opens the guide for the latest version of the solution, not necessarily the minimum version that Asset requires.

©2026 Tanium Inc. All Rights Reserved

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Asset, the Tanium Server automatically imports all your licensed solutions at the same time. For more information, see Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Asset to import, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are earlier than the minimum required for Asset, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Asset has the following required dependencies:

- Tanium™ Blob Service
- Tanium™ Core Content
- Tanium™ Data Service (TDS)
- Tanium™ Default Computer Groups
- Tanium™ Default Content
- Tanium™ Interact
- Tanium™ Endpoint Configuration
- Tanium™ RDB Service
- Tanium™ Secrets Service

Feature-specific dependencies

If you select only Asset to import, you must manually import or update its feature-specific dependencies regardless of the Tanium Console or Tanium Core Platform versions. Asset has the

©2026 Tanium Inc. All Rights Reserved

following feature-specific dependencies:

- Tanium Cloud Workloads is required to see container details. For more information, see Viewing containers on page 188.
- Tanium Connect is required to create connections with Asset reports as a data source.
- Tanium Reporting is required to create a report to export Tanium data to Microsoft Azure Migrate.
- Tanium Gateway is required to access the Asset database from third-party integrations. For more information, see API access on page 39.

Note: Asset 1.19.158 and later includes the Tanium™ Client Index Extension (Index CX) to support the SBOM add-in. Asset does not start the Index process on endpoints, but it might already be running on endpoints to support other Tanium solutions. For more information, see Overview on page 159.

Client extensions and endpoint tools

Tanium Endpoint Configuration installs Client Extensions and other tools for endpoints. Client extensions perform tasks that are common to certain Tanium solutions. Each Client Extension and tool might have recommended security exclusions to allow them to run without interference. For a list of all Client Extensions and tools, see Reference: Client extensions used for Tanium solutions.

Note: The change management feature of Endpoint Configuration might affect the version of each endpoint tool installed on endpoints.

Tanium™ Module Server

Asset runs as a service on the Tanium Module Server.

Disk space

Asset requires disk storage capacity that is necessary to support the number of endpoints in the

©2026 Tanium Inc. All Rights Reserved

environment. For planning purposes, use 100 MB per 1000 endpoints:

- 5,000 endpoints: 500 MB
- 50,000 endpoints: 5 GB
- 100,000 endpoints: 10 GB
- 250,000 endpoints: 25 GB
- 500,000 endpoints: consult your Technical Account Manager

Usage might vary significantly based on the following variables:

- Number of endpoints
- Number of applications
- Attributes that you add on the **Inventory Management** > **Attributes** page.

These suggested sizes are considered a good estimate for most environments.

Endpoints

Supported internet protocols

Asset communicates over IPv4 and IPv6 networks. For more information, see Tanium™ Client Management User Guide: Network connectivity, ports, and firewalls.

Supported operating systems

For more information about Tanium Client operating system support, see Tanium Client Management User Guide: Client version and operating system requirements.

For more information about Tanium Connector for Microsoft Intune support, see Tanium Integrations Gallery User Guide.

©2026 Tanium Inc. All Rights Reserved

Supported operating systems for Tanium Asset

Operating System	Version	Notes
Windows	• Windows 7 SP1 or later • Windows 2008 R2 SP1 or later	• Windows 7 SP1 requires Microsoft KB2758857. • Windows Server 2008 R2 SP1 requires Microsoft KB2758857. • Asset supports Windows 11 endpoints with Arm processors.
macOS	Same as Tanium Client support	
Linux	Same as Tanium Client support	Software Inventory & Usage is not available on Linux operating systems.
Solaris	Same as Tanium Client support	**Note:** Software Inventory & Usage and the Software Bill of Materials (SBOM) add-in are not available on Solaris operating systems.
AIX	7.1.4 or later	The IBM XL C++ runtime libraries file set (xlC.rte), version 16.1.0.0 or later, and the IBM LLVM runtime libraries file set (libc++.rte) must be installed. For more information, see Tanium Client Management User Guide: Deploy the Tanium Client to AIX endpoints using a package file . **Note:** Software Inventory & Usage and the Software Bill of Materials (SBOM) add-in are not available on AIX operating systems.

Third-party software

The following third-party software is optional:

©2026 Tanium Inc. All Rights Reserved

- For the ServiceNow CMDB connector to export data from Asset, the Jakarta release or later is required.
- For Flexera integration to export data from Asset, you must have an SQL database that can be configured to receive data from Asset. For more information, Contact Tanium Support on page 222.
- To use the **Asset Collect MS Exchange Info** package to collect Microsoft Exchange data, the Microsoft Exchange Server Computer objects need to be a member of the **View-Only Organization Management** group for **Microsoft Exchange Security Groups**.
- To ingest Microsoft Intune device data into Asset, configure a Microsoft Intune custom source to communicate with a Microsoft Intune instance. For more information about how to ingest Microsoft Intune device data, see Create a Microsoft Intune source on page 90.

Host and network security requirements

Specific ports and processes are needed to run Asset.

Ports

The following ports are required for Asset communication.

Ports for Tanium Asset communication

Source	Destination	Port	Protocol	Purpose
Module Server	ServiceNow	443	TCP	Access to your ServiceNow instance
ServiceNow MID Server	Tanium Server	443	TCP	If using the Service Graph Connector for Tanium Asset app, access to the Tanium Server
Module Server	Module Server (loopback)	17459 17461	TCP	Internal purposes; not externally accessible

©2026 Tanium Inc. All Rights Reserved

Best Practice: Configure firewall policies to open ports for Tanium traffic with TCP-based rules instead of application identity-based rules. For example, on a Palo Alto Networks firewall, configure the rules with service objects or service groups instead of application objects or application groups.

Security exclusions

If antivirus (AV) or other security software is in use in the environment to monitor and block unknown host system processes, Tanium requires that a security administrator create exclusions to allow the Tanium processes to run without interference. This software can include security applications that are included with an endpoint operating system, such as fapolicyd on some Linux distributions, or Microsoft Defender on Windows. The configuration of these exclusions varies depending on the security software.

For more information about security exclusions to define across Tanium, see Reference: Endpoint security exclusions. For Windows-based Tanium Core Platform deployments, see Tanium Core Platform Server security exclusions.

Note: If the required exclusions are not configured, or if Tanium suspects interference from AV or security software, Tanium might require you to remove or disable the AV or security software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.

Asset endpoint exclusions

Asset security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows	For integration with Flexera	Process	*<Tanium Client>* \Tools\EPI\TaniumEndpointIndex.exe
		File	*<Tanium Client>* \extensions\TaniumSoftwareManager.dll

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* \extensions\TaniumSoftwareManager.dll.sig
		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		File	<Tanium Client>\extensions\TaniumIndex.dll
		File	<Tanium Client>\extensions\TaniumIndex.dll.sig
		File	<Tanium Client>\extensions\index\index.db
		File	<Tanium Client>\extensions\index\index.db-shm
		File	<Tanium Client>\extensions\index\index.db-wal
		File	*<Tanium Client>* \extensions\SupportCX.dll
		File	*<Tanium Client>* \extensions\SupportCX.dll.sig
		File	*<Tanium Client>* \extensions\TaniumConfig.dll
		File	*<Tanium Client>* \extensions\TaniumConfig.dll.sig
macOS	For integration with Flexera	Process	*<Tanium Client>* /Tools/EPI/TaniumEndpointIndex
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.dylib
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.dylib.sig
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib
		File	*<Tanium Client>* /libTaniumClientExtensions.dylib.sig
		File	<Tanium Client>/extensions/libTaniumIndex.dylib

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	<Tanium Client>/extensions/libTaniumIndex.dylib.sig
		File	<Tanium Client>/extensions/index/index.db
		File	<Tanium Client>/extensions/index/index.db-shm
		File	<Tanium Client>/extensions/index/index.db-wal
		File	*<Tanium Client>* /extensions/libSupportCX.dylib
		File	*<Tanium Client>* /extensions/libSupportCX.dylib.sig
		File	*<Tanium Client>* /extensions/libTaniumConfig.dylib
		File	*<Tanium Client>* /extensions/libTaniumConfig.dylib.sig
Linux	For integration with Flexera	Process	*<Tanium Client>* /Tools/EPI/TaniumEndpointIndex
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.so
		File	*<Tanium Client>* /extensions/libTaniumSoftwareManager.so.sig
		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	<Tanium Client>/extensions/libTaniumIndex.so
		File	<Tanium Client>/extensions/libTaniumIndex.so.sig
		File	<Tanium Client>/extensions/index/index.db
		File	<Tanium Client>/extensions/index/index.db-shm
		File	<Tanium Client>/extensions/index/index.db-wal

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		File	*<Tanium Client>* /extensions/libSupportCX.so
		File	*<Tanium Client>* /extensions/libSupportCX.so.sig
		File	*<Tanium Client>* /extensions/libTaniumConfig.so
		File	*<Tanium Client>* /extensions/libTaniumConfig.so.sig

Third-party internet URLs

If security software is deployed in the environment to monitor and block unknown URLs, a security administrator might need to allow the following URLs on the Tanium Module Server for the Asset service.

- ServiceNow instance: (yourcompany.service-now.com)
- Microsoft Azure sources:
    - management.azure.com
    - login.microsoftonline.com
- Microsoft Intune sources:
    - graph.microsoft.com
    - login.microsoftonline.com
- Google Chromebook and Google Cloud sources:
    - https://googleapis.com
    - https://cloudresourcemanager.googleapis.com
    - https://compute.googleapis.com
-
    - organizations.us-east-1.amazonaws.com

©2026 Tanium Inc. All Rights Reserved

- sts.amazonaws.com
- ec2.eu-north-1.amazonaws.com
- ec2.ap-south-1.amazonaws.com
- ec2.eu-west-3.amazonaws.com
- ec2.eu-west-2.amazonaws.com
- ec2.eu-west-1.amazonaws.com
- ec2.ap-northeast-3.amazonaws.com
- ec2.me-south-1.amazonaws.com
- ec2.ap-northeast-2.amazonaws.com
- ec2.ap-northeast-1.amazonaws.com
- ec2.sa-east-1.amazonaws.com
- ec2.ca-central-1.amazonaws.com
- ec2.ap-east-1.amazonaws.com
- ec2.ap-southeast-1.amazonaws.com
- ec2.ap-southeast-2.amazonaws.com
- ec2.eu-central-1.amazonaws.com
- ec2.us-east-1.amazonaws.com
- ec2.us-east-2.amazonaws.com
- ec2.us-west-1.amazonaws.com
- ec2.us-west-2.amazonaws.com
- ssm.eu-north-1.amazonaws.com
- ssm.ap-south-1.amazonaws.com

©2026 Tanium Inc. All Rights Reserved

        - ssm.eu-west-3.amazonaws.com
        - ssm.eu-west-2.amazonaws.com
        - ssm.eu-west-1.amazonaws.com
        - ssm.ap-northeast-3.amazonaws.com
        - ssm.me-south-1.amazonaws.com
        - ssm.ap-northeast-2.amazonaws.com
        - ssm.ap-northeast-1.amazonaws.com
        - ssm.sa-east-1.amazonaws.com
        - ssm.ca-central-1.amazonaws.com
        - ssm.ap-east-1.amazonaws.com
        - ssm.ap-southeast-1.amazonaws.com
        - ssm.ap-southeast-2.amazonaws.com
        - ssm.eu-central-1.amazonaws.com
        - ssm.us-east-1.amazonaws.com
        - ssm.us-east-2.amazonaws.com
        - ssm.us-west-1.amazonaws.com
        - ssm.us-west-2.amazonaws.com
- AWS sources:
    - organizations.us-east-1.amazonaws.com
    - sts.amazonaws.com
    - ec2.eu-north-1.amazonaws.com
    - ec2.ap-south-1.amazonaws.com

©2026 Tanium Inc. All Rights Reserved

- ec2.eu-west-3.amazonaws.com
- ec2.eu-west-2.amazonaws.com
- ec2.eu-west-1.amazonaws.com
- ec2.ap-northeast-3.amazonaws.com
- ec2.me-south-1.amazonaws.com
- ec2.ap-northeast-2.amazonaws.com
- ec2.ap-northeast-1.amazonaws.com
- ec2.sa-east-1.amazonaws.com
- ec2.ca-central-1.amazonaws.com
- ec2.ap-east-1.amazonaws.com
- ec2.ap-southeast-1.amazonaws.com
- ec2.ap-southeast-2.amazonaws.com
- ec2.eu-central-1.amazonaws.com
- ec2.us-east-1.amazonaws.com
- ec2.us-east-2.amazonaws.com
- ec2.us-west-1.amazonaws.com
- ec2.us-west-2.amazonaws.com
- ssm.eu-north-1.amazonaws.com
- ssm.ap-south-1.amazonaws.com
- ssm.eu-west-3.amazonaws.com
- ssm.eu-west-2.amazonaws.com
- ssm.eu-west-1.amazonaws.com

©2026 Tanium Inc. All Rights Reserved

- ssm.ap-northeast-3.amazonaws.com
- ssm.me-south-1.amazonaws.com
- ssm.ap-northeast-2.amazonaws.com
- ssm.ap-northeast-1.amazonaws.com
- ssm.sa-east-1.amazonaws.com
- ssm.ca-central-1.amazonaws.com
- ssm.ap-east-1.amazonaws.com
- ssm.ap-southeast-1.amazonaws.com
- ssm.ap-southeast-2.amazonaws.com
- ssm.eu-central-1.amazonaws.com
- ssm.us-east-1.amazonaws.com
- ssm.us-east-2.amazonaws.com
- ssm.us-west-1.amazonaws.com
- ssm.us-west-2.amazonaws.com

API access

- To access the Asset database from third-party integrations, you must first create an API Token. For more information, see Tanium™ Console User Guide: Create API tokens.
- Your user account must have the **Asset Report Reader** role and the **Gateway User** role.

Use the following URL for Asset access:

<*taniumServerURL*>/plugin/products/asset

User role requirements

©2026 Tanium Inc. All Rights Reserved

Predefined roles grant the following permissions, which are required to use Asset functionality:

- Asset solution permissions
- Asset administration and platform content permissions: The solution permissions automatically provide some of these permissions.

For more information about predefined roles, see Set up Asset users on page 52.

Some Asset solution permissions provide permissions that are associated with other solutions. Furthermore, all the platform content permissions and some solution permissions apply to content sets that might contain content for other solutions in addition to Asset. If you create custom roles for Asset users, be sure to assign all the solution permissions and content set permissions that are required for Asset functionality. If you are not sure which permissions are required for a custom role, view the permissions of the predefined roles. For more information, see the following sections of the Tanium Console User Guide:

- RBAC overview (provides an overview of roles, permissions, and content sets)
- Provided role permissions
- View effective role permissions
- Configure a custom role

Note: Do not assign the **Asset Service Account** and **Asset Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

Asset solution permissions

Permission	Asset Administrator [1,2,3]	Asset Operator [1, 2, 3]	Asset User [1, 2, 3]	Asset Report Reader [1, 2, 3]	Asset API User	Asset Limited Report Reader [1, 2, 3]	Asset Endpoint Configuration Approver [1, 2, 3]
Asset View Asset workbench	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✗	✓ SHOW	✓ SHOW
Asset API	✗	✗	✗	✗	✓	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Asset Administrator [1,2,3]	Asset Operator [1, 2, 3]	Asset User [1, 2, 3]	Asset Report Reader [1, 2, 3]	Asset API User	Asset Limited Report Reader [1, 2, 3]	Asset Endpoint Configuration Approver [1, 2, 3]
User Read and write data through the API					READ WRITE		
Asset Configuration Item Configure all aspects of Asset (service settings, schedules, sources, attributes, destinations). This permission provides access to the **Software Inventory & Usage** pages.	✓ WRITE	✓ WRITE	✗	✗	✗	✗	✗
Asset Endpoint Configuration Approve Asset configuration changes in the Tanium™	✗	✗	✗	✗	✗	✗	✓ APPROVE

©2026 Tanium Inc. All Rights Reserved

Permission	Asset Administrator [1,2,3]	Asset Operator [1, 2, 3]	Asset User [1, 2, 3]	Asset Report Reader [1, 2, 3]	Asset API User	Asset Limited Report Reader [1, 2, 3]	Asset Endpoint Configuration Approver [1, 2, 3]
Endpoint Configuration service							
Asset Limited Report View and export read-only public reports	✗	✗	✗	✗	✗	✓ READ	
Asset Profile View, create, edit, and delete profiles	✓ USER	✓ USER	✗	✗	✗	✗	✗
Asset Report View, create, edit, and delete reports and views, view SBOM reports, and view the **Software Inventory & Usage** pages	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE [3]	✓ READ	✗	✗	✗
Asset Service Configure all	✓ CONFIGURE	✗	✗	✗	✗	✗	

©2026 Tanium Inc. All Rights Reserved

Permission	Asset Administrator [1,2,3]	Asset Operator [1, 2, 3]	Asset User [1, 2, 3]	Asset Report Reader [1, 2, 3]	Asset API User	Asset Limited Report Reader [1, 2, 3]	Asset Endpoint Configuration Approver [1, 2, 3]
aspects of Asset services							

[1] The permissions for this role provide solution permissions for other solutions. To view the provided permissions, see View effective role permissions .

[2] This role grants access to view only the **Reports** and **Views** pages.

[3] For owned reports and views only.

Asset administration and platform content permissions

Permission	Permission Type	Asset Administrator	Asset Operator	Asset User	Asset Report Reader	Asset API User	Asset Limited Report Reader	Asset Endpoint Configuration Approver
Action Group	Administration	READ WRITE	READ WRITE	READ	READ		READ	READ
Token - Use	Administration							
User Group	Administration	READ	READ					
Action	Platform Content	READ WRITE	READ WRITE					

©2026 Tanium Inc. All Rights Reserved

Permission	Permission Type	Asset Administrator	Asset Operator	Asset User	Asset Report Reader	Asset API User	Asset Limited Report Reader	Asset Endpoint Configuration Approver
Filter Group	Platform Content	READ	READ	READ	READ		READ	
Own Action	Platform Content	READ	READ					
Package	Platform Content	READ	READ					
Plugin	Platform Content	READ EXECUTE	READ EXECUTE	READ EXECUTE		READ EXECUTE		
Sensor	Platform Content	READ	READ	READ		READ		

To view the content sets to which the platform content permissions apply, see View effective role permissions .

Optional roles for Asset

Role	Enables
Connect Administrator (prior to Connect 4.8 only)	Create, edit, or delete a Flexera destination
Connect User (Connect 4.8 and later)	Create, edit, or delete a Flexera destination

Optional Asset roles for Guide observations

Optional Asset roles for Guide observations

Role	Enables
A custom role that includes the **Asset Report read** , **Asset Configuration Item write** , and **Token - Use** permissions	Access to Asset observations about anomalous software

©2026 Tanium Inc. All Rights Reserved

Role	Enables
	detection. For more information, see Detect anomalous software . For more information about custom roles, see Tanium Console User Guide: Configure a custom role .

©2026 Tanium Inc. All Rights Reserved

Installing Asset

About this task

Use the **Solutions** page to install Asset.

Asset is installed along with all other licensed solutions. After installation, the Tanium Server automatically configures the action group and import schedule for Asset. For more information about the automatic configuration for Asset, see Import Asset on page 46

Before you begin

- Read the .
- Review the Asset requirements on page 26.

Import Asset

When you import Asset, the following default settings are configured:

Default settings for Tanium Asset

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group For more information about how the action group relates to what actions Asset can take on particular endpoints, and how to change the action group, see Configure the Asset action group on page 51 .
Import schedule	The import schedule is set to start collecting data and generating reports.

For more information about how to import Asset and configure default settings, see Tanium Console User Guide: Import all modules and services. To verify that the correct version is installed after the import, see Verify Asset version on page 47.

©2026 Tanium Inc. All Rights Reserved

You can set the Asset action group to target the **No Computers** filter group by enabling restricted targeting before importing Asset. This option enables you to control Asset tools deployment through scheduled actions that are created during the import and that target the Asset tools action group. For example, you might want to test Asset tools on a subset of endpoints before deploying the Asset tools to all endpoints. In this case, you can manually deploy the Asset tools to an action group that you configured to target only the subset. To configure an action group, see Targeting actions through action groups. To enable or disable restricted targeting, see Tools deployment and restricted targeting.

Manage solution dependencies

About this task

Other Tanium solutions are required for Asset to function (required dependencies) or for specific Asset features to work (feature-specific dependencies). For more information, see Core platform dependencies on page 26.

Upgrade Asset

To upgrade Asset, see Tanium Console User Guide: Managing Tanium solutions. For more information about how to verify that the correct version is installed after the upgrade, see Verify Asset version on page 47.

Verify Asset version

About this task

After you import or upgrade Asset, verify that the correct version is installed:

1. Refresh your browser.
2. From the Main menu, go to **Modules** > **Asset** to open the Asset**Overview** page.
3. To show version information, click Info .

©2026 Tanium Inc. All Rights Reserved

Configuring Asset

If you did not install Asset with the **Apply All Tanium recommended configurations**, you must enable and configure certain features.

Default settings for Asset

When you import Asset, the following default settings are configured:

Default settings for Tanium Asset

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group For more information about how the action group relates to what actions Asset can take on particular endpoints, and how to change the action group, see Configure the Asset action group on page 51 .
Import schedule	The import schedule is set to start collecting data and generating reports.

Enable collection of Active Directory (AD) information

About this task

(Optional) To gather user data from Windows and domain-joined macOS endpoints, including Full Name, Email, Phone, Department, and Location, install the Core ADQuery Content solution and verify that the Core Content - AD Query action group targets the appropriate computer groups.

For macOS endpoints that are **not** domain-joined and Linux endpoints, you do not need to deploy any actions to get this information.

Install the Active Directory Query content-only solution

1. From the Main menu, go to **Administration** > **Solutions**.
2. In the **Content** section, select the **Core ADQuery Content** row and click **Import**.

©2026 Tanium Inc. All Rights Reserved

3. Review the list of packages and sensors and click **Begin Import**.

Set the targeting for the Tanium Core AD Query action group and create a scheduled action

About this task

To set the targeting for the Tanium Core AD Query action group and create a scheduled action to collect Active Directory Query information, complete the steps in the "Required Configuration Steps" and "Additional Core Content - AD Query Configuration" sections in this article: Configure Delivery of Endpoint Tools and Content.

The action gets recent sign ins and the primary user of each system. A primary user has the most interactive sign ins the past 30 days. You can access this information with the **Primary User Details** sensor or by adding the **User Name** column to a report.

For more information about how to view the status of content-only solutions in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: View the status of content-only solutions.

Install and configure Tanium Endpoint Configuration

About this task

Manage solution configurations with Tanium Endpoint Configuration

Tanium Endpoint Configuration delivers configuration information and required tools for Tanium Solutions to endpoints. Endpoint Configuration consolidates the configuration actions that traditionally accompany additional Tanium functionality and eliminates the potential for timing errors that occur between when a solution configuration is made and the time that configuration reaches an endpoint. Managing configuration in this way greatly reduces the time to install, configure, and use Tanium functionality, and improves the flexibility to target specific configurations to groups of endpoints.

Endpoint tools are bundled together in a versioned toolset. Each toolset contains a specific version of each tool. The Endpoint Configuration Toolset Solution provides upgrades to the toolset, and it imports upgraded versions of the entire toolset as needed by upgraded or newly installed solutions.

©2026 Tanium Inc. All Rights Reserved

Important:

When you upgrade Asset, the change management feature enables you to perform a staged rollout of the endpoint tools associated with the new version of Asset. Asset remains compatible with earlier versions of the endpoint tools and so continues to function with endpoints in rings that have not yet received the latest tools. However, any functionality added in the upgrade of Asset might not be available on these endpoints until they receive the upgraded tools.

In some cases, multiple solutions install the same endpoint tool, but upgraded endpoint tools remain compatible with all associated solutions. For example, both Tanium™ Threat Response and Tanium™ Reveal install and use index-cx. When you upgrade Threat Response, it might install version x.6.yyyy of index-cx, superseding version x.5.zzzz that Reveal previously installed. The index-cx upgrade from Threat Response does not affect the Index-related functionality of Reveal on the upgraded endpoints. For more information about the change management feature, see Tanium Endpoint Configuration User Guide: Managing endpoint tool upgrade rollouts.

Note: For information about how to install Endpoint Configuration, see Installing Endpoint Configuration.

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Asset, see User role requirements. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Managing approvals.

Important: For solutions to perform configuration changes or tool deployment through Endpoint Configuration on endpoints with action locks turned on, you must enable the **Manifest Package Ignore Action Lock** and **Deploy Client Configuration and Support Package Ignore Action Lock** settings. To access these settings, from the Endpoint Configuration **Overview** page, click Settings and select **Global**. For more information about action locks, see Managing action locks.

©2026 Tanium Inc. All Rights Reserved

For more information about Endpoint Configuration, see Tanium Endpoint Configuration User Guide.

Configure Asset

Configure the Asset action group

About this task

The action group determines on which endpoints the following Asset activities can be performed:

- Asset collection of software inventory and usage data
- Asset tool distribution
- Asset collection of Microsoft Exchange information

Importing the Asset module automatically creates an action group to target specific endpoints. If you did not use automatic configuration or you enabled restricted targeting when you imported Asset, the action group targets **No Computers**.

If restricted targeting was disabled when you imported Asset, the computer group target for the Tanium Asset action group targets **All Computers**, and configuring the Asset action group is optional.

Select the computer groups to include in the Asset action group.

Best Practice: Clear the selection for **No Computers** and make sure that all operating systems that are supported by Asset are included in the Asset action group.

Important: Asset inventory information is collected only for endpoints that are included in the Asset action group.

1. From the Main menu, go to **Administration** > **Actions** > **Action Groups**.
2. Click Tanium Asset.
3. Select the computer groups that you want to include in the action group and click **Save**. If you select multiple computer groups, choose an operator (AND or OR) to combine the

©2026 Tanium Inc. All Rights Reserved

groups.

Result

For more information about Flexera integration, see Flexera on page 142.

Import ServiceNow and Flexera content packs

About this task

By default, views and reports for Flexera and ServiceNow integrations are not imported for new Asset installations. You can choose to import one or both content packs.

1. From the Main menu, go to **Modules** > **Asset** > **Overview**.
2. From the **Asset Overview** page, click Settings .
3. From the **Content Packs** tab, click **Import Content** for the integrations that you want to use.

Tip: Content packs are automatically imported when you add corresponding views to Asset. For more information, see Create a ServiceNow view on page 126 or Create Flexera views on page 127.

Set up Asset users

You can use the following set of predefined user roles to set up Asset users.

For more information about how to review specific permissions for each role, see User role requirements on page 39.

For more information about how to assign user roles, see Tanium Core Platform User Guide: Manage role assignments for a user.

Asset Administrator

Assign the **Asset Administrator** role to users who manage all configuration and deployment of Asset functionality to endpoints. This role can perform the following tasks:

- Configure all Asset service settings

©2026 Tanium Inc. All Rights Reserved

- Manage the Tanium source and custom sources
- View, create, edit, and delete all reports and views
- Access the **Software Inventory & Usage** pages

Asset Operator

Assign the **Asset Operator** role to users who manage most configuration and deployment of Asset functionality to endpoints. This role can perform the following tasks:

- Configure some Asset settings, including data retention, report timeout, and permissions
- Manage the Tanium source and custom sources
- View, create, edit, and delete all reports and views
- Access the **Software Inventory & Usage** pages

Asset User

Assign the **Asset User** role to users who manage reports and views. This role can view, create, edit, and delete owned reports and views, and view the **Software Inventory & Usage** pages.

Asset Report Reader

Assign the **Asset Report Reader** role to users who view reports and views, and view the **Software Inventory & Usage** pages.

Asset API User

Assign the **Asset API User** role to a user who accesses the Asset API using Gateway.

Asset Limited Report Reader

Assign the **Asset Limited Report Reader** role to a user who views only public reports.

Asset Endpoint Configuration Approver

Assign the **Asset Endpoint Configuration Approver** role to a user who approves or rejects Asset configuration items in Tanium Endpoint Configuration. This role can approve, reject, or dismiss changes that target endpoints where Asset is installed.

©2026 Tanium Inc. All Rights Reserved

> **Note:** Do not assign the **Asset Service Account** and **Asset Service Account - All Content Sets** roles to users. These roles are used for internal purposes only.

Set user permissions on computers

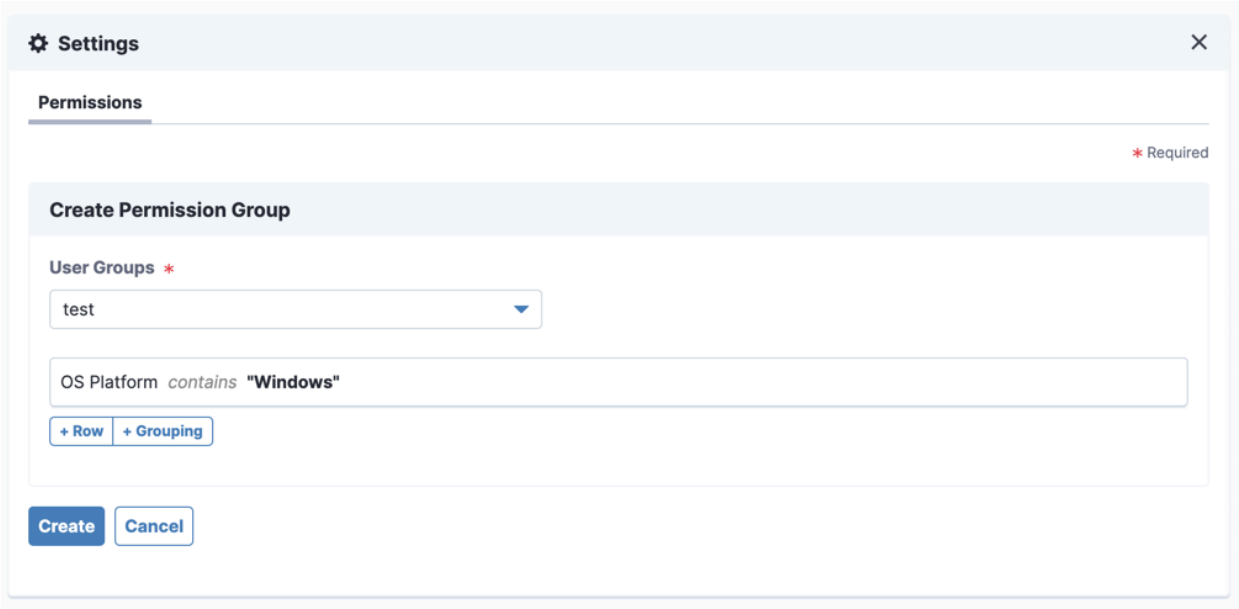
About this task

In addition to the Asset user roles that control access to Asset reports and settings as a whole, you can define more detailed permissions on computers that are based on individual attribute values. For example, you can create permissions that assign a user group permission to access information about only Windows or only macOS operating system assets. If a user belongs to multiple user groups that are granted permissions in Asset, all user groups that are assigned to the user must evaluate to true for the corresponding assets to be visible.

Before you begin, you must have a user group to which you want to assign the Asset permissions. For more information, see Tanium Core Platform User Guide: Managing user groups. For the users in this user group to access Asset, they also must have an Asset user role assigned. For more information, see User role requirements on page 26.

1. From the Asset **Overview** page, click Settings, and then click the **Permissions** tab.
2. Click **Create Permission**.
3. In the **User Groups** list, select the user group to which you want to assign Asset permissions.
4. Add a condition.
   This list of attributes is from the **ci_item** table of the Asset database. For example, to assign the selected user group permission to view only Windows assets, set the values to `OS Platform contains Windows`.

©2026 Tanium Inc. All Rights Reserved



5. Click Apply ✓ to create each condition.
6. Click **Create**.

©2026 Tanium Inc. All Rights Reserved

Building reports

You can build reports based on the existing built-in reports, or you can build your own reports from any sensor information that Tanium provides.

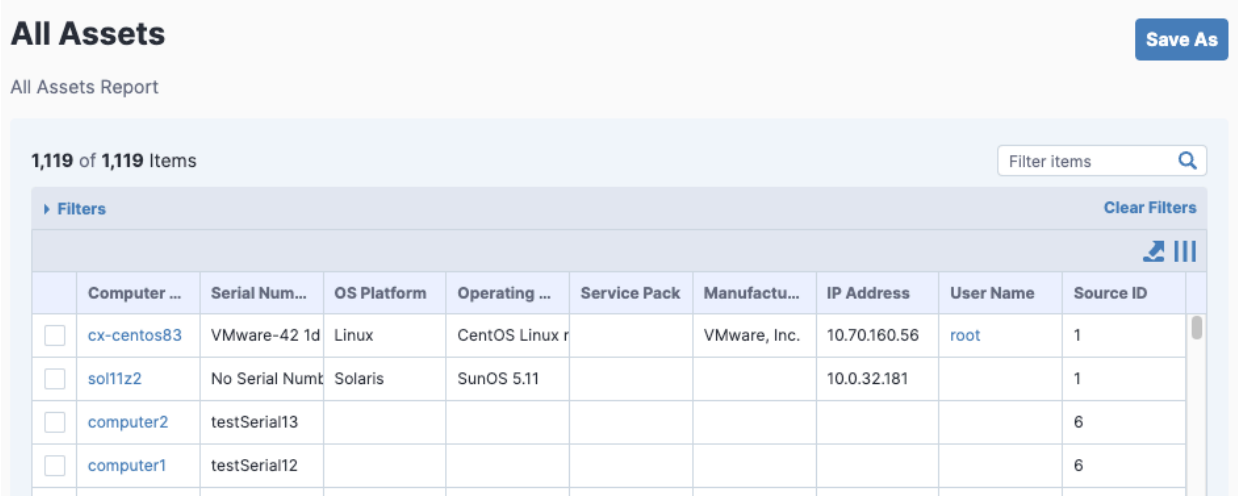
Work with existing reports

View reports

About this task

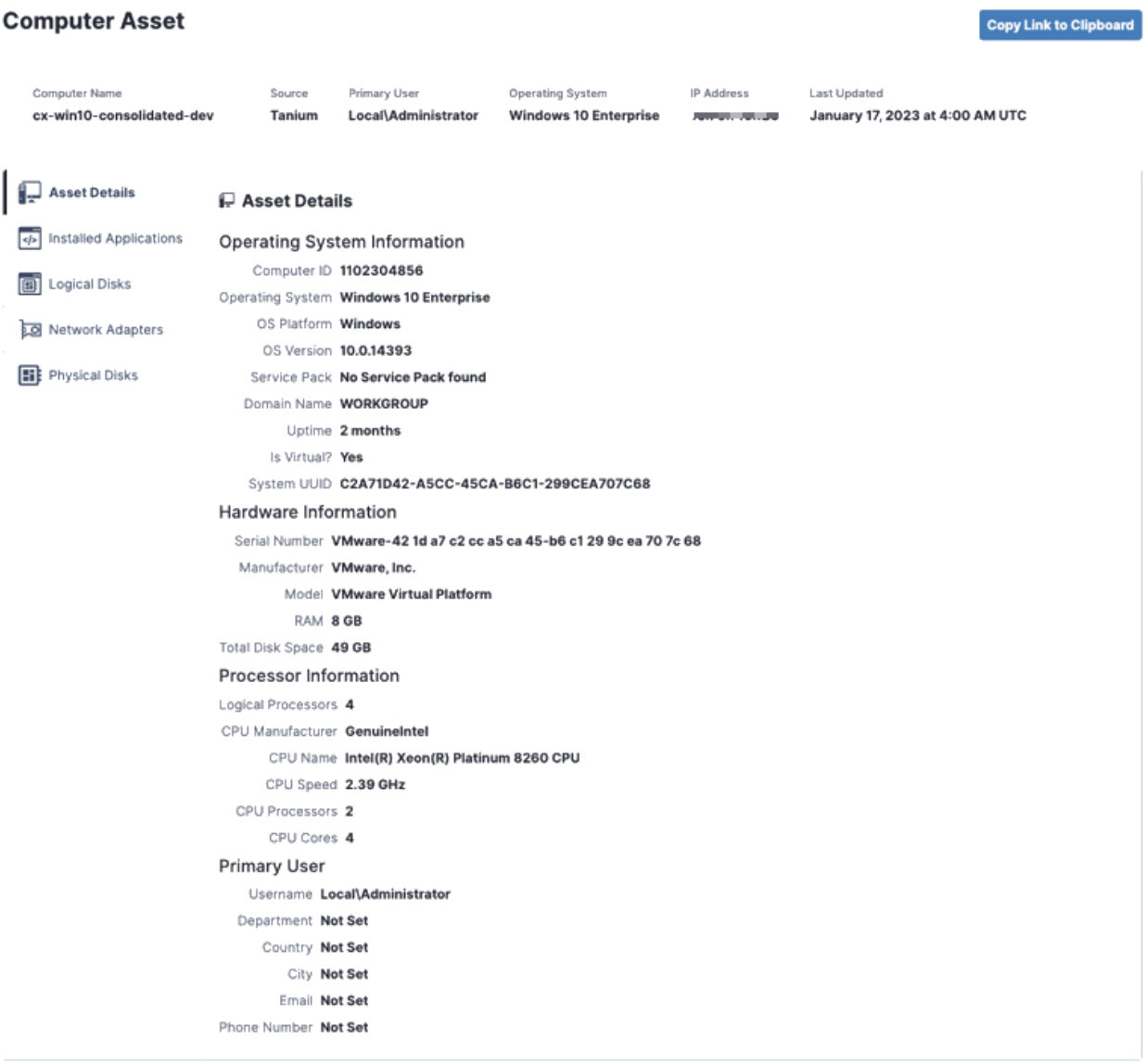
You view reports and assets within reports based on your permissions. For more information about how users receive permissions, see Tanium Console User Guide: RBAC overview.

1. From the Main menu, go to **Modules** > **Asset** > **Reports**. You can view all built-in and custom reports on the **Reports** page. To view a report, click the report name.
2. If you are viewing a summary report, you can drill down into the data in a report by clicking links in the report data grid.
   For example, in the **All Assets** report, you can click the **Computer Name** to view information about that asset. You can also click the **User Name** to view information about assets that are owned by the user.



3. In the detail report, you can see more information about the selected asset.

©2026 Tanium Inc. All Rights Reserved



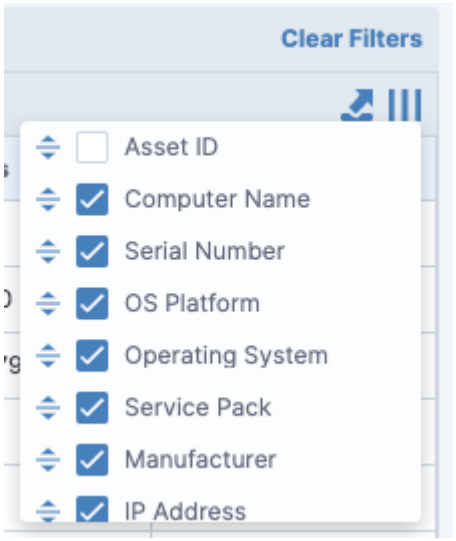
Customize columns

About this task

You can change which columns appear in the report and adjust the order of the columns.

1. In the report, click Customize Columns .

©2026 Tanium Inc. All Rights Reserved



2. To remove a column, clear the checkbox for the column.
3. To adjust the column order, click and drag the column names.

Filter reports

About this task

To quickly search the values in the report, use filter items. To filter the values based on certain column values with operators (greater or less than, contains, is equal to, and so on), create a report filter.

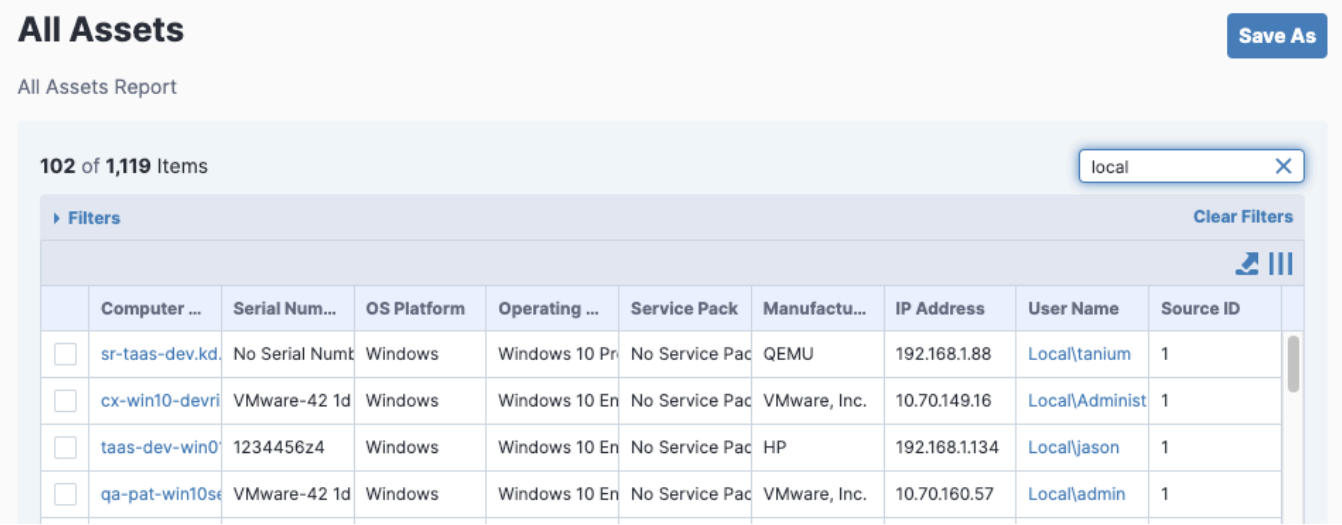
FILTER ITEMS

About this task

In a report, you can quickly filter items by searching the report.

Figure 2. Search reports to quickly filter items

©2026 Tanium Inc. All Rights Reserved



These filters are not saved when you leave the report page.

Note: You cannot filter on columns with numeric values.

CREATE REPORT FILTERS

About this task

You can perform live filtering on any report and optionally save the filter for future use.

Tip: If you want to create a filter to match a **Source ID**, you can find the ID when you edit a source. For more information, see Edit source on page 99.

1. In a report, expand the **Filters** section. If the report contains a filter, that filter is already listed.
2. Add filters. You can add to the filter with the following methods:
   - Create a quick filter: Hover over a value in your report, click Options and click Add is equal to filter or Add is not equal to filter. The appropriate condition is added to the **Filters** section.

©2026 Tanium Inc. All Rights Reserved



- Edit the filter directly:

  Click Add + and then select **Add Row** to create a filter rule that is at the same level as the selected rule. When you create the rule, you can choose the attribute and whether the filter applies AND or OR operators with the other filters at that level. Click Apply ✓. To create nested groups of filters, click Add + and then select **Add Group**.

3. Update the report data. Click **Apply All** to refresh the report based on the filters.
4. (Optional) Save report filters.
   - If you want to save the filter you defined in a custom report, click **Save**, or **Save As** to create a copy of the report that contains the filter.
   - If you want to save filtering for a predefined report, click **Save As** and create a copy of the report that contains the filter.

Create a report

About this task

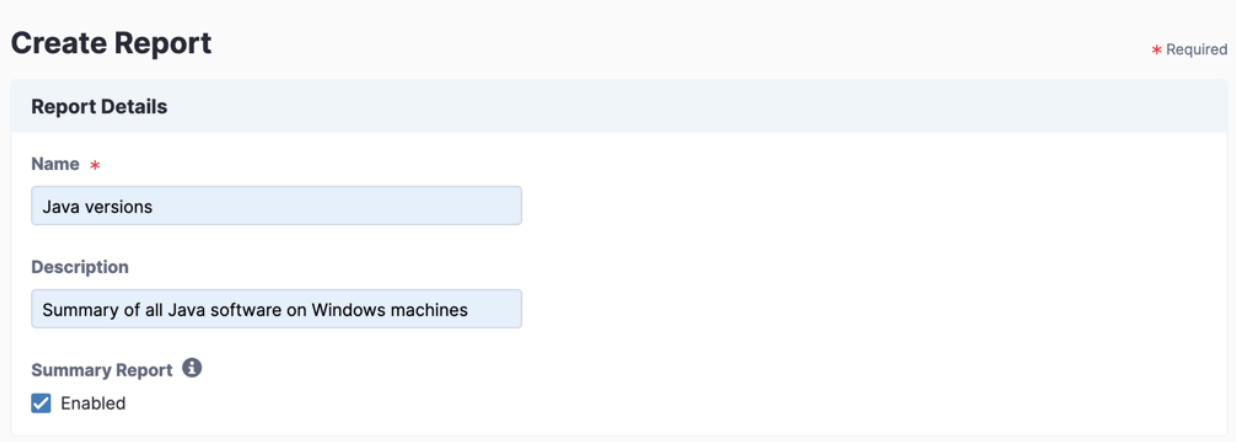
You can create a new custom report, or you can copy from an existing report:

- To create a new report on the **Reports** page, click **Create Custom Report**.
- In an existing report, click **Save As** to create a copy of the report, give the report a new name, and click **Accept**. The new report opens. Click **Edit** to change report details.

Specify general report information

©2026 Tanium Inc. All Rights Reserved

1. Enter a report name and description to help you remember the purpose of the report later. The report name must be unique among all reports in Asset, including reports created by other users.
2. If you select **Summary Report**, the data is grouped into rows with an associated count that you can click to view more details.



   For example, if you create a report that lists SQL installations, with this option enabled, you get a result that lists a count of the computers that have each SQL version. You can then click the count to view the list of computers with that software installed.

3. If you select **Public Access**, any user with the **Asset Limited Report Reader** role (which provides the **Asset Limited Report** permission) can view the report. If this setting is disabled, only users that are assigned a role with the **Asset Report read** or **Asset Report write** permissions can view the report.

   > **Note:** This access limitation obscures visibility to non-public Asset reports for limited users but does not secure against these users accessing individual data points within a public report.

Select columns

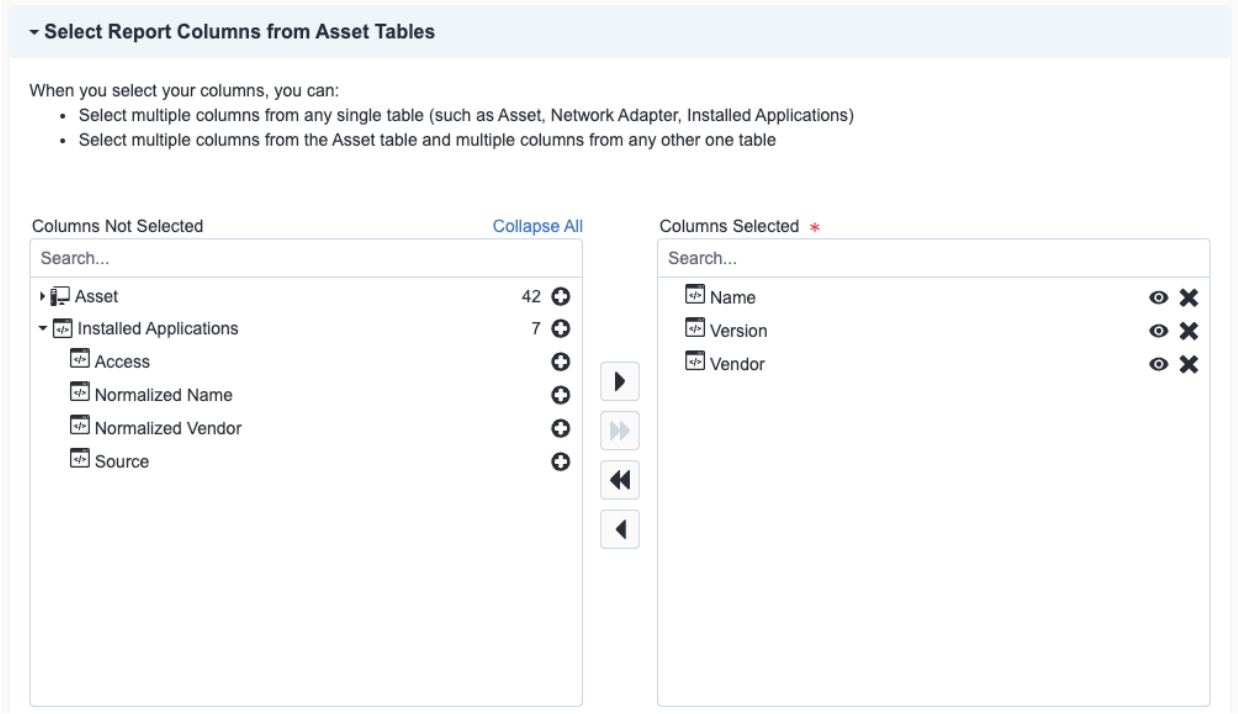
About this task

The columns that are available to include in your reports come from the asset sources that you define. To define sources, from the Main menu, go to **Modules** > **Asset** > **Inventory Management** > **Sources**.

©2026 Tanium Inc. All Rights Reserved

Tip: When you select columns, you can select multiple columns from the Asset table and any other single table (such as Network Adapter, Installed Applications, or Logical Disk). For example, you cannot select columns from both the Network Adapter and Installed Applications tables.

1. In the **Select Report Columns from Asset Tables** section, select the data that you want to include in your report.
   You can search for the column that you want to use or expand and collapse the data categories to find which columns you want to include.



2. Specify the order that you want your columns to appear. In the **Columns Selected** section, click and drag the column names to arrange them in the order you want them from left to right in the resulting report. If you do not want the column to show up in the report but want the data to be available for filtering, change the **Show** value to **Hide**.

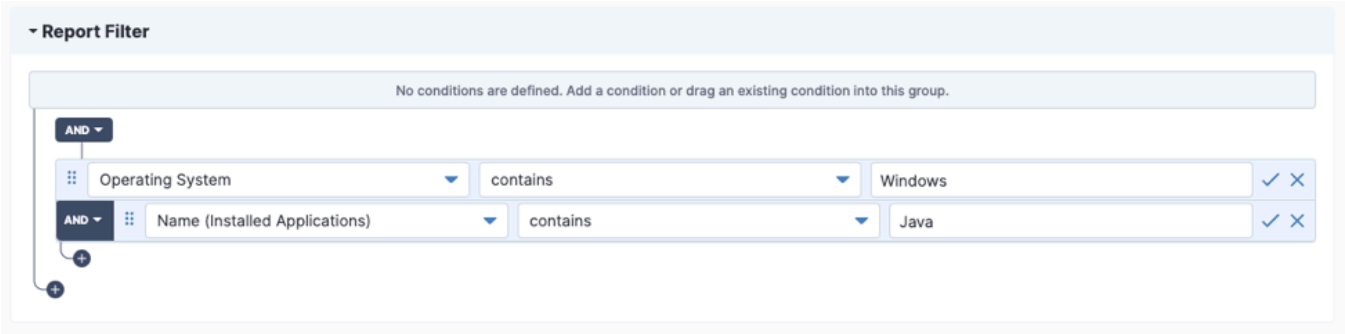
Define default filter

About this task

You can create a filter that is always applied when the report runs.

Figure 3. Example of a persistent report filter

©2026 Tanium Inc. All Rights Reserved



Click Add + and then select **Add Row** to create a filter rule that is at the same level as the selected rule. When you create the rule, you can choose the attribute and whether the filter applies AND or OR operators with the other filters at that level. Click Apply ✓. To create nested groups of filters, click Add + and then select **Add Group**.

- To save a filter rule, click Apply ✓.
- To edit a filter rule, click Edit ✎.
- To discard changes to a filter rule you are editing, click Cancel ✕.
- To delete a filter rule, click Delete 🗑.

FILTER CALCULATIONS

About this task

- If you use a `Size` data type in your report (such as the **Total Disk Space** or **Free Space** fields), the values are converted with a base of 1024. For example, 450,000 MB is converted to 439 GB.
- If you use a `Date` data type in your report (such as the **Created Date** field), you can filter on dates or calendar dates. For example, if you enter a filter for `created in the last "10 Days"`, the origin date and time are calculated from the exact current date and time. If you enter a filter `created in the last "10 Calendar Days"`, the origin date and time is always 12:00 AM on the specified number of days back from the current date. You can preview the date range when you save the rule.

Finish report

To save the report, click **Submit**. For more information about how to work with reports, see Work

©2026 Tanium Inc. All Rights Reserved

with existing reports on page 56.

Delete report

About this task

To delete a report, go to the **Reports** page and click Delete on the row of the report you want to delete. You can delete only custom reports.

Purge assets

Asset purges stale assets on an individual basis. Asset purges endpoints if not seen within the configured stale data age for the source from which the asset originates, or based on a purge report. For more information, see Configure data retention and vacuuming on page 214.

Asset Administrators or Asset Operators can manually remove assets from the Asset database earlier than the stale data age. In a report that shows the assets you want to remove, select the rows and click **Delete**.

If the asset you deleted returns results for sensors registered with Tanium Data Service, the asset is re-added to the Asset database. Note that when the asset is re-added, the asset might only contain partial data due to incremental loads from Tanium Data Service. To fully re-add a purged asset, you can perform a one-time import for a complete load from Tanium Data Service. For more information, see Reset differential load on page 203.

©2026 Tanium Inc. All Rights Reserved

Configuring sources

Sources define how Asset gets data. By default, the source data in Asset comes from Tanium, populated from sensor data stored in Tanium Data Service. You can augment Asset inventory data with external data from an SQL Server database, custom sources, or data pushed to Asset by Gateway using an Import API source. By importing data that is typically not available on an endpoint into the Asset data store, you can enable filtering and reporting on information such as department, cost center, building, and location.



Note: The AWS, Microsoft Azure, Microsoft Intune, and Google compute sources, as well as Google Chromebook sources, are currently beta features.

Asset reconciliation

Asset reconciliation compares assets in cloud sources with existing Tanium-managed assets during the import process. If two assets have 1:1 matching reconciliation keys, the assets are merged and the asset is deleted from the cloud source. Only custom entities can be merged. Attributes associated with Tanium sensors are not overwritten. These keys are matched to identify an asset for reconciliation:

Asset reconciliation keys

Source	Key used to match for reconciliation
AWS	`cloud_instance_id`
Google Cloud	`cloud_instance_id`
Import API	Selected when you create the source: `computer_id`, `computer_name`, `serial_number`, `cloud_instance_id`, `system_uuid`
Microsoft Azure	`cloud_instance_id`

©2026 Tanium Inc. All Rights Reserved

Source	Key used to match for reconciliation
Microsoft Intune	`computer_name` and `serial_number`

If a reconciled asset from a cloud source is not seen for 30 days, Tanium Data Service purges the asset. Asset keeps the asset in the Asset database for a few minutes beyond that but then purges the asset if still not seen. If the asset appears again in the cloud source, Asset adds the asset to the Asset database but does not reconcile and merge the asset into the Tanium source until the asset is seen by Tanium Data Service again.

Note: Reconciliation is not supported for Google Chromebook sources because the Tanium Client cannot be installed on Chromebooks.

Note: For more information about how Asset deduplicates assets supplied from Tanium Data Service, see Sources on page 13.

About the Tanium source

The Tanium source imports data that has been collected by sensors through Tanium Data Service into the Asset database. Use the data collected by the Tanium source to configure attributes in Asset.

By default, Asset imports asset data from Tanium Data Service into the Asset database every hour. Once added, you can add attributes collected from Tanium sensors into Asset. For more information, see Configuring attributes on page 109.

Note: Depending on the amount of data, an import might take longer than the configured import schedule. If an import is scheduled to run while the previous import is still running, the new import is canceled so the previous import can finish.

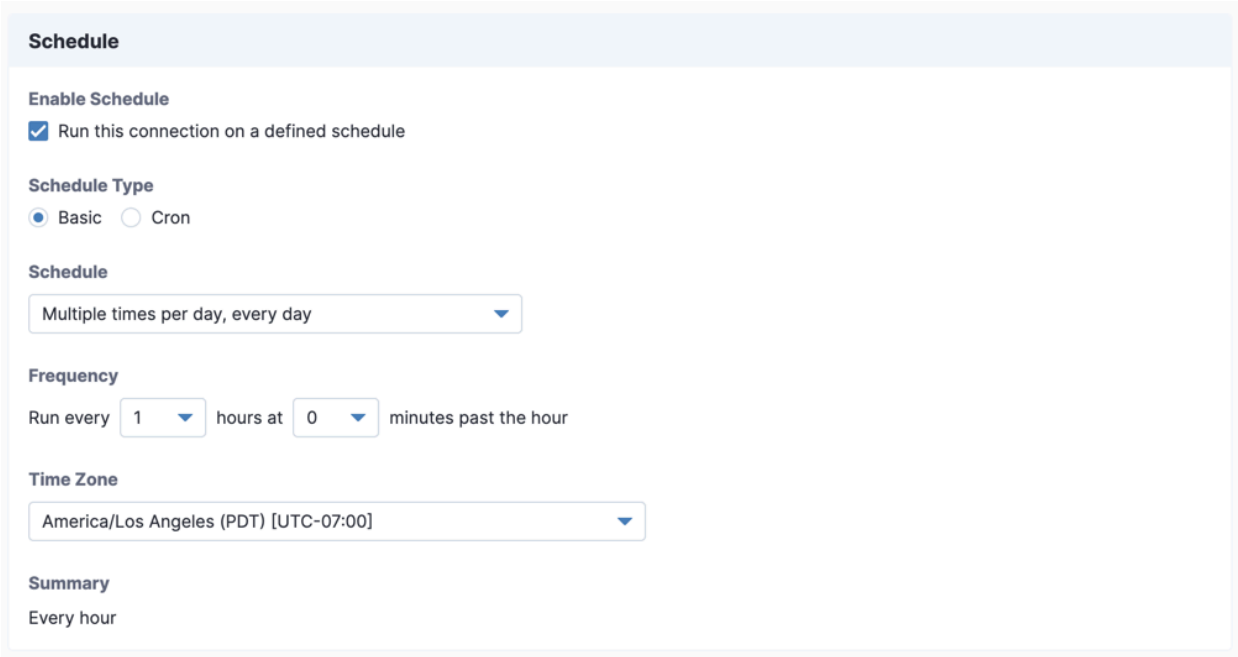
Configure the Tanium source

©2026 Tanium Inc. All Rights Reserved

About this task

The Tanium source is configured by default, and you cannot delete the Tanium source.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Sources**.
2. In the **Actions** column in the row for the Tanium source, click Edit .
3. Configure the log level settings for the Asset import process.
4. Configure the schedule. The schedule determines how often asset data is imported from Tanium Data Service into the Asset database.



   This database provides data for offline assets. You can create a standard interval or a cron schedule. For example, you might create one of the following intervals based on your environment size:

   - Less than 50,000 devices: every 1-2 hours.
   - Less than 250,000 devices: every 4 hours.
   - Greater than 500,000 devices: contact Tanium Support to configure the import schedule. For more information, see Contact Tanium Support on page 222.

   For more information about the cron syntax, see Reference: Cron syntax for Asset.

5. Click **Update** to save your changes.

©2026 Tanium Inc. All Rights Reserved

6. Wait at least two import cycles for attributes to appear in Asset. During this time, Asset registers the sensor with Tanium Data Service. Tanium Data Service then gathers results from endpoints after which Asset retrieves those results from Tanium Data Service.

What to do next

Add attributes from Tanium sensors into Asset. For more information, see Configuring attributes on page 109.

Create an AWS source

About this task

Create an AWS source to pull data from an AWS EC2 instance into Asset on a schedule.

Create an AWS Access Key and IAM role

About this task

1. Use the AWS Console, CLI, or API to create an AWS access key. For more information, see AWS Identity and Access Management documentation: Managing access keys for IAM users.

2. Create or identify an existing IAM role to use for the connection. For more information, see AWS Identity and Access Management documentation: Creating a role to delegate permissions to an IAM user. If you want to create one source for all accounts in your AWS organization using the **This account is an AWS Organization** option for the source, you must also specify a child role to assume when accessing child accounts. This role must have the appropriate permissions to access those accounts.

3. Attach the following policy to the IAM role in AWS. This policy limits the access of the user to the minimum requirements for Asset. For more information, see AWS docs: Create and Attach Your First Customer Managed Policy.

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Effect": "Allow",
```

©2026 Tanium Inc. All Rights Reserved

```
                        "Action": [
                                "ec2:DescribeInstances",
                                "ec2:DescribeRegions",
                                "ssm:DescribeInstanceInformation",
                                "organizations:ListAccounts"
                        ],
                        "Resource": "*"
                }
        ]
}
```

Create the AWS source

Before you begin

Complete Create an AWS Access Key and IAM role on page 68.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Sources**.
2. Click **Create Source**.
3. Specify a **Name** for the source.
4. In the **Provider** field, select **Amazon Web Services (AWS)**.
5. In the **Type** field, select **Compute Source**.
6. Set the **Log Level**.
7. In the **Access Key ID** field, specify the AWS access key ID part of the access key that you created.
8. In the **Secret Access Key** field, specify the AWS secret access key part of the access key that you created.
9. In the **Assume IAM Role** field, specify the IAM role that you created to use for the connection.
10. Select a **Default Region**.
11. (Optional) Select **AWS Organization** if you want this source to span your entire AWS organization, rather than individual accounts. If you select this option, specify the **Role to assume on child accounts**.
12. Click **Verify Connection** to confirm that the connection is valid. This step is required to save

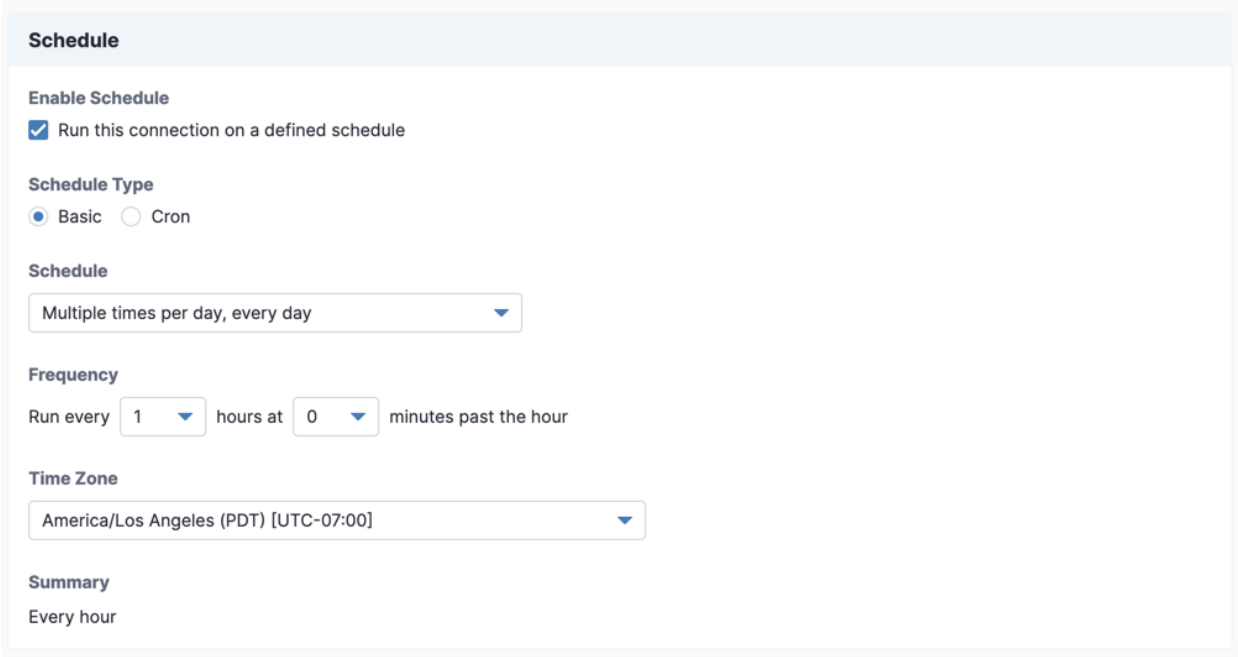
©2026 Tanium Inc. All Rights Reserved

the source.

13. (Optional) Enable reconciliation if you want to merge assets in this source with matching Tanium-managed assets during the import process. For more information, see Asset reconciliation on page 65.

14. (Optional) In the **Data Retention** section, configure when to purge stale assets from this source. The minimum value is 7 days, maximum is 180 days. Default is 30 days.

15. Configure the schedule.
    The schedule determines how often to import asset data from the AWS data into the Asset database.



    This database provides data for offline assets. You can create a standard interval or a cron schedule. For example, you might create one of the following intervals based on your environment size:

    - Less than 50,000 devices: every 1-2 hours.
    - Less than 250,000 devices: every 4 hours.
    - Greater than 500,000 devices: contact Tanium Support to configure the import schedule. For more information, see Contact Tanium Support on page 222.

    For more information about the cron syntax, see Reference: Cron syntax on page 223.

16. Click **Create** to save your changes.

Result

©2026 Tanium Inc. All Rights Reserved

Tip: Fields in the AWS source automatically map to the corresponding fields in the Asset database. After you create the source, you can edit the source to view the default field mappings.

Create a Microsoft Azure source

About this task

Create a Microsoft Azure source to pull data into Asset on a schedule.

Create a Microsoft Azure client ID and secret

About this task

In the Microsoft Azure portal, create an application registration. Note the associated **Application (client) ID** and add a client secret to use for authentication. Add the **Reader** role to the service principal object that was created when you registered the application.

For more information, see the following articles:

- Microsoft Entra documentation: Quickstart: Register an application with the Microsoft identity platform
- Microsoft Entra documentation: Add a client secret
- Microsoft Azure documentation: Assign Azure roles using the Azure portal

Important: Be sure to record the value of the client secret that you add in the Microsoft Entra admin center. The value only appears when you add the secret and does not appear again.

Create the Microsoft Azure source

Before you begin

Complete Create a Microsoft Azure client ID and secret on page 71.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management** > **Sources**.
2. Click **Create Source**.

©2026 Tanium Inc. All Rights Reserved

3. Specify a **Name** for the source.
4. In the **Provider** field, select **Microsoft Azure**.
5. In the **Type** field, select **Compute Source**.
6. Set the **Log Level**.
7. In the **Directory (tenant) ID** field, specify your Entra ID tenant ID.
   For more information about how to find your tenant ID, see Microsoft Azure documentation: Find your Microsoft Entra tenant.

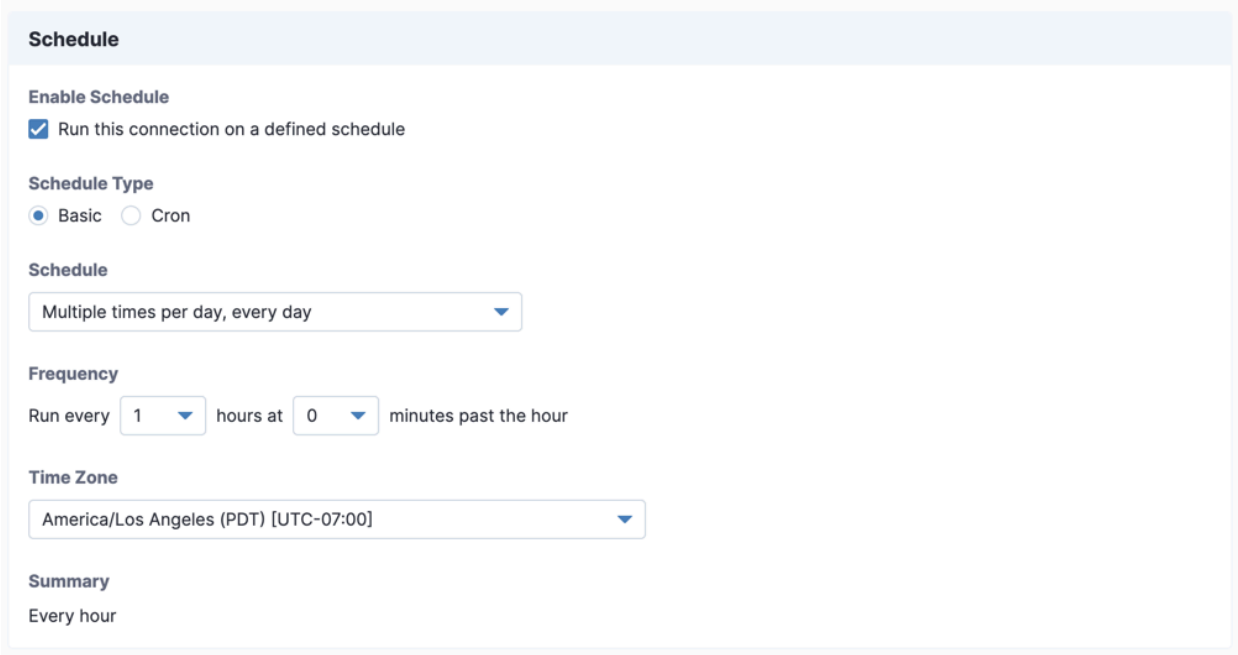
   > **Note:** Microsoft Entra ID was previously known as Microsoft Azure Active Directory or Microsoft Azure AD.

8. In the **Application (client) ID** field, specify the Microsoft Azure client ID that you created.
9. Provide the value of the **Client Secret** that you generated in the Microsoft Entra admin center.

   > **Important:** Be sure to provide the ***value*** of the client secret, and not the ID. The value only appears when you add the secret in the Microsoft Entra admin center and does not appear again. For more information, see Microsoft Entra documentation: Add a client secret.

10. Click **Verify Connection** to confirm that the connection is valid. This step is required to save the source.
11. (Optional) Enable reconciliation if you want to merge assets in this source with matching Tanium-managed assets during the import process. For more information, see Asset reconciliation on page 65.
12. (Optional) In the **Data Retention** section, configure when to purge stale assets from this source. The minimum value is 7 days, maximum is 180 days. Default is 30 days.
13. Configure the schedule.
    The schedule determines how often to import asset data from the Microsoft Azure source into the Asset database.

©2026 Tanium Inc. All Rights Reserved



This database provides data for offline assets. You can create a standard interval or a cron schedule. For example, you might create one of the following intervals based on your environment size:

- Less than 50,000 devices: every 1-2 hours.
- Less than 250,000 devices: every 4 hours.
- Greater than 500,000 devices: contact Tanium Support to configure the import schedule. For more information, see Contact Tanium Support on page 222.

For more information about the cron syntax, see Reference: Cron syntax on page 223.

14. Click **Create** to save your changes.

Result

Tip: Fields in the Microsoft Azure source automatically map to the corresponding fields in the Asset database. After you create the source, you can edit the source to view the default field mappings.

Create a database source

About this task

Enrich Asset inventory data with information from an external database. For example, you might have a database that has department or location information that you want to associate with the

©2026 Tanium Inc. All Rights Reserved

computers you are already tracking in Asset. To import this data, map columns from your SQL database to the Asset database.

When the data import runs, each row of your import table is evaluated against the data that is already in Asset. For example, if you create a mapping for your computer ID in the import table, that ID gets matched to the Computer ID column in Asset. If a match is found, the attributes that you configure to get imported from your source table are inserted into Asset. If you map an import column that has duplicate values in the table, only the last value is stored in Asset after the load has completed.

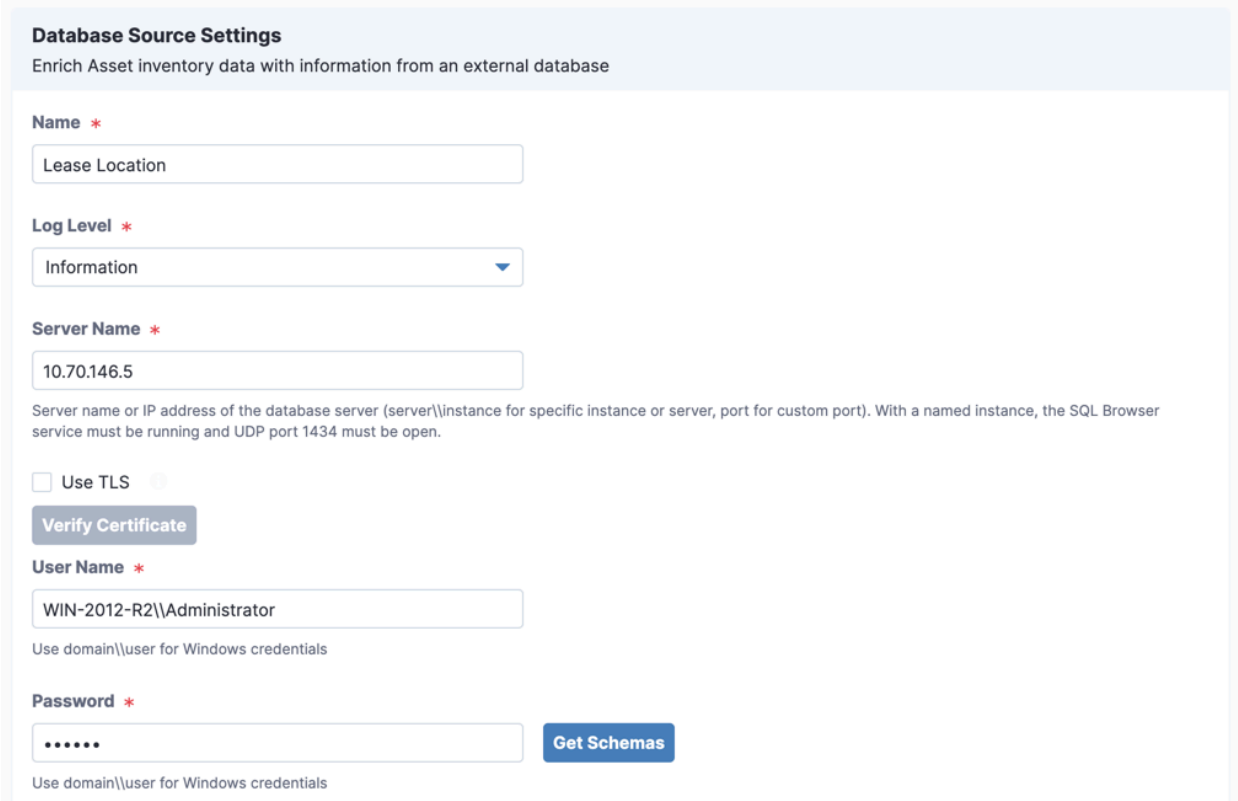


Important: If you use column types (like `nchar`) that pad values with spaces, your identity mappings on the database source might not work correctly. For example, a computer name like `win1` might come through as `win1 ` (with six spaces after it). These values do not match a value `win1` in Asset.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Sources**.
2. Click **Create Source**.
3. In the **Provider** field, select **External Database**. Note the **Type** field is now disabled.
4. Configure source settings, including a name for the data source, the log level, and the server name. (Optional) If your database server has Transport Layer Security (TLS) configured, perform the following:
    a. Ensure **Use TLS** is selected.
    b. To validate the certificate from the database source, keep **Validate Server's TLS Certificate** selected (recommended).
    c. Click **Add Certificate**, verify the certificate details are correct, and then click **Add**.

    For more information about how to enable TLS on SQL Server, see Microsoft SQL Docs: Enable Encrypted Connections to the Database Engine.
5. Enter the user name and password for the database connection, and then click **Get Schemas** to choose the database and schema.
    Asset connects to the database and gets the database and schema information.

©2026 Tanium Inc. All Rights Reserved



6. Configure source mappings. Source mappings uniquely identify the assets in your source data and define how the columns in your source table relate to the Asset database. For an attribute to be available as a reference for mapping, it must only return a single row of value. You can add multiple source mappings from your database source. All the mappings must match for the data to be imported into the Asset database.
    a. Click **Add Mapping**. Choose a source table.
    b. Create identification rules. The columns associated with the selected source table are loaded into the **Source Columns** field.
    c. Choose a destination attribute. Choose a column in the Asset database. You can create multiple identification rules as necessary.

> **Tip:** Make sure the source mappings are correct before you continue to the next step.
>
> Source mappings are not editable after you save the profile.

7. Configure the import schedule. The schedule determines how often to import asset data from the external database into the Asset database. You can create a standard interval or a cron schedule.
   For more information about the cron syntax, see Reference: Cron syntax for Asset.

8. Click **Create**.

©2026 Tanium Inc. All Rights Reserved

Result

To modify the source, go to **Inventory Management** > **Sources**, and click Edit . You can edit the name of the source, log level, server name, credentials, and the run schedule. Source mappings are not editable.

Important: A maximum of 20,000 asset updates are performed for each 100 database source records during the load process. You might need to run an import several times to update all the data.

Next steps

Add the attributes from your import table into Asset. For more information, see Configuring attributes on page 109.

Create a Google Chromebook source

About this task

Create a Google Chromebook source to pull data into Asset on a schedule.

Create a Google Cloud service account to use for authentication

About this task

For more information about how to create a Google Cloud service account to use for authentication, see Google Cloud documentation: Creating a service account.

For more information about Google Cloud service accounts, see Google Cloud documentation: Understanding service accounts.

Create the Google Chromebook source

Before you begin

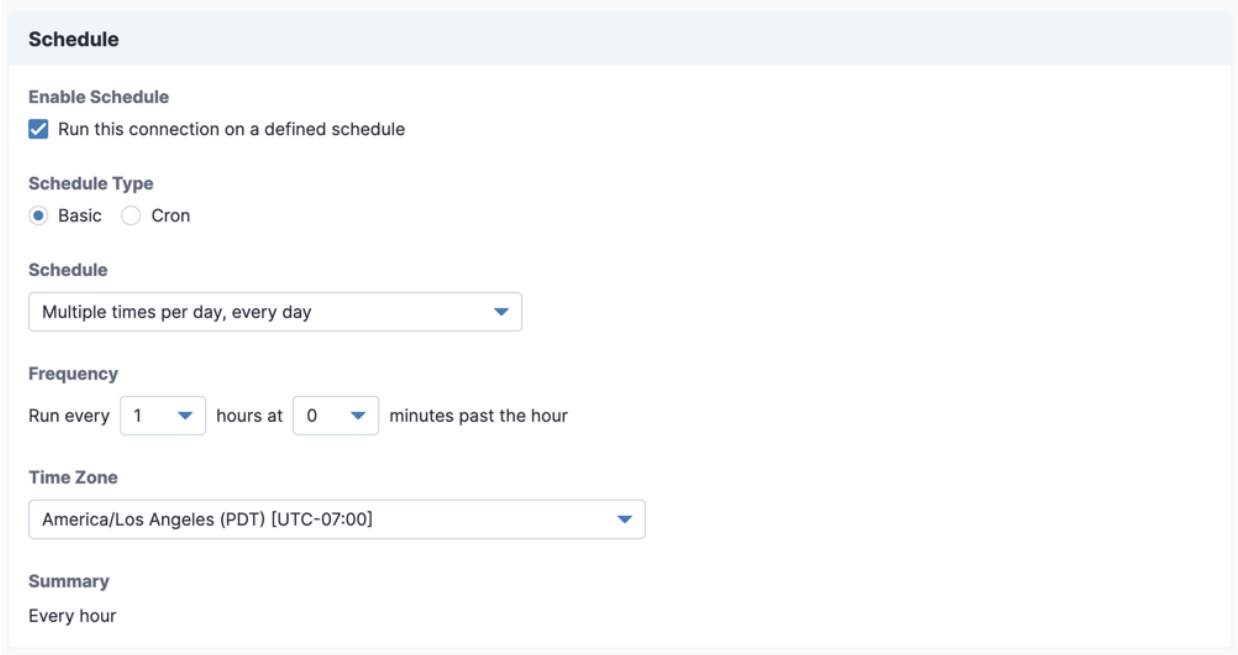
Complete Create a Google Cloud service account to use for authentication on page 76.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Sources**.
2. Click **Create Source**.

©2026 Tanium Inc. All Rights Reserved

3. Specify a **Name** for the source.
4. In the **Provider** field, select **Google Cloud Platform (GCP)**.
5. In the **Type** field, select **Google Chromebooks**.
6. Set the **Log Level**.
7. In the **Client Email** field, specify the email address associated with the Google Cloud service account that you created.
8. In the **Subject** field, specify the email address for the Google account to impersonate when making the request.
   For more information, see Google Identity documentation: Preparing to make an authorized API call (HTTP/REST tab).
9. Provide the **Private Key** that you generated for the Google Cloud service account.
10. Click **Verify Connection** to confirm that the connection is valid. This step is required to save the source.
    If the test fails, use the Google API Console to confirm that the credentials that you provided are valid. For more information, see Google Cloud documentation: Creating a service account.
11. (Optional) In the **Data Retention** section, configure when to purge stale assets from this source. The minimum value is 7 days, maximum is 180 days. Default is 30 days.
12. Configure the schedule.
    The schedule determines how often to import asset data from the source into the Asset database.

©2026 Tanium Inc. All Rights Reserved



This database provides data for offline assets. You can create a standard interval or a cron schedule. For example, you might create one of the following intervals based on your environment size:

- Less than 50,000 devices: every 1-2 hours.
- Less than 250,000 devices: every 4 hours.
- Greater than 500,000 devices: contact Tanium Support to configure the import schedule. For more information, see Contact Tanium Support on page 222.

For more information about the cron syntax, see Reference: Cron syntax on page 223.

13. Click **Create** to save your changes.

Result

Tip: Fields in the Google Chromebook source automatically map to the corresponding fields in the Asset database. After you create the source, you can edit the source to view the default field mappings.

Create a Google Cloud source

About this task

Create a Google Cloud source to pull data into Asset on a schedule.

©2026 Tanium Inc. All Rights Reserved

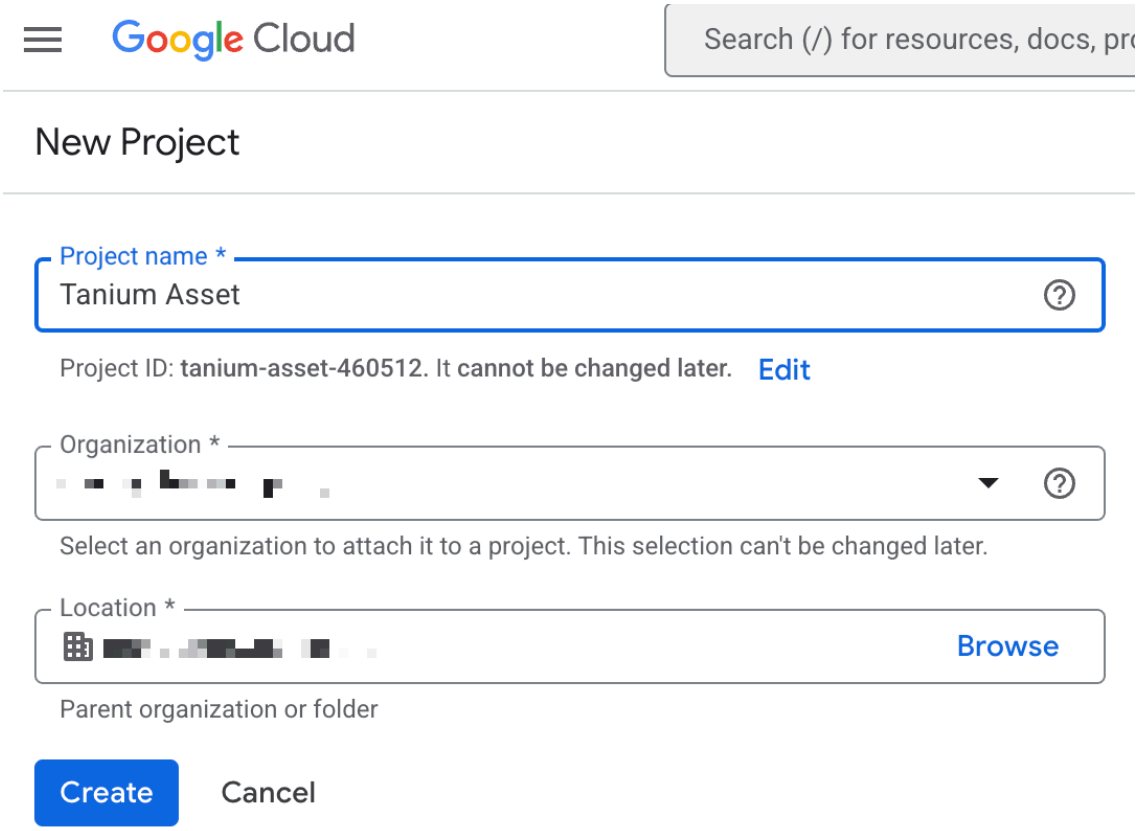
Configure the Google Cloud source

About this task

Use the following steps to create a project, add a service account, and then create a private key.

> **Note:** For more information about how to create a Google Cloud service account, see Google Cloud documentation: Creating a service account. For more information about Google Cloud service accounts, see Google Cloud documentation: Understanding service accounts.

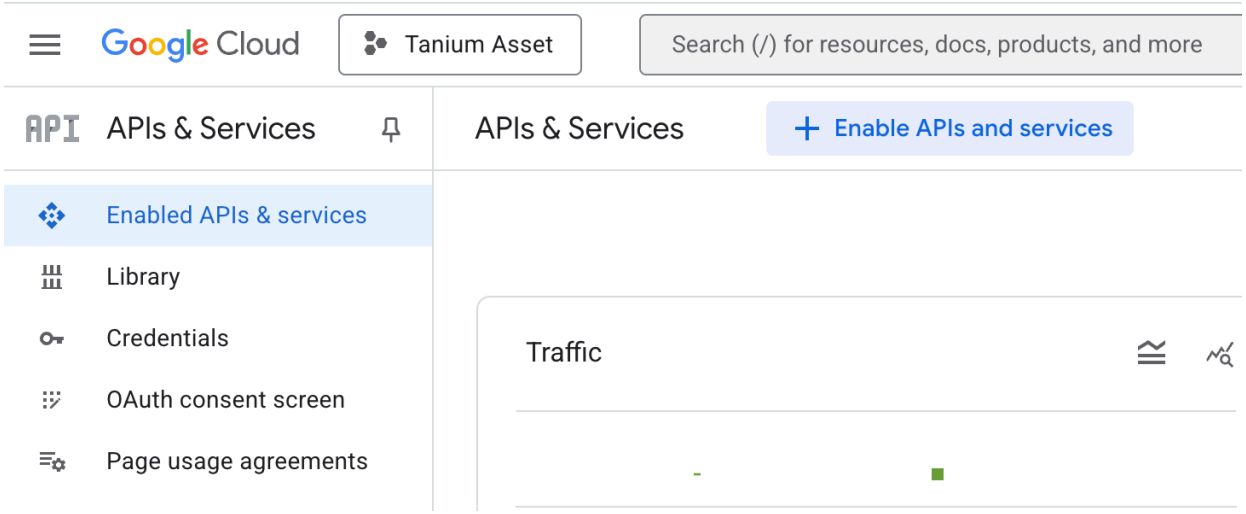
1. Sign in to your Google Cloud account.
2. Select or create a project:
   - To use an existing project, click **Select project**, and then click the name of the project that you want to use.
   - To create a project, click **Create project**. Specify the **Project name**, **Organization**, and **Location**, and then click **Create**.



3. In the Google Cloud console, go to the **APIs & Services** page.

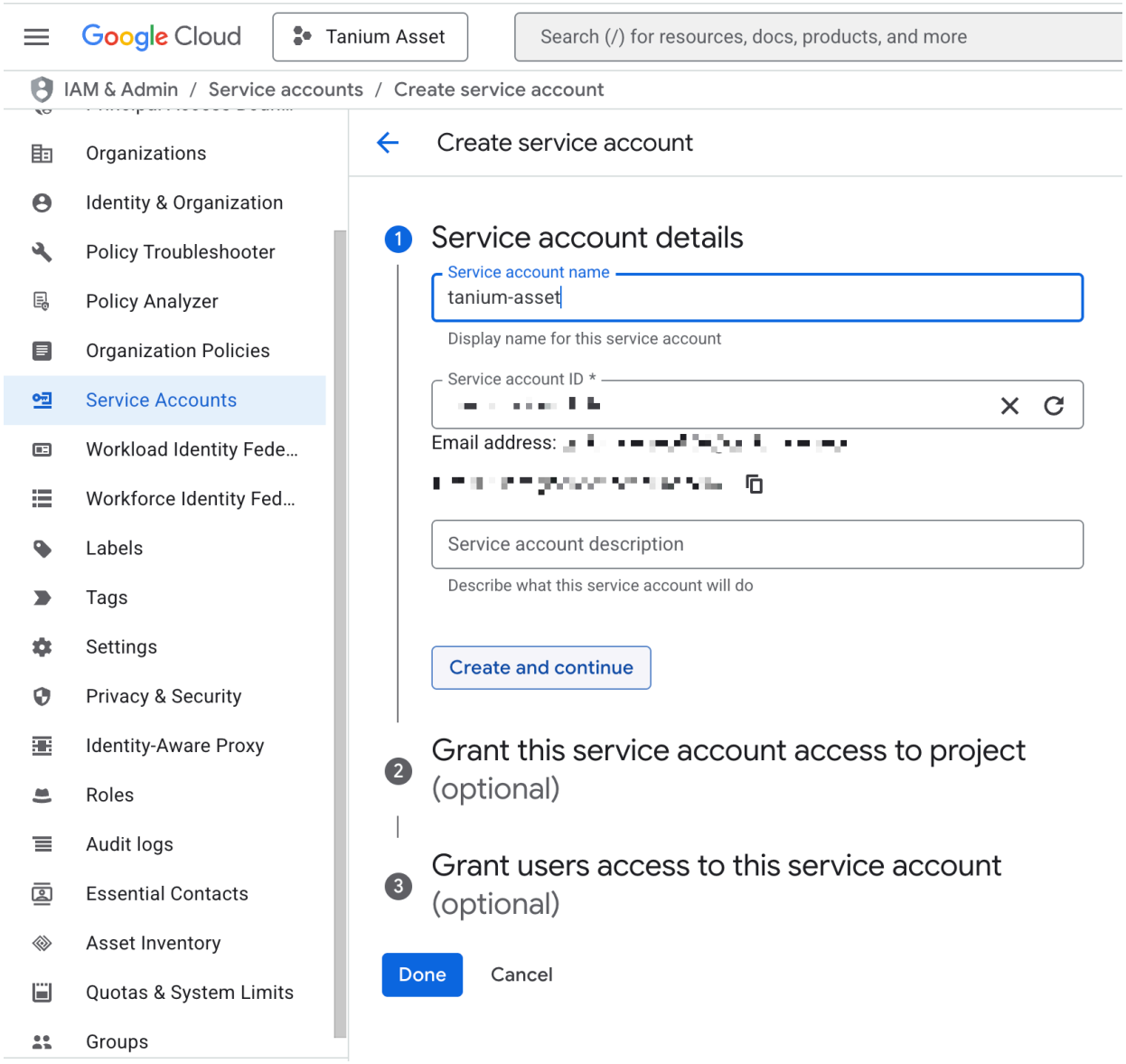
©2026 Tanium Inc. All Rights Reserved

4. Select **+ Enable APIs** and services and then enable the **Compute Engine API** and the **Cloud Resource Manager API**.



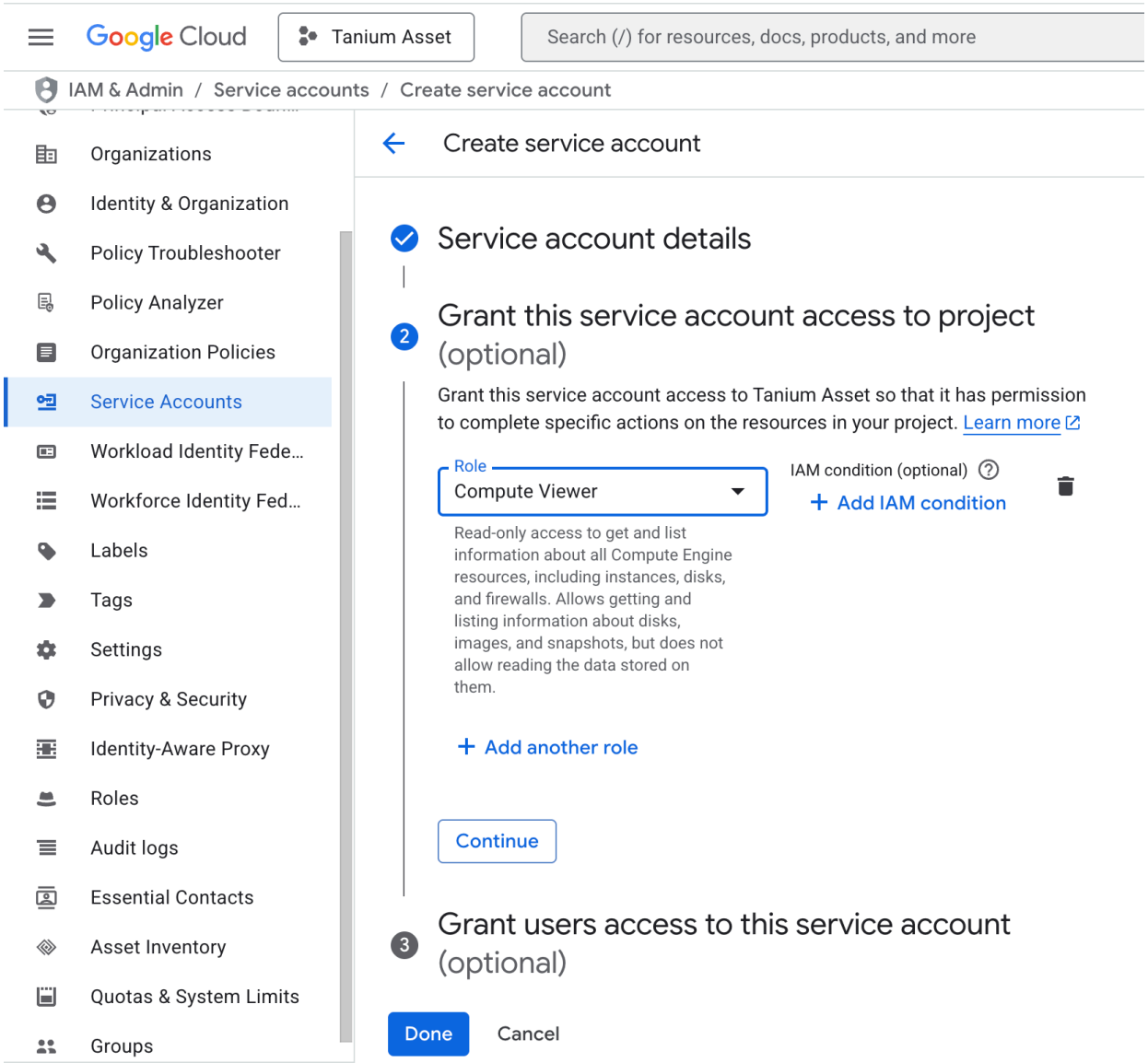
5. From the Google Cloud console menu, go to **IAM & Admin** > **Service Accounts**.
6. Click **+ Create service account**.
7. Specify the **Service account name**, **Service account ID**, and **Service account description**. Click **Create and continue**.

©2026 Tanium Inc. All Rights Reserved



8. Grant the **Compute Viewer** role to the service account, and then click **Done**.

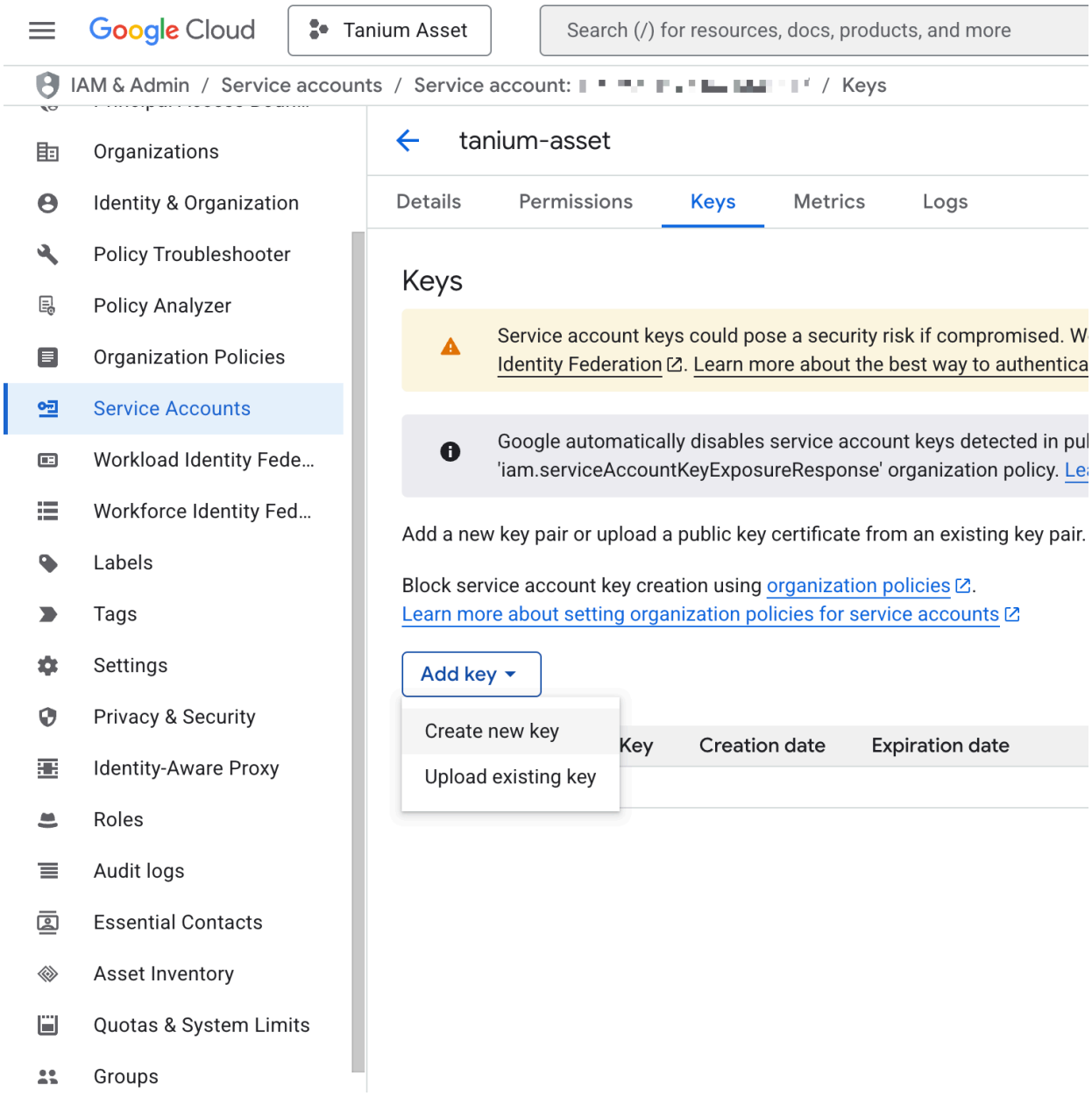
©2026 Tanium Inc. All Rights Reserved



Tip: The **Compute Viewer** role is only available after you enable the Compute Engine API for the project.

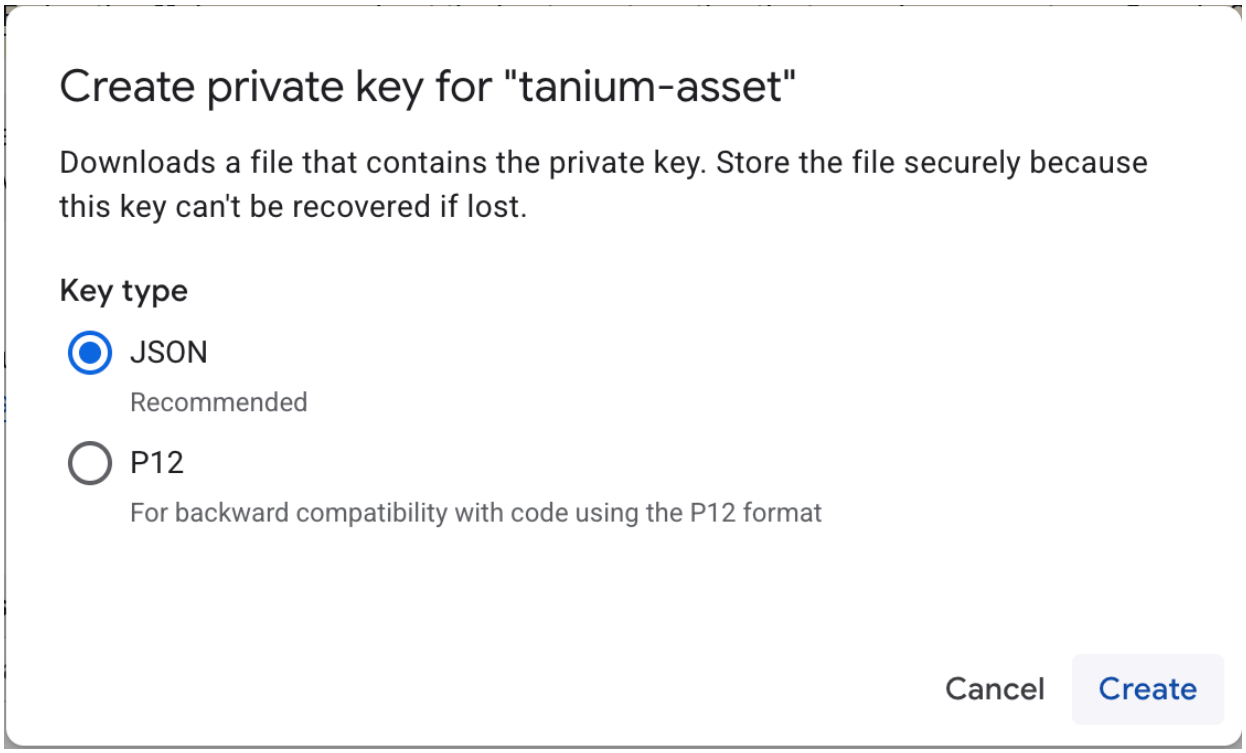
9. From the service account page, go to the **Permissions** tab and click **Grant access**.
10. From the service account page, go to the **Keys** tab, click **Add key**, and then select **Create new key**.

©2026 Tanium Inc. All Rights Reserved

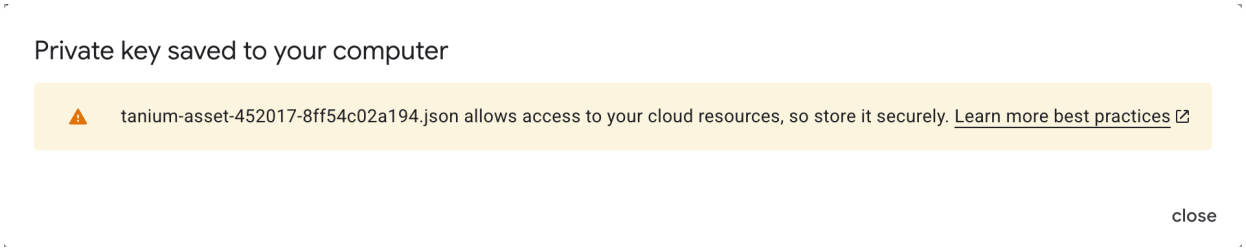


11. Select `JSON` for the **Key type** and then click **Create**.

©2026 Tanium Inc. All Rights Reserved

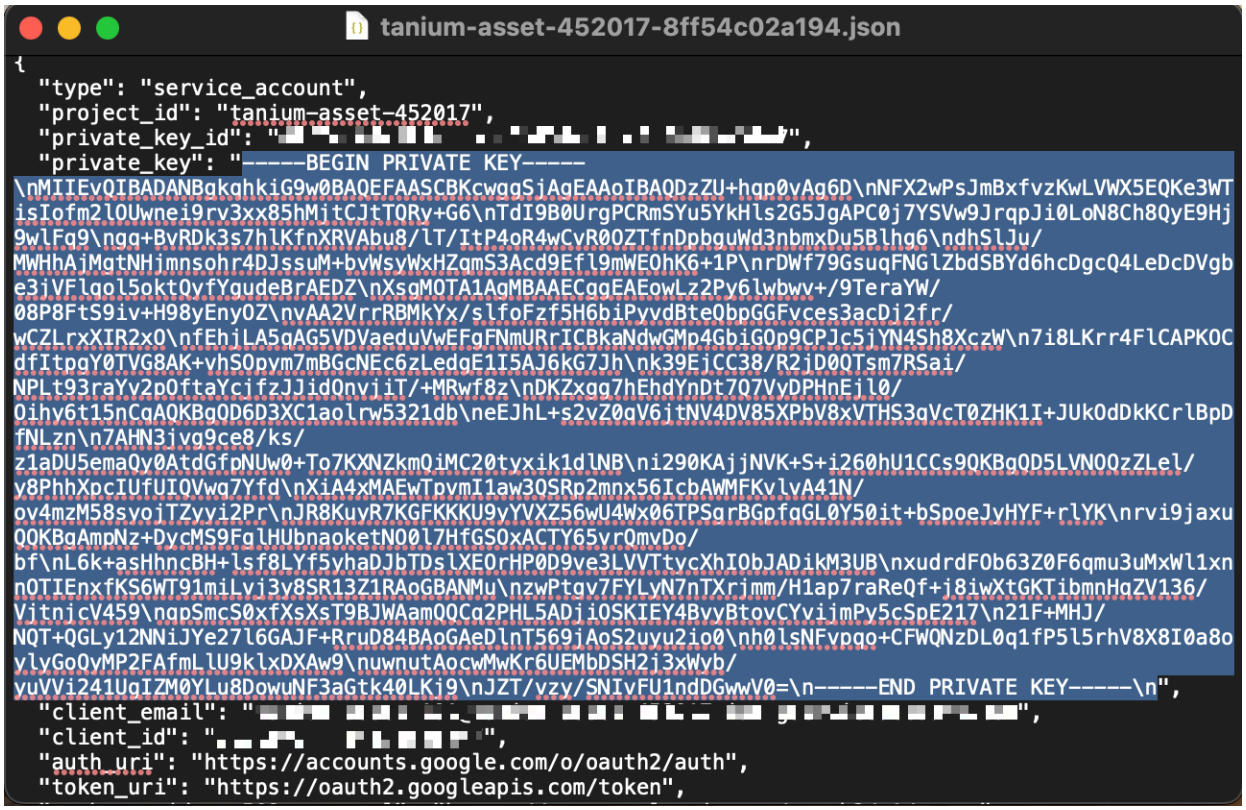


Google shows a notification that the private key downloads to your local machine. Click **close**.



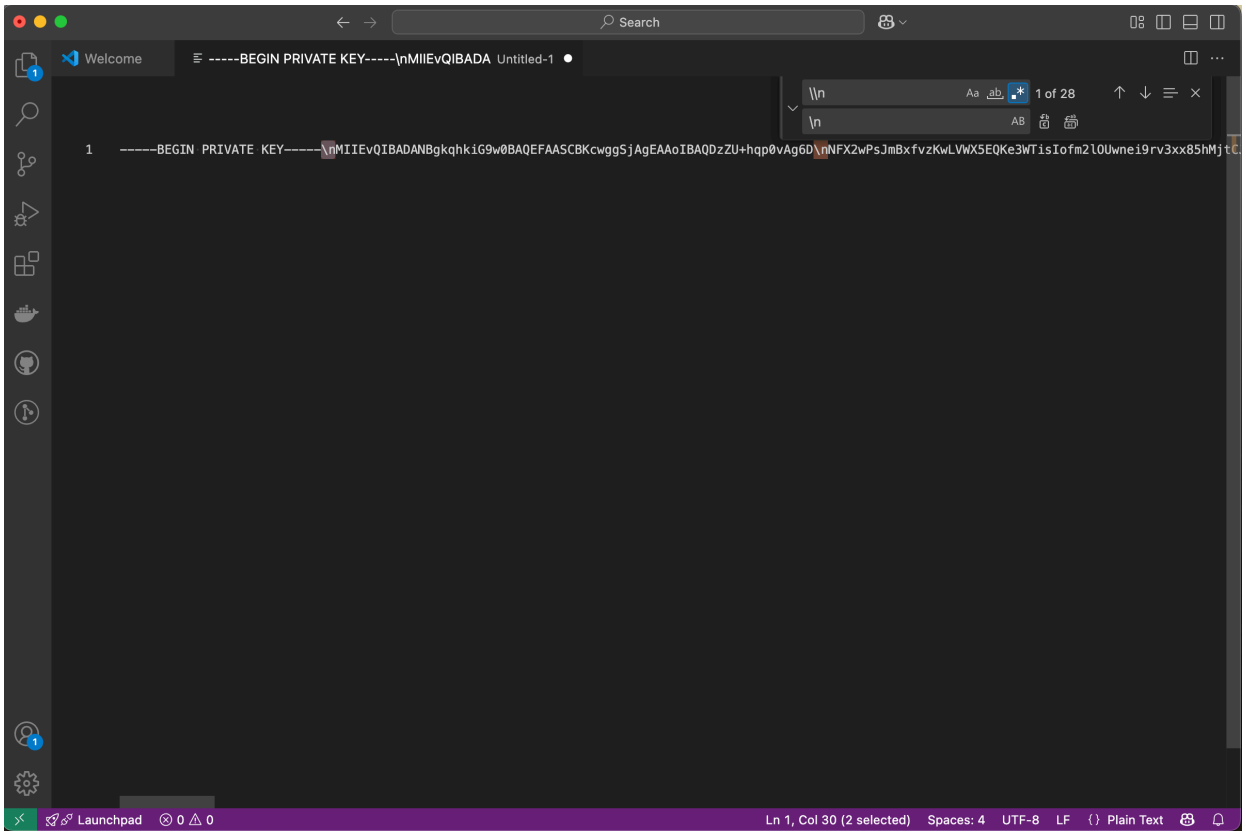
12. Navigate to the download location and edit the private key file. Record the contents of the `client_email` field.
13. Copy the contents of the `private_key` field to your clipboard.

©2026 Tanium Inc. All Rights Reserved



14. Paste the key into a new file.

    Remove the escape characters from all newline characters (change instances of `\\n` to `\n`).



©2026 Tanium Inc. All Rights Reserved

Sample key:



15. Make sure to have the key available for the next steps to configure a Google Cloud source in Asset.

Create the Google Cloud source

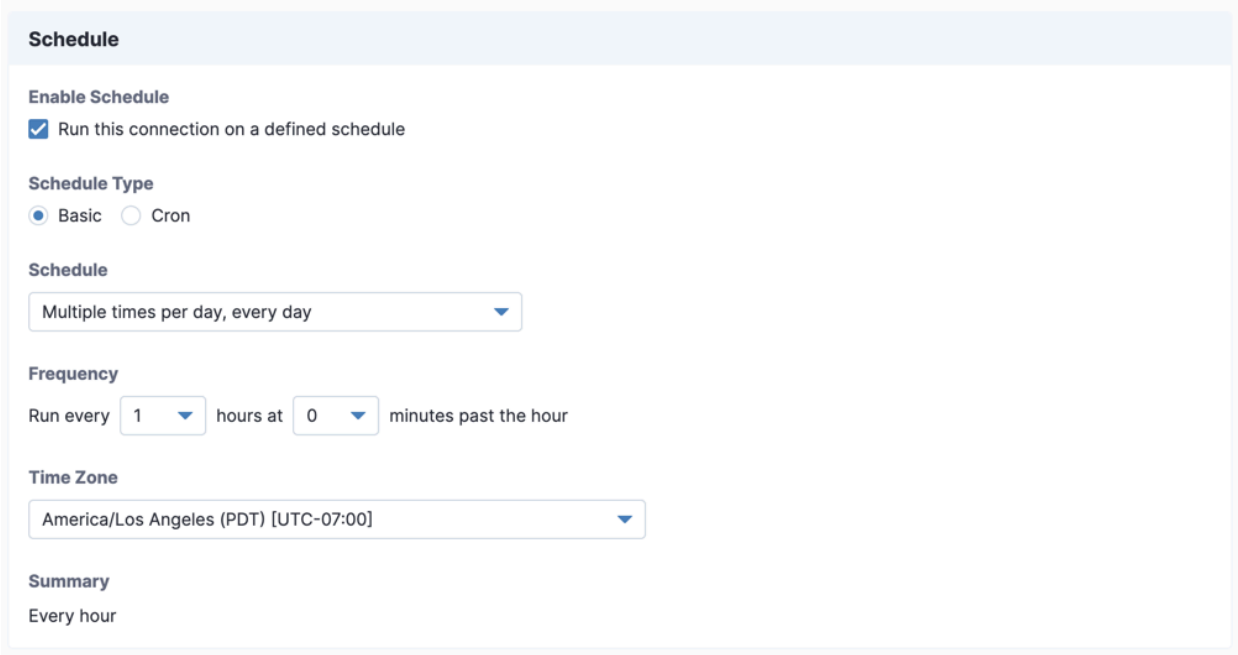
Before you begin

©2026 Tanium Inc. All Rights Reserved

Complete Configure the Google Cloud source on page 79.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Sources**.
2. Click **Create Source**.
3. Specify a **Name** for the source.
4. In the **Provider** field, select **Google Cloud Platform (GCP)**.
5. In the **Type** field, select **Compute Source**.
6. Set the **Log Level**.
7. In the **Client Email** field, specify the email address associated with the Google Cloud service account that you created.
8. In the **Subject** field, specify the email address for the Google account to impersonate when making the request.
   For more information, see Google Identity documentation: Preparing to make an authorized API call (HTTP/REST tab).
9. Provide the **Private Key** that you generated for the Google Cloud service account.
10. Click **Verify Connection** to confirm that the connection is valid. This step is required to save the source.
    If the test fails, use the Google API Console to confirm that the credentials that you provided are valid. For more information, see Google Cloud documentation: Creating a service account.
11. (Optional) Enable reconciliation if you want to merge assets in this source with matching Tanium-managed assets during the import process. For more information, see Asset reconciliation on page 65.
12. (Optional) In the **Data Retention** section, configure when to purge stale assets from this source. The minimum value is 7 days, maximum is 180 days. Default is 30 days.
13. Configure the schedule.
    The schedule determines how often to import asset data from Google Cloud into the Asset database.

©2026 Tanium Inc. All Rights Reserved



This database provides data for offline assets. You can create a standard interval or a cron schedule. For example, you might create one of the following intervals based on your environment size:

- Less than 50,000 devices: every 1-2 hours.
- Less than 250,000 devices: every 4 hours.
- Greater than 500,000 devices: contact Tanium Support to configure the import schedule. For more information, see Contact Tanium Support on page 222.

For more information about the cron syntax, see Reference: Cron syntax on page 223.

14. Click **Create** to save your changes.

Result

Tip: Fields in the Google Cloud source automatically map to the corresponding fields in the Asset database. After you create the source, you can edit the source to view the default field mappings.

Create an Import API source

About this task

When you create an Import API source, data is pushed to Asset using Tanium Gateway, rather than Asset periodically pulling data from a source. For more information about Gateway, see Tanium

©2026 Tanium Inc. All Rights Reserved

Gateway User Guide: Overview.

Note: There are two types of Import API sources, a **Standard** version and a **Legacy** version. The legacy version is deprecated. This task guides you through how to set up the standard version of the Import API source. For questions about the legacy version of the Import API source, Contact Tanium Support on page 222.

Tip: Field mapping is automatically determined for standard versions of the Import API source. For the legacy version, you must manually define field mappings. For more information about how to add additional field mapping to legacy versions of Import API sources, see Map additional fields for a source on page 230.

Create the Import API source

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Sources**.
2. Click **Create Source**.
3. Specify a **Name** for the source.
4. In the **Provider** field, select **Import API**.
5. In the **Type** field, select **Standard**.
6. Set the **Log Level**.
7. Select the source keys to use as unique identifiers for assets from this source. Any keys are combined with AND operators to determine uniqueness for an endpoint.
8. (Optional) Enable reconciliation if you want to merge assets in this source with matching Tanium-managed assets during the import process. For more information, see Asset reconciliation on page 65.
    a. Select the keys to match for reconciliation: `computer_id`, `computer_name`, `serial_number`, `cloud_instance_id`, `system_uuid`.
    b. Select any entities to merge data into an asset for reconciliation. Asset uses source keys to find 1:1 matching assets in the Tanium source.
9. (Optional) In the **Data Retention** section, configure when to purge stale assets from this

©2026 Tanium Inc. All Rights Reserved

source. The minimum value is 7 days, maximum is 180 days. Default is 30 days.

10. Click **Create** to save your changes.

Example

Example workflow

The following example represents a typical workflow using an Import API source:

1. Create an Import API source in Asset.
2. Pass the JSON data with the assets that you want to push to Asset using a Gateway mutation request. For more information, see the following mutations in Reference: Gateway examples for Asset on page 237:
    - Update Asset endpoints based on endpoint ID (EID) on page 250
    - Upsert (create or update by ID) Asset endpoint on page 252
3. Verify the results by checking Asset to confirm that the assets are available. For more information, see Building reports on page 56.

Create a Microsoft Intune source

About this task

Create a Microsoft Intune source to pull data into Asset on a schedule.

Create a Microsoft Azure client ID and secret

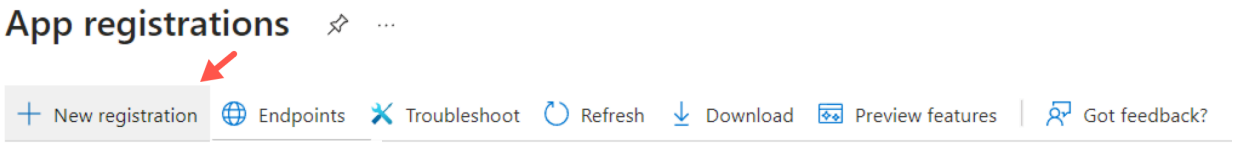
About this task

In the Microsoft Azure portal, create an application registration, configure the application permissions, and then create an Microsoft Azure client ID and secret for Asset to use for authentication.

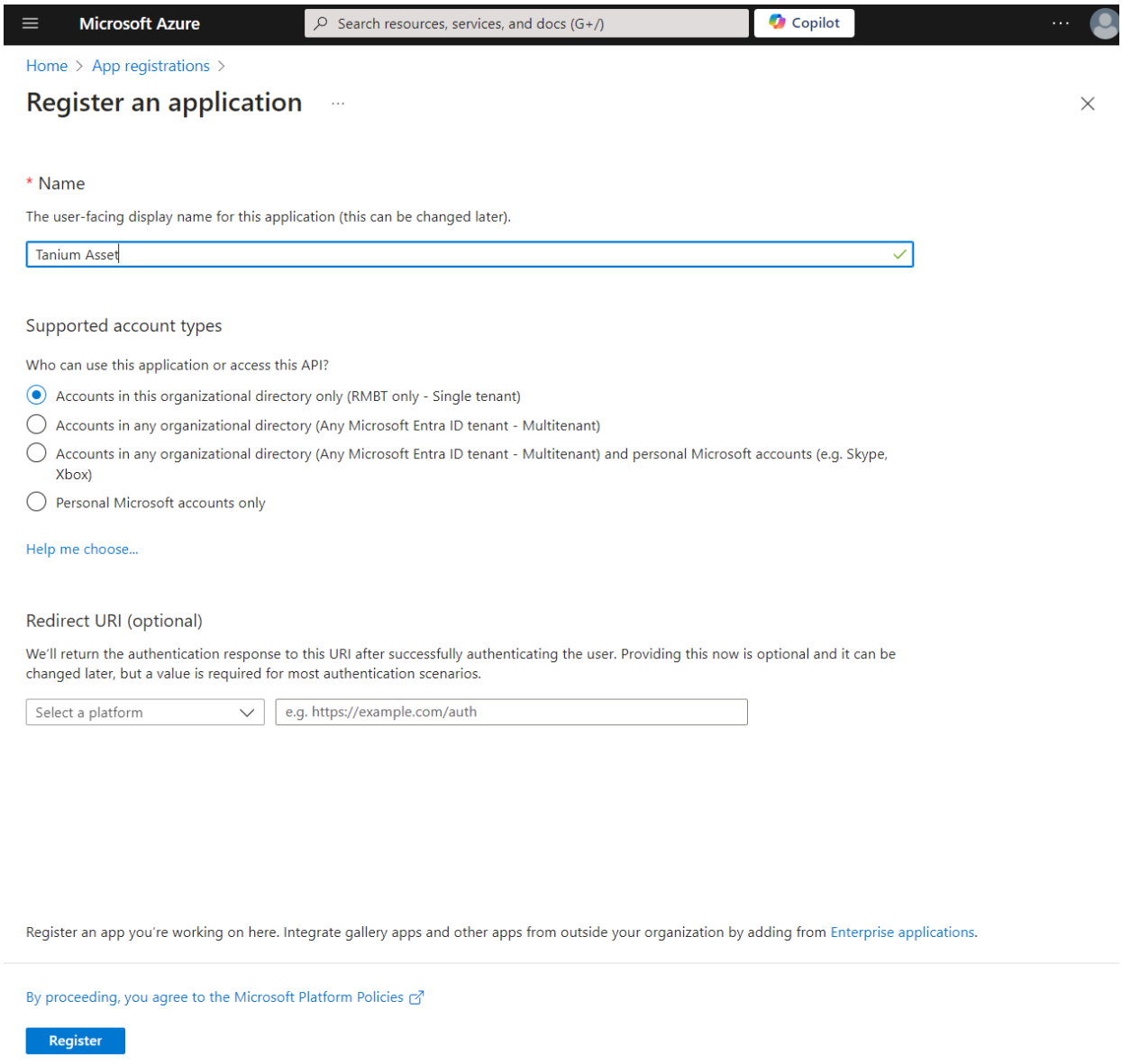
For more information, see Microsoft Entra documentation: Quickstart: Register an application with the Microsoft identity platform.

©2026 Tanium Inc. All Rights Reserved

1. In the Microsoft Azure portal, go to **App registrations** and click **New registration**.



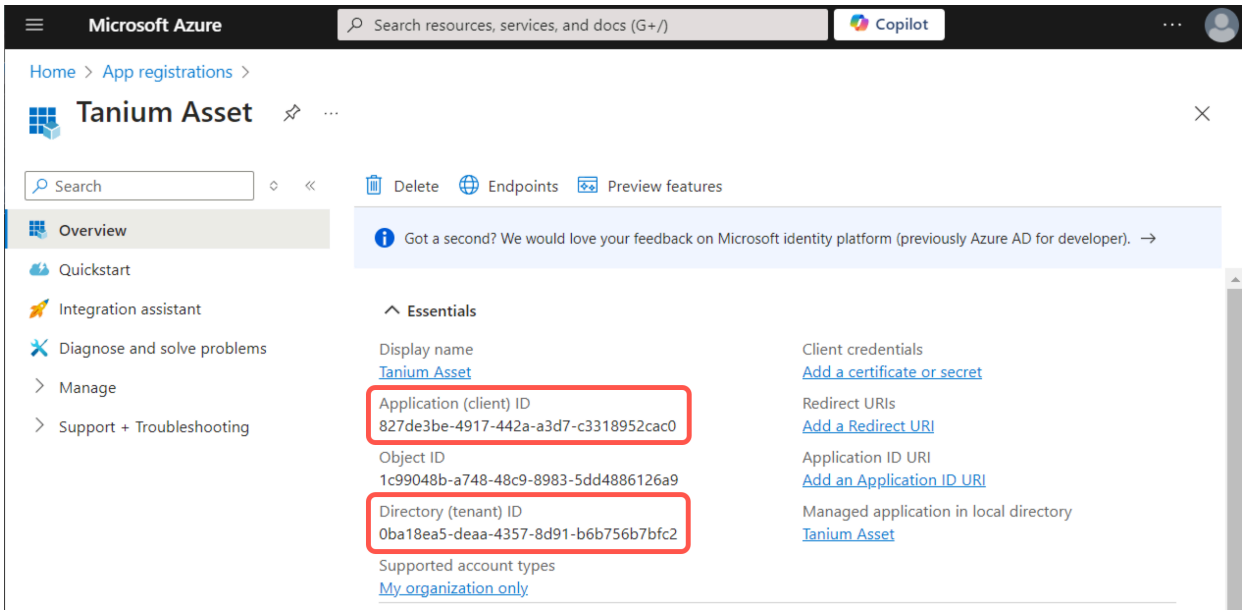
2. Enter a name for the Asset registration and then select the supported account types. When finished, click **Register**.



Tip: For more information about how to register an application, see [Microsoft Entra documentation: Quickstart: Register an application](#).

©2026 Tanium Inc. All Rights Reserved

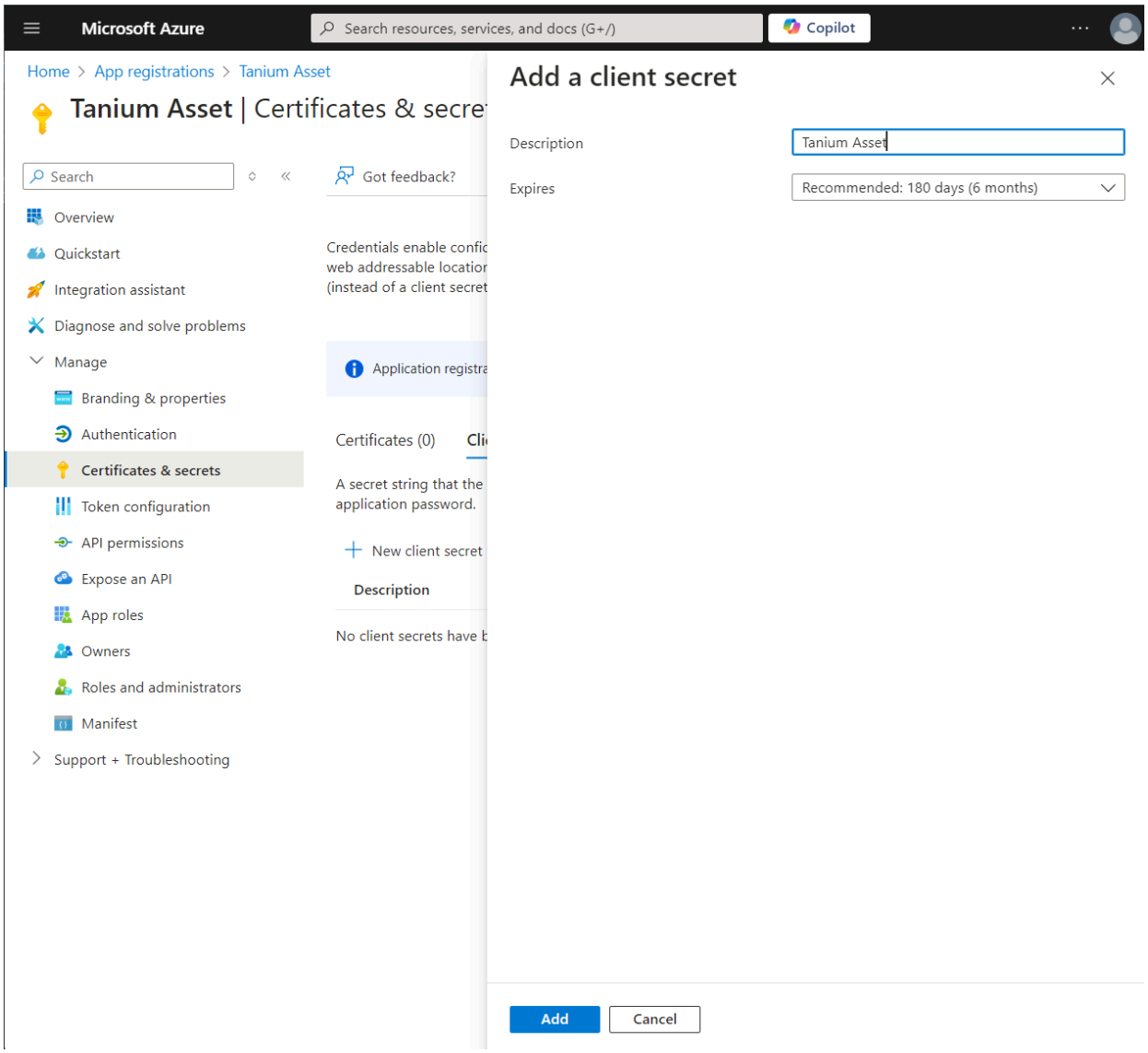
3. Record the **Application (client) ID** and **Directory (tenant) ID**.



4. Add a client secret.

   Go to **Certificates & secrets**, open the **Client secrets** tab, and click **New client secret**. Enter a description and expiration for the secret and then click **Add**.

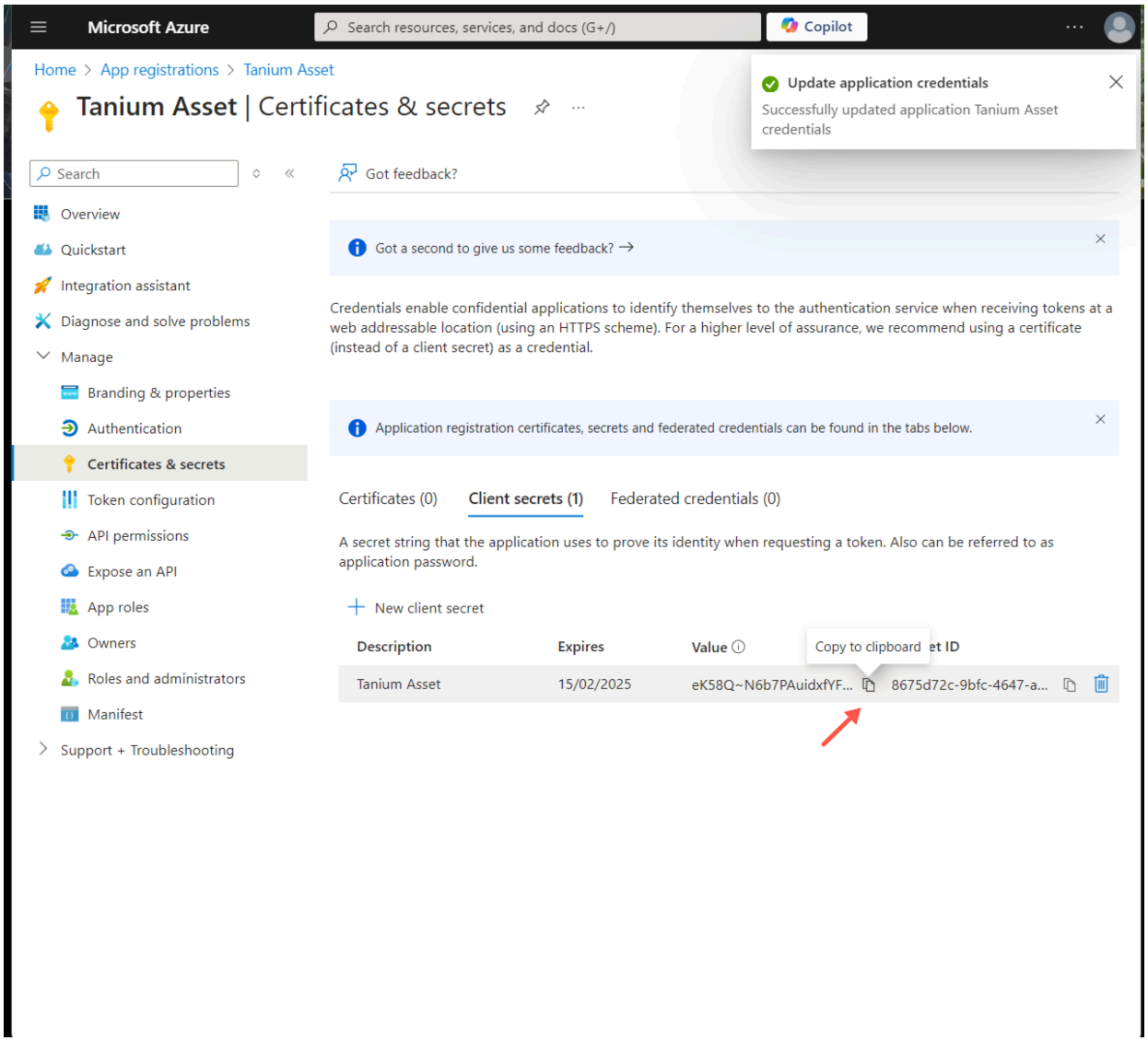
©2026 Tanium Inc. All Rights Reserved



Tip: For more information about how to create a client secret, see Microsoft Entra documentation: Quickstart: Add a client secret

5. After you add the client secret, record the **Value** for the client secret and save it to a secure location.

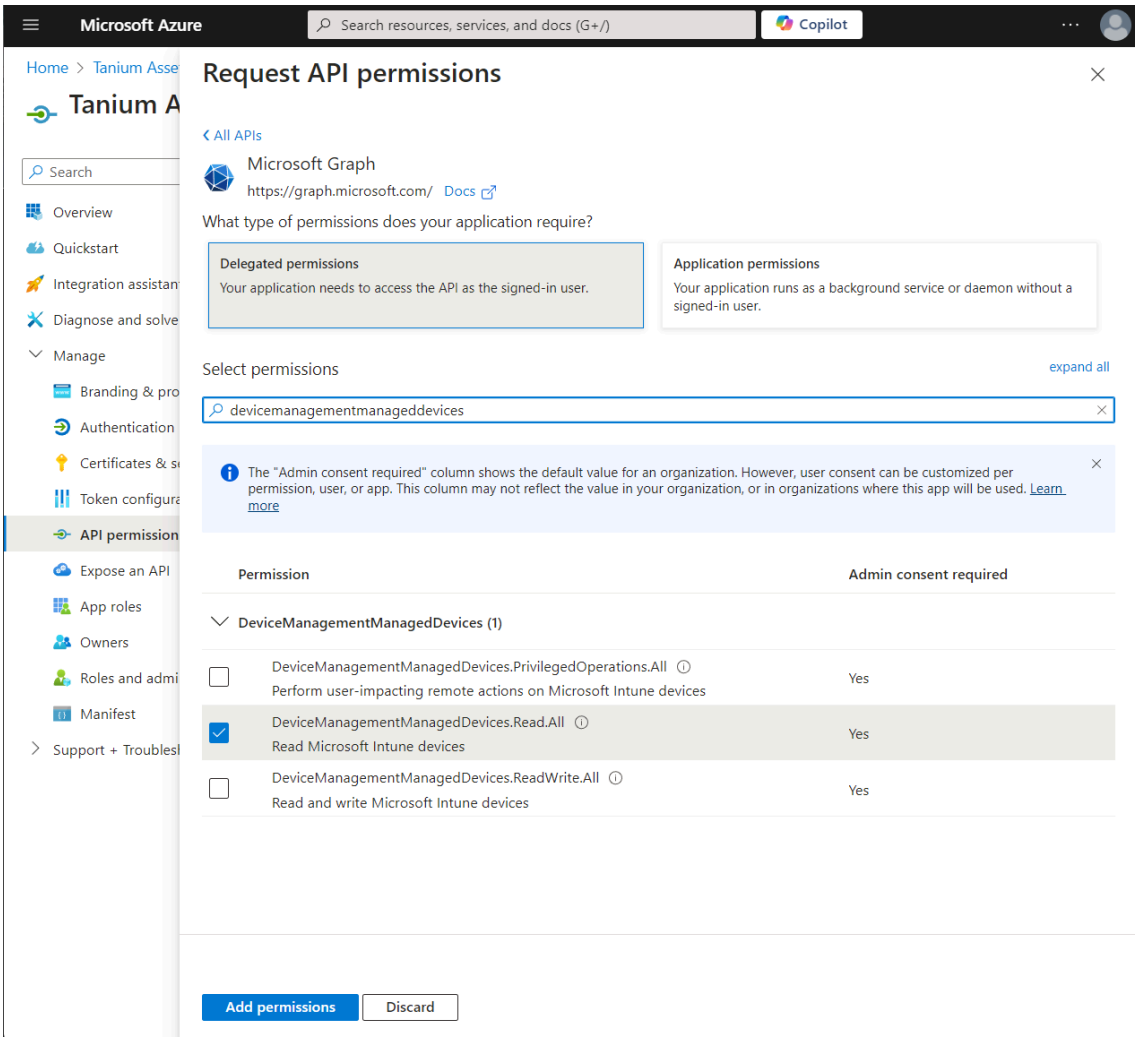
©2026 Tanium Inc. All Rights Reserved



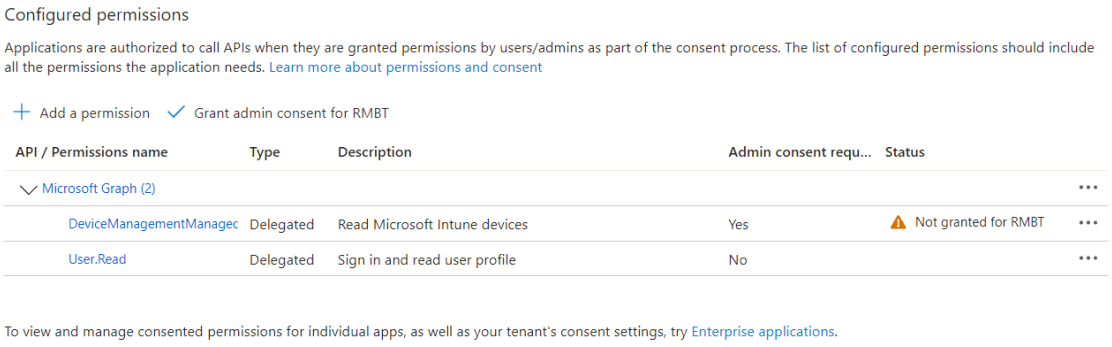
Important: You cannot see the client secret value again after you leave this page.

6. Add the **DeviceManagementManagedDevices** permission to the application registration.
    a. From the left-hand navigation menu, go to **API permissions**.
    b. Click **Add a permission**.
    c. Select **Microsoft Graph > Application Permissions**.
    d. Search for **DeviceManagementManagedDevices**.
    e. Select the **DeviceManagementManagedDevices.ReadAll** permission and then click **Add Permissions**.

©2026 Tanium Inc. All Rights Reserved

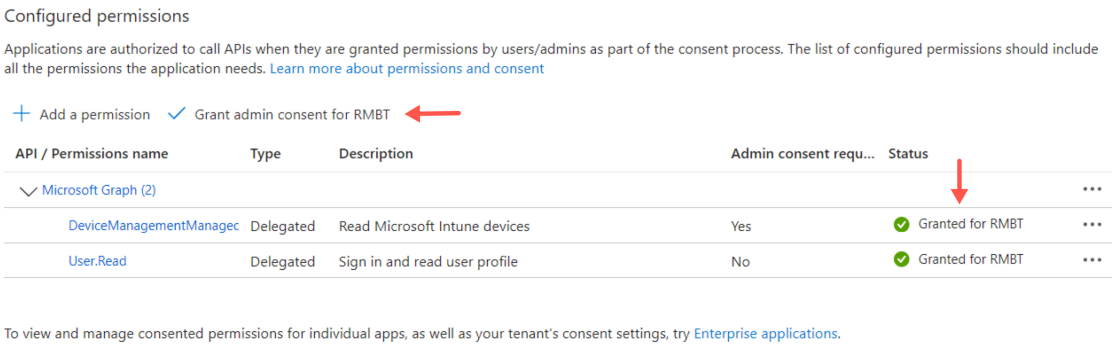


f. The configured API permissions appear with the added **DeviceManagementManagedDevices** permission.



g. Click **Grant admin consent for <your_tenant>**. A message appears to confirm that admin consent is granted to the permissions.

©2026 Tanium Inc. All Rights Reserved



(Optional) Include Microsoft Intune devices in Asset views

About this task

By default, Tanium Asset views do not include devices managed using Tanium Connector for Microsoft Intune. If you want to include these devices, configure Asset to include devices managed using Tanium Connector for Microsoft Intune.

Important: Do not enable this without understanding potential third-party provider and integration costs and limitations. Enabling this includes additional data in an Asset view, which might result in additional bandwidth and storage use, monetary charges, and other related costs.

1. From the Main menu, go to **Modules** > **Asset** > **Overview**, and then click Settings.
2. From the **Advanced** tab, in the **Tanium Entity Providers** section, click to enable **Microsoft Intune-Mobile Device** in addition to any other third-party providers that you want to enable.
3. Click **Save**.

Create the Microsoft Intune source

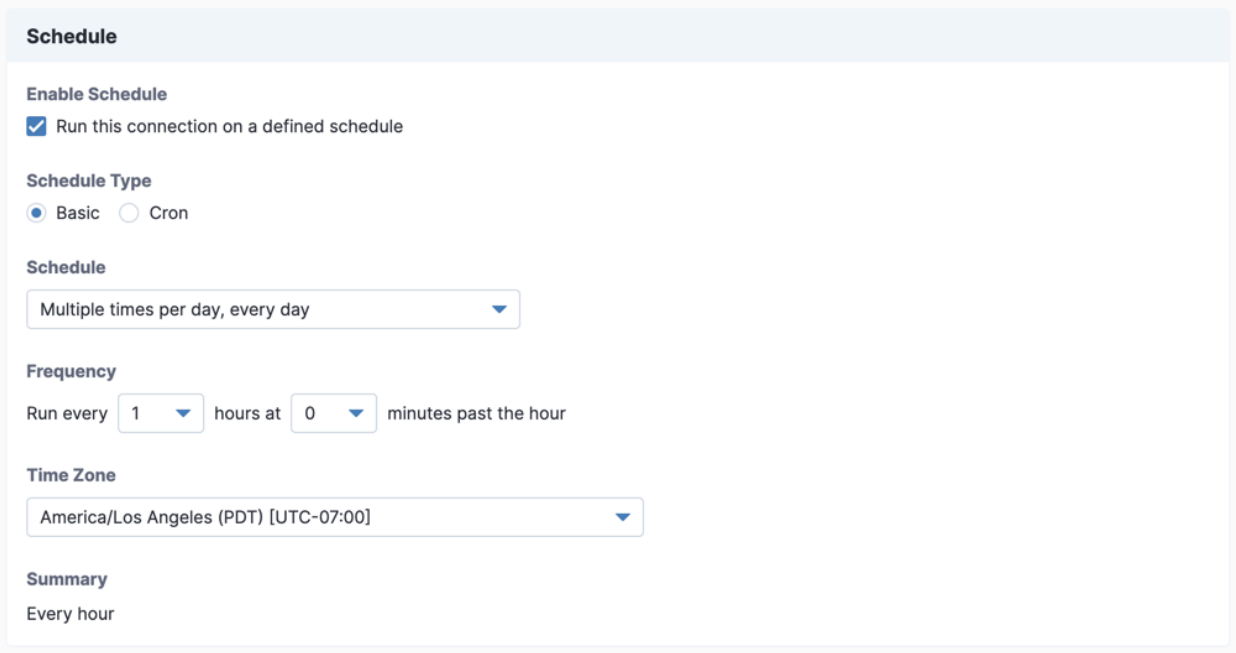
Before you begin

Complete Create a Microsoft Azure client ID and secret on page 71.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management** > **Sources**.
2. Click **Create Source**.
3. Specify a **Name** for the source.
4. In the **Provider** field, select **Microsoft Azure**.

©2026 Tanium Inc. All Rights Reserved

5. In the **Type** field, select **Microsoft Intune**.
6. Set the **Log Level**.
7. In the **Directory (tenant) ID** field, specify your Entra ID tenant ID.
   For more information about how to find your tenant ID, see Microsoft Azure documentation: Find your Microsoft Entra tenant.
8. In the **Application (client) ID** field, specify the Microsoft Azure client ID that you created.
9. Provide the **Client Secret** that you generated in the Microsoft Azure Portal.
10. Click **Verify Connection** to confirm that the connection is valid. This step is required to save the source.
11. (Optional) Enable reconciliation if you want to merge assets in this source with matching Tanium-managed assets during the import process. For more information, see Asset reconciliation on page 65.
12. (Optional) In the **Data Retention** section, configure when to purge stale assets from this source. The minimum value is 7 days, maximum is 180 days. Default is 30 days.
13. Configure the schedule.
    The schedule determines how often to import asset data from the Microsoft Intune data into the Asset database.



This database provides data for offline assets. You can create a standard interval or a cron schedule. For example, you might create one of the following intervals based on your

©2026 Tanium Inc. All Rights Reserved

environment size:

- Less than 50,000 devices: every 1-2 hours.
- Less than 250,000 devices: every 4 hours.
- Greater than 500,000 devices: contact Tanium Support to configure the import schedule. For more information, see Contact Tanium Support on page 222.

For more information about the cron syntax, see Reference: Cron syntax on page 223.

14. Click **Create** to save your changes.

Result

Tip: Fields in the Microsoft Intune source automatically map to the corresponding fields in the Asset database. After you create the source, you can edit the source to view the default field mappings.

Monitor compute source import runs

About this task

You can view logs for the latest runs of each source from the **Schedules** page.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Schedules**.
   Step result:

   The **Schedules** page appears with the **Import Schedules** tab open.

2. Click Expand next to the source that you want to monitor.
   Step result:

   The **Run History** section appears and contains up to the last four runs for the source.

3. To view details for a log, click the value in the **Start Time** column.

   Tip: Alternatively, to view the log for the most recent run, click the value in the **Last Run** column. If the value of the **Last Run** column is not clickable, either the source is not a compute source or there is no log available.

4. Review the following sections on the **Job Run History** page:

©2026 Tanium Inc. All Rights Reserved

Available sections on the Job Run History page

Section	Description
Run Results	Shows the start date for the latest run, the duration of the run, and the status.
Total Devices	(AWS organization accounts) Contains a donut chart that shows the number of devices in the run for each individual account.
Devices	(Non-AWS organization accounts) Contains a chart that shows the number of devices by region. Hover over the bar chart in any region to view the number of devices that were created, updated, or were reconciled in the run.
Devices By Account	(AWS organization accounts) Select an account to view a chart that shows the number of devices by region for the account.
Errors	Contains a log of errors encountered during the run in a JSON format. Errors appear in two sections: • **jobErrors**: Contains any overall errors for the run, such as if import credentials have expired or if the role for the IAM provider is not valid. • **batchErrors**: Contains errors for individual assets.

Edit source

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Sources**.
2. In the row of the source that you want to edit, click Edit .
3. Edit any fields as necessary. Fields that are not editable appear as disabled.

> **Note:** Each external source contains a **Source ID** and **Namespace**. These fields are not editable.
>
> - The **Namespace** value is required for some mutations and queries in GraphQL APIs. For more information about Asset mutations and queries, see Reference: Gateway examples for Asset on page 237.
> - Use the **Source ID** value to filter reports by the source ID. For more information, see Create report filters on page 59.

©2026 Tanium Inc. All Rights Reserved

4. When finished, click **Update**.

Disable sources

About this task

Data imports for a source run on a configured schedule by default. You can disable this schedule to resolve issues or to run the import manually.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Schedules**.
2. In the row of the import schedule for the source that you want to disable, click Edit .
3. Clear the **Run this connection on a defined schedule** setting, and then click **Update**.
4. If you want to manually run an import, go to the **Inventory Management** > **Schedules** page. In the row of the source that you want to import on the **Import Schedules** tab, click Run Now .

©2026 Tanium Inc. All Rights Reserved

Configuring profiles

Configure profiles to identify files and file types on the endpoint. With Asset, you can create the following types of profiles:

- **File evidence profile**: The file evidence profile collects data for the Flexera integration only. It defines the computer groups to scan for file evidence and how often to scan. Asset can collect file evidence from endpoints in the Tanium Asset File Evidence action group, which typically targets all computers. For more information about the Flexera integration, see Exporting data on page 138. For more information about creating an action group in Asset, see Configure Asset

  To make collected file evidence data available to Flexera, create a Flexera File Evidence View. For more information, see Configuring views on page 123.

- **SBOM profiles**: The SBOM add-in identifies candidate files on the endpoint by querying Index CX, which has indexed the file system, for the files and file types that you specify in the SBOM profile.

Important: SBOM profiles are only available if you have a license for Tanium SBOM. For more information, see Creating a Software Bill of Materials on page 159.

Data collected by the file evidence profile

Important: Asset collects file evidence data exclusively for Flexera. File evidence data is not reflected in Installed Applications or Software Inventory and Usage.

When you create the file evidence profile, Asset instructs Index CX to search designated folders for executable files at rest and capture specific properties for each file. Index CX searches folders listed in the following table.

©2026 Tanium Inc. All Rights Reserved

Folders searched for files

Operating system	Folder
Linux and macOS	• /opt • /usr • /var
Windows	C:\Program Files

From these folders, Index CX collects evidence for files with the following extensions:

- *DTAG
- *PTAG
- *SYS2
- .*WTAG
- .EXE
- .LAX
- .SIG
- .SYS

Index CX then captures the following attributes for each file:

Attributes captured for each file

Attribute	Operating system
Company	Windows only
Description	Windows only
File name	Windows, macOS, Linux
File path	Windows, macOS, Linux

©2026 Tanium Inc. All Rights Reserved

Attribute	Operating system
File size	Windows, macOS, Linux
File version	Windows only
Language	Windows only
Product name	Windows only
Product version	Windows only

Create the file evidence profile

About this task

Create the file evidence profile to configure settings for targeted endpoints so that you can gather file evidence data.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Profiles**.
2. Click **Create Profile** and select **File Evidence**.

   Tip: You can create one file evidence profile in Asset. If the **File Evidence** option does not appear, ensure that the file evidence profile does not already exist.
3. In the **General Information** section, specify the **Profile Name** and optional **Profile Description**.
4. In the **Target** section, click **Select Computer Groups**.
5. Select one or more computer groups to target with this profile and click **Save**.

   Note: If you change the computer group targeting at a later time, any data collected by the file evidence profile is reset.
6. In the **Settings** section, adjust the Index CX settings as needed:

©2026 Tanium Inc. All Rights Reserved

Setting	Description
Tanium Index Scan Frequency	Controls how often the Tanium Index scan runs.
Tanium Index First Scan Distribute Over Time	Sets the time distribution for the initial Tanium Index scan.

Note:

- Index CX is a service that is shared with other Tanium solutions. If you updated any Index CX settings through the configuration options in another module that uses Index CX, such as Tanium™ Threat Response, those changes are not applied to the File Evidence Index subscription. If you updated these settings globally, by using the `TaniumClient config` command or by deploying an action to endpoints to update the settings, those changes are applied to the File Evidence Index subscription.
- If other solutions use Index CX in your environment, you might see file evidence files in Asset that are not targeted by the file evidence profile, or you might see file evidence data for endpoints not targeted by the file evidence profile. It is possible the other solutions already assigned Index CX to collect this data and Asset automatically retrieves that data based on the supported file extensions.

7. Click **Create**.

Result

Note: The initial Index CX scan must finish before you can review results. The timing of the first scan depends on the **Tanium Index First Scan Distribute Over Time** setting in the profile.

After you create the file evidence profile, you can view the file evidence data in Asset or export the data to an external destination.

View file evidence data in Asset

1. Add attributes from the **Asset File Evidence** entity:
    a. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Entities & Attributes**.

©2026 Tanium Inc. All Rights Reserved

b. Select **Add Attribute** > **Add Existing Attribute**.
c. Search for the **Asset File Evidence** entity.
d. Expand the **Asset File Evidence** entity and select the attributes to add to Asset.
e. Click **Add**.

2. Add data from the attributes as columns in your reports and views.
   - For more information about how to create a report, see Building reports on page 56.
   - For more information about how to create a view, see Configuring views on page 123.

Export file evidence data

About this task

- Create a Flexera view. For more information, see Configuring views on page 123.
- Create a Flexera destination to pull file evidence data from Asset. For more information, see Exporting data on page 138.

Create an SBOM profile

About this task

Create an SBOM profile to configure SBOM settings for targeted endpoints so that you can generate and gather SBOM data.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Profiles**.
2. Click **Create Profile** and select **Software Bill of Materials (SBOM)**.
3. In the **General Information** section, specify the **Profile Name** and optional **Profile Description**.
4. In the **Target** section, click **Select Computer Groups**.
5. Select one or more computer groups to target with this profile and click **Save**.

   Best Practice: Target only endpoints on operating systems that are supported by SBOM.

6. In the **Candidate Ecosystems** section, select the file types to identify on targeted endpoints.
7. In the **Settings** section, adjust the Index CX settings as needed:

©2026 Tanium Inc. All Rights Reserved

Index-CX settings available through SBOM profiles

Setting	Description
Tanium Index Scan Frequency	Controls how often the Tanium Index scan runs.
Tanium Index First Scan Distribute Over Time	Sets the time distribution for the initial Tanium Index scan.
File Exclusions by Regular Expression	Use a regular expression to specify files to exclude from file system indexes.
Directory Exclusions by Regular Expression	Use a regular expression to specify directories to exclude from file system indexes. **Best Practice:** Use directory exclusions rather than file exclusions since directory exclusions are more efficient.

Note:

- The SBOM Index subscription calculates SHA-256 hashes and limits the scope of the scan to all local drives.
- If you updated any Index CX settings through the configuration options in another module that uses Index CX, such as Threat Response, those changes are not applied to the SBOM Index subscription. If you updated these settings globally, by using the `TaniumClient config` command or by deploying an action to endpoints to update the settings, those changes are applied to the SBOM Index subscription.

8. Click **Create**.

Note: The initial Index CX scan must finish before you can review SBOM results. The timing of the first scan depends on the **Tanium Index First Scan Distribute Over Time** setting in the SBOM profile.

View profile status

About this task

©2026 Tanium Inc. All Rights Reserved

Note: Asset uses Tanium Endpoint Configuration to deploy profiles to endpoints. For more information about Endpoint Configuration, see Tanium Endpoint Configuration User Guide.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management** > **Profiles**.
2. Review the **Status** column on the **Profiles** page to see the state of each profile.

Icon	Status	Description
	Unknown	The status of the profile is unknown.
	Creating	The profile is created but not yet sent to Endpoint Configuration for deployment to endpoints.
	Updating	The profile is updated but not yet sent to Endpoint Configuration for deployment to endpoints.
	Disabling	The profile is being disabled and has not been sent to Endpoint Configuration for deployment to endpoints.
	Pending	The profile is waiting for approval from Endpoint Configuration.
	Deployed	The profile is approved and sent to Endpoint Configuration for deployment to endpoints.
	Rejected	The profile is rejected and any previous profile is still deployed to endpoints.
	Not Deployed	The profile is not deployed to endpoints.

Edit a profile

About this task

Important: If you edit the file evidence profile and update the computer groups to target, Asset deletes any previously collected data from the Asset database.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management** > **Profiles**.
2. Select the profile.

©2026 Tanium Inc. All Rights Reserved

3. Click **Edit**.
4. Make the necessary changes and click **Save**.

Delete a profile

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Profiles**.
2. Select one or more profiles and then click **Delete**.

Result

When you delete an SBOM profile, the SBOM Index CX subscription is removed for endpoints that were targeted by that profile.

©2026 Tanium Inc. All Rights Reserved

Configuring attributes

You can configure the attributes that get populated as asset data. These attributes can come from Tanium or a configured source entity. In Asset, an entity is a group of similar attributes. Attributes become the columns that you can include in your reports.

Asset solution content

When Asset is installed, solution content is also installed. Some of this solution content is similar to the content packs that were imported when you installed Tanium. In most cases, the Asset version of the content adds attributes or improves the information beyond the existing sensor. The Asset custom content is hidden on the **Administration** > **Content** > **Sensors** page.

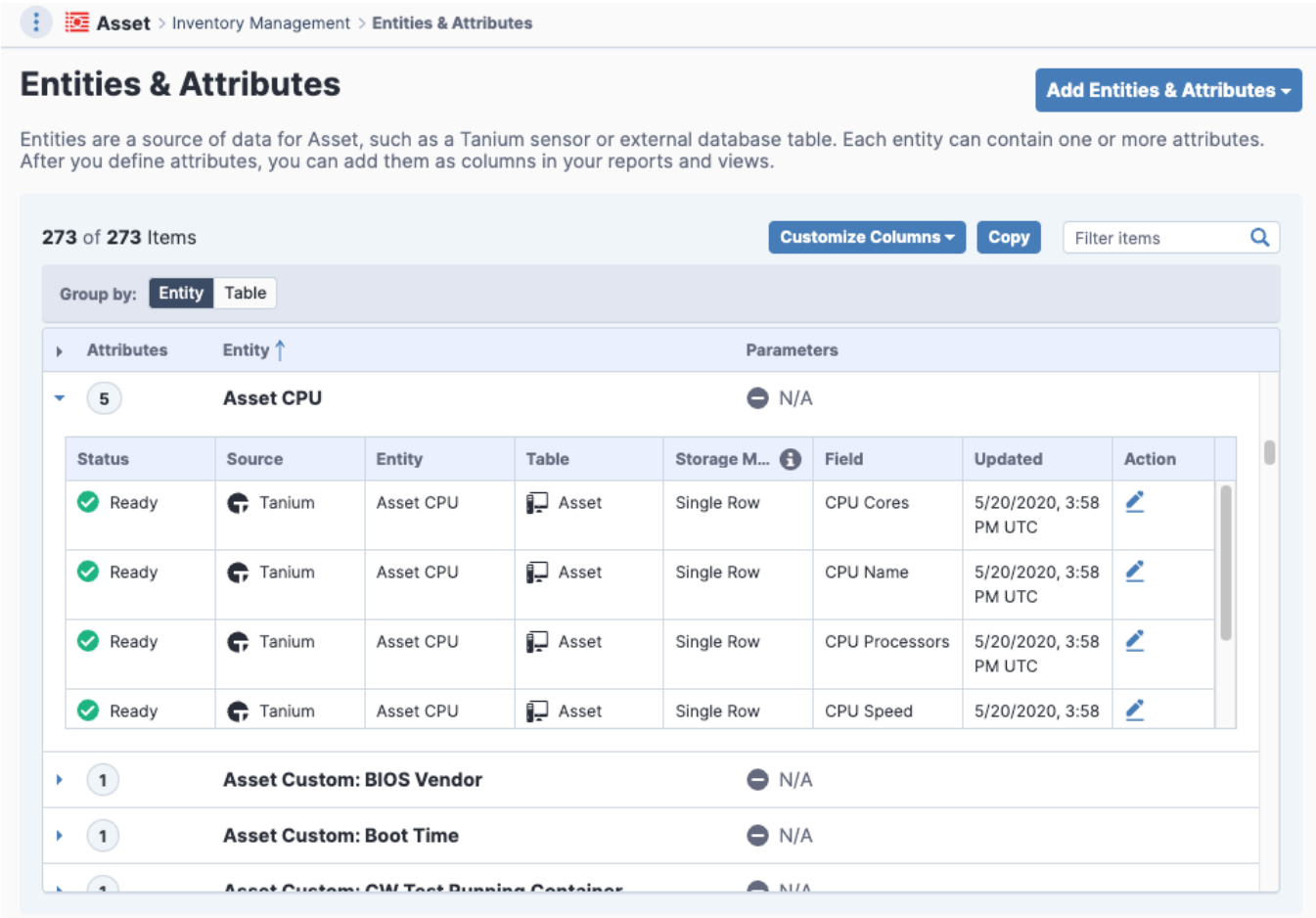
View and edit default asset attributes

About this task

By default, Asset imports the most common attributes from Tanium sensors.

Figure 4. Example Entities & Attributes page

©2026 Tanium Inc. All Rights Reserved



To view the list of default attributes:

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Entities & Attributes**.
2. **Optional:** You can group the attributes by the table in the Asset database or the entity type (for Tanium attributes, the entity types match the sensor names).
3. **Optional:** To sort a column, click the column header.
4. **Optional:** To filter the list, use the **Filter Items** field.
5. **Optional:** To customize the columns that appear and column order, click **Customize Columns**. For example, to view the column name returned from a sensor, select **Source Attribute**. You can add or remove columns, and then drag the columns to change the order.
6. **Optional:** To copy a CSV version of the data listed in the table to the clipboard, click **Copy**.
7. **Optional:** To edit an individual attribute, expand the section and click Edit .

©2026 Tanium Inc. All Rights Reserved

Normalized attributes

The **Installed Applications** table contains fields for **Normalized Name** and **Normalized Vendor**. Normalized values resolve variants on a vendor or software name. For example, the following vendor values: `CompanyName, Inc.`, `CompanyName Inc`, and `CompanyName LLC`, are resolved to `CompanyName` for the **Normalized Vendor** column.

Normalization occurs after data load. If values are in the **Name** or **Vendor** columns, a normalized value is also calculated.

Configure additional Tanium entities and attributes

You can import attributes from Tanium sensor data. For example, you might choose to import additional critical configuration information from other Tanium products, solutions, or custom content.

Important considerations for attributes

- Add sensors that return a single line when possible.
- Before you add a new attribute, determine the storage method. Using the automatic evaluation of storage method sometimes results in a single-row sensor being seen as a multiple-row sensor, which is less efficient and can have unforeseen connotations when reporting.
- Avoid adding attributes that change often, especially attributes that return a large amount of data.
- Consider how frequently Asset inventories your environment. If the attribute data becomes stale before the next scheduled import, it might not be a beneficial attribute to add.

Add attributes

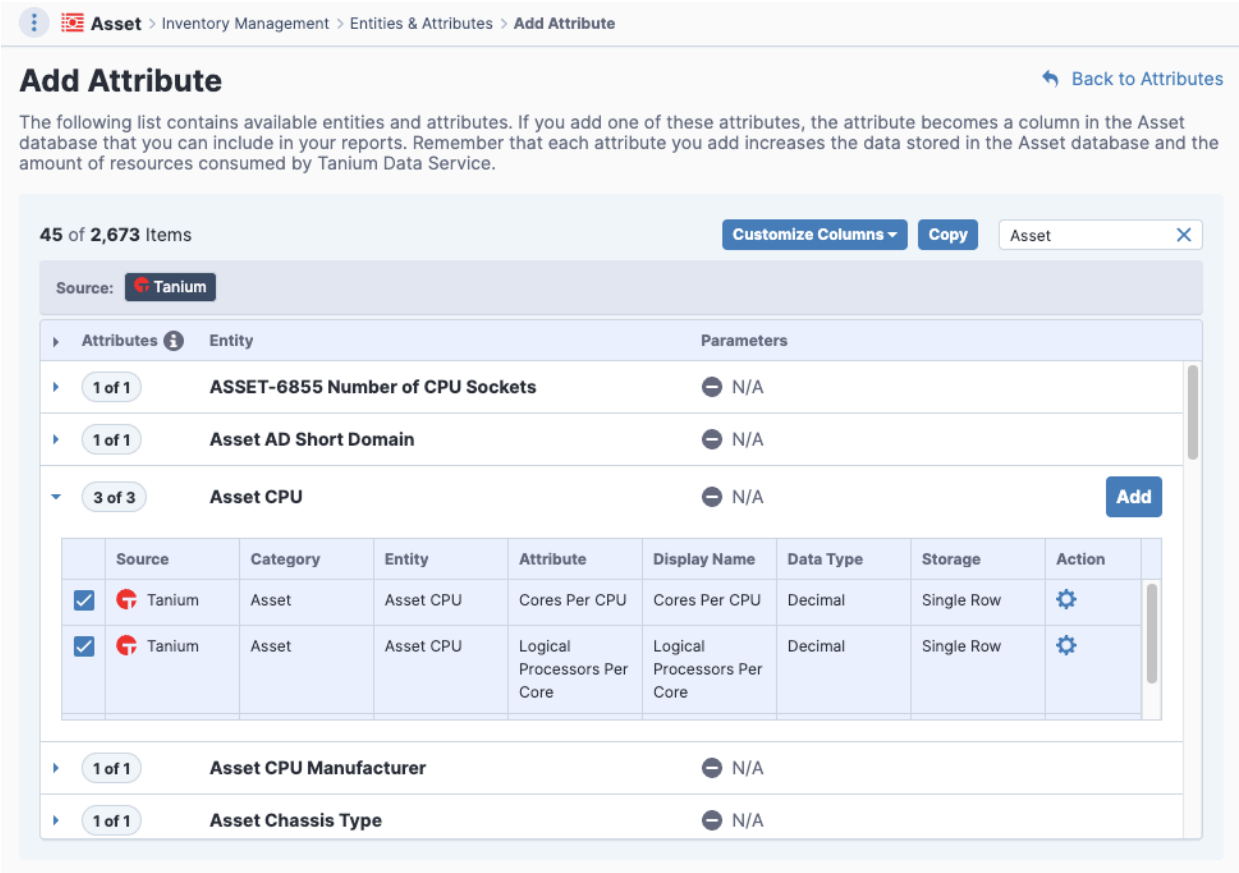
About this task



Important: This task makes changes to the Asset database. Review and verify carefully.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Entities & Attributes**.
2. Select **Add Entitites & Attributes** > **Add Existing Entities & Attributes**.
3. Search for and select the sensors from which you want to add attributes.
   To view all Asset solution content, you can search for Asset in this sensor list.

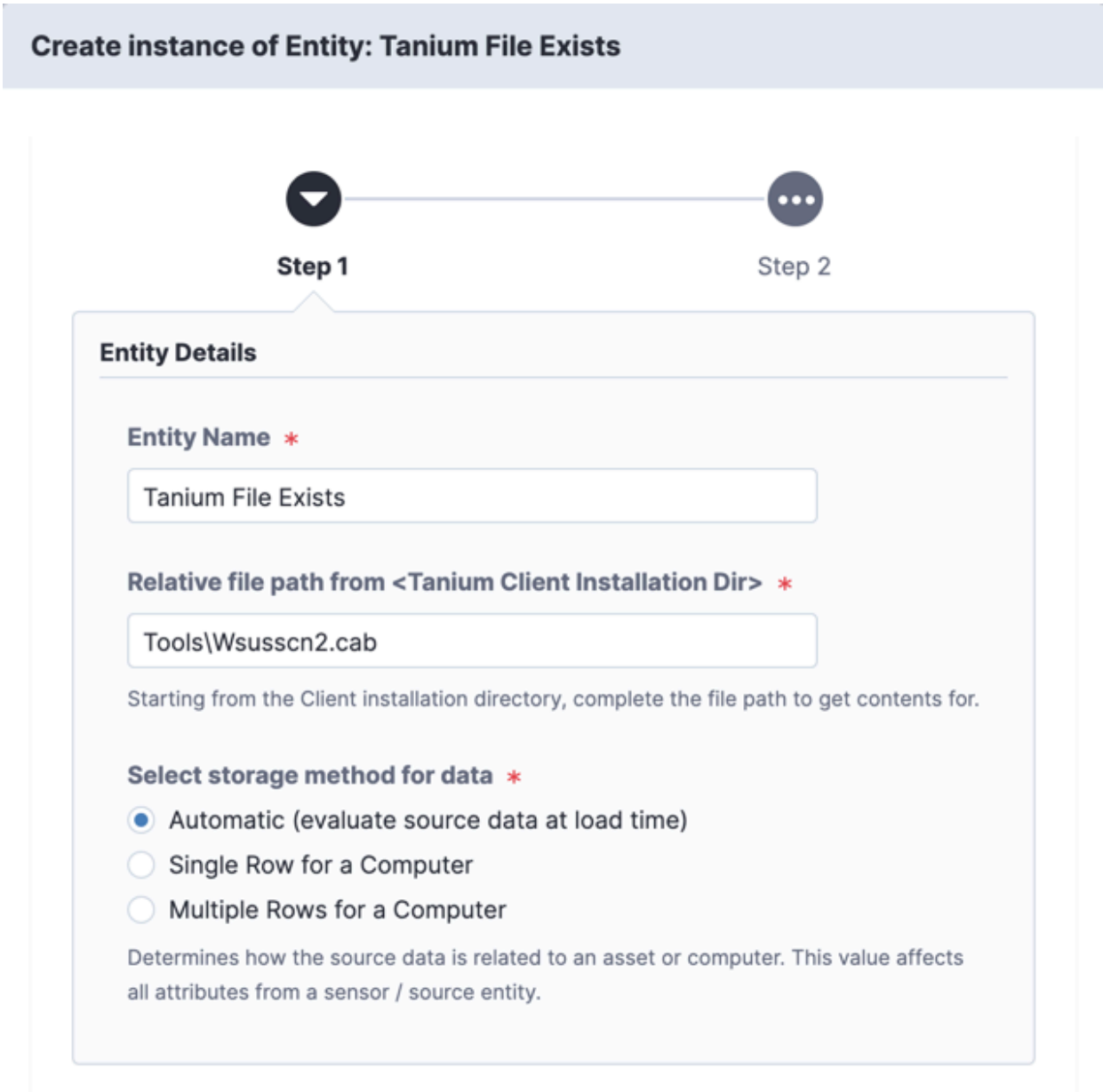


> **Note:** Data for Tanium attributes comes from sensors that are registered with Tanium Data Service. If a sensor returns results with high cardinality, Tanium Data Service automatically blocks the sensor from registration. As a result, attributes from blocked sensors do not appear as options in Asset. For more information about Tanium Data Service, see Tanium Interact User Guide: Managing Tanium Data Service.

4. (Optional) To change the data type, display name, or storage method for an attribute, expand the section for the attribute and click Settings.
5. Select the attributes that you want to import. Click **Add**.
6. If you are adding an attribute from a parameterized sensor, indicate the values that you want

©2026 Tanium Inc. All Rights Reserved

to pass to the parameters.



You can also choose how to store the data that gets returned in the database. If you set the storage method for data to be automatically evaluated at load time, this selection adds time to the load process. Click **Next**. Click **Create** and verify that the changes are correct.

7. If you are not adding an attribute from a parameterized sensor, click **Add Attribute**.

Result

After the database updates finish, you can see the new attribute in the main list of attributes in **Pending** state. The new attribute stays in pending state until the next time the Tanium source import job runs, and data gets populated in the database. For more information about how to run this job immediately, see View schedule and run import on page 117. When populated, the attribute displays

©2026 Tanium Inc. All Rights Reserved

in **Ready** state. You can add attributes that are in **Ready** state to custom reports.

Configure external attributes

Before you begin

If you are importing data into Tanium from an external data source, configure the import first. Configuring the source defines which database tables to import and how to correlate the data with the ci_item table in the Asset database. For more information, see Configuring sources on page 65.

About this task

You can import attributes from an external data source:

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Entities & Attributes**.
2. Select **Add Entities & Attributes** > **Add Existing Entities & Attributes**.
3. In the **Source** section, select the data source that you configured. You can search for and select the field that you want to add as an attribute.
4. Asset automatically converts values in the database based on the following type mapping:

   #### Field mapping conversions for external entities

SQL data type	Asset data type
BIGINT	BIGINT
DATE	DATEONLY
DATETIME, TIMESTAMP WITH TIME ZONE	DATE
BIT, BOOLEAN, TINYINT	BOOLEAN
STRING, CHARACTER VARYING (255), VARCHAR (255)	STRING
FLOAT, DOUBLE PRECISION	FLOAT
INT, INTEGER, SMALLINT	INTEGER
CHAR, NCHAR, NVARCHAR, TEXT, VARCHAR	TEXT

5. Click **Create** and verify that the changes are correct.

©2026 Tanium Inc. All Rights Reserved

> **Important:** This step makes changes to the Asset database. Review and verify carefully.

Result

After the database updates finish, you can see the new attribute in the main list of attributes in **Pending** state. The new attribute stays in pending state until the next time the **External database** job runs, and data gets populated in the database. For more information about how to run this job immediately, see View schedule and run import on page 117. When populated, the attribute displays in **Ready** state. You can add attributes that are in **Ready** state to custom reports.

Configure custom entities

About this task

You can add custom entities to the Asset database that you can update using the Asset API. Attributes in custom entities are also available to add to views in Asset and to reports through Tanium Reporting.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Entities & Attributes**.
2. Select **Add Entities & Attributes** > **Create Custom Entity**.
3. Specify a name for the entity.
4. For the **Storage Method**, select **Single row per endpoint** if the incoming data is contained in a single row. Otherwise, select **Multiple rows per endpoint**.
5. Add attributes to the entity.
    - To add one attribute that has the same name as the entity, specify a **Data Type**. You do not need to supply an **Attribute Name**; the attribute assumes the same name as the custom entity.
    - To add more than one attribute, click **+ Add Attribute**. For each attribute, specify the **Attribute Name**, **Data Type**, and whether the attribute is enabled or disabled. Attributes in custom entities are available in both Asset and Tanium Data Service when enabled. When disabled, the attribute still appears in Tanium Data Service but is not available in Asset. You can add up to 10 attributes to a custom entity.
    - For more information about Asset data types, see Asset data types on page 121.

©2026 Tanium Inc. All Rights Reserved

Tip: To use an attribute as a key for a custom source, the custom entity must be set to **Single row per endpoint** and must only contain one attribute.

6. Click **Submit**.

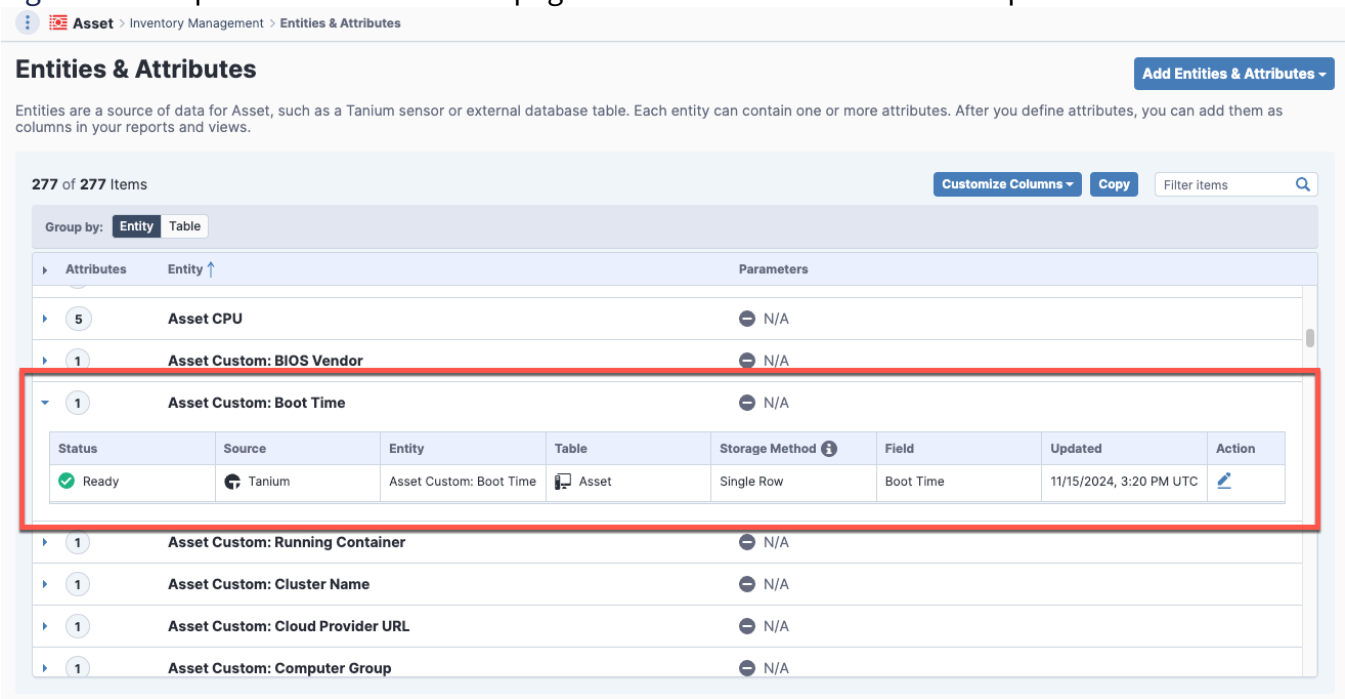
Important: This step makes changes to the Asset database. Review and verify carefully.

Virtual sensor creation

When you create a custom entity, Asset registers the custom entity as a virtual sensor in Tanium Data Service. Use the Asset API to populate data for the custom entity in Tanium Data Service. Then, on the next load from the Tanium Data Service, Asset imports the data from the virtual sensor into the Asset database, and the custom entity is available for use in Asset. You can see the new attribute on the **Entities & Attributes** page. Custom entities are prefixed with **Asset Custom:** on both the **Entities & Attributes** page and through Tanium Data Service.

For more information about virtual sensors, see Tanium Console User Guide: Virtual sensors.

Figure 5. Example Entities & Attributes page that shows the "Asset Custom:" prefix for custom entities



©2026 Tanium Inc. All Rights Reserved

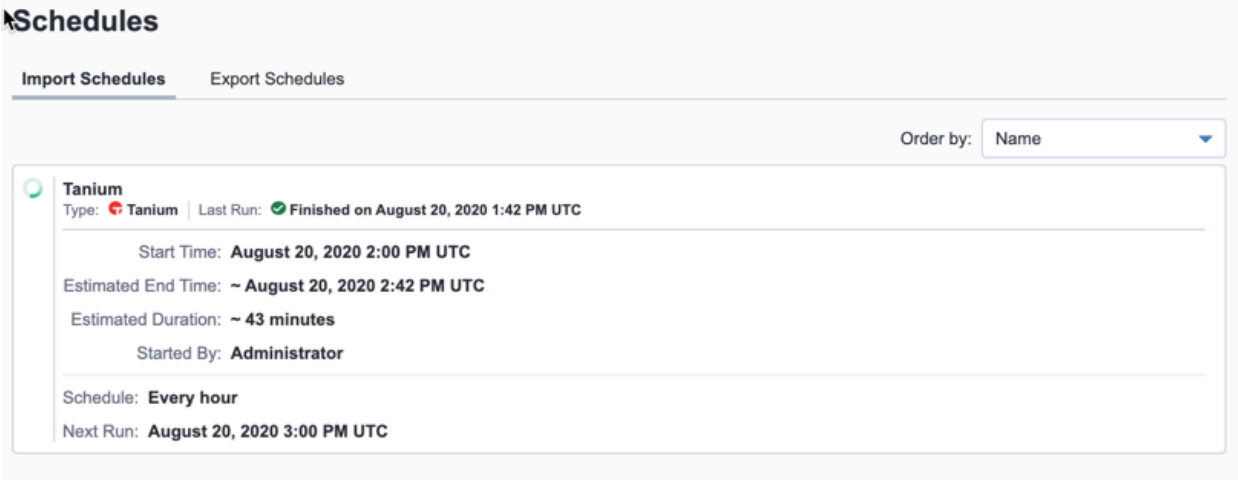
Best Practice: To optimize resource consumption by Tanium Data Service, add only low cardinality attributes to custom entities. For more information, see Tanium Interact User Guide: Resource consumption for registered sensors.

Schedule and run Asset data imports

The import asset data schedule determines how often Asset pulls data from Tanium or an external data source to save in the Asset database. This database is used to provide information for offline assets.

View schedule and run import

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Schedules**. The **Import Schedules** tab shows the schedule.



2. Click Run Now to override the schedule and have Asset immediately pull source data into the Asset database.
3. If you have any attributes that are in **Pending** state, you can watch the attributes change to **Ready** state on the **Inventory Management** > **Entities & Attributes** page. You can add attributes that are in **Ready** state to custom reports.

Result

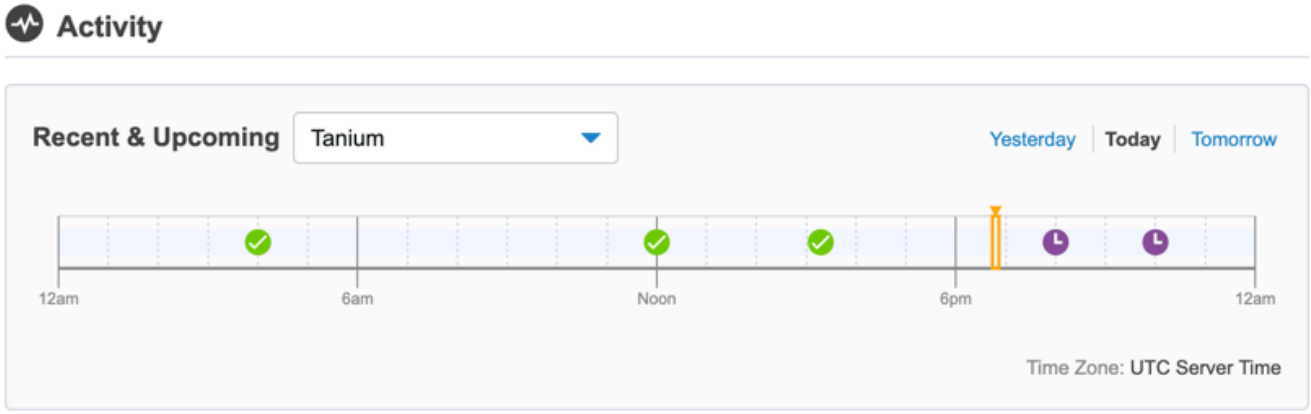
If you want to change the import schedule, update the asset source. For more information, see Configuring sources on page 65.

©2026 Tanium Inc. All Rights Reserved

View status of imports and exports

On the Asset **Overview** page in the **Activity** section, you can view a timeline of the recent imports and exports.

Figure 6. Example Activity section from the Asset Overview page



The timeline contains each job run, with one of the following statuses:

Icon	Status
	Scheduled
	Successful
	Error

To view the **Job Run History** page for runs that finished successfully or failed with an error , click the status icon of the run on the timeline.

Tip: You can view the log for the latest import of each AWS, Microsoft Azure, Microsoft Intune, and Google compute source in Asset. For more information, see Monitor compute source import runs on page 98.

Set user permissions on computers

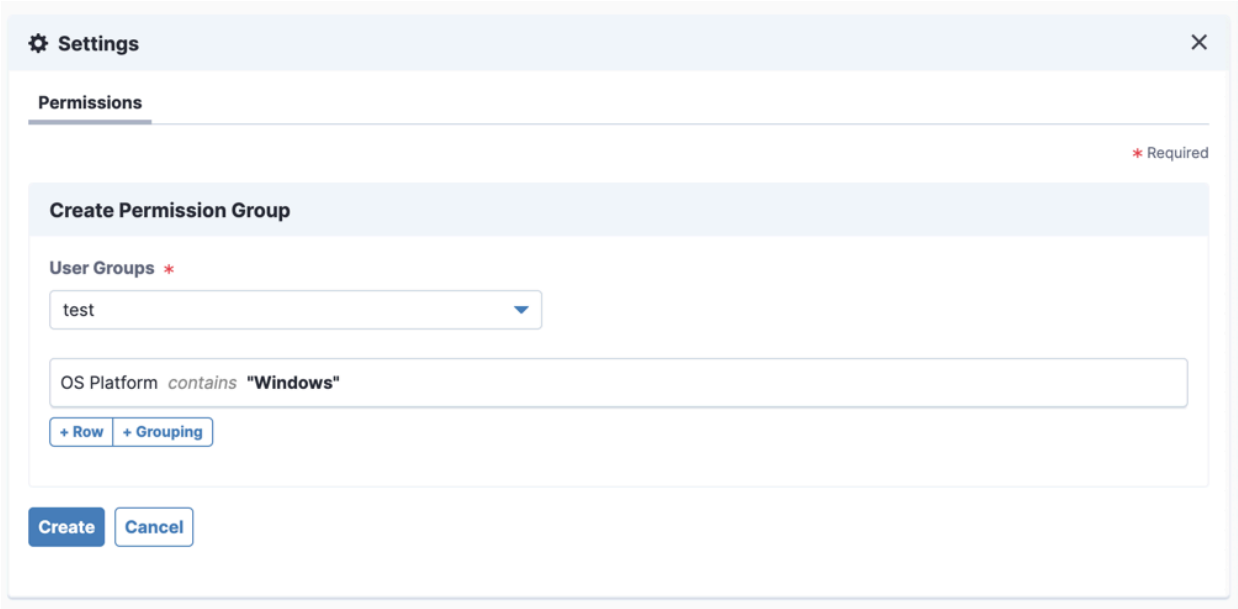
©2026 Tanium Inc. All Rights Reserved

About this task

In addition to the Asset user roles that control access to Asset reports and settings as a whole, you can define more detailed permissions on computers that are based on individual attribute values. For example, you can create permissions that assign a user group permission to access information about only Windows or only macOS operating system assets. If a user belongs to multiple user groups that are granted permissions in Asset, all user groups that are assigned to the user must evaluate to true for the corresponding assets to be visible.

Before you begin, you must have a user group to which you want to assign the Asset permissions. For more information, see Tanium Core Platform User Guide: Managing user groups. For the users in this user group to access Asset, they also must have an Asset user role assigned. For more information, see User role requirements on page 26.

1. From the Asset **Overview** page, click Settings, and then click the **Permissions** tab.
2. Click **Create Permission**.
3. In the **User Groups** list, select the user group to which you want to assign Asset permissions.
4. Add a condition.
   This list of attributes is from the **ci_item** table of the Asset database. For example, to assign the selected user group permission to view only Windows assets, set the values to `OS Platform contains Windows`.



5. Click Apply to create each condition.

©2026 Tanium Inc. All Rights Reserved

6. Click **Create**.

Delete attributes

About this task

To delete an attribute, you must disable the attribute, then remove references.

> **Note:** When you disable an attribute, Tanium Data Service unregisters the underlying sensor if the sensor is not registered by another Tanium solution.

1. Disable the attribute.
    a. From the Main menu, go to **Modules >** Asset **> Inventory Management > Entities & Attributes**.
    b. Expand the entity that contains the attribute and click Edit next to the attribute that you want to disable.
    c. Clear the **Enabled** setting. Click **Save**.
2. Remove references to the attribute from all reports, views, permissions, and ServiceNow destinations.
    a. Click Delete next to the attribute that you want to remove.
    If the option to delete an attribute does not appear, make sure to disable the attribute, wait one minute, and then refresh the **Entities & Attributes** page.
    b. A list of known locations where the attribute is used appears. Click the link for each item and then edit the item to remove the use of the attribute.
    c. Click **Refresh** to list the remaining references.
3. After you remove the references, type the name of the attribute to confirm its deletion. Click **Delete Attribute**.

Result

The attribute is deleted from the Asset database on the next load of data from Tanium Data Service.

> **Note:** When you delete the last attribute for an entity, including custom entities, Asset also deletes the entity.

©2026 Tanium Inc. All Rights Reserved

Asset data types

Fields in the Asset database must be one of the following data types:

Supported data types for Asset fields

Data type	Acceptable formats	Notes
`bigint`	Valid from -9223372036854775000 to 9223372036854775000	
`boolean`	`0/1`, `true/false`, `"true"/"false"`, and `"yes"/"no"`	
`datetime`	• ISO-8601 and RFC-2822 • Windows Management Instrumentation (WMI) • Unix Millisecond Timestamp	Datetime values are converted to UTC via the MomentJS library. • For more information about ISO-8601 and RFC-2822 formats, see MomentJS documentation: String + Format. • For more information about Windows Management Instrumentation (WMI) formats, see Windows App Development documentation: CIM_DATETIME. • Unix Millisecond Timestamp is the number of seconds (integer) since January 1st, 1970 at 00:00:00 UTC.
`decimal`	Float, Integer, String	
`duration`	BigInt	Stored in total milliseconds as a BigInt (valid from -9223372036854775000 to 9223372036854775000)
`integer`	Integer, String	• Integer is valid from -2147483647 to 2147483647 • String is valid from -2147483647 to 2147483647
`ipAddress`	String	
`size`	Acceptable unit values include the following, grouped by unit and preceded by an integer value (for example, `500gb`): • Byte: b	Stored In total bytes as a BigInt (valid from -9223372036854775000 to 9223372036854775000)

©2026 Tanium Inc. All Rights Reserved

Data type	Acceptable formats	Notes
	• Kilobyte: kb • Megabyte: mb • Gigabyte: gb • Terabyte: tb • Petabyte: pb • Exabyte: eb • Zettabyte: zb • Yottabyte: yb	
`speed`	Acceptable unit values include the following, grouped by unit and preceded by an integer value (for example, `100ghz`): • Hertz: hz • Kilohertz: khz • Megahertz: mhz • Gigahertz: ghz • Terahertz: thz • Petahertz: phz • Exahertz: ehz • Zettahertz: zhz • Yottahertz: yhz	Stored In total hertz as a BigInt (valid from -9223372036854775000 to 9223372036854775000)
`text`	String	

©2026 Tanium Inc. All Rights Reserved

Configuring views

About this task

Use views to create filtered versions of Asset data for exporting to destinations. Depending on your destination, you might need to create views or Asset might automatically create views for you.

How to create a create an Asset view for each destination

Destination	How view is created
Tanium Connect	Create custom views on page 123 .
Flexera FlexNet Manager Suite 2019 R2.2 or later	Create Flexera views on page 127 .
Flexera FlexNet Manager Suite 2019 R1 or earlier	(Automatic) Asset creates views when you create the destination.
ServiceNow: Tanium Asset integration	(Automatic) Asset creates a view when you create the destination.
ServiceNow: Service Graph Connector	Create a ServiceNow view on page 126 .

Create custom views

About this task

You can specify attributes to include in the data set and use filters to limit the computers that are included in the view. You can include fewer attributes than the default view, depending on the use of your view.

Specify view details

1. From the Main menu, go to **Modules** > **Asset** > **Views**, click **Create Views**, and then select **Create View**. If you already created the reserved views, go to **Views** and then select **Create View**.
2. Give your view a name and description to help you remember the purpose of the view later. The view name must be unique among all views in Asset, including views created by other

©2026 Tanium Inc. All Rights Reserved

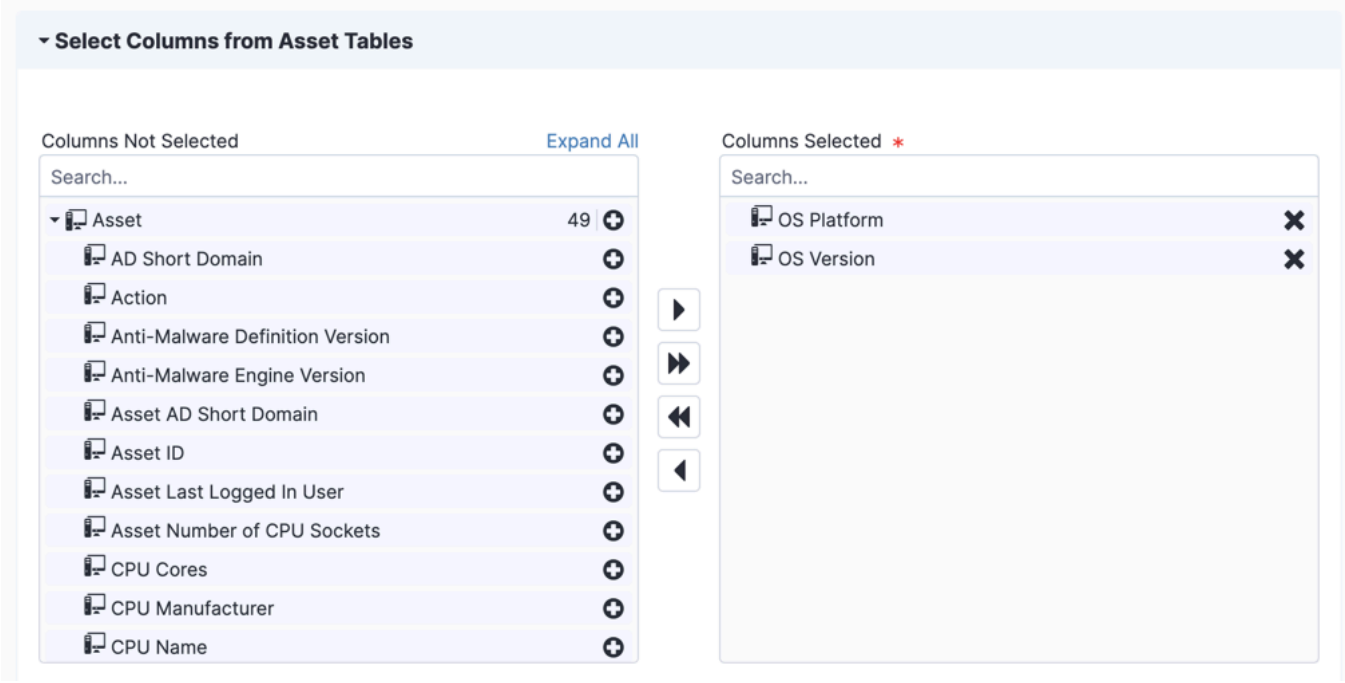
users.

Select columns

About this task

In the **Select Columns from Asset Tables** section, select the data that you want to include in your view. You can search for the column that you want to use or you can expand and collapse the data categories to find which columns you want to include.

Figure 7. Example Select Columns from Asset Tables section



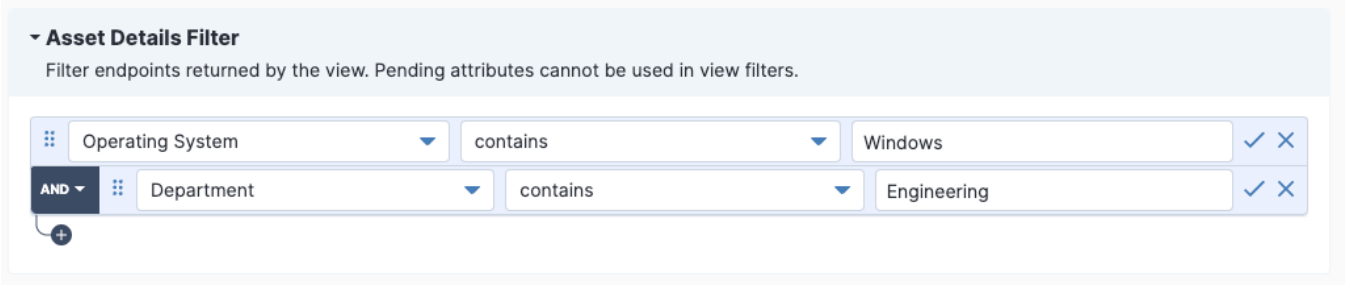
Define filter

About this task

(Optional) Add filters to limit the computers that are included in the view. You can create filters for Asset Details, Asset Installed Applications, Asset Logical Disk, Asset Network Adapter, Asset Physical Disk, Asset Windows Installer Applications, or any custom reference attributes that you have added to Asset. The available filters correspond to the data categories for the selected columns.

Figure 8. Use the Asset Details Filter section to limit computers in the view

©2026 Tanium Inc. All Rights Reserved



1. Click Add and then select **Add Row** to create a filter rule that is at the same level as the selected rule. When you create the rule, you can choose the attribute and whether the filter applies AND or OR operators with the other filters at that level. Click Apply. To create nested groups of filters, click Add and then select **Add Group**.
2. Click Expand to view a JSON representation of the rule, which can be helpful to evaluate complex filtering.
3. Go to **Views** and then select **Create Views** > **Create View**
    - To save a filter rule, click Apply.
    - To edit a filter rule, click Edit.
    - To discard changes to a filter rule you are editing, click Cancel.
    - To delete a filter rule, click Delete.

    Step result:

    By default, computers are in the view even if the fields in the filter do not have associated values. If you want to require that results are returned for the fields in the filter for a row be included in the view, select **Should be filtered out of the view** for the filter.

Filter calculations

About this task

- If you use a `Size` data type in your report (such as the **Total Disk Space** or **Free Space** fields), the values are converted with a base of 1024. For example, 450,000 MB is converted to 439 GB.
- If you use a `Date` data type in your report (such as the **Created Date** field), you can filter on dates or calendar dates. For example, if you enter a filter for `created in the last`

©2026 Tanium Inc. All Rights Reserved

`"10 Days"`, the origin date and time are calculated from the exact current date and time. If you enter a filter `created in the last "10 Calendar Days"`, the origin date and time is always 12:00 AM on the specified number of days back from the current date. You can preview the date range when you save the rule.

Finish and test the view

1. To save the view, click **Submit**.
2. Test the view. On the **Views** page, hover over a view and click Test View ✓, which runs the view for a single asset. The resulting message states whether the view can run successfully or contains errors such as pending attributes.

Create a ServiceNow view

About this task

If you are using ServiceNow Orlando Patch 7 or later, you must create a ServiceNow view. The view creates the ServiceNow-specific data that is exported from Tanium into ServiceNow.

> **Note:** You do not need to create a ServiceNow view if you are using ServiceNow: Tanium Asset integration. The view is automatically created when you create the ServiceNow destination.

> **Tip:** When you create the ServiceNow view, Asset imports the ServiceNow content pack that includes the ServiceNow view, sensors, and reports. For more information, see Import ServiceNow and Flexera content packs on page 52.

1. From the Main menu, go to **Modules** > **Asset** > **Views**, click **Create Views**, and then select **Create ServiceNow View**.
2. Test the view. On the **Views** page, hover over a view and click Test View ✓, which runs the view for a single asset. The resulting message states whether the view can run successfully or contains errors such as pending attributes.

©2026 Tanium Inc. All Rights Reserved

Create Flexera views

About this task

If you are using the Flexera FlexNet Manager Suite 2019 R2.2 or later, create the Flexera views. The views create the Flexera-specific data that is exported from Tanium into FlexNet Manager Suite.

Tip: For more information about how to set up access to the Asset API, see API access on page 39.

Note: You do not need to create Flexera views if you use FlexNet Manager Suite 2019 R1 or earlier. The views are automatically created when you create the Flexera destination.

Tip: When you create the Flexera views, Asset imports the Flexera content pack that includes the Flexera views, sensors, and reports. For more information, see Import ServiceNow and Flexera content packs on page 52.

1. From the Main menu, go to **Modules** > **Asset** > **Views**, click **Create Views**, and then select **Create Flexera View**.
   This step adds all Flexera views to Asset and then disables the **Create Flexera Views** option.
2. Test the views. On the **Views** page, hover over a view and click Test View, which runs the view for a single asset. The resulting message states whether the view can run successfully or contains errors such as pending attributes.

Export data from views

To see what data is in a view, you must create a destination.

©2026 Tanium Inc. All Rights Reserved

Tip: Using the Tanium Asset API, you can also view the data with any tool that enables you to make and inspect web requests without creating a destination.

Tanium Connect

Export data from a view to Connect destinations such as email, file, HTTP, Socket Receiver, Splunk, and SQL Server. For more information about how to configure connections and the recommended formatting options to use for each connect destination type, see Tanium Connect on page 138.

ServiceNow

The ServiceNow view contains default fields and filters for integration with ServiceNow.

This reserved view is read-only. If you want to customize the fields or filters, click Create Copy. Edit and rename the view. You might want to create a new view to limit the computers that are included in the ServiceNow export or to include new attributes in the data, in conjunction with modifying the mappings.

For more information, see ServiceNow: Tanium Asset integration on page 149.

Flexera

The Flexera views contain default fields and filters for integration with Flexera.

These reserved views are read-only. If you want to customize the fields or filters, click Create Copy. Edit and rename the view. You might want to create a new view to limit the computers that are included in the Flexera export.

For more information, see Flexera FlexNet Manager Suite: 2019 R2.2 or later on page 144 or Flexera FlexNet Manager Suite: 2019 R1 or earlier on page 145

©2026 Tanium Inc. All Rights Reserved

Monitoring software inventory and usage

About this task

You can track and report software inventory and usage (SIU) on Tanium Client managed endpoints. For example, you might report the usage of a product to confirm that your enterprise uses the number of purchased licenses for the product and reclaim unused licenses.

Important: To view the **Software Inventory & Usage** pages, you require a role with the **Asset Report read** or **Asset Configuration Item write** permission. You also must have management rights to view endpoints in SIU pages.

The process for tracking software inventory usage involves both collecting and reporting data.

1. After the Tanium Client is installed on a Microsoft Windows or macOS endpoint, Asset starts collecting software inventory and usage on the endpoint. Usage is collected each minute. The data is retained for 30 days.
2. Reports on software inventory and usage generate after the following conditions are met:
   - You enable tracking for the product in the Asset **Software Inventory & Usage** > **All Products** page.
   - The Tanium Client and applicable product are installed for at least seven days or the specified baseline period.

   Asset reports the vendor, product, version, number of endpoints with installed product, and usage of the installed product on the endpoints, including last used date and usage levels.

   Tip: The **Software Inventory & Usage** > **All Products** page shows software usage for tracked and untracked products. You can also view software usage for products that are not tracked and reported through the **SIU - Installed Products, SIU - Product First Used, SIU - Product Last Used,** and **SIU - Product Used** sensors. For more information about how to get assistance, see Contact Tanium Support on page 222.

©2026 Tanium Inc. All Rights Reserved

Enable tracking in Asset

About this task

Asset starts to collect software inventory and usage data immediately after the Tanium Client is installed on a Microsoft Windows or macOS endpoint. The **All Products** tab on the **Software Inventory & Usage** > **All Products** page shows whether a product was used within the last 90 days, regardless of the product's tracking status. Enabling tracking for a product or suite supports the following capabilities:

- Customize usage parameters that define the reporting and baseline periods and usage thresholds that determine what is considered high or normal
- Create executive reports that summarize key metrics
- Create compliance reports that expose required applications missing from endpoints

You can only track a product or suite listed on the **Software Inventory & Usage** > **All Products** page. For example, if Microsoft Office 365 is listed on the page, Asset tracks usage for the suite and not for individual products within the suite. Products with tracking enabled appear on the **Tracked Products** tab.



Important: Tracking is limited to 300 applications to minimize the impact on the Tanium Server. Only enable tracking for products with an associated cost or similar concern. Enabling tracking for all products might create Asset performance issues.

1. From the Main menu, go to **Modules** > **Asset** > **Software Inventory & Usage > All Products**.
2. Track products with one of the following methods:
    - Track a single product: In the **Track** column of the row of the product that you want to track, click the slider to toggle tracking for the product.
    - Track multiple products: To enable tracking on multiple products, select the checkbox in the first column of each product row that you want to track, and select **Actions** > **Start Tracking**. To disable tracking on multiple products, select the checkbox in the first column of each product row that you no longer want to track, and select **Actions** > **Stop Tracking**. If you select products that are tracked and products that are not tracked, the option appears as **Actions** > **Stop Tracking**; selecting that option stops tracking on any products that had tracking enabled.

©2026 Tanium Inc. All Rights Reserved

3. To edit the usage parameters, click Expand Details in the row of the product and then click **Configure Usage Parameters**.
    a. Configure the reporting and baseline periods.
    b. Specify the total number of minutes per day for high and normal usage levels. The minutes do not need to be consecutive. The default high value is 240. The default normal value is 60.
    c. Click **Save**.

View software inventory and usage

About this task

Important: Fields and columns that show AI-estimated data, such as software lifecycle details, certainty ratings, and cost and waste estimates, are available only in Tanium Cloud. They are not available in on-premises deployments and appear empty.

You can view software inventory and usage details from the **Software Inventory & Usage** and **Reports** pages. To drill down for specific endpoint details, use the **Software Inventory & Usage** > **All Products** page or use the reports available on the **Reports** page.

The **All Products** page contains two tabs. The **All Products** tab lists all installed products, whether or not tracking is enabled. The **Tracked Products** tab lists all tracked products, including products that have no installations.

View product inventory and general usage

1. From the Main menu, go to **Modules** > **Asset** > **Software Inventory & Usage** > **All Products**.
2. The tables on the **All Products** page contain the following columns:

Columns on the All Products page

Option	Description
Vendor	The vendor for the product. Click the vendor to show a list of products from that vendor on the **All Vendors** page.
Name	The name of the product. Click the product name to show details for the product. You must have tracking enabled on the product to view endpoint and usage information. For more information, see Enable

©2026 Tanium Inc. All Rights Reserved

Option	Description
	tracking in Asset on page 130 .
Installations	The number of products from the vendor that are installed in the environment.
Used	The number of installations on which usage was detected in the last 90 days by the Tanium Client.
Unused	The number of installations on which usage was not detected in the last 90 days by the Tanium Client.
Track	Contains a toggler to start and stop tracking the product. For more information, see Enable tracking in Asset on page 130 .

3. The following actions are available on the **All Products** tab:

Available actions on the All Products tab

Option	Description
Track product	In the **Track** column of the row of the product that you want to track, click the slider to toggle tracking for the product. For more information about how to bulk enable tracking for multiple products, see Enable tracking in Asset on page 130 . **Tip:** You can also enable and disable product tracking when you view details for a product.
View vendor details	In any row, click the **Vendor** to show a list of products from that vendor on the **All Vendors** page.
View product details	In any row, click the **Name** to show details for the product, including usage information if the product is tracked. From the details page, you can configure usage parameters, manage tracking for the product, and view libraries that are associated with the product. The options to **Configure Usage Parameters** , **Start Tracking** , and **Stop Tracking** appear at the top of the product details page. Click a **Version** in the grid on the product details page to open the **Version Lifecycle** page for that version. Click **Associated SBOM Libraries** to view any libraries found that might be associated with that version. For more information, see Manage products based on product usage on page 135 . **Note:** The association of a product with a library is based on product application install paths and is a best estimate.

©2026 Tanium Inc. All Rights Reserved

Option	Description
View usage in Interact	Select the checkboxes in the rows of one or more products, click **Actions**, and then select **View in Interact**. **Note:** Interact retrieves live data from a Tanium question and might not match the data stored in the Asset database.
View usage details by endpoint	Click Expand Details in the row of the product to view usage details for each endpoint. **Note:** The expanded details retrieves live data from a Tanium question and might not match the data stored in the Asset database.
View endpoint details	You can view details for an endpoint when you view usage details. a. From the **All Products** page, click Expand Details in the row of the product to view usage details for each endpoint. b. Click Endpoint Details to view basic details for the endpoint. c. Click **View Details** to open the Endpoint Details page in Tanium Reporting. For more information about the Endpoint Details page, see Tanium Reporting User Guide: View endpoint details.
Configure usage parameters	Choose one of the following: • To configure usage parameters for one product, click Expand Details in the row of the product and then click **Configure Usage Parameters**. For more information, see Enable tracking in Asset on page 130. • To configure usage parameters for one or more products, select the checkboxes in the rows of the products and then click Configure Usage Parameters.
Filter items	Enter an alphanumeric string to match text in the **Vendor** and **Name** columns.
Advanced filters	Expand **Filters** and specify any additional filters.
Download data	To export the data to a CSV file, click Export. The export includes the data that currently appears in the data grid.
Manage columns	In the header, click Customize Columns. To remove a column, clear the checkbox for the column. To

©2026 Tanium Inc. All Rights Reserved

Option	Description
	adjust the column order, click and drag the column names.

4. Click the **Tracked Products** tab to view all tracked products that are installed and not installed. To disable tracking for one or more products, click the checkboxes in their rows and click **Disable Tracking**.

View last used date of a product

About this task

The last used date is the date the endpoint most recently reported usage for the product. For endpoints shared with multiple users, this is the last date that any user on the endpoint used the product:

1. From the Main menu, go to **Modules** > **Asset** > **Reports** > **SIU Product Last Used**.
2. View the **Last Used Date** for the product.

View usage levels of a product

1. From the Main menu, go to **Modules** > **Asset** > **Reports** > **SIU Product Usage**.
2. View the **Usage** for the product.
   The report includes the average daily usage level for a product.

Product usage levels for Software Inventory and Usage

Level	Description
High	Number of minutes defined in **Software Inventory & Usage** > **All Products** > **Expand Details** > **Configure Usage Parameters** .
Normal	Number of minutes defined in **Software Inventory & Usage** > **All Products** > **Expand Details** > **Configure Usage Parameters** .
Limited	Number of minutes between one and the Normal usage level.
Baselining	Product is newly installed and not reporting usage in Asset . Go to **Software Inventory & Usage** > **All Products** > **Expand Details** > **Configure Usage Parameters** to define the **Baseline Period** .

©2026 Tanium Inc. All Rights Reserved

Level	Description
Usage not detected	Tanium Client does not detect usage of the product. For example, the baseline period has passed and the product has not been used.
Not installed	Endpoint does not have the software installed or is unable to install the software.

View installed version of product

1. From the Asset menu, go to **Reports** > **SIU Installed Products**.
2. View the **Version** for the product.

Manage products based on product usage

About this task

Based on SIU usage reports, you can install or remove products on targeted endpoints.

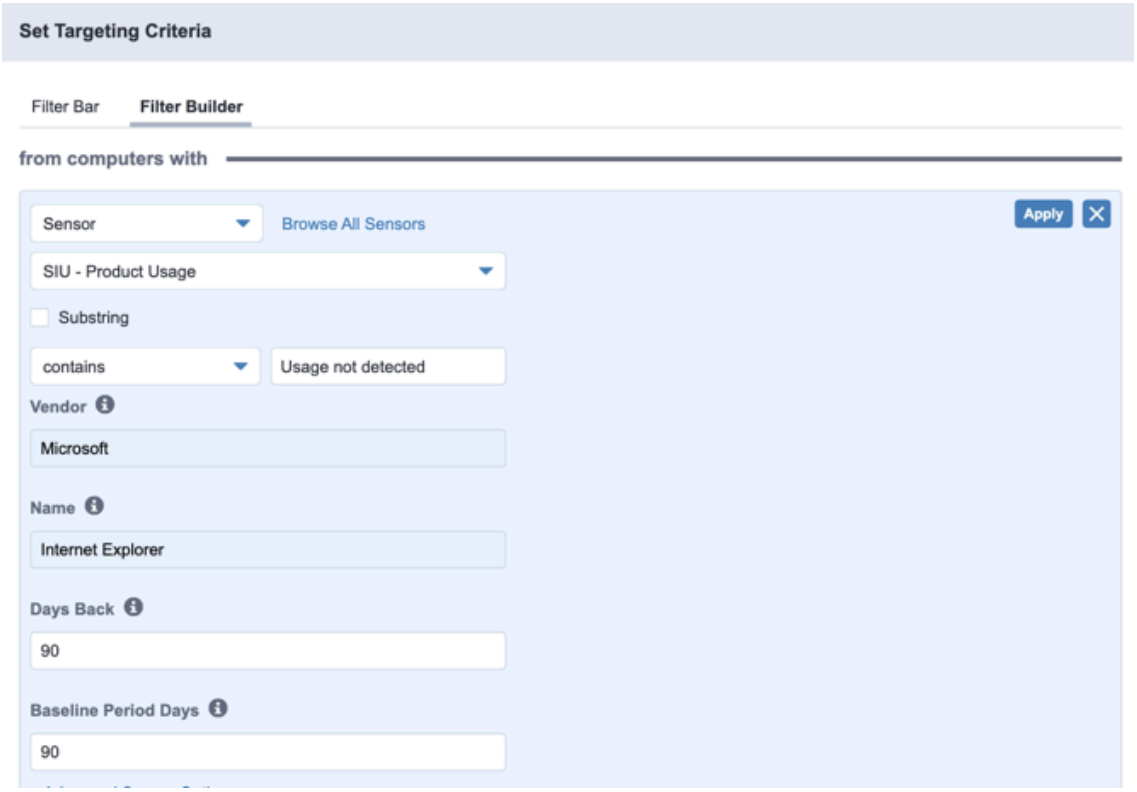
Remove unused products from endpoints

About this task

Use Tanium™ Deploy to remove unused products from endpoints. The following example removes Microsoft Internet Explorer on endpoints that have not used the software in the last 90 days. Adjust the example as needed.

1. Create a software package to remove the product. For more information, see Tanium Deploy User Guide: Create a software package.
2. Create a deployment package that uses the software package. For more information, see Tanium Deploy User Guide: Deploy a software package or bundle.
   Part of creating a deployment package is targeting endpoints. Target endpoints that have not used Internet Explorer in the last 90 days.
   a. In the **Targeting** section, click **Set Targeting Criteria**. Click **Filter Builder** > **+ Row**.
   b. Select **Sensor** and then select the **SIU - Product Usage** sensor.

©2026 Tanium Inc. All Rights Reserved



c. Select **contains** and enter `Usage not detected`.
d. In the **Vendor** field, enter `Microsoft`.
e. In the **Name** field, enter `Internet Explorer`.
f. In the **Days Back** field, enter `90`. This value specifies the maximum number of days to evaluate.
g. In the **Baseline Period Days** field, enter `90`. This value specifies the minimum number of days that Internet Explorer needs to be on the endpoint.
h. Click **Apply**.

Install required products on endpoints

About this task

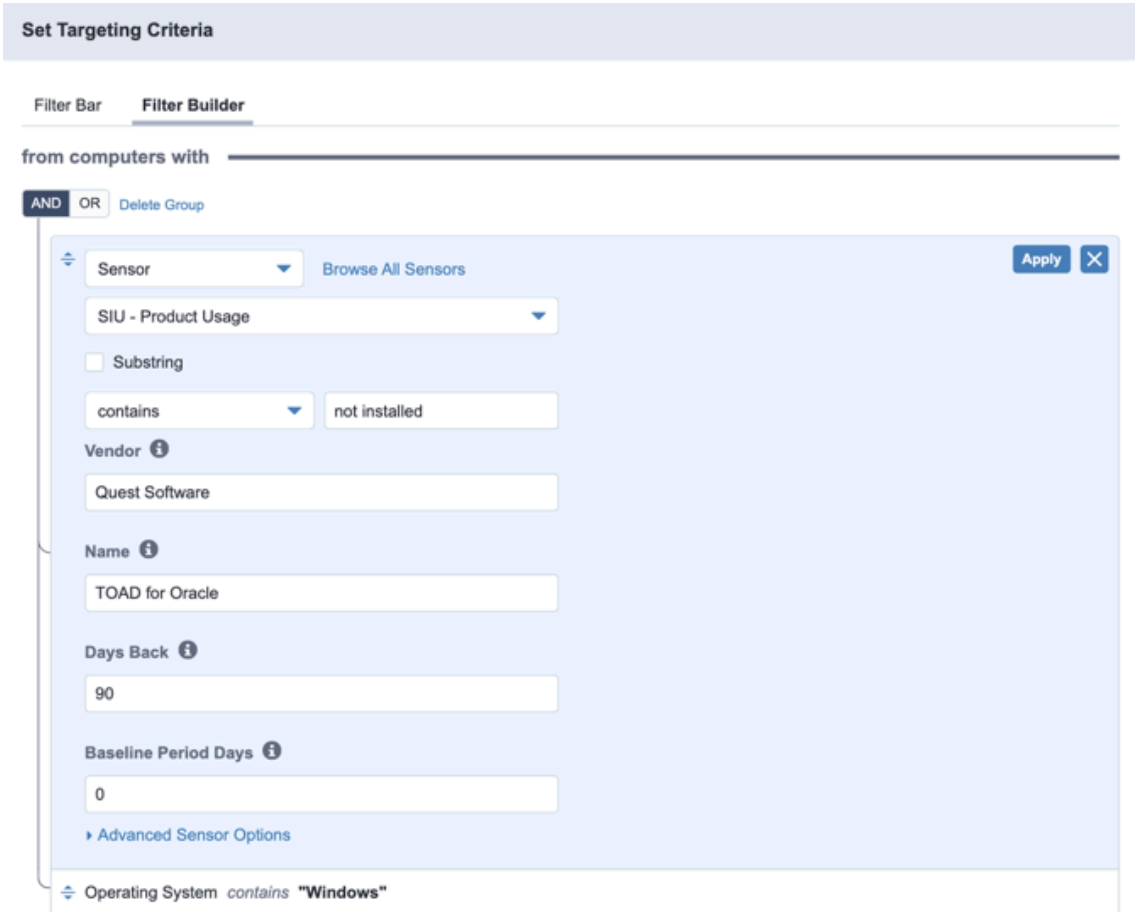
Use Deploy to install a product on endpoints. The following example installs Quest Software TOAD for Oracle on Windows endpoints that have not had it installed. Adjust the example as needed.

1. Create a software package to install the product. For more information, see Tanium Deploy User Guide: Create a software package.
2. Create a deployment package that uses the software package. For more information, see Tanium Deploy User Guide: Deploy a software package or bundle.
   Part of creating a deployment package is targeting endpoints. Target Windows endpoints

©2026 Tanium Inc. All Rights Reserved

that have not had TOAD for Oracle installed.

a. In **Endpoints to target**, click **Question Criteria** > **Filter Builder** > **Row**.
b. Select the **SIU - Product Usage** sensor.



c. Select **contains** and enter `not installed`.
d. In the **Vendor** field, enter `Quest Software`.
e. In the **Product** field, enter `TOAD for Oracle`.
f. In the **Days Back** field, enter `90`. This value specifies the maximum number of days to evaluate.
g. In the **Baseline Period Days** field, enter `0`. This value specifies the minimum number of days that TOAD for Oracle needs to be on the endpoint.
h. Click **Apply**.
i. Click **Row**.
j. Select the **Operating System** sensor.
k. Select **contains** and enter **Windows**.
l. Click **Apply**.

©2026 Tanium Inc. All Rights Reserved

Exporting data

About this task

You can configure Asset to export data to external destinations, such as Tanium Connect, Flexera, and ServiceNow.

CSV file

You can copy data from an Asset report table to the clipboard and paste the data in an application that can interpret a CSV file, such as a database. Select the rows that you want to copy and click **Copy**. You can then paste the information about the rows you selected.

To save the entire report as displayed in a CSV file, click Export . You might see an **Export requested** status message before you see a **Download** link for the CSV file. Each Asset user can export a single report at a time. Multiple Asset users can be signed in, each exporting a single report at the same time.

For scheduling, formatting, and large data sets, consider setting up a Connect destination that uses a view.

Tanium Connect

To export data from Asset to Connect destinations such as email, file, HTTP, Socket Receiver, Splunk, and SQL Server, create a connection.

Important: SQL Server on Microsoft Azure, Amazon Relational Database Service, and other database-as-a-service providers are not supported as **SQL Server** destinations.

Requirements

- Access to Connect with the **Connect User** role.
- An Asset report or view from which you want to export data. For more information, see

©2026 Tanium Inc. All Rights Reserved

Building reports on page 56 and Configuring views on page 123.

CAUTION:

Exporting reports with large data sets (more than 100,000 results) can have a significant performance impact.

If you need to export a large data set, select **Asset Computers** as the **Type** for the source and use a view. This source is available with Connect 4.8 and later. For more information about views, see Configuring views on page 123.

Create a connection

About this task

With Connect 4.3 to 4.7, choose **Asset Report** as the connection source. You can choose a predefined or custom Asset report as a connection source.

With Connect 4.8 and later, choose **Tanium Asset** as the connection source. You can choose from the following types of Asset source:

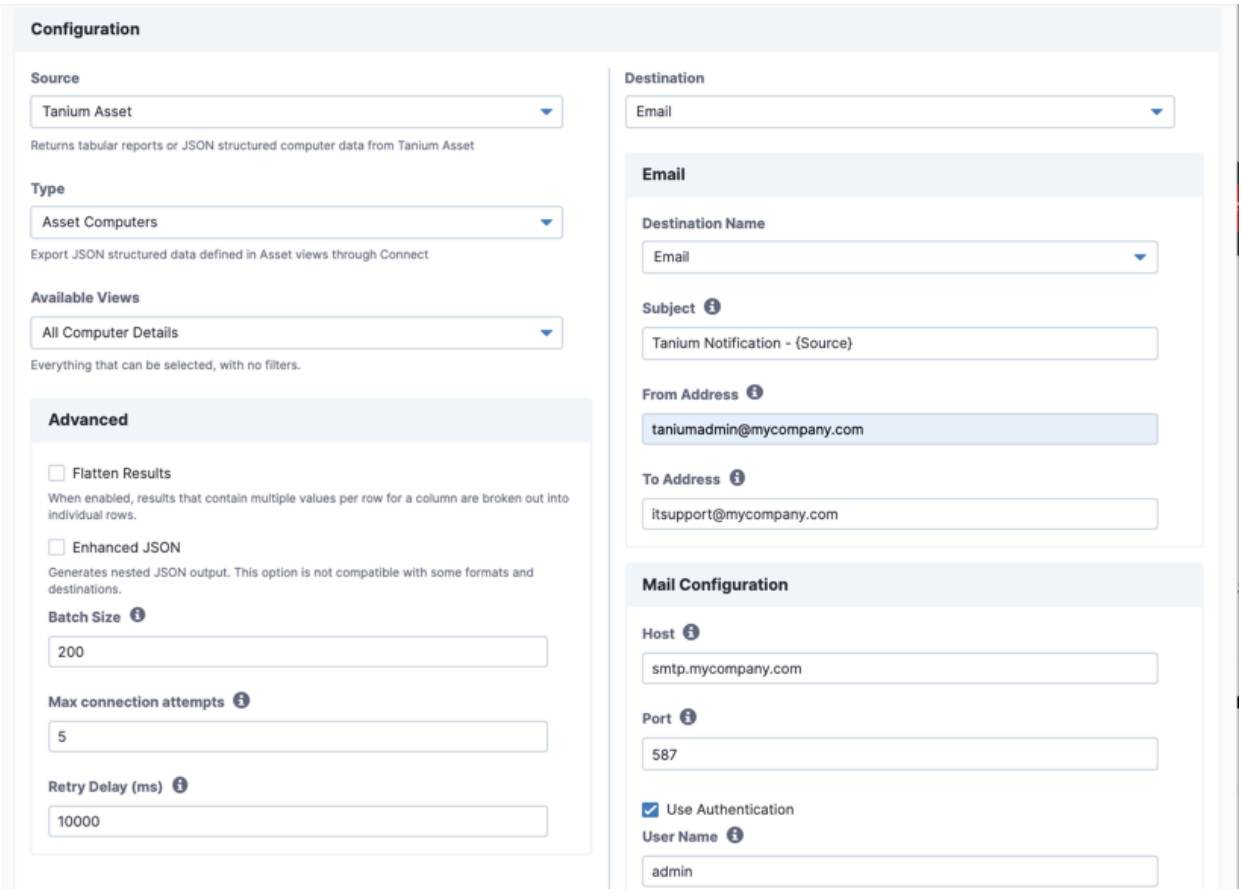
ASSET REPORTS

Select a predefined or custom report as the connection source.

ASSET COMPUTERS

1. Select any view as a connection source and export structured data using an Asset view.

©2026 Tanium Inc. All Rights Reserved



2. If you do not enable **Flatten Results**, the entire data set that is retrieved for one computer is a single record. For example, if you are exporting Installed Applications, a computer has a single row with the entire list of installed applications in that same record. Any change that is made to this data set shows up in the destination. By enabling the **Flatten Results** setting, each installed application for a computer is processed as a single record.

3. With **Enhanced JSON**, the results contain an array of objects for each reference table, instead of an array of strings, numbers, or dates for each reference attribute. The correlation between attributes and destinations can be easier to implement.

4. Use the default batch size (200). Higher batch sizes can be slower due to increased processing for each batch.

5. Configure the export format.

    - If you enable **Enhanced JSON**, you must also choose JSON as the format for your connection.

    - To customize the column names, expand the **Columns** section and click **Add or**

©2026 Tanium Inc. All Rights Reserved

Modify Columns. Change the display values in the **Destination** column as needed.

- If you customize the columns, leave the **Value Type** as **Unmodified** to get the expected object output.

COMPATIBILITY

Use the following recommendations for Enhanced JSON and Flatten Results settings for each format in Connect. If you use an unsupported combination, connection failures might occur, or incorrect data might get written to the destination.

Connect destination format compatibility

Format	Enhanced JSON Support	Recommendation
CEF	✗	Use Flatten Results
CSV	✗	Use Flatten Results
Delimiter separated	✗	Use Flatten Results
Elasticsearch	✓	Use Enhanced JSON without Flatten Results
HTML	✓	Use Flatten Results without Enhanced JSON
JSON	✓	Use Enhanced JSON without Flatten Results
LEEF	✗	(Optional) Use Flatten Results
SQL Server	✗	(Required) Use Flatten Results
Syslog	✗	(Optional) Use Flatten Results

FILTERING NO RESULTS AND ERRORS

About this task

Asset automatically filters `no results` and common error messages and does not send that data

to the connection destination.

EXAMPLES

Compare the data that is returned from Asset installed applications.

EXAMPLE: ENHANCED JSON

```
{
        "Computer Name": "WIN-2012-R2",
        "Asset Installed Applications": [{
                "name": "Tanium Server 7.2.314.3019",
                "version": "7.2.314.3019",
                "vendor": "Tanium Inc."
        }, {
                "name": "Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.23026",
                "version": "14.0.23026.0",
                "vendor": "Microsoft Corporation"
        }, {
                "name": "Microsoft SQL Server 2012 Native Client",
                "version": "11.3.6540.0",
                "vendor": "Microsoft Corporation"
                }]
}
```

EXAMPLE: FLATTENED JSON

```
[{
        "computer name": "WIN-2012-R2",
        "name": "Tanium Server 7.2.314.3019",
        "vendor": "Tanium Inc.",
        "version": "7.2.314.3019"
}, {
        "computer name": "WIN-2012-R2",
        "name": "Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.23026",
        "vendor": "Microsoft Corporation",
        "version": "14.0.23026.0"
}, {
        "computer name": "WIN-2012-R2",
        "name": "Microsoft SQL Server 2012 Native Client",
        "vendor": "Microsoft Corporation",
        "version": "11.3.6540.0"
}]
```

For more information about how to create connections, see Tanium Connect User Guide.

Flexera

You can configure Flexera One or Flexera FlexNet Manager Suite to pull data from Asset.

©2026 Tanium Inc. All Rights Reserved

Flexera One

If you use Flexera One with the IT Visibility or IT Asset Management applications, you can use Tanium as a data source.

> **Important:** Tanium Core Platform 7.6 and later no longer supports basic authentication for API integrations. Use Tanium API tokens for all connections. For more information about API tokens, see Tanium Console User Guide: Managing API tokens.

Before you begin

Create a Tanium REST API authentication token to use to authenticate from Flexera One. For more information, see API access on page 39.

For more information about token-based authentication with Flexera One, see Flexera One documentation: Tanium Adapter Enhanced To Support Token Based Authentication and Flexera One documentation: Tanium Adapter.

FLEXERA ONE IT VISIBILITY

For more information about Tanium with Flexera One IT Visibility, see Flexera One documentation: Getting Started with IT Visibility and Flexera One documentation: Uploading Inventory Data into IT Visibility.

FLEXERA ONE IT ASSET MANAGEMENT

For more information about Tanium with Flexera One IT Asset Management (formerly known as FlexNet Manager Suite Cloud), see Flexera One documentation: Managing Tanium Connections.

©2026 Tanium Inc. All Rights Reserved

Note:

- To create the Flexera views, from the Main menu, go to **Modules** > **Asset** > **Views**, click **Create Views**, and then select **Create Flexera Views**.
- Steps 1a and 1b in the "Configuring Integration with Tanium" section of Flexera One documentation: Managing Tanium Connections are no longer applicable because staging databases are not used by Flexera One. The API is used for data exports.

Flexera FlexNet Manager Suite: 2019 R2.2 or later

If you have FlexNet Manager Suite 2019 R2.2 or later, you can use the Tanium Connector in FlexNet Manager Suite (FNMS) and the existing Tanium Client on your endpoints to export inventory data from Tanium into FNMS. Asset includes content with sensors that are specific to Flexera, including MS Exchange server, SQL server, **Last Logged In**, **CPU Details** > **Total Physical Processors**, **OS Version**, **Short Domain**, and so on.

Important: Tanium Core Platform 7.6 and later no longer supports basic authentication for API integrations. Use Tanium API tokens for all connections. For more information about API tokens, see Tanium Console User Guide: Managing API tokens.

FLEXNET MANAGER SUITE REQUIREMENTS

- FlexNet Manager Suite 2019 R2.2 or later
- FlexNet Beacon 14.2 or later

TANIUM REQUIREMENTS

- Tanium Server 7.3.0 or later
- Tanium Asset 1.11 or later

©2026 Tanium Inc. All Rights Reserved

Important: You do not need to configure a Flexera destination in Asset. If you already have a Flexera destination configured in Asset that you set up for a previous version of Flexera, disable the destination after you complete the integration instructions.

BEFORE YOU BEGIN

Create a Tanium REST API authentication token to use to authenticate from Flexera FlexNet Manager Suite. For more information, see API access on page 39.

INTEGRATION INSTRUCTIONS

For more information about integration prerequisites and instructions, see Flexera documentation: Managing Tanium Connections.

Note:

- The provided link is to the FlexNet Manager Suite 2022 R2 (On-Premises) documentation. For other versions, go to https://docs.flexera.com, select **FlexNet Manager Suite** and the version that you are using, and click the HTML link for **FlexNet Manager Suite - Online Help**. Search for Tanium and open the "Managing Tanium Connections" topic.
- To create the Flexera views, from the Main menu, go to **Modules** > **Asset** > **Views**, click **Create Views**, and then select **Create Flexera Views**. Do not edit or delete these views.
- Steps 1a and 1b in Flexera documentation: Managing Tanium Connections are no longer applicable because staging databases are not used by Flexera FlexNet Manager Suite 2019 R2.2 and later. The API is used for data exports.

Flexera FlexNet Manager Suite: 2019 R1 or earlier

If you have Flexera FlexNet Manager Suite 2019 R1 or earlier, you can use the Asset Flexera destination to populate endpoint information in FNMS. When you create a Flexera destination, you enable the Flexera-specific content, and a set of custom reports and views are created that include

©2026 Tanium Inc. All Rights Reserved

the results of these sensors. To send the results of these reports to Flexera, a set of connections in Tanium Connect are automatically created that connect to the SQL database. Flexera communicates with this SQL database to populate information.

REQUIREMENTS

- Access to Connect with **Connect User** role.
- Connect 4.3.0 or later. With Connect 4.8.0 and later, you can configure your Flexera connections to use views, which is better for large environments.
- An SQL server to use for staging the Flexera data. This database can use Windows or mixed mode authentication. For more information, see Microsoft Docs: Authentication in SQL Server.

CONFIGURE FLEXERA STAGING DATABASE

About this task

You must have an SQL database configured that implements the required Flexera database schema.

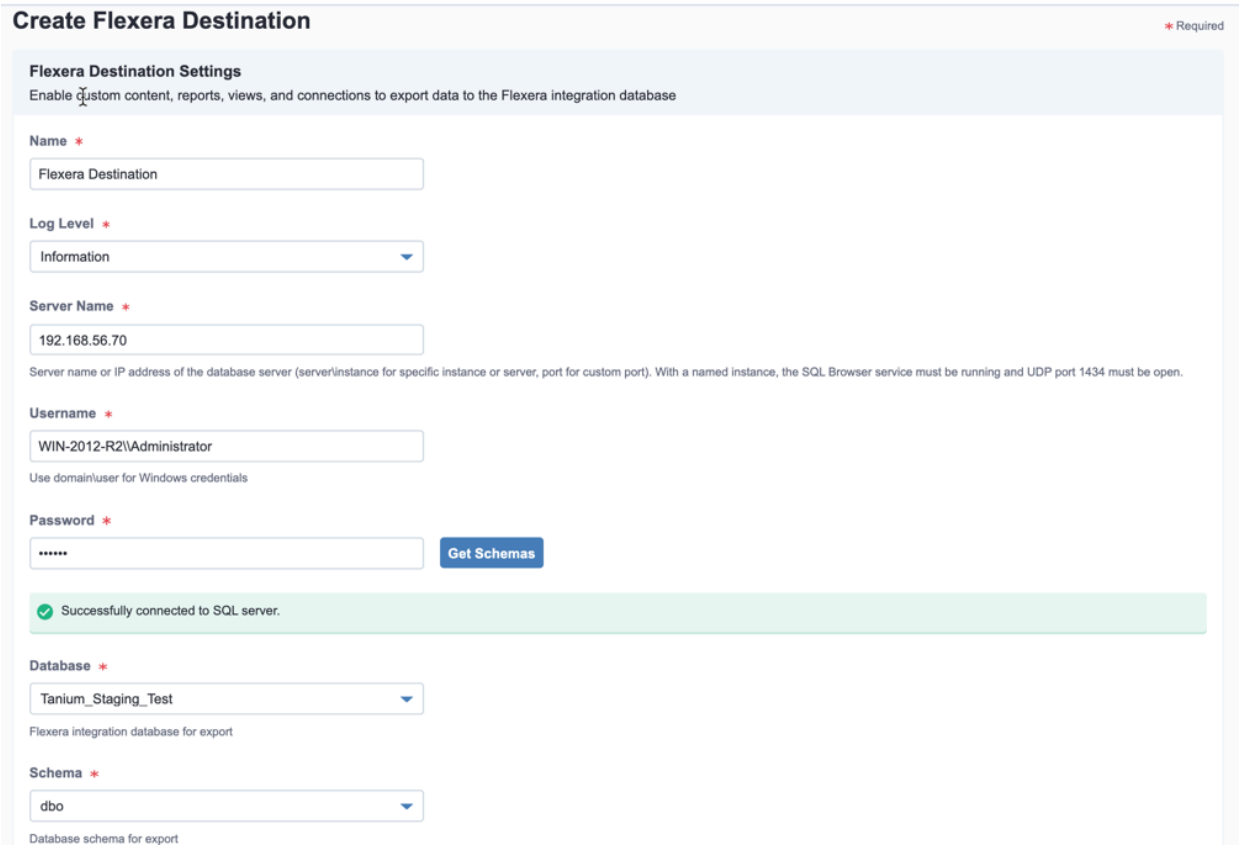
Use the following query to create the required tables and schema for the Flexera staging database: *<Module Server>*\services\asset-service\content\flexera\CreateTaniumStagingDatabase.sql

For more information about how to configure Microsoft SQL database to stage data for Flexera, Contact Tanium Support on page 222.

ADD FLEXERA DESTINATION

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Destinations**.
2. Click **Create Destination** > **Flexera Destination**.
3. Edit the Flexera settings, including URL and credentials for the SQL server, log level, and the schedule at which you want the export to occur.

©2026 Tanium Inc. All Rights Reserved



Click **Get Schemas**. When you click this button, a connection is established with the SQL server that looks for databases that match the basic required schema to export Asset data. If a database matches these requirements, the database appears in the **Database** and **Schema** fields.

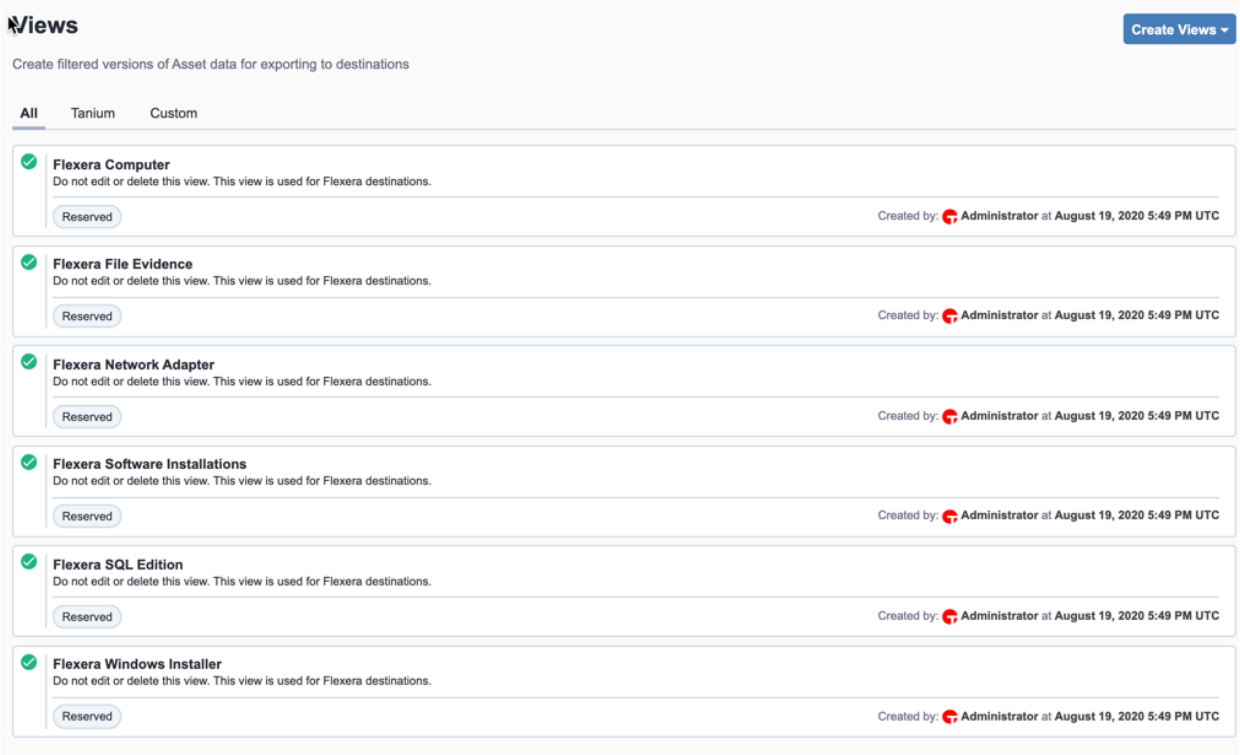
4. Click **Create**.

Result

When you add a Flexera destination, the following actions occur:

- Additional attributes are added to Asset. These attributes will be pending until the next Tanium import. For more information, see View schedule and run import on page 117.
- Flexera reports are created in Asset. View these reports in the **Reports** section under **Tanium Reports**. Do not delete or modify these reports. Modifying these reports disrupts the Flexera export.
- Flexera views are created.

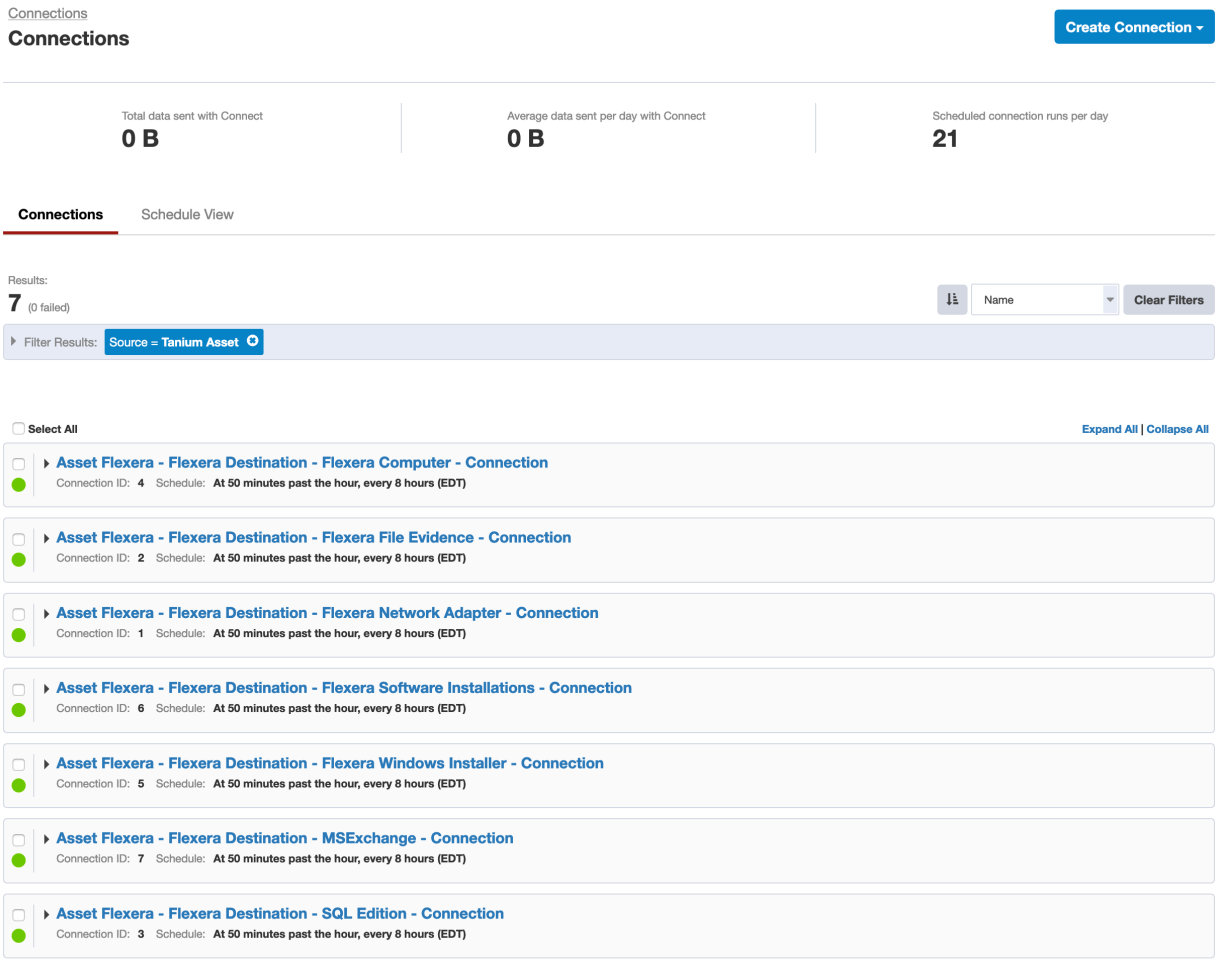
©2026 Tanium Inc. All Rights Reserved



Do not edit these views because they can be overwritten. If necessary, you can look at the fields that are included in the Flexera views to create a copy of the view that includes different settings.

- For each report, a connection is created in Connect that sends the report data to the SQL server using the views as a source.

©2026 Tanium Inc. All Rights Reserved



Use Connect for all troubleshooting of the data transfer to the SQL server. Each Flexera connection contains information about the schedule and success or failure of the data transfer.

CONFIGURE FLEXERA TO RECEIVE DATA FROM TANIUM ASSET

About this task

Check the contents of your custom reports in Asset and the data that is being exported to the configured SQL server. After the data you want is being exported, configure FlexNet Manager Suite to get data from the database. Work with your Flexera to configure this integration.

ServiceNow: Tanium Asset integration

You can configure Tanium as a discovery source in ServiceNow, and then create a destination in Asset to export data to ServiceNow with a defined schedule.

©2026 Tanium Inc. All Rights Reserved

Requirements

- ServiceNow Australia or later release. ServiceNow Software Asset Management Pro is also supported.
- Access to both a test and production instance of your ServiceNow Enterprise CMDB.
- A service account for ServiceNow that has elevated privileges. After the initial integration is complete, you can Configure least privileged access for ServiceNow integration.

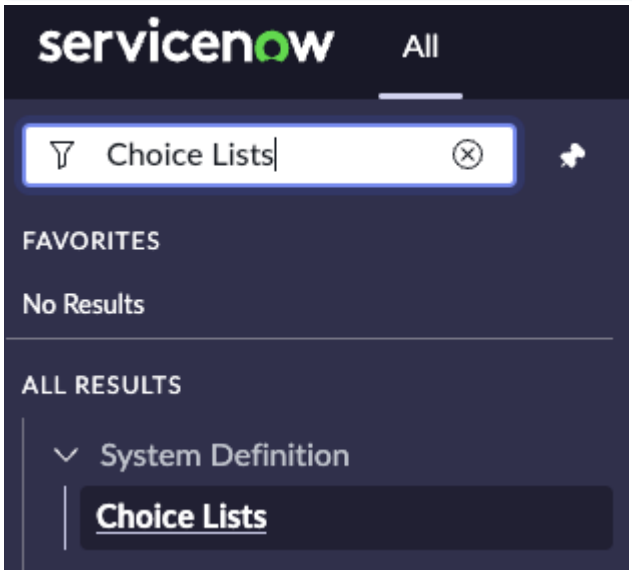
Important: Test the data export against a copy of your ServiceNow instance before you configure Tanium Asset to export all data to your production instance of ServiceNow. Because the built in identification rules in ServiceNow assume unique computer names or serial numbers, you might need to add one or more identification rules to achieve consistent and expected results.

Prepare ServiceNow to receive Tanium data

About this task

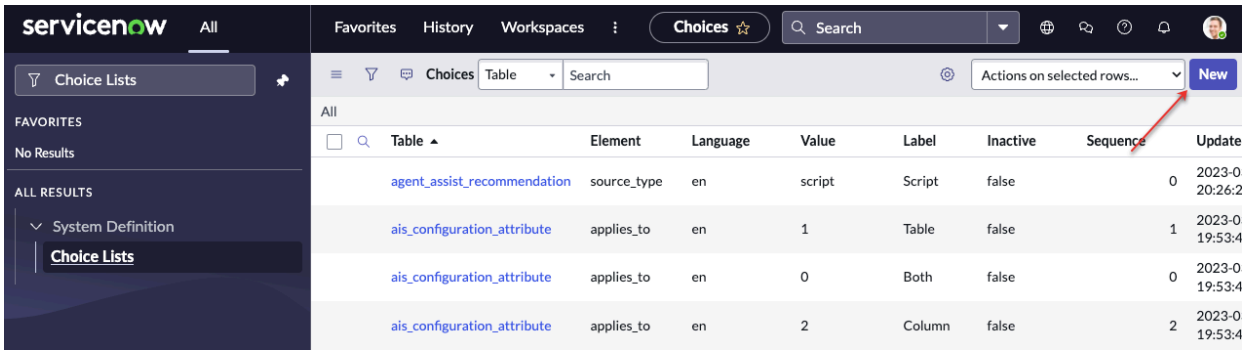
1. In ServiceNow, go to **All** > **System Definition** > **Choice Lists**.

   Tip: Enter `Choice Lists` in the menu filter to quickly navigate to that menu item.

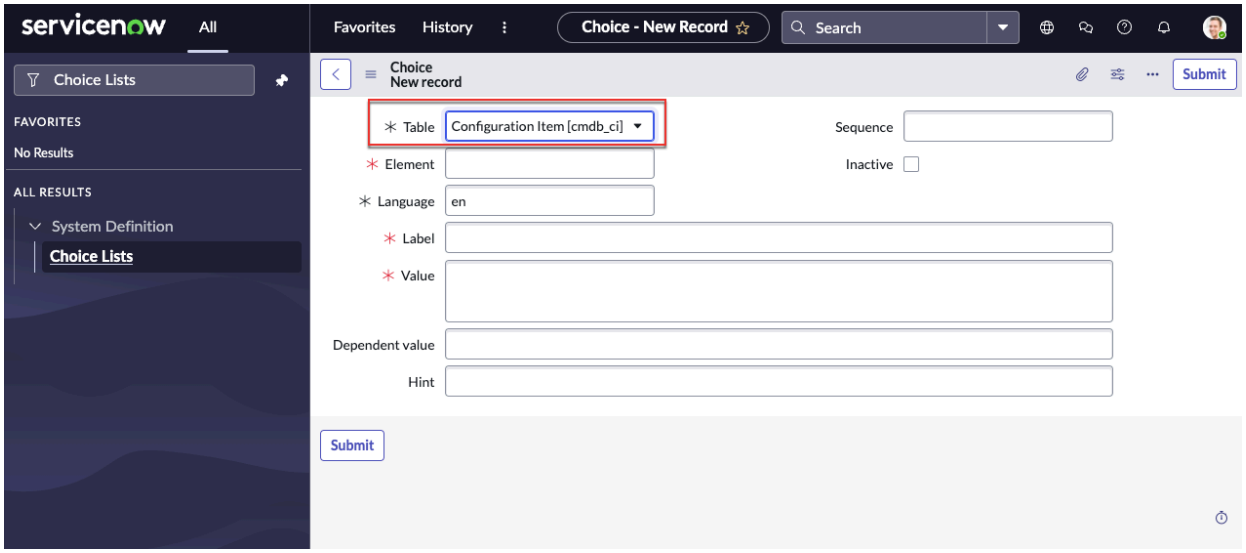
   

2. Click **New**.

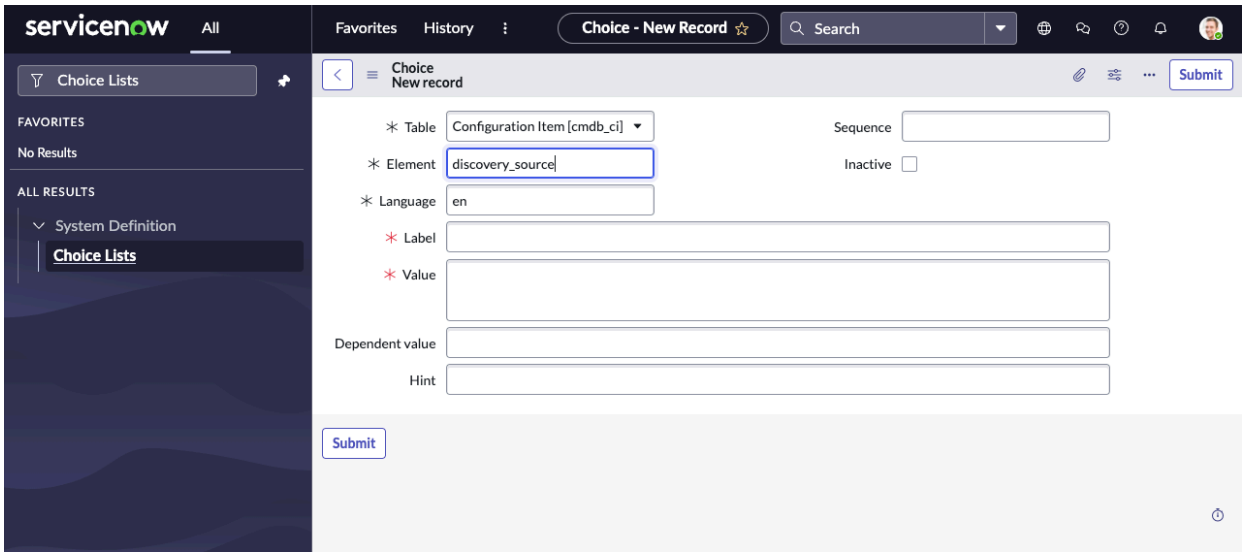
©2026 Tanium Inc. All Rights Reserved



3. For **Table**, select **Configuration Item [cmdb_ci]**.



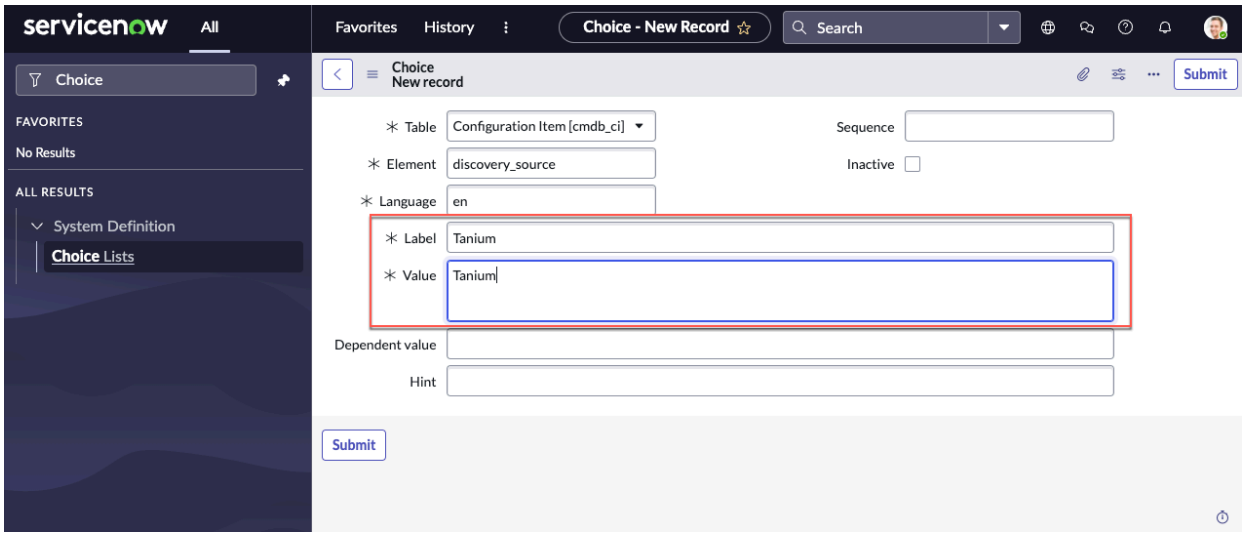
4. In the **Element** field, enter `discovery_source`.



5. In the **Label** field, enter `Tanium`.

6. In the **Value** field, enter `Tanium`.

©2026 Tanium Inc. All Rights Reserved



7. Click **Submit**.

Result

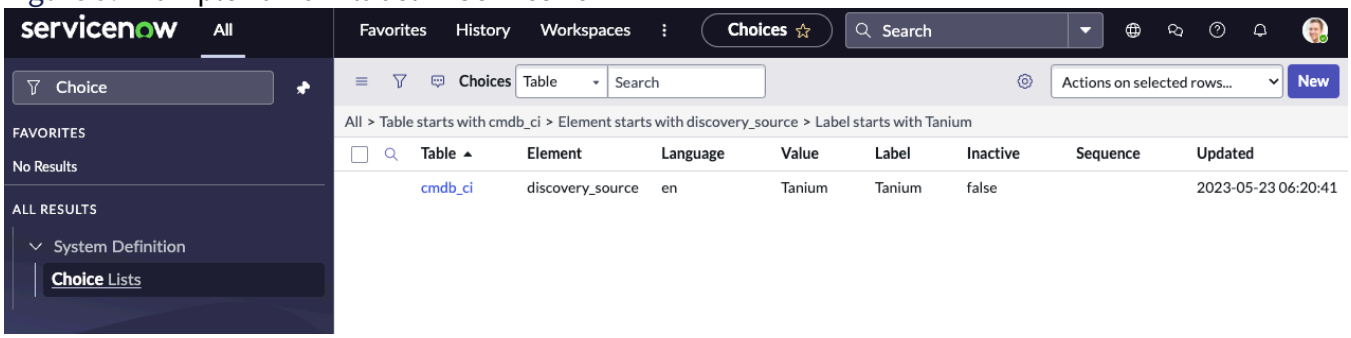
Confirm that you successfully created the item:

1. Go to **All** > **System Definition** > **Choice Lists**.
2. Click Show/Hide filter .
3. For the **-- choose field --** menu, select **Table**.
4. Leave the default operator, **starts with**, and in the **Input value** field, enter `cmdb_ci`.
5. Click **AND**.
6. For the **-- choose field --** menu, select **Element**.
7. Leave the default operator, **starts with**, and in the **Input value** field, enter `discovery_source`.
8. Click **AND**.
9. For the **-- choose field --** menu, select **Label**.
10. Leave the default operator, **starts with**, and in the **Input value** field, enter `Tanium`.
11. Click **Run**.

©2026 Tanium Inc. All Rights Reserved

You should see the Tanium choice that you added. If you do not see it, go back and check to confirm that you completed each step.

Figure 9. Example Tanium label in ServiceNow



Note: If you are using ServiceNow Paris 10 or Quebec or later with the Tanium Asset integration, ServiceNow creates duplicate entries for some CIs (such as Network Adapters, Storage Devices, and File Systems) in the ServiceNow CMDB when an export runs. For more information about how to resolve this issue, see Fix duplicate entries in ServiceNow with Tanium Asset integration on page 208.

ADD TABLES AND UPDATE IDENTIFICATION RULES

About this task

You can optionally work with Tanium Support and your ServiceNow administrator to add tables or update identification rules in ServiceNow. For more information about how to contact Tanium Support, see Contact Tanium Support on page 222.

Configure ServiceNow export settings

About this task

By default, Asset supports up to two concurrent exports to ServiceNow destinations. If an export is scheduled to run and there are already two exports running, Asset queues the export to run when another export completes. By default, exports can remain in the queue for 24 hours.

You can configure the number of concurrent exports to ServiceNow destinations and how long an export can remain in the queue.

©2026 Tanium Inc. All Rights Reserved

Note: To edit Asset settings, you require a role with the **Asset Configure Item write** permission.

1. From the **Asset Overview** page, click Settings.
2. On the **Advanced** tab, go to the **Asset Destination Job Queue** section.
3. Edit the **Concurrent Destinations** and **Max Time in Queue** values as needed.
4. When finished, click **Save**.

Result

The export settings only apply to "push" exports that are initiated in Asset. This includes scheduled ServiceNow exports and ServiceNow exports that a user manually runs outside of a schedule.

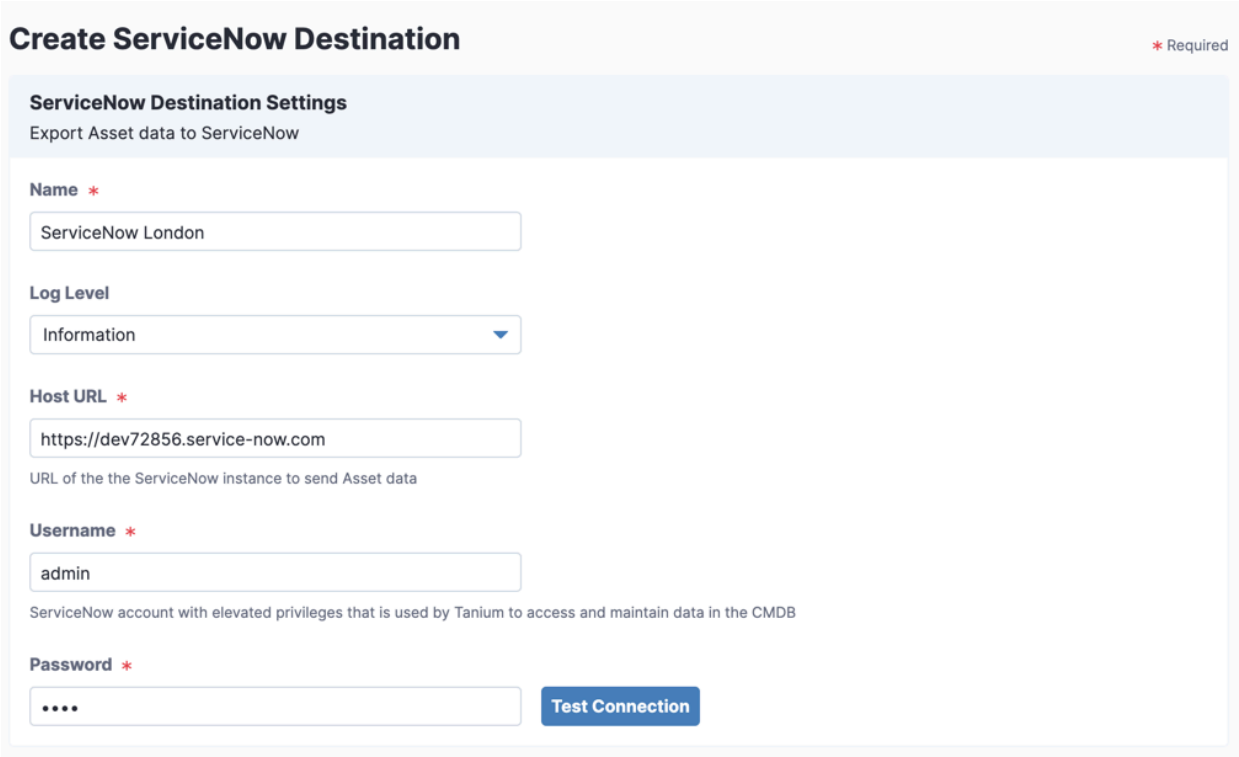
Add ServiceNow as a destination

About this task

To enable data to be exported to the ServiceNow CMDB from Asset, enter your ServiceNow Host URL and credentials.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Destinations**.
2. Click **Create ServiceNow Destination**.
3. Edit the settings, including the ServiceNow Host URL and credentials, log level, view, and the schedule at which you want the export to occur.

©2026 Tanium Inc. All Rights Reserved



The log level affects the logging in the job/date_time_job#_servicenow_config#.log files. If you enable `Trace` level logging on your ServiceNow configuration, numbered subdirectories, for example job/65, are created that contain all POST and GET requests for that job. For more information about cron, see Reference: Cron syntax on page 223.

4. Click **Create**.

Exclude computers from exported ServiceNow data

About this task

(Optional) When you create a ServiceNow destination, a reserved view is created. The ServiceNow (reserved) view includes all computers. Create a view with filters enabled if you want to narrow the scope of the export.

1. From the Main menu, go to **Modules** > **Asset** > **Views**. Hover over the **ServiceNow (reserved)** view and click Create Copy .
2. Edit and rename the copy of the reserved view. Add a filter to limit the computers that are exported. In this new view, do not select **Should be filtered out of the view** on any of the filters.
3. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Destinations** and

©2026 Tanium Inc. All Rights Reserved

click the ServiceNow_Destination. Click Edit .

4. In the **View** section, select the new view that you created.
5. Click **Update** to save the changes.

Edit ServiceNow export mappings

About this task

(Optional) After you create the ServiceNow destination, you can edit the Asset to ServiceNow mappings.

1. To add an attribute, find the details for the attribute.
    a. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Entities & Attributes**.
    b. Click **Customize Columns** and select **Table Name** and **Field Name**.
    c. Use the **Filter Items** search to find the attribute.
2. Edit the ServiceNow mappings in the destination.
    a. From the Main menu, click **Inventory Management** > **Destinations** > **ServiceNow**.
    b. Click Edit in the row of the destination for which you want to update mappings.
    c. In the **ServiceNow Export Mapping** section, add the new mapping. You can also edit individual mappings.
    d. (Optional) To test the mappings, click **Validate All Tanium Mappings**. Once clicked, Asset continuously monitors the mappings for issues, and the button appears as **Revalidate All Tanium Mappings**.

    > **Note:** Asset only validates Tanium field values within ServiceNow mapping definitions.

    For more information about the mappings, see Reference: ServiceNow mappings on page 224. To properly edit the ServiceNow export mappings, Contact Tanium Support on page 222.

Run export

About this task

You can run an export to ServiceNow CMDB outside of the configured schedule. From the Main menu,

©2026 Tanium Inc. All Rights Reserved

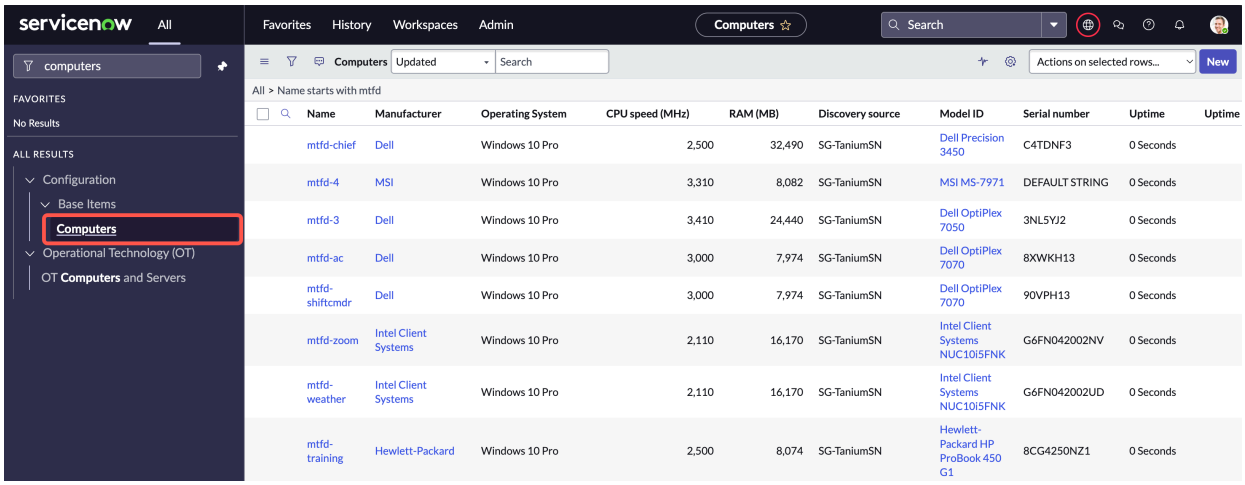
go to **Modules > Asset > Inventory Management > Schedules**, and then go to the **Export Schedules** tab. Under the ServiceNow destination in the **Asset Export Destinations** section, click Run Now .

Check data in ServiceNow

About this task

After the Status in the schedule says complete, you can check for the data in ServiceNow CMDB.

1. Sign in to your ServiceNow Enterprise CMDB.
2. Search for an Asset attribute, such as `Computer`.



3. Check the data that got imported into the table.

Configure least privilege access in ServiceNow

About this task

After the initial integration with ServiceNow is complete, you can create a role for the Tanium Service Account. This role has an ACL that provides only the necessary permissions.

For more information, see Configuring least privileged access for ServiceNow integration.

ServiceNow: Service Graph Connector

For comprehensive documentation about the Service Graph Connector for Tanium integration, including requirements, installation, configuration, and verification steps, see Tanium ServiceNow Integrations: Tanium IT Asset Management.

©2026 Tanium Inc. All Rights Reserved

For more information about purchasing the Service Graph Connector for Tanium, see Service Graph Connector for Tanium.

©2026 Tanium Inc. All Rights Reserved

Creating a Software Bill of Materials

About this task

The Software Bill of Materials (SBOM) add-in for Asset uses Tanium™ Client Index Extension (Index CX) to generate an SBOM for Windows, macOS, and Linux endpoints.

When you have a complete inventory of the software on endpoints, including dependencies, you can quickly respond to emergent vulnerabilities that are identified in a specific component.

Important: This add-in requires a license for Asset plus an additional license for SBOM.

Overview

The SBOM add-in identifies candidate files on the endpoint by querying Index CX, which has indexed the file system, for the files and file types that you specify in the SBOM profile.

The identified files are then processed to define and extract their software bill of materials, providing identifying details such as the dependency name and version.

For more information about changes for each SBOM release, see the SBOM release notes.

Requirements

Required dependencies

About this task

- Asset 1.24.76 or later
- Tanium™ Client:

  Any supported version of Tanium Client. For more information, see Client version and host system requirements. If you use a Client version that is not listed, certain product features

©2026 Tanium Inc. All Rights Reserved

might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed Client versions.

- Tanium Client Index Extension (installed as part of Asset 1.24.76 or later)
- Extras Client Extension (installed as part of Asset 1.24.76 or later)
- Software Manager Client Extension (installed as part of Asset 1.24.76 or later)

CAUTION: Tanium Client Index Extension (Index CX) is required for the proper operation of Software Manager CX. Removing or disabling Index CX will result in the inoperability of SBOM and other modules and features.

Required RBAC permissions

About this task

To view SBOM content and the SBOM content set, you require the **Administrator** reserved role, or the **Asset Operator** role and a custom role with the special show permission for SBOM. For more information about custom roles, see Tanium Console User Guide: Custom and system roles. For more information about the special show permission, see Tanium Console User Guide: Roles and permissions.

To work with SBOM content, you must have the required RBAC permission for the operation. For more information, see Tanium Console User Guide: Action management permissions. For more information about content sets, see Tanium Console User Guide: Managing content sets.

Endpoints

SUPPORTED OPERATING SYSTEMS

The following endpoint operating systems are supported for use with SBOM:

Supported endpoints for SBOM

Operating System	Version	Notes
Windows	• Windows 7 SP1 or later	• 32-bit (x86)* and 64-bit (x64)

©2026 Tanium Inc. All Rights Reserved

Operating System	Version	Notes
	• Windows 2008 R2 SP1 or later	• Windows 7 SP1 requires Microsoft KB2758857. • Windows Server 2008 R2 SP1 requires Microsoft KB2758857.
macOS	Same as Tanium Client support	32-bit (x86)* and 64-bit (x64 and arm64)
Linux	Same as Tanium Client support	32-bit (x86)* and 64-bit (x64 and aarch64)
* Go file types are not supported for identification on 32-bit (x86) systems.		

DISK SPACE REQUIREMENTS

Endpoint disk space requirements for SBOM are the same as the requirements for Client Index Extension. For more information, see Tanium Client Index Extension User Guide: Endpoints - Disk space requirements.

Supported ecosystems

About this task

SBOM supports scanning for the following file types:

- Java
- JavaScript
- Python
- Ruby
- PHP
- Go
- Native library files*

* Native library files include shared libraries and executable files for the endpoint operating system.

For more information about specific files and file types that are supported for scanning, see

©2026 Tanium Inc. All Rights Reserved

Reference: SBOM files and file types on page 272.

Install SBOM

About this task

If you are upgrading from SBOM 1.x to SBOM 2.x, read the upgrade notes at .

> **Note:** If you upgrade from SBOM 1.x to SBOM 2.x, SBOM 1.x data is removed from endpoints when an SBOM 2.x profile is pushed to the endpoint.

1. Sign in to the Tanium Console with an account that has the **Administrator** reserved role.
2. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.
3. In the **Content** section, select the row for **SBOM** and click **Install**.
4. Review the content to import and click **Begin Install**.
5. Depending on your Tanium Server configuration, enter your credentials and click **Submit**, or click **Yes**.

Work with SBOM profiles

About this task

For more information about how to create, edit, and delete SBOM profiles, see Configuring profiles on page 101.

View SBOM results

View SBOM results in Asset

About this task

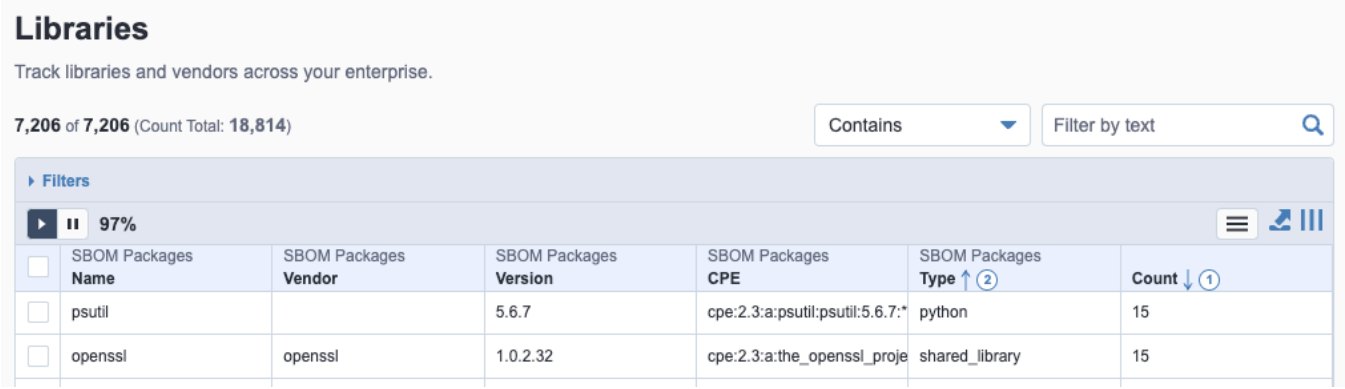
You can view SBOM results on the **Tracked Components & Libraries** page. From the Main menu, go to **Modules** > **Asset** > **Software Bill of Materials > Tracked Components & Libraries**.

©2026 Tanium Inc. All Rights Reserved

The **Libraries** section of this page shows the live data results of this question: `Get SBOM Packages from all machines with SBOM Has Results contains true`. Use the **Filter by text** field to filter the results.

The **SBOM Packages** sensor returns a subset of packages and libraries on each endpoint. For more information about how to find a specific library or package, see Track libraries and vendors on page 163.

Figure 10. Example Libraries page



View SBOM results in Interact

About this task

If you want to drill down further into the SBOM results, you can ask a question in Interact using one of the SBOM Packages sensors.

1. From the Main menu, go to **Modules** > **Interact**.
2. Ask a question using one of the SBOM Packages sensors: **SBOM Packages**, **SBOM Package Information Filtered By**, or **SBOM Package Information For Hash** with `SBOM Has Results contains true`.
   For example, ask this question: `Get SBOM Packages from all machines with SBOM Has Results contains true`.
3. Drill down into the results to review the data. For example, you can select a package and drill down using **Computer Name** to determine the endpoints on which the component is installed.

Track libraries and vendors

©2026 Tanium Inc. All Rights Reserved

You can track libraries and vendors to monitor the endpoints on which a specific library or version exists. When you enable tracking, a new reserved entity named **SBOM Package Information - *<library or vendor name> - type***, with a set of attributes for the tracked component is created and enabled for collection in Asset. A new SBOM report using the attributes, also named **SBOM Package Information - *<library or vendor name> - type***, is automatically created and populated after the first data collection.

1. From the Main menu, go to **Modules** > **Asset** > **Software Bill of Materials > Tracked Components & Libraries**.
2. In the **Libraries** section, select the row for the library or vendor that you want to track.

   Note: You can track multiple components concurrently, but you must enable tracking on each one separately.

3. Click **Enable Tracking**.
4. Select one or more keys that you want to track. Options include **name** and **vendor**.
5. Click **Track**.

Important: Tracking components adds additional attributes to the Asset database. Tracking more than 20 components at a time can lead to increased import times and performance issues in Asset. For more information about performance implications for attributes, see Configure additional Tanium entities and attributes on page 111.

Manage tracked components

About this task

Tracked components are libraries and vendors for which you enabled tracking in the **Libraries** section of the **Tracked Components & Libraries** page. For more information about tracking libraries and vendors, see Track libraries and vendors on page 163. If needed, you can disable, enable, or stop tracking components.

Disable a tracked component

©2026 Tanium Inc. All Rights Reserved

About this task

When you disable a tracked component, the corresponding attributes are disabled, but the attributes and report remain.

1. From the Main menu, go to **Modules** > **Asset** > **Software Bill of Materials > Tracked Components & Libraries**.
2. In the **Tracked Components** section, select the row for the tracked component that you want to disable.
3. Click **Disable**.

Result

The status for the tracked component changes to Disabled ⚠.

Enable a tracked component

About this task

If you previously disabled a tracked component, you can re-enable tracking to move the corresponding attributes back to a Ready ✔ state and re-activate the corresponding report.

1. From the Main menu, go to **Modules** > **Asset** > **Software Bill of Materials > Tracked Components & Libraries**.
2. In the **Tracked Components** section, select the row for the disabled component that you want to enable.
3. Click **Enable**.

Result

The status for the tracked component changes to Enabled ✔.

Stop tracking a component

About this task

When you stop tracking a tracked component, the corresponding attributes and report are deleted.

1. From the Main menu, go to **Modules** > **Asset** > **Software Bill of Materials > Tracked**

©2026 Tanium Inc. All Rights Reserved

Components & Libraries.

2. In the **Tracked Components** section, select the row for the component that you want to stop tracking.
3. Click **Stop Tracking**.
4. Click **Yes** to confirm your action.

Result

The tracked component and associated report are deleted. The status for the corresponding attributes changes to Deleting, and they are deleted from the Asset database on the next scheduled load of data from the Tanium source for Asset. For more information, see Configure the Tanium source on page 66 and Schedule and run Asset data imports on page 117.

View library details

About this task

For any library, you can view which products are associated with the library and instances of the library in your environment.

1. From the Main menu, go to **Modules** > **Asset** > **Software Bill of Materials > Tracked Components and Libraries**.
2. Go to the **Libraries** section.
3. In the row of the library for which you want to view details, click the value in the **CPE** column. The **Library Details** page opens.
4. Review the library details. The **Products** tab shows which products are associated with the library. The **Instances** tab shows which endpoints contain the library.

   Note: The association of a product with a library is based on product application install paths and is a best estimate.

View reports for tracked components

About this task

©2026 Tanium Inc. All Rights Reserved

When you enable tracking for a library or vendor, a report that uses the associated attributes is automatically generated. You can view these automatically generated reports for tracked components on the **SBOM Reports** page.

1. From the Main menu, go to **Modules** > **Asset** > **Software Bill of Materials > SBOM Reports**.
2. Click the name of the report that you want to view.
   Reports for actively tracked components have a Ready status. Reports for tracked components that are disabled have a Disabled status and are not updated.

Result

For more information about working with reports, see Work with existing reports on page 56.

Tip: You can also view the reports from the **Reports** page in Asset.

Create reports for unlisted libraries

About this task

Create a custom report in Asset that includes columns with **SBOM Packages** to review SBOM data.

Tip: Perform this task only if you want to create a report for libraries that are not listed on the **Tracked Components & Libraries** page.

Create a report to show all SBOM package details

ADD THE REQUIRED ATTRIBUTES

About this task

Add SBOM attributes as available columns in the Asset database so that you can include them in reports.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Entities &**

©2026 Tanium Inc. All Rights Reserved

Attributes.

2. Click **Add Attribute** and select **Add Existing Attribute**.
3. Expand the section for **SBOM Packages**.
4. (Optional) As a best practice, click Settings next to one of the **SBOM Packages** attributes and select **Multiple Rows for a Computer**.
5. Select the five attributes for this entity: **CPE**, **Name**, **Type**, **Vendor**, and **Version**.
6. Click **Add** in the section for **SBOM Packages**.
7. Click **Add Attributes**.

Result

The attribute status is Pending until the next import job runs. Wait until the attribute status is Ready before you create a report. For more information about how to add attributes, see Configure additional Tanium entities and attributes on page 111. For more information about how to run the import job immediately, see View schedule and run import on page 117.

CREATE THE REPORT

1. From the Main menu, go to **Modules** > **Asset** > **Reports**.
2. Click **Create Custom Report**.
3. Specify a **Name** and optional **Description**.
4. (Optional) Select **Enabled** for **Summary Report** if you want the data grouped into rows with an associated count that you can click to view more details.
5. In the **Select Report Columns from Asset Tables** section, expand the **Asset** table.
6. Select the **CPE**, **Name**, **Type**, **Vendor**, and **Version** attributes.
7. Click Add selected .
8. Click **Submit**.

Next steps

For more information about how to create reports, see Create a report on page 60.

©2026 Tanium Inc. All Rights Reserved

Create a report to show SBOM package details for a specific component

About this task

If you need to determine which endpoints have a specific component installed, create a report that uses attributes from the **SBOM Discovered Package Information For Name** entity. The following example looks for instances of log4j on endpoints, but you can substitute that value with another component name.

ADD THE REQUIRED ATTRIBUTES

About this task

Add SBOM attributes as available columns in the Asset database so that you can include them in reports.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Entities & Attributes**.
2. Click **Add Attribute** and select **Add Existing Attribute**.
3. Expand the section for **SBOM Package Information Filtered By**.
4. Select the attributes for this entity: **CPE**, **Library Hash**, **Name**, **Package Hash**, **Parent**, **Type**, **Vendor**, and **Version**.
5. Click **Add** in the section for **SBOM Package Information Filtered By**.
6. Specify the details on the **Create Instance of Entity: SBOM Discovered Package Information For Name** page:
    a. Change the **Entity Name** to a value you can use to identify this entity set later, such as `SBOM Package Information For Log4J`.
    b. In the **Name** field, specify the component that you want to look for, such as `log4j`.
    c. In the **Select storage method for data** section, select **Multiple Rows for a Computer**.
    d. Click **Next**.
    e. Click **Create**.
7. Review the attributes and click **Add Attributes**.

Result

©2026 Tanium Inc. All Rights Reserved

The attribute status is Pending until the next import job runs. Wait until the attribute status is Ready before you create a report. For more information about how to add attributes, see Configure additional Tanium entities and attributes on page 111. For more information about how to run the import job immediately, see View schedule and run import on page 117.

CREATE THE REPORT

1. From the Main menu, go to **Modules** > **Asset** > **Reports**.
2. Click **Create Custom Report**.
3. Specify a **Name** and optional **Description**.
4. (Optional) Select **Enabled** for **Summary Report** if you want the data grouped into rows with an associated count that you can click to view more details.
5. In the **Select Report Columns from Asset Tables** section, expand the **Asset** table.
6. Select the **CPE**, **Library Hash**, **Name**, **Package Hash**, **Parent**, **Type**, **Vendor**, and **Version** attributes.
7. Click Add selected .
8. Click **Submit**.

Next steps

For more information about how to create reports, see Create a report on page 60.

Export SBOM data

About this task

Create a view to export SBOM data to a destination, such as Tanium Connect, Flexera FlexNet Manager Suite, or ServiceNow. The steps to create a view vary based on the destination. For more information, see Configuring views on page 123.

SBOM Sensors

SBOM uses the following sensors. Do not delete these sensors from the Tanium Server.

©2026 Tanium Inc. All Rights Reserved

Sensors used by SBOM

Sensor	Description
SBOM Has Results	Returns true if the endpoint processed BOMs and components were found.
SBOM Package Information Filtered By	Returns the SBOM package information from endpoints, filtered by a specific field and value. Includes these columns: **Name** , **Vendor** , **Version** , **CPE** , **Type** , **Library Hash** , **Parent** , **Package Hash** .  **Note:** Use a regular expression to specify the version. The version field supports Perl-style syntax, except for backreferences. Leave the field blank to match any version.
SBOM Package Information For Hash	Returns the SBOM package detailed information from endpoints, filtered by a specific hash. Includes these columns: **Name** , **Vendor** , **Version** , **CPE** , **Type** , **Library Hash** , **Parent** , **Package Hash** .
SBOM Packages	Returns an overview of the SBOM package information from endpoints. Includes these columns: **Name** , **Vendor** , **Version** , **CPE** , **Type** .
SBOM Packages Count	Returns the count of all discovered packages on the endpoint.
SBOM Packages Filtered By	Returns an overview of the SBOM package information from endpoints for the specified Name, Vendor, Version, or Ecosystem.  **Note:** Use a regular expression to specify the version. The version field supports Perl-style syntax, except for backreferences. Leave the field blank to match any version.

©2026 Tanium Inc. All Rights Reserved

Integrating with Microsoft Azure Migrate

About this task

Note: This integration is currently available as a public preview. For access, contact: tanium-azuremigrate@tanium.com.

Use assessments in Asset to combine the real-time operational state of your on-premises environment, as known by Tanium, with the robust capabilities of Microsoft Azure Migrate to quantify the economic impact of running workloads in Microsoft Azure without using separate appliances or agents.

Overview

Assessments in Asset provide an automated method to provide Tanium data to your Microsoft Azure Migrate project and run total cost of ownership (TCO) and return on investment (ROI) assessments. You can target an assessment to any segment of your endpoint estate. For example, you might want to assess all on-premises servers that belong to a specific business unit or all servers in a particular geographical region.

For more information about Microsoft Azure Migrate, see Microsoft Azure Migrate documentation: About Azure Migrate.

Before you begin

Before you create a Microsoft Azure Migrate assessment in Asset, you must complete several prerequisite tasks, as detailed in the following sections:

1. Step 1. Create a Microsoft Azure account and configure required permissions on page 173
2. Step 2. Create a Microsoft Azure Migrate project on page 173

©2026 Tanium Inc. All Rights Reserved

3. Step 3: Create an app registration, Microsoft Azure client ID, and secret on page 174
4. Step 4: Grant the necessary permissions to the service principal for the registered app on page 177
5. Step 5: Enable assessments in Asset on page 177
6. Step 6: Confirm that the necessary URLs are allowed through your security software on page 178

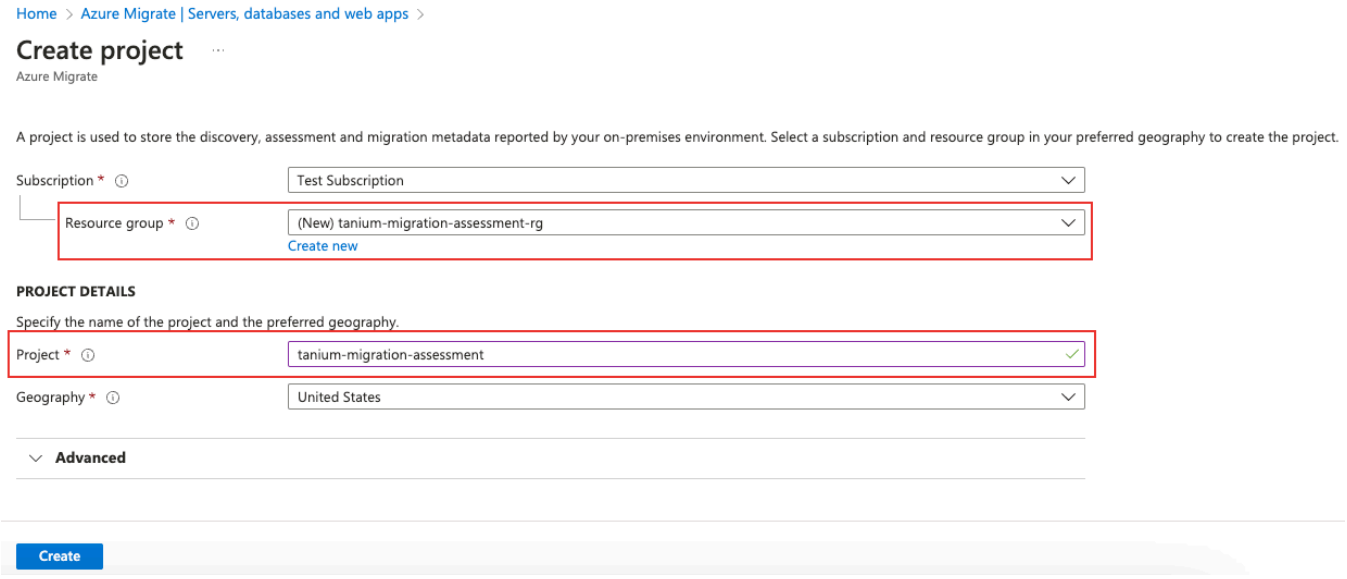
After you complete these tasks, you are ready to Create an assessment in Asset on page 178.

Step 1. Create a Microsoft Azure account and configure required permissions

If you do not have a Microsoft Azure user account, you must create one to use for the assessment. For an existing user account, confirm that the user account has the required permissions. For more information, see Microsoft Azure Migrate documentation: Prepare an Azure user account.

Step 2. Create a Microsoft Azure Migrate project

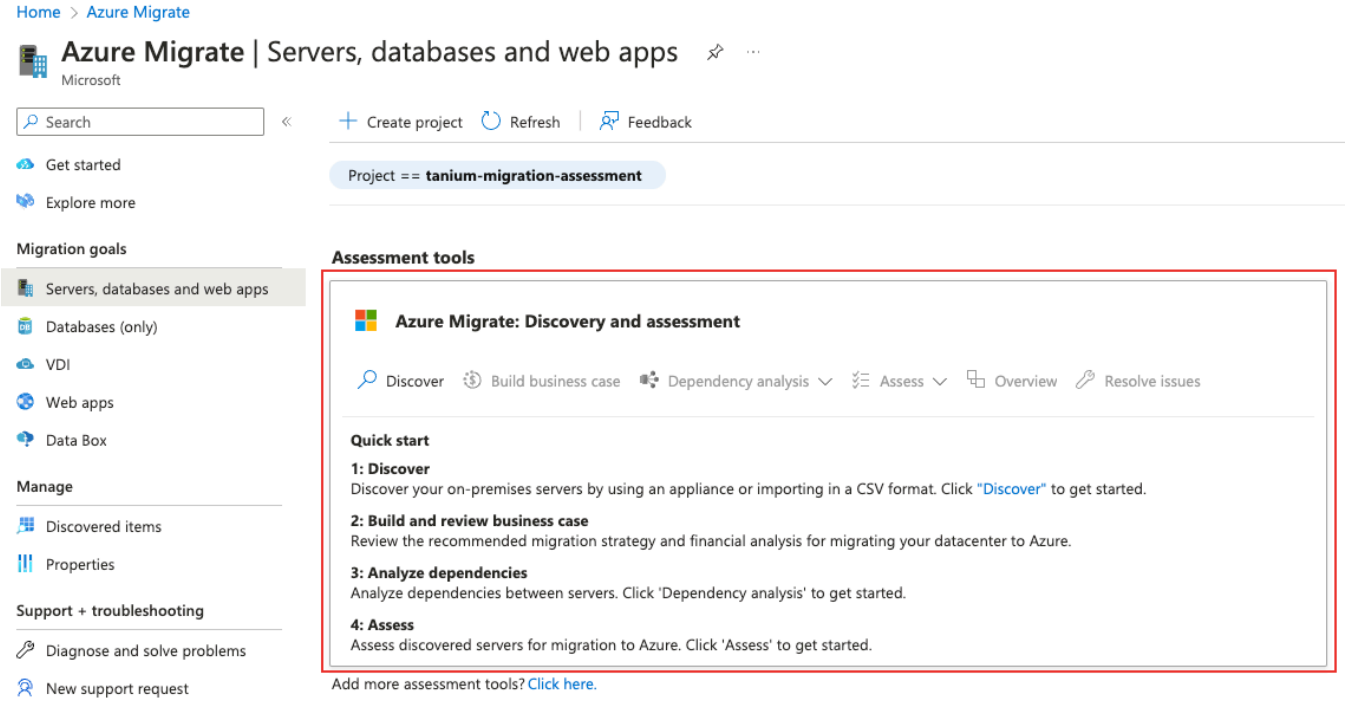
If you do not have a Microsoft Azure Migrate project, you must create one to use for the assessment. For more information, see Microsoft Azure Migrate documentation: Create a project for the first time.



If you are using an existing Microsoft Azure Migrate project, confirm that the **Azure Migrate: Discovery and assessment** tool is available in the project. If you did not create the project from the **Discover, assess and migrate** option on the Microsoft Azure Migrate **Get Started** page, you must add this tool to the project. For more information, see Microsoft Azure Migrate documentation: Select a

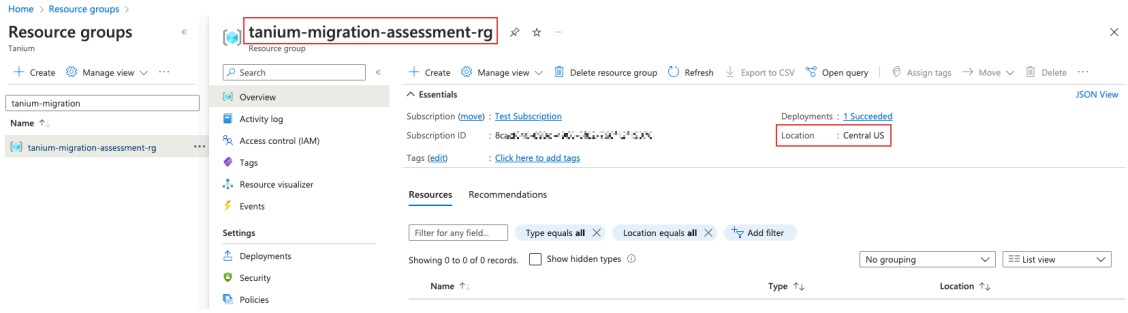
©2026 Tanium Inc. All Rights Reserved

discovery and assessment tool.



Note the following details about the project so that you can provide them when you create the assessment in Asset:

- Name of the project
- Subscription UUID for the subscription in which you create the project. For more information about how to find your subscription ID, see Microsoft Azure documentation: Find your Azure subscription.
- Resource group that you selected or created for the project
    - Location for the resource group



Step 3: Create an app registration, Microsoft Azure client ID, and secret

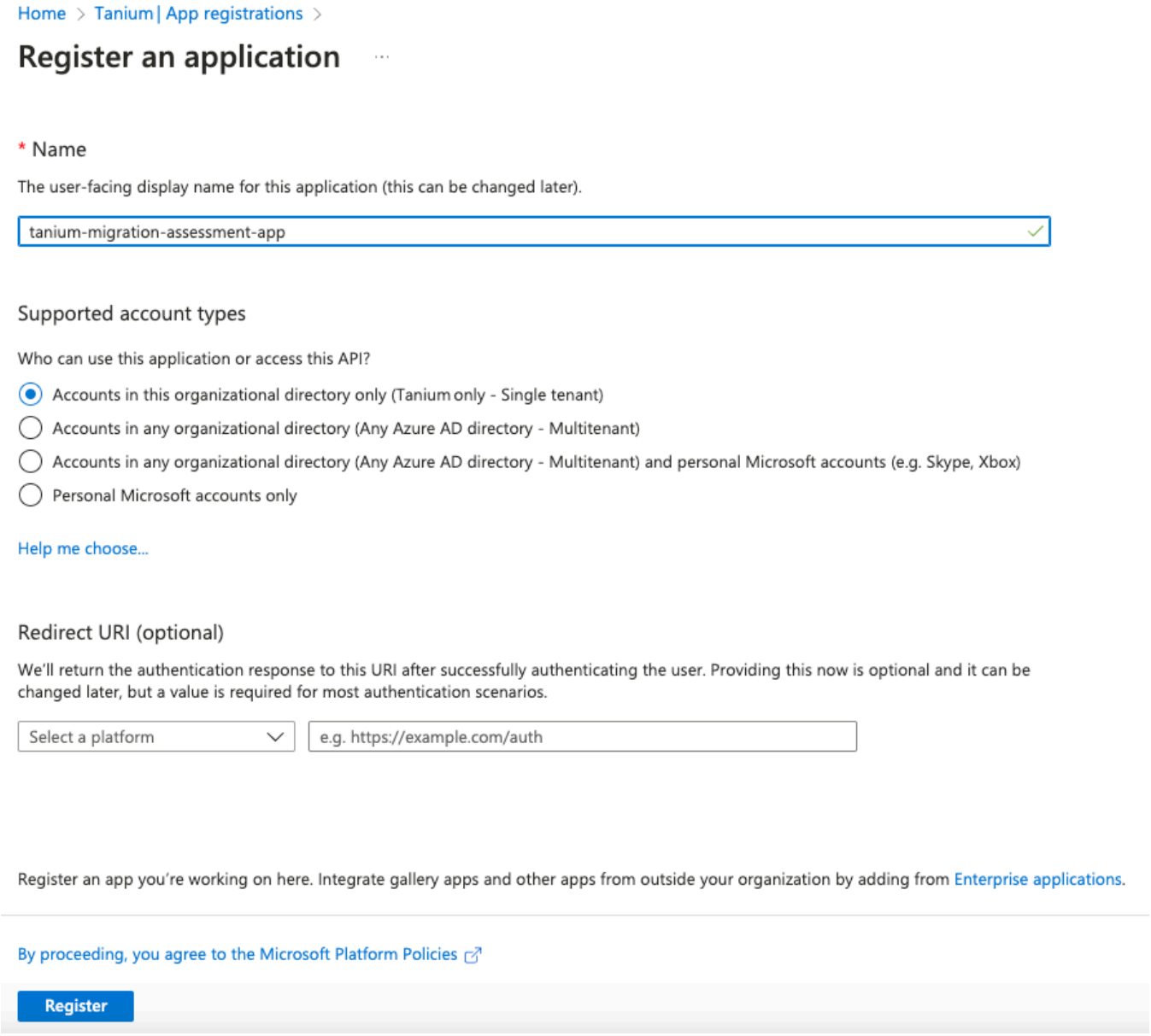
©2026 Tanium Inc. All Rights Reserved

In the Microsoft Azure portal, create an app registration and then create a Microsoft Azure client ID and secret for that app to use for authentication.

REGISTER AN APPLICATION

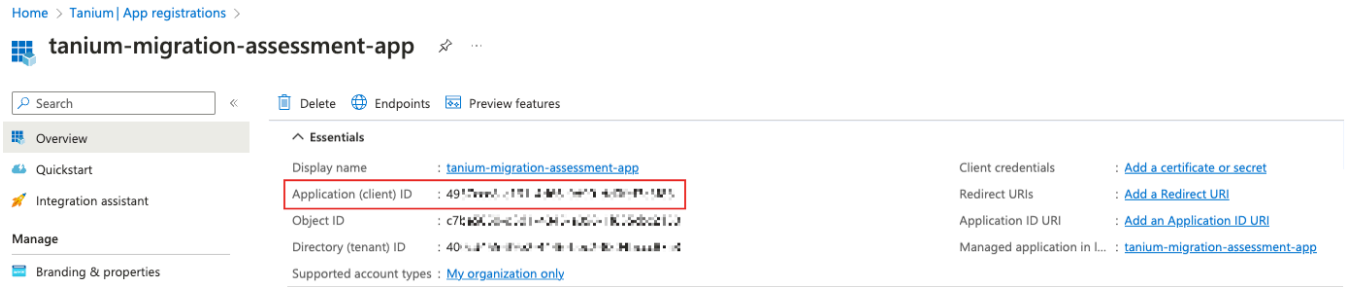
About this task

For more information, see Microsoft Entra documentation: Quickstart: Register an application. You do not need to configure the optional **Redirect URI**.



When you save the registration, note the **Application (client) ID** to use when you create the assessment.

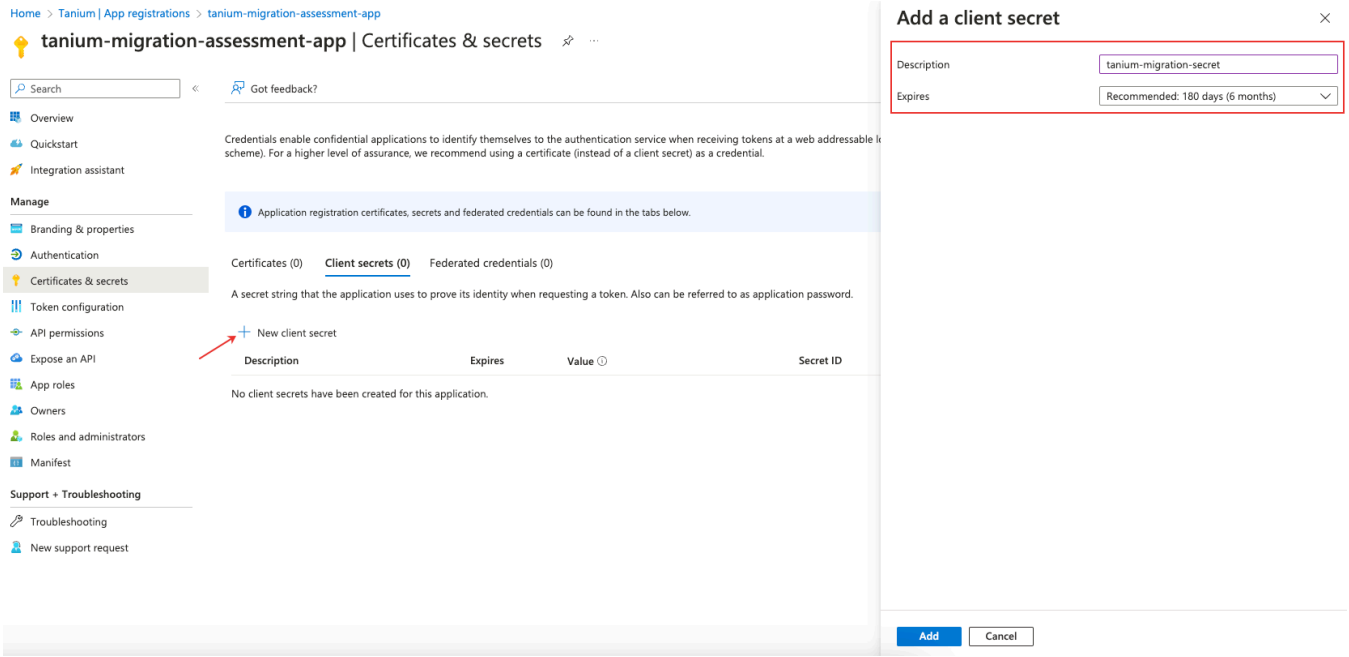
©2026 Tanium Inc. All Rights Reserved



ADD A CLIENT SECRET

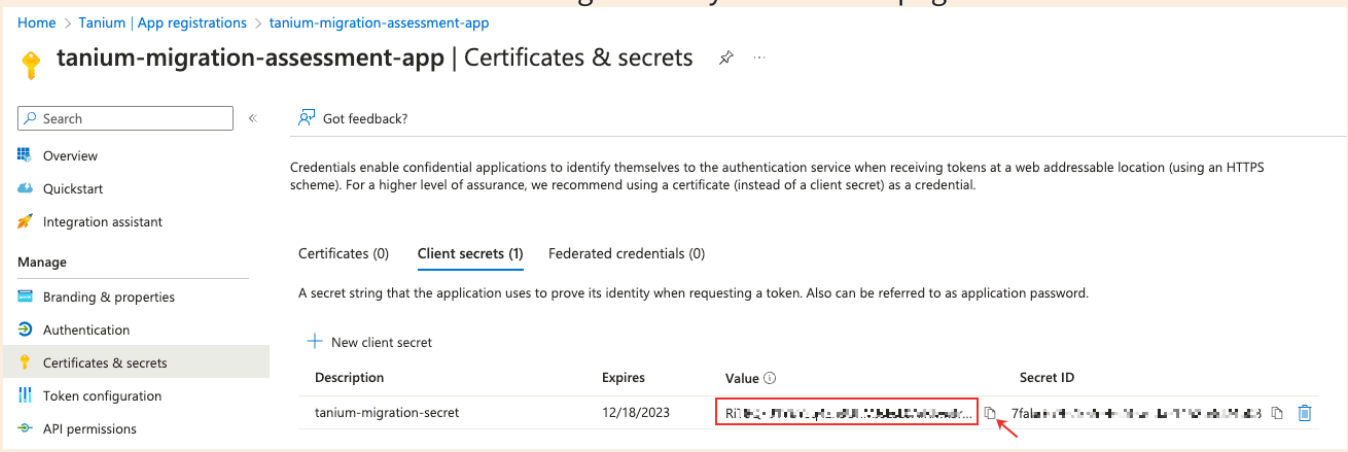
About this task

For more information, see Microsoft Entra documentation: Quickstart: Add a client secret



©2026 Tanium Inc. All Rights Reserved

Important: After you add the client secret, record the **Value** for the client secret and save it to a secure location. You cannot see this value again after you leave this page.



You do not need to complete the other sections in the article.

Step 4: Grant the necessary permissions to the service principal for the registered app

Microsoft Azure automatically creates a service principal object when you register an app (which you completed in Step 3). This service principal object must have Contributor or Owner roles on the associated Microsoft Azure subscription for the assessment to complete successfully. For more information, see Microsoft Azure documentation: Assign Azure roles using the Azure portal.

Tip:

- In Step 3 of the article, select the **Privileged administrator roles** tab to see the Contributor or Owner roles.
- In Step 4 of the article, select the service principal that was created for your registered app.

Step 5: Enable assessments in Asset

ENABLE THE ASSESSMENTS FEATURE

About this task

©2026 Tanium Inc. All Rights Reserved

Add a Tanium Core Platform advanced setting to add the assessments feature to Asset. For more information about Tanium Core Platform settings, see Tanium Console User Guide: Managing Tanium Core Platform settings.

1. From the Main menu, go to **Administration** > **Configuration** > **Settings** > **Advanced Settings**.
2. Click **Add Setting**, configure the following properties, and click **Save**:
    a. **Setting Type**: Select **Server**.
    b. **Name**: Enter `console_enable_asset_assessments`.
    c. **Value Type**: Select **Numeric**.
    d. **Value**: Enter `1`.

Result

Note: A Tanium Server restart is not needed to apply this setting. Refresh the **Asset Settings** page to see the **Assessments** setting.

ENABLE ASSESSMENTS IN THE ASSET SETTINGS

1. From the Main menu, go to **Modules** > **Asset** > **Overview** and then click Settings.
2. On the **Advanced** tab, select to enable **Assessments**.
3. Click **Save**.

Step 6: Confirm that the necessary URLs are allowed through your security software

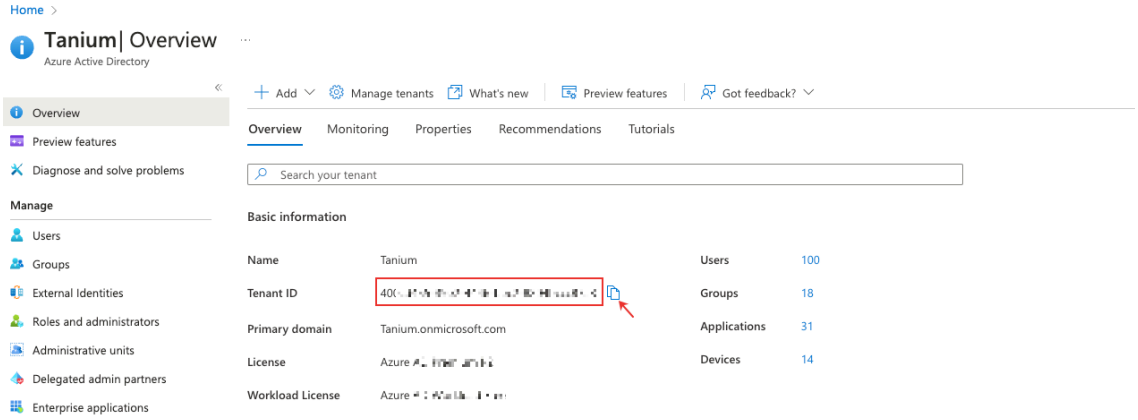
If security software is deployed in your environment to monitor and block unknown URLs, your security administrator must allow the following URLs:

- discoverysrvprodcusrepsa.blob.core.windows.net
- management.azure.com
- login.microsoftonline.com

Create an assessment in Asset

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Asset** > **Assessments**.
2. Create the assessment:
    - To create a new assessment, click **Create Assessment Azure Migrate**.
    - To create an assessment based on an existing assessment, click Copy in the row for the assessment that you want to use as the base configuration.
3. Specify a **Name** and optional **Description** for the assessment.
4. (Optional) Set the **Log Level**.
   The default log level (Information) is sufficient for typical usage. Adjust the log level only when you are troubleshooting an issue.
5. In the **Azure Connection Details** section, provide these details:
    a. **Directory (tenant) ID**: Enter your Entra ID tenant ID.
    For more information about how to find your tenant ID, see [Microsoft Azure documentation: Find your Microsoft Entra tenant]().

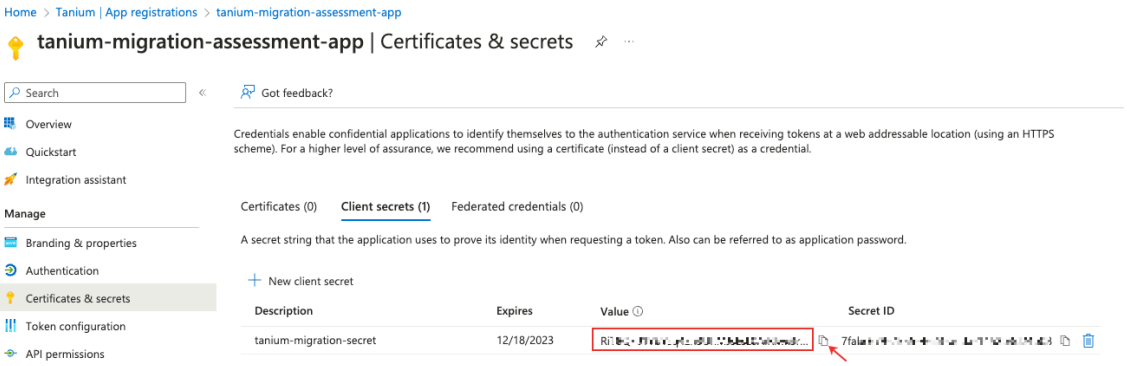


    b. **Application (client) ID**: Enter the Microsoft Azure Application (client) ID for the application that you created and registered with the Microsoft identity platform in the "Before you begin" section.



    c. **Client Secret**: Provide the **Value** for the client secret that you generated for the application that you created and registered with the Microsoft identity platform in the "Before you begin" section.

©2026 Tanium Inc. All Rights Reserved

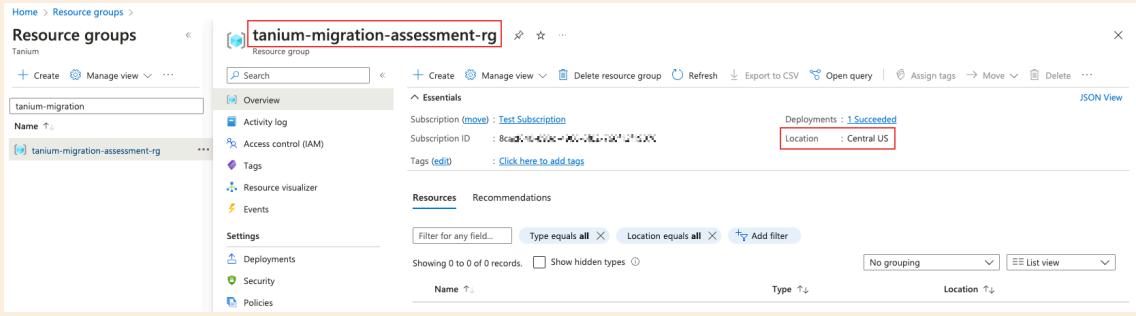


d. Click **Verify Connection** to confirm that the connection is valid.
Ensure that you receive a `Connection successful` message before you proceed to the next section. For more information about how to proceed if the verification fails, see Troubleshoot Microsoft Azure assessments on page 209.

6. In the **Azure Project Details** section, provide these details:
   a. **Subscription ID**: Enter the UUID for the subscription in which you created the Microsoft Azure Migrate project.
   For more information about how to find your subscription ID, see Microsoft Azure documentation: Find your Azure subscription.

   b. **Resource Group Name**: Enter the resource group that you selected or created when you created the Microsoft Azure Migrate project.
   c. **Azure Migration Project Name**: Enter the name of the Microsoft Azure Migrate project that you created to use for the assessment.
   d. **Azure Location**: Select the Microsoft Azure location to use for the assessment.

> **Important:** This location must match the location for your resource group. If you did not record the location when you created the project in the "Before you begin" section, you can find it in the **Essentials** for the resource group. In the Microsoft Azure portal, search for the Resource groups service. Open the Resource groups service and then click the name of your resource group.



7. In the **Targeting** section, click **Select Computer Groups**. Select the computer groups to

©2026 Tanium Inc. All Rights Reserved

target with this assessment and click **Save**.

8. In the **Configuration** section, provide these details:
    a. **Azure Offer Code**: Enter the Microsoft Azure offer code to use for the assessment. For more information about the current Microsoft Azure offers, see Microsoft: Microsoft Azure Offer Details.

    b. **Savings Options**: If you plan to use Microsoft Azure Reserved Instances (RI), select the savings plan you want to use for the assessment. Select **None** if you do not plan to use Microsoft Azure Reserved Instances.
    For more information about Reserved Instances, see Microsoft Azure: Azure Reserved Virtual Machine Instances.

    c. (Optional) **Discount Percentage**: If you selected **None** for **Savings Options** and have a discount offer to apply in addition to the Microsoft Azure offer code, specify the discount percentage to apply on the final price in the assessment. Valid values are numbers from `0 - 100`.
    d. **Sizing Criteria**: Select the sizing criteria to use for the assessment.
    For more information about sizing criteria, see Microsoft Azure Migrate documentation: Azure VM Assessment overview.

9. Click **Submit** to save your changes.

Result

The assessment is available on the **Assessments** page in Asset. The status is Ready to Run ••• until it runs for the first time. To run the assessment, click Run ▶.

> **Note:** Depending on the number of targeted endpoints, an assessment can take several hours to complete.

Work with assessments

About this task

After you create an assessment, run the assessment from the **Assessments** page in Asset to generate the assessment results in Microsoft Azure Migrate. Assessments in Asset can have the following states:

©2026 Tanium Inc. All Rights Reserved

Assessment states

Status	Description
Ready to Run	The assessment is configured and ready to run. Click Run to run the assessment.
In Progress	The assessment is in progress.
Completed	The assessment is complete and ready to open in Microsoft Azure Migrate. Click the link for the assessment on the **Assessments** page in Asset to open the resulting report in Microsoft Azure Migrate.
Canceled	The assessment was canceled while in progress.
Failed	The assessment failed to complete. Edit the assessment and confirm that all details are correct before you attempt to run the assessment again. For more information about troubleshooting, see Troubleshoot Microsoft Azure assessments on page 209 .

Run an assessment

1. From the Main menu, go to **Modules** > **Asset** > **Assessments**.
2. In the row for the assessment, click Run .

Result

Note: Depending on the number of targeted endpoints, an assessment can take several hours to complete.

Edit an assessment

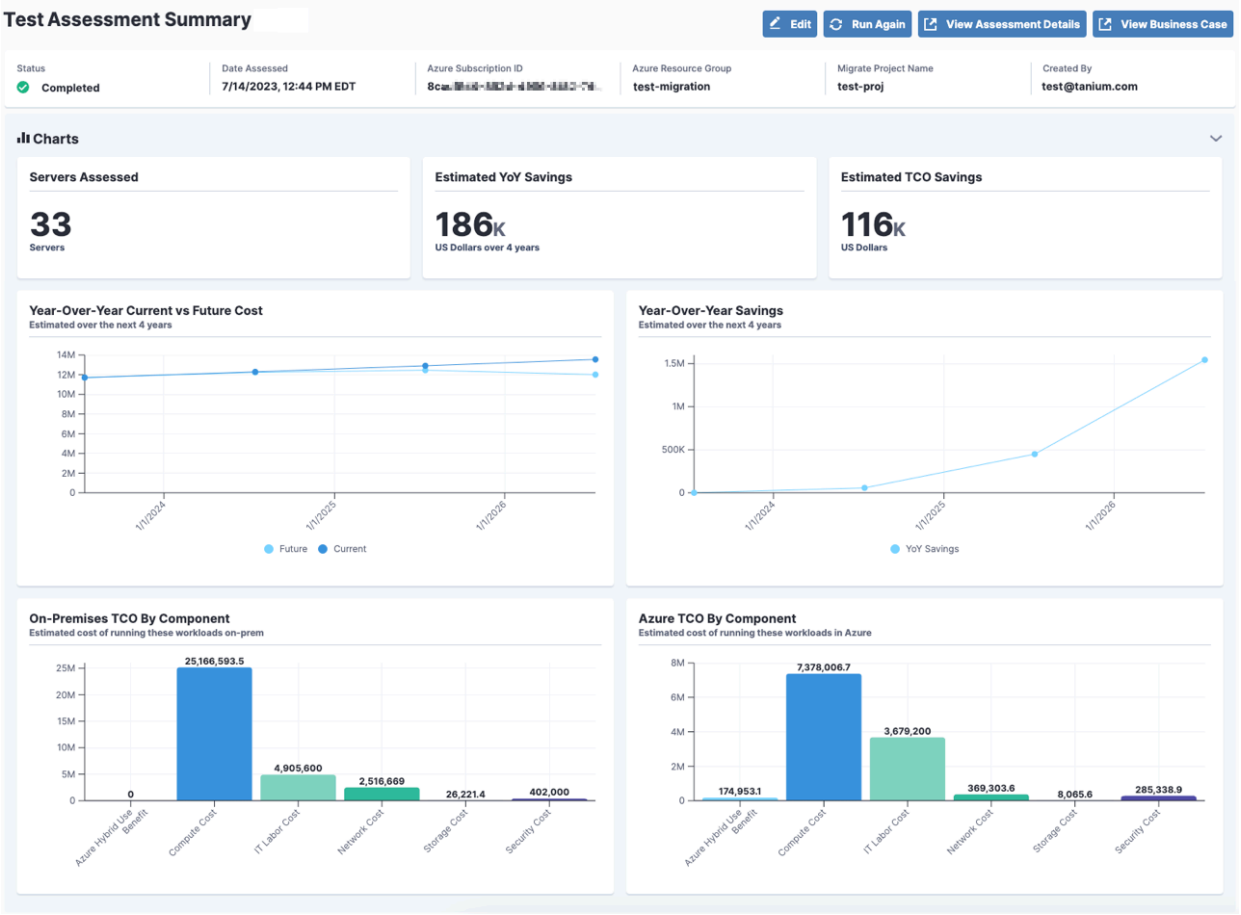
1. From the Main menu, go to **Modules** > **Asset** > **Assessments**.
2. In the row for the assessment, click Edit .
3. Make the necessary changes and click **Save**. Run the assessment again to use the updated details in the assessment results.

Open a completed assessment

1. From the Main menu, go to **Modules** > **Asset** > **Assessments**.

©2026 Tanium Inc. All Rights Reserved

2. Click the name of the assessment to open the assessment results.



3. (Optional) On the assessment page, click **View Assessment Details** to open the assessment in Microsoft Azure Migrate or **View Business Case** to open the business case in Microsoft Azure Migrate.
   For more information about interpreting the assessment results, see Microsoft Azure Migrate documentation: Review an assessment. For more information about business case reports, see Microsoft Azure Migrate documentation: Overview report.

Delete an assessment

1. From the Main menu, go to **Modules** > **Asset** > **Assessments**.
2. In the row for the assessment, click Delete .

Add Tanium data to a Microsoft Azure Migrate assessment

About this task

©2026 Tanium Inc. All Rights Reserved

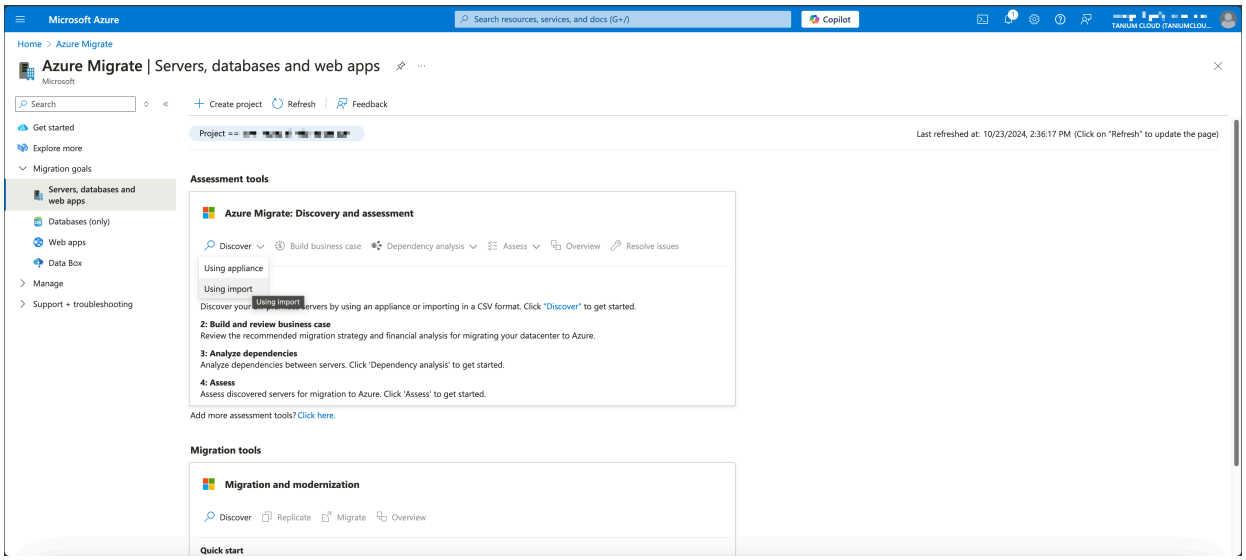
Use Tanium reports to build a report with the fields that you want to migrate, and then export the data to an Microsoft Azure Migrate project for assessment.

Prerequisites

- Complete steps one and two of Before you begin on page 172 to create a Microsoft Azure account and a Microsoft Azure Migrate project.
- You must have Tanium Reporting installed in your environment.
- You must have a user role with the **Report write** and **Report API user** permissions.

Steps

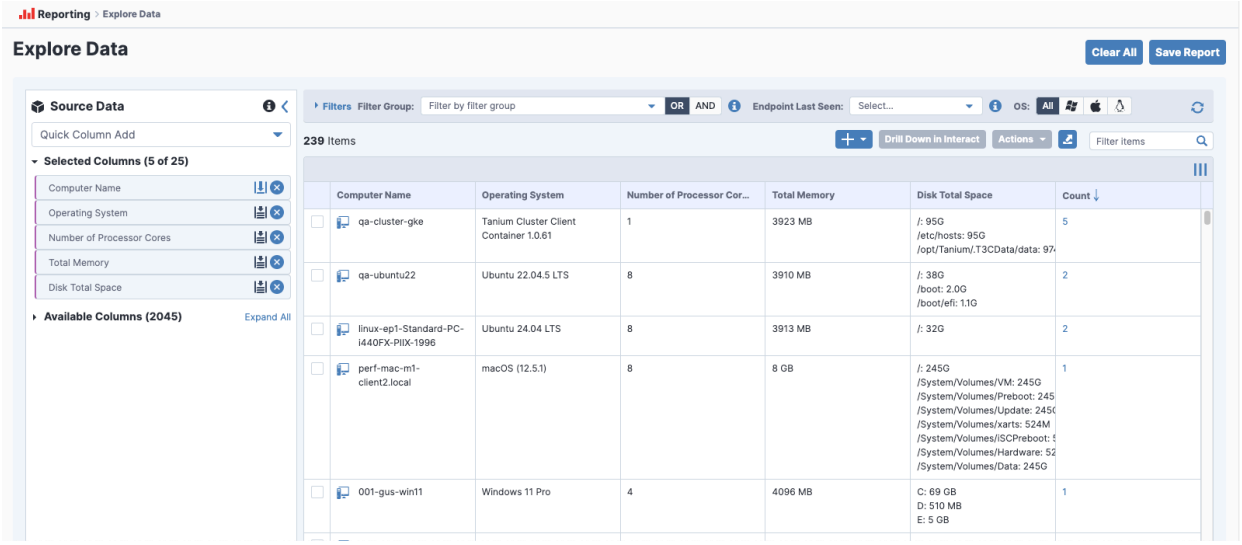
1. In the Microsoft Azure portal, go to the **Assessment tools** section and select **Discover** > **Using Import**.
   The **Discover** page opens.



2. Follow the steps listed on the **Discover** page. To start, download and review the example CSV template provided by Microsoft.
3. From the Main menu in Tanium Console, go to **Data** > **Reports**. The **Reports** page appears.
4. Click **Create Report** and create a report to target the Windows, Linux, and SQL Server endpoints in your environment that you want to migrate. Include the following initial fields:
   - Computer Name
   - Operating System

©2026 Tanium Inc. All Rights Reserved

- Number of Processor Cores
- Total Memory
- Disk Total Space



Note: For more information about additional functionality available in Tanium Reporting, see Tanium Reporting User Guide: Working with reports.

5. Include any additional fields listed in the example CSV template from Microsoft. You can find similar columns through the **Quick Column Add** option to add them to the Tanium Report.

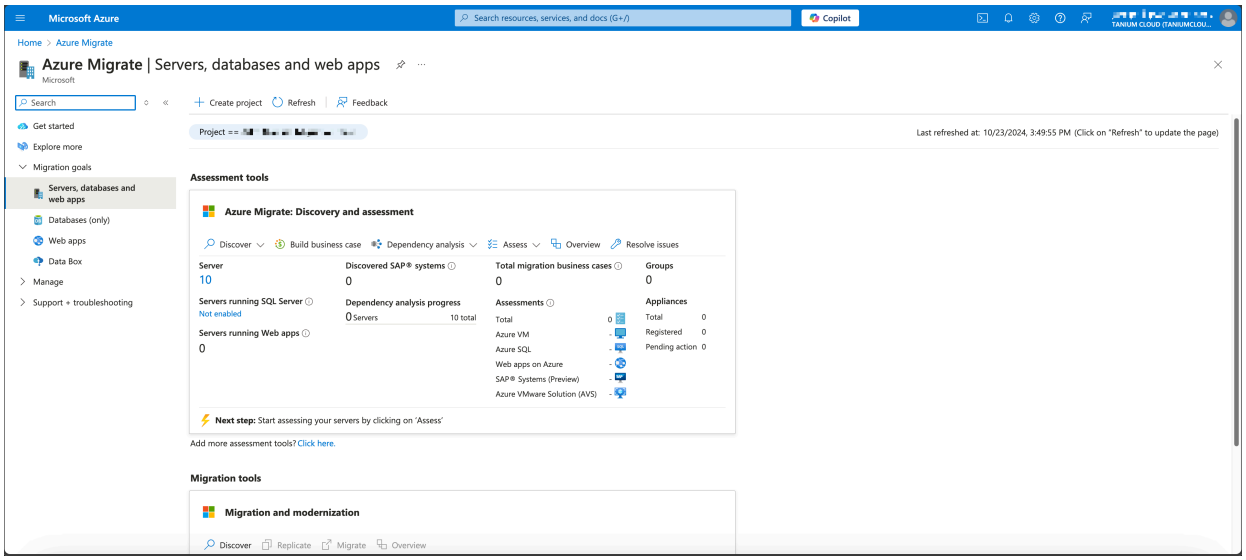
   Note: This step might take some time depending on how thorough you want the migration assessment. While only a handful of fields are required, you can select additional fields to increase the accuracy of the assessment data from the Microsoft Azure Migrate project.

6. Export the Tanium report to CSV and then manually add your Tanium data rows into the appropriate columns of the example CSV template from Microsoft. You might need to slightly modify some values from the Tanium data, such as **Memory** and **Storage**, to match the expected format from Microsoft.

7. After you add data from the Tanium report to match the example CSV template from Microsoft, follow step 3 on the **Discover** page to import the CSV file.

8. After the import process completes, return to the Microsoft Azure Migrate project page to verify that your servers are now visible, and that the **Build business case** and **Assess** options are now available.

©2026 Tanium Inc. All Rights Reserved



9. Build business cases or assess as needed, and then view the results.

Figure 11. Business case

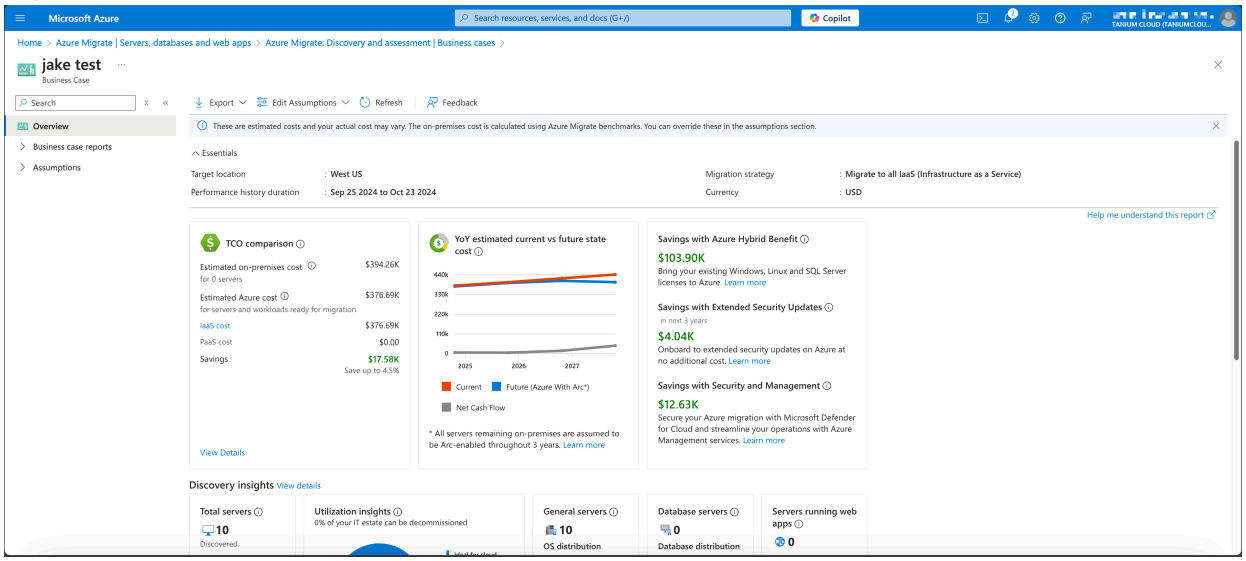
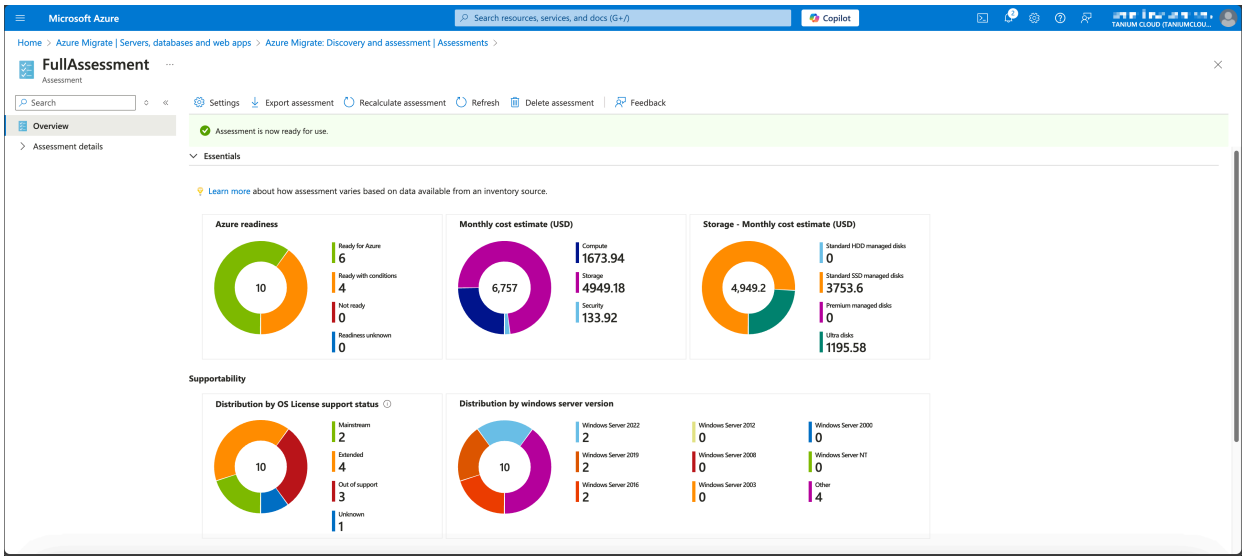


Figure 12. Asessment

©2026 Tanium Inc. All Rights Reserved



©2026 Tanium Inc. All Rights Reserved

Viewing containers

About this task

Use Asset to view the containers in your environment.

- To view containers in Asset, Tanium™ Cloud Workloads must be installed on the Tanium Server. For more information, see Asset requirements on page 26.
- You must have a role with the **Asset Report read** permission to view container reports and details.

View container charts

About this task

The **Asset Overview** page includes a **Containers** section with the following chart panels:

- Hosts Running the Most Containers
- Clusters Running the Most Containers
- Running Privileged Containers Over Time
- Running Unprivileged Containers Over Time

Figure 13. Example Container Inventory section

©2026 Tanium Inc. All Rights Reserved



Click a data point on any chart to view that chart data in a report. For more information about how to view additional report options, see Tanium Reporting User Guide: Working with reports.

View container images

1. From the Main menu, go to **Modules** > **Asset** > **Container Details**.
2. Click **Container Image Inventory Report for Scanned Registries**.
   The **Container Image Inventory Report for Scanned Registries** page opens to show container images in registries that are enabled for scanning.

©2026 Tanium Inc. All Rights Reserved

3. The following actions are available:

Available actions on the Container Image Inventory Report for Scanned Registries page

Option	Description
Filter by publish date	Select an option for the **Published** filter to limit which images appear.
Filter by text	Enter an alphanumeric string in the **Filter items** field to match text in any column.
Sort by column	Click any column header to sort the list of rules by that column.
Export to CSV	To download a CSV file of the table as it currently appears, click Export to CSV .
Refresh page	Click Refresh .
Manage columns	Click Customize Columns and drag the column names in the desired order. To remove a column, deselect the checkbox next to the column name.
View image details	Click Expand Details in the row of the image that you want to view. A slide-out panel opens to show a list of hashes found in the environment. Click a hash to view details for the hash, including a list of the endpoints on which the hash is found. For more information, see View image details on page 192 .

View image SBOM

About this task

Note: To view container image SBOMs, you must have the SBOM add-in installed. For more information, see Creating a Software Bill of Materials on page 159.

1. From the Main menu, go to **Modules** > **Asset** > **Container Details**.
2. Click **Container Image Inventory Report for Scanned Registries**.
   The **Container Image Inventory Report for Scanned Registries** page opens to show

©2026 Tanium Inc. All Rights Reserved

container images in registries that are enabled for scanning.

3. Click Expand Details in the row of the image that you want to view. The **Present in Registries** slide-out panel opens to show a list of matching hashes found in registries of endpoints in the environment appears.
   The following options are available on the **Present in Registries** slide-out panel:

Available options on the Present in Registries panel

Option	Description
Filter by text	Enter an alphanumeric string in the **Filter items** field to match text in any column except the **Tag** column.
Sort by column	Click any column header to sort the list of rules by that column.
Export to CSV	To download a CSV file of the table as it currently appears, click Export to CSV .
Refresh page	Click Refresh .
Manage columns	Click Customize Columns and drag the column names in the desired order. To remove a column, deselect the checkbox next to the column name.
Close dialog	Click **X** in the upper right corner of the page to return to the **Container Image Inventory Report for Scanned Registries** page.
View image details	Click the name of a **Hash** to view image details for the corresponding hash, including a list of the endpoints on which the image is found.
View image SBOM	Click the value in the **Packages** column to view the software bill of materials (SBOM) for the image.

4. Click a value in the **Packages** column to view the image SBOM for the matching hash.
   The **Image SBOM** page appears to show the image hash, instances of the hash in registries, and packages for the hash.

   The following options are available for both the **Instances** table and **Packages** table:

©2026 Tanium Inc. All Rights Reserved

Available options on the Image SBOM page

Option	Description
Filter by text	Enter an alphanumeric string in the **Filter items** field to match text in selected columns. • For the **Instances** table, the filter looks for matching text in the **Image Name** and **Registry** columns. • For the **Packages** table, the filter looks for matching text in all columns.
Sort by column	Click any column header to sort the list of rules by that column.
Export table data	To download a CSV file of the table as it currently appears, click **Export** and then select **Export to CSV**. To copy the table data to the clipboard, click **Export** and then select **Copy to clipboard**.
View image details	(**Instances** table only) Click in the **Image Details** column to view the image details.
Filter by value	(**Packages** table only) To filter the table by one or more specific columns, expand **Filters** and enter values in the corresponding column filters.

View image details

About this task

Note: To view container image SBOMs, you must have the SBOM add-in installed. For more information, see Creating a Software Bill of Materials on page 159.

1. From the Main menu, go to **Modules** > **Asset** > **Container Details**.
2. Click **Container Image Inventory Report for Scanned Registries**.
   The **Container Image Inventory Report for Scanned Registries** page opens to show container images in registries that are enabled for scanning.
3. Click Expand Details in the row of the image that you want to view. A list of matching hashes found in registries of endpoints in the environment appears.
   For more information about available options when viewing matching hashes, see View container images on page 189.

©2026 Tanium Inc. All Rights Reserved

4. Click the name of a **Hash** to view image details for the corresponding hash, including a list of the endpoints on which the image is found.
   The following options are available when viewing image details:

Available options when viewing image details

Option	Description
Filter by text	Enter an alphanumeric string in the **Filter items** field to match text in the **Cluster Name**, **IP Address**, **Currently Running**, **Runs in 30 Days**, **Type**, and **Computer ID** columns. To show columns that do not contain matching text, toggle **Contains** to **Does not contain**.
Sort by column	Click any column header to sort the list of rules by that column.
Export usage table	To download a CSV file of the **Usage** table as it currently appears, click Export All, select any naming and format options, then click **Export**.
Refresh page	Click Refresh.
Manage columns	Click Customize Columns and drag the column names in the desired order. To remove a column, deselect the checkbox next to the column name.
Wrap words in usage table	Word wrap is enabled by default. To unwrap words in the table, toggle the Wrap option.
View image SBOM	Click the **Hash** value in the **Image Details** section.

View endpoints that host clusters

1. From the Main menu, go to **Modules** > **Asset** > **Container Details**.
2. Click **Endpoints Hosting Clusters**.
   The **Endpoints Hosting Clusters** page opens to show all endpoints with running containers in the environment.

©2026 Tanium Inc. All Rights Reserved

3. The following actions are available:

Available actions on the Endpoints Hosting Clusters page

Option	Description
Filter by vulnerability	Toggle to show endpoints with software vulnerabilities. Software vulnerability information is supplied by Tanium Comply; this toggle only appears in you have Comply installed and licensed in your environment.
Filter by text	Enter an alphanumeric string in the **Filter items** field to match text in any column.
Apply advanced filters	To add advanced filters, expand **Filters** and then add individual or groups of filters. You can then add filters in rows and groups. **Note:** Tanium Asset processes nested filters (group filters) and applies Boolean AND/OR logic in the same way that Tanium Interact does for question results. For more information, see Tanium Interact User Guide: Overview of advanced filters .
Sort by column	Click any column header to sort the list of rules by that column.
Export to CSV	To download a CSV file of the list of containers as it currently appears, click .
Refresh page	Click Refresh .
Manage columns	Click Customize Columns and drag the column names in the desired order. To remove a column, deselect the checkbox next to the column name.

View Kubernetes clusters

About this task

Perform the following steps to view managed and unmanaged Kubernetes clusters in the environment.

1. From the Main menu, go to **Modules** > **Asset** > **Container Details**.
2. Click **Kubernetes Clusters**.
   The **Kubernetes Clusters** page opens to show managed and unmanaged Kubernetes clusters

©2026 Tanium Inc. All Rights Reserved

in the environment.

3. The following actions are available for both **Managed Clusters** and **Unmanaged Clusters**:

Available actions on the Kubernetes Clusters page

Option	Description
Filter by text	Enter an alphanumeric string in the **Filter items** field to match text in any column except the **Labels** and **Actions** columns.
Filter by provider	To add advanced filters, expand **Filters** and then add individual or groups of filters. You can then add filters in rows and groups. • To add an individual filter, click **+ Row**, select a source, column (if applicable), operator, and value that endpoints must match, and then click **Apply**. • To add related filters, click **+ Grouping**. For each filter, select a source, column (if applicable), operator, and value that endpoints must match, and then click **Apply**. Select this option to nest a Boolean operator and then add rows or more groups to build the nested expression.
Sort by column	Click any column header to sort the list of rules by that column.
Export to CSV	To download a CSV file of the list of containers as it currently appears, click .
Copy cluster info to clipboard	Select the checkboxes next to one or more clusters and click **Copy** . Asset copies information for the selected clusters to the clipboard in a JSON format.
Refresh table	Click Refresh .
Manage columns	Click Customize Columns  and drag the column names in the desired order. To remove a column, deselect the checkbox next to the column name.
Edit cluster management YAML	To edit the cluster management YAML details for a managed cluster, click Edit  in the row of a cluster in the **Managed Clusters** table. For more information about how to complete the **Generate Cluster Management YAML** form, see Tanium Cloud Workloads User Guide: Generate the deployment files .
Manage a cluster	To have Tanium manage a cluster, click **Manage** in the row of a cluster in the **Unmanaged Clusters** table. For more information about how to complete the **Generate Cluster Management YAML** form,

©2026 Tanium Inc. All Rights Reserved

Option	Description
	see Tanium Cloud Workloads User Guide: Generate the deployment files .
View cluster details	Click the name of a cluster to view details for the cluster. You can only view details of clusters that are currently online.

View running Kubernetes containers in the environment

1. From the Main menu, go to **Modules** > **Asset** > **Container Details**.
2. Click **Running Containers**.
   The **Running Containers** page opens to show endpoints that host one or more Kubernetes container images in the environment. The grid contains the following columns by default:

Columns on the Running Containers page

Option	Description
Endpoint	The name of the endpoint with the running container. Click Endpoint Details  to view basic details for the specific endpoint. From the Endpoint Details dialog, click **View Details** to view more comprehensive details on the **Endpoint Details** page. For more information, see Tanium Reporting User Guide: Working with a single endpoint .
Container ID	The ID of the container.
Image Name	The name of the container image. Click to view image details for the container, including a list of the endpoints on which the image is found.
Image Hash	The name of the image hash. Click to view image details for the container, including a list of the endpoints on which the image is found.
Tag	The version of the image.
Privileged	Value is  if the container is running in privileged mode.
Rogue	Value is  if the container is not in a registry that Tanium Cloud Workloads can manage. For more information about how to enable Cloud Workloads to manage the registry, see Tanium Cloud Workloads User Guide: Configure Cloud Workloads .

©2026 Tanium Inc. All Rights Reserved

3. The following options are available:

Available options on the Running Containers page

Option	Description
Filter by text	Enter an alphanumeric string in the **Filter items** field to match text in any column except the **Tag** and **Rogue** columns. To show columns that do not contain matching text, toggle **Contains** to **Does not contain**.
Apply advanced filters	To add advanced filters, expand **Filters** and then add individual or groups of filters. You can then add filters in rows and groups.  **Note:** Tanium Asset processes nested filters (group filters) and applies Boolean AND/OR logic in the same way that Tanium Interact does for question results. For more information, see Tanium Interact User Guide: Overview of advanced filters.
Sort by column	Click any column header to sort the list of rules by that column.
Export to CSV	To download a CSV file of the table as it currently appears, click Export All , select any naming and format options, then click **Export**.
Manage columns	Click Customize Columns  and drag the column names in the desired order. To remove a column, deselect the checkbox next to the column name.
Wrap words in table	Word wrap is enabled by default. To unwrap words in the table, toggle the Wrap  option.
View image details	Click an **Image Name** or **Image Hash** to view image details for the corresponding hash, including a list of the endpoints on which the image is found.
View Endpoint Details page	In the Endpoint column, click Endpoint Details  next to an endpoint name to view basic details for the specific endpoint. From the Endpoint Details dialog, click **View Details** to view more comprehensive details on the **Endpoint Details** page. For more information, see Tanium Reporting User Guide: Working with a single endpoint.

View image run history

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Asset** > **Container Details**.
2. Click **Container Image Inventory Report for Scanned Registries**.
   The **Container Image Inventory Report for Scanned Registries** page opens to show container images in registries that are enabled for scanning. For more information about how to review available options on the **Container Image Inventory Report for Scanned Registries** page, see View container images on page 189.
3. Click Expand Details  in the row of the image that you want to view. A list of matching hashes found in registries of endpoints in the environment appears.
4. Click the name of a **Hash** to view image details, including a list of the endpoints on which the image is found.
5. In the **Usage** section, click a value in the **Runs in 30 Days** column to view the image run history for the corresponding endpoint.
6. The following options are available on the **Image Run History** page:

Available options on the Image Run History page

Option	Description
Filter by text	Enter an alphanumeric string in the **Filter items** field to match text in the **Start**, **End**, and **Run Time** columns.
Filter by column	To add advanced filters, expand **Filters** and then add individual or groups of filters. You can then add filters in rows and groups. • To add an individual filter, click **+ Row**, select a source, column (if applicable), operator, and value that endpoints must match, and then click **Apply**. • To add related filters, click **+ Grouping**. For each filter, select a source, column (if applicable), operator, and value that endpoints must match, and then click **Apply**. Select this option to nest a Boolean operator and then add rows or more groups to build the nested expression.
Sort by column	Click any column header to sort the list of rules by that column.
Export run history	To download a CSV file of the **Run History** table as it currently appears, click **Export** and then select **Export to CSV**. To copy the table data to the clipboard, click **Export** and then select **Copy to clipboard**.

©2026 Tanium Inc. All Rights Reserved

Maintaining Asset

About this task

Perform regular maintenance tasks to ensure that Asset successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Asset is not performing as expected, you might need to troubleshoot issues or change settings. For more information about how to view related procedures, see Troubleshooting Asset on page 202.

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**.

©2026 Tanium Inc. All Rights Reserved

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**.

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**.

Monitor and troubleshoot key vendors with tracked products

The following table lists contributing factors into why the Key Vendors with Tracked Products metric might be lower than expected and corrective actions you can make.

Factors that contribute to a lower-than-expected Key Vendors with Tracked Products metric

Contributing factor	Corrective action
Products are not tracked	In **Software Inventory & Usage** > **All Products**, track products from key vendors.
Lack of knowledge on which products to track	Use the hidden **Asset** **SIU** sensors for ad hoc validation of endpoint usage. Based on that informal validation, identify products to track.

©2026 Tanium Inc. All Rights Reserved

Monitor and troubleshoot unused tracked software

The following table lists contributing factors into why the Unused Tracked Software metric might be lower than expected and corrective actions you can make.

Factors that contribute to a lower-than-expected Unused Tracked Software metric

Contributing factor	Corrective action
Extraneous software is being tracked	• Only track software that is valuable to the business • Only track software when tracking is in accordance with your company's software asset management charter
No formal software reclamation guidelines exist	Work with your asset management team to clearly define when software should be reclaimed. This could be based on last used date or overall usage over time. An example might be consistent low usage of an expensive piece of software.

©2026 Tanium Inc. All Rights Reserved

Troubleshooting Asset

About this task

To collect and send information to Tanium for troubleshooting, collect log and other relevant information.

Collect logs

About this task

The information is saved as a ZIP file that you can download with your browser. The zip file is also known as a support bundle.

1. From the **Asset Overview** page, click Help ?.
2. Go to the **Troubleshooting** tab and click **Collect**. When the ZIP file is ready, you can download the tanium-asset-support-[timestamp].zip file to your local download directory.
3. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 222.

Update service log level

1. From the **Asset Overview** page, click Settings ⚙, and then go to the **Advanced** tab.
2. Change the **Service Log Level**. The following log levels are available:

   #### Log levels in the Asset service log

Log Level	Numeric Level	Description
Error	50	Generally fatal within the scope of logged operation.
Warning	40	Not immediately fatal but requires attention.
Informational	30	Normal operations.

©2026 Tanium Inc. All Rights Reserved

Log Level	Numeric Level	Description
Debug	20	Additional level of information detail generally too verbose for log level 30.
Trace	10	Highly detailed application-level logging; helpful when more detail is needed. For example: what events occurred before, during and after a warning or error occurred.

3. Click **Save**.

Configure report timeout period

About this task

Configure the report timeout period to increase or decrease the amount of time that Asset tries to load a report page before presenting a timeout error. To troubleshoot the error, see Troubleshoot reports on page 204.

1. From the **Asset Overview** page, click Settings, and then go to the **Advanced** tab.
2. Specify the **Report Timeout** in minutes. After this timeout period, Asset presents an error.
3. Click **Save**.

Reset differential load

About this task

To optimize performance, Asset imports data from Tanium Data Service incrementally. As an Asset administrator, you have the option to perform a one-time import for a complete load from Tanium Data Service. Be aware that importing a complete load might take longer than the regular incremental loads.

1. From the **Asset Overview** page, click Settings and then go to the **Advanced** tab.
2. In the **Reset Differential Load** section, select **Enabled**.
3. Click **Save**.

Result

©2026 Tanium Inc. All Rights Reserved

The next time Asset is scheduled to import data, Asset imports a complete load from Tanium Data Service. Asset reverts the **Reset Differential Load** option and future scheduled imports retrieve incremental data.

Troubleshoot reports

About this task

If you see a report timeout error message when trying to view a report, consider the following resolutions or workarounds.

- Try to view the report again.
- Configure report timeout period on page 203.
- Look at the data using a view.
    - Create a view that includes the assets. For more information, see Configuring views on page 123.
    - Export the data to Connect or another destination. For more information, see Exporting data on page 138.

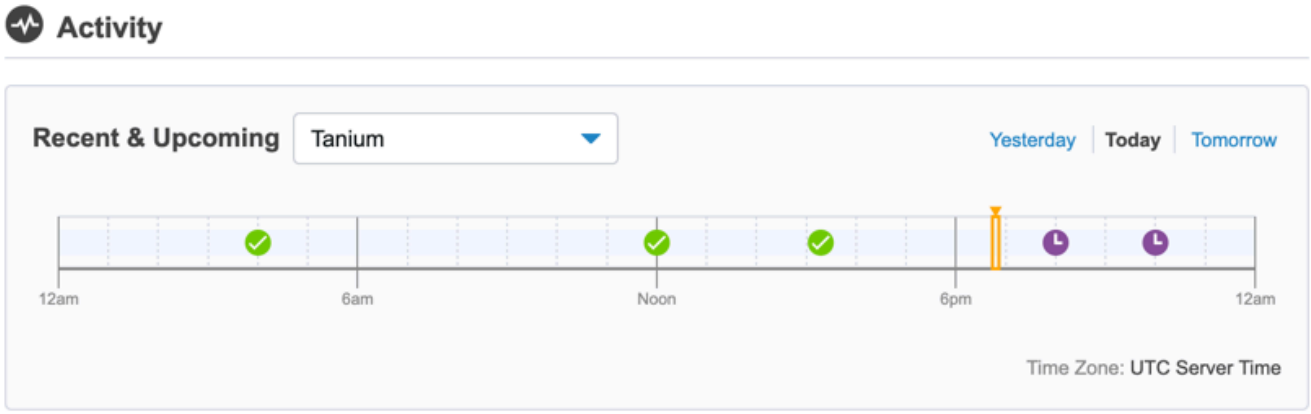
Troubleshoot asset data exports and imports

View status of imports and exports

On the Asset **Overview** page in the **Activity** section, you can view a timeline of the recent imports and exports.

Figure 14. Example Activity section from the Asset Overview page

©2026 Tanium Inc. All Rights Reserved



The timeline contains each job run, with one of the following statuses:

Icon	Status
	Scheduled
	Successful
	Error

To view the **Job Run History** page for runs that finished successfully or failed with an error , click the status icon of the run on the timeline.

Tip: You can view the log for the latest import of each AWS, Microsoft Azure, Microsoft Intune, and Google compute source in Asset. For more information, see Monitor compute source import runs on page 98.

View import and export logs

About this task

In the ZIP file that you download from the **Help** section, you can view logs for the data imports and exports. These logs are in the job directory:

©2026 Tanium Inc. All Rights Reserved

ServiceNow exports

ServiceNow export logs are named with the following format: job/date_time_job#_servicenow_config#.log. If you enable `Trace` level logging on your ServiceNow configuration, numbered subdirectories, for example job/65, are created that contain all of the POST and GET requests for that job. To configure logging, see Add ServiceNow as a destination on page 154.

Asset data imports

You can use these logs to view details about the scheduled runs that are occurring to import asset data from Tanium into your Asset database. Tanium data import logs are named with the following format: job/date_time_job#_tanium_1.log. For data you are importing from a database, import logs are named with the following format: job/date_time_job#_database_1.log. To change the log level for imports, see Configuring sources on page 65.

Tip: You can view the log for the latest import of each AWS, Microsoft Azure, Microsoft Intune, and Google compute source in Asset. For more information, see Monitor compute source import runs on page 98.

Disable imports and exports

About this task

Data imports and exports run on a configured schedule by default. You can disable this schedule to resolve issues, or you can run the import or export manually.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Schedules**.
2. Hover over the import or export schedule that you want to disable and click Edit .
3. Clear the **Run this connection on a defined schedule** setting. Click **Update**.
4. If you want to manually run an import or export, go to the **Inventory Management** > **Schedules** page. In the row of the source that you want to import or export, click Run Now .

©2026 Tanium Inc. All Rights Reserved

Fix Error: MULTIPLE_DUPLICATE_RECORDS error message in ServiceNow log file

About this task

If you see an `Error: MULTIPLE_DUPLICATE_RECORDS` error message in the ServiceNow log file, contact Tanium Support to verify that the ServiceNow export mapping configuration is configured correctly. For more information, Contact Tanium Support on page 222.

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Destinations**.
2. Click Edit next to the destination.
3. In the **ServiceNow Mappings** section, add the following property to the **cmdb_ci_computer** mapping:

```
identificationFields: [
  [
    "name",
    "serial_number"
  ]
],
```

4. Click **Update**.

Fix missing information in export to ServiceNow with Tanium Asset integration

About this task

If Asset has finished exporting data to ServiceNow using the Tanium Asset integration and some endpoints are missing or are missing information, work with Tanium Support to review trace logs and make necessary changes.

1. Update the ServiceNow destination log level to trace.
    a. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Destinations**.
    b. Click Edit next to the destination.
    c. Set the **Log Level** to **Trace**.
    d. Click **Update**.
2. Run the export again.
    a. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Schedules**

©2026 Tanium Inc. All Rights Reserved

and then go to the **Export Schedules** tab.

b. Click **Run Now** next to the schedule.

3. Collect logs on page 202.
   The logs include a ServiceNow > Jobs folder that contains job IDs for the requests and responses made to ServiceNow.

4. Contact Tanium Support on page 222 for assistance reviewing logs and making necessary changes.
   Search the logs for the following errors.

Potential log errors for missing information in ServiceNow exports

Error	Explanation
`ABANDONED`	Generally, jobs are abandoned because of a large number of errors. These errors might occur because of the difference between identifying an endpoint in Asset and ServiceNow. Asset identifies endpoints based on multiple attributes, and ServiceNow (by default) identifies endpoints based on a unique name and serial number. This error might also indicate missing required fields in ServiceNow because of data class customization or a different business rule.
`TIMED`	Timed out jobs are usually caused by a business rule or other database issue within ServiceNow. If the `duration` field in the log file is around 300, Asset might have exported too much data to ServiceNow. You can decrease the job size using an `API Settings` mapping.
`logContextID`	`logContextId` indicates that an entry in the job was logged. Errors are usually categorized as `ABANDONED` or `TIMED`.

Fix duplicate entries in ServiceNow with Tanium Asset integration

About this task

If you use ServiceNow Paris, Quebec, or Rome with the Tanium Asset integration, ServiceNow creates duplicate entries for some CIs (such as Network Adapters, Storage Devices, and File Systems) in the ServiceNow CMDB when an export runs. This is a known ServiceNow issue. Update the ServiceNow system properties to work around this issue.

1. In ServiceNow, enter `sys_properties.list` in the **Filter navigator**.

2. In **System Properties**, click **New**.

©2026 Tanium Inc. All Rights Reserved

3. Enter `glide.identification_engine.dependent_items_bulk_query` as the **Name** and `true` as the **Value**.
4. Click **Submit**.

Troubleshoot software inventory and usage monitoring

About this task

To return inventory and usage data, endpoints must have the correct version of Asset and the **swmgr** tool installed.

1. In Interact, ask the following question: `Get Endpoint Configuration - Tools Status Details from all machines`
2. For the Asset tool name, confirm that the installed version is correct.
3. For the **swmgr-cx** tool name, confirm that the installed version is 2.0.34 or later.

Troubleshoot Microsoft Azure assessments

About this task

If the connection verification in a Microsoft Azure assessment fails, check these details:

- Confirm that the required URLs are allowed in your environment. For more information, see Step 6: Confirm that the necessary URLs are allowed through your security software on page 178.
- Confirm that the service principal has the Contributor or Owner role. For more information, see Step 4: Grant the necessary permissions to the service principal for the registered app on page 177.
- Check to confirm that you are using the correct values for **Directory (tenant) ID**, **Application (client) ID**, and **Client Secret**.
- Check the Microsoft Azure migration log on the Tanium Module Server for errors. You can find this log in *<Module Server>*\services\asset-files\logs\job

©2026 Tanium Inc. All Rights Reserved

Troubleshoot disabled attributes

Issue

Attributes are automatically disabled on the **Modules** > **Asset** > **Inventory Management > Entities & Attributes** page.

Causes

Asset disables attributes for the following reasons:

- Attributes are supplied to Asset through sensor results harvested by Tanium Data Service. If harvesting for the underlying sensor is disabled in Tanium Data Service, Asset disables the attribute. For more information about data collection through Tanium Data Service, see Tanium Interact User Guide: Managing Tanium Data Service.
- When a change occurs to the underlying sensor that retrieves data for a custom attribute, Asset disables the attribute.

Solution

1. Check to see if the sensor recently changed:
    a. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Entities & Attributes**. Search for the attribute and then expand the attribute. Remember the name in the **Entity** column.
    b. From the Main menu, go to **Administration** > **Content** > **Sensors**.
    c. Search for the name that was in the **Entity** column on the **Entities & Attributes** page.
    d. View the timestamp in the **Last Modification** column to see when the sensor last changed.

©2026 Tanium Inc. All Rights Reserved

> **Tip:** Ensure that you can view the entire width of the table. If the **Last Modification** column does not appear, click Customize Columns  and select the option to show the **Last Modification** column.

2. If the sensor recently changed, perform the following steps to enable the attribute:

    a. Manually delete the attribute. For more information, see Delete attributes on page 213.

    b. Wait a minimum of one hour for the next load from Tanium Data Service.

    c. Re-add the attribute to Asset. For more information, see Configure additional Tanium entities and attributes on page 111.

    d. Wait at least two import cycles from the Tanium source. Tanium Data Service gathers results from endpoints after which Asset retrieves those results from Tanium Data Service.

    > **Note:** For more information about import intervals, see About the Tanium source on page 66.

    e. Verify the attribute is enabled. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Entities & Attributes** and search for the attribute. Expand the attribute entry and verify the status of the attribute is **Ready**.

3. If the sensor did not recently change, the sensor might not be compatible with Tanium Data Service. If the sensor returns multiple columns of data, such as the **Running Applications** sensor, you might be able to clone the sensor and remove any columns that you do not need.

> **Tip:** When you create a sensor to register with Tanium Data Service, consider that results collection consumes resources such as network bandwidth, processing on endpoints, and resources on the Tanium Server. Resource consumption increases with the cardinality of sensors. For more information, see Tanium Interact User Guide: Resource consumption for registered sensors.

©2026 Tanium Inc. All Rights Reserved

a. Clone the sensor and update the sensor script to reduce the amount of information returned. For more information, see Tanium Console User Guide: Clone a sensor.

b. Add the attribute to Asset. For more information, see Configure additional Tanium entities and attributes on page 111.

c. Wait at least two import cycles from the Tanium source. During this time, Asset registers the sensor with Tanium Data Service. Tanium Data Service then gathers results from endpoints after which Asset retrieves those results from Tanium Data Service.

> **Note:** For more information about import intervals, see Configure the Tanium source on page 66.

d. Verify the attribute is enabled. From the Main menu, go to **Modules** > **Asset** > **Inventory Management** > **Entities & Attributes** and search for the attribute. Expand the attribute entry and verify the status of the attribute is **Ready**. If the attribute is disabled, the underlying sensor is most likely high cardinality and cannot be registered with Tanium Data Service.

Back up and restore the Asset database

About this task

You can back up or restore all configuration and Asset data. You might want to create a backup before making configuration updates. You must have the Tanium Administrator role to perform a backup operation.

> **Important:** The Asset database is migrated to RDB in Asset 1.19. After you install this release, you will be unable to restore data from database backups generated from previous versions of Asset. You can generate new backups after the migration and use those to restore data at a future point using the same process.

1. From the **Asset Overview** page, click Settings, and then go to the **Database** tab.
2. To create a backup of the Asset database, click **Back Up Database**.

©2026 Tanium Inc. All Rights Reserved

3. Use the backups.
    - Download backup on local computer: Click Download Database Backup .
    - Restore database backup: Click Restore Database Backup . Before you restore, verify that no Asset destination exports or Tanium Connect connection runs are running. When you run the restoration, the current Asset database is backed up, the Asset service is shut down, the selected database is restored, and the Asset service is restarted. Any jobs that are running during the restoration process do not complete. To restore the database on a different Module server, Contact Tanium Support on page 222.
    - Delete a backup: Click Delete Database Backup .

Remove unneeded data from the Asset database

Purge assets

Asset purges stale assets on an individual basis. Asset purges endpoints if not seen within the configured stale data age for the source from which the asset originates, or based on a purge report. For more information, see Configure data retention and vacuuming on page 214.

Asset Administrators or Asset Operators can manually remove assets from the Asset database earlier than the stale data age. In a report that shows the assets you want to remove, select the rows and click **Delete**.

If the asset you deleted returns results for sensors registered with Tanium Data Service, the asset is re-added to the Asset database. Note that when the asset is re-added, the asset might only contain partial data due to incremental loads from Tanium Data Service. To fully re-add a purged asset, you can perform a one-time import for a complete load from Tanium Data Service. For more information, see Reset differential load on page 203.

Delete attributes

About this task

To delete an attribute, you must disable the attribute, then remove references.

©2026 Tanium Inc. All Rights Reserved

Note: When you disable an attribute, Tanium Data Service unregisters the underlying sensor if the sensor is not registered by another Tanium solution.

1. Disable the attribute.
    a. From the Main menu, go to **Modules >** Asset **> Inventory Management > Entities & Attributes**.
    b. Expand the entity that contains the attribute and click Edit next to the attribute that you want to disable.
    c. Clear the **Enabled** setting. Click **Save**.
2. Remove references to the attribute from all reports, views, permissions, and ServiceNow destinations.
    a. Click Delete next to the attribute that you want to remove.
    If the option to delete an attribute does not appear, make sure to disable the attribute, wait one minute, and then refresh the **Entities & Attributes** page.
    b. A list of known locations where the attribute is used appears. Click the link for each item and then edit the item to remove the use of the attribute.
    c. Click **Refresh** to list the remaining references.
3. After you remove the references, type the name of the attribute to confirm its deletion. Click **Delete Attribute**.

Result

The attribute is deleted from the Asset database on the next load of data from Tanium Data Service.

Note: When you delete the last attribute for an entity, including custom entities, Asset also deletes the entity.

Configure data retention and vacuuming

About this task

You can configure data retention and automatic vacuuming on the Asset database.

1. From the **Asset Overview** page, click Settings, and then go to the **Advanced** tab.
    - Asset purges stale assets by source. To purge stale assets from the Tanium source that have not been seen by Asset within the timeframe of the configured stale data

©2026 Tanium Inc. All Rights Reserved

age, enable **Purge Stale Assets**. Then, indicate the age of stale data to remove. The minimum number is seven days. The default is 180 days. The maximum number is 3,660 days.

Tip: If you set the maximum number to a large number, consider filtering old assets from reports and views.

- To purge assets based on a report, enable **Purge by Report** and select the report. To select a report, you must be an Asset Administrator or Asset Operator and not assigned to an Asset user permissions group. The report must meet the following criteria:
  - Is not a summary or reserved report.
  - Only has attributes from the Asset column.
  - Has a filter with attributes that do not include parentheses. For example, the report can include **Asset ID** but not **Device ID (Physical Disk)**.
- To purge short-lived assets, enable **Purge Short-lived Assets**. Short-lived assets are endpoints that are online less than 1% of the time (approximately 30 minutes) in the first 48 hours after Asset adds them to the Asset database. When you select this option, Asset purges endpoints that have less than 1% usage through the first 30 days. Purges run at the start of every hour. If an asset falls below the 1% usage threshold, Asset purges the asset from its database.

  Note: Asset computes usage as `(online time / (days * 24 hours) = usage)`. For example, if an endpoint is added to Asset and is used for an hour in the first two days, the endpoint is not purged as the endpoint is online for approximately 2% of the time, or `(1 hour / 48 hours = ~2.08%)`. If the endpoint is not used for the next three days, the usage falls to less than 1% usage and Asset purges the asset as short-lived `(1 hour / 120 hours = ~0.8%)`. For more information about how Tanium Data Service purges short-lived assets, see Tanium Interact User Guide: Purging short-lived endpoints.

  After 30 days, Asset no longer considers the asset as short-lived and does not purge the asset as short-lived.

©2026 Tanium Inc. All Rights Reserved

- To adjust the trigger and amount of work done during automatic vacuuming, navigate to the **Automatic Vacuuming** section to adjust the **Cost Limit** and **Scale Factor** values. The Postgres VACUUM operation reclaims storage that is occupied by dead tuples. By default, the database is vacuumed when 1% of tuples are considered dead, and the cost limit (amount of work per vacuum cycle) is set to 1000.

2. Click **Save**.
3. For custom sources, configure when to purge stale assets from each source when you create or edit the source. For more information about how to create or edit custom sources, see Configuring sources on page 65.

Verify endpoint tools

If you are experiencing issues such as a feature not working on an endpoint or seeing incorrect data in the workbench, confirm that your endpoints have the latest toolset version.

For more information, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or Client Extensions and Reference: Client extensions and endpoint tools used for Tanium solutions.

Identify and resolve issues with Client Extensions

About this task

Use the following steps to troubleshoot issues with the Client Extensions that Asset installs and uses. During troubleshooting, consider environmental factors such as security exclusions, file locks, CPU usage, RAM usage, and disk failures.

Tip: For more information about the Client Extensions that Asset installs and uses, see Client Extensions on page 28.

1. If endpoints have Client Extension shared process mode enabled and you need to troubleshoot resource usage or crashes in the combined TaniumCX.exe or TaniumCX process, disable shared process mode on the affected endpoints, and then reproduce the issue if possible. For more information, see Manage Client Extension shared process mode.

©2026 Tanium Inc. All Rights Reserved

2. To review the health of Client Extensions or to start an investigation into an existing error, ask a question using the `Client Extensions - Status` sensor.
   The results of these questions help to identify endpoints with errors and provide a starting point to deploy actions that might help correct the issue. Filter the results and drill down as necessary to investigate results that indicate errors.

   Tip: Consider whether endpoints with errors share common characteristics, such as operating system, domain or organization unit, or the antivirus software that is installed.

3. Target one or more endpoints with errors, and uninstall tools that report errors without blocking reinstallation. For more information, see Remove Asset tools from endpoints on page 219 and Endpoint Configuration User Guide: Uninstall a tool installed by Endpoint Configuration.

   CAUTION: When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

   Wait for automatic reinstallation of the tool. If the reinstallation does not resolve the issue, continue to the next step.

4. Ask a question using the `Endpoint Configuration - Tools Status Details` sensor, and include filters to limit the results to the tool that you are investigating. For example:
   `Get Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains <Tool_Name> from all machines with Endpoint Configuration - Tools Status:Tool Name contains <Tool_Name>`

   Review the columns in the results for specific information about errors. The following table provides guidance for some common error conditions:

Potential errors returned by the Endpoint Configuration - Tools Status Details sensor

Error Condition	Possible Resolution
No error appears, but an	Review the **Targeted Version** column to make sure that the endpoint has received the

©2026 Tanium Inc. All Rights Reserved

Error Condition	Possible Resolution
available new version has not been installed	latest manifest. If the targeted version does not yet show the updated version, the Endpoint Configuration manifest has not updated on the endpoint, usually for one of the following reasons: • The manifest update is still pending. Either wait for the manifest to update and then review the results again, or follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest. • Action lock is enabled on the endpoint. Follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest to identify endpoints with action lock turned on. • Asset is no longer installed, or it is no longer targeting the endpoint. In some cases, Asset might stop targeting an endpoint because it no longer needs the endpoint for a particular workload. Consider whether Asset should still target the endpoint: • If it is expected or intentional that Asset no longer targets the endpoint, you can optionally uninstall Asset tools and dependencies. For more information, see Remove Asset tools from endpoints on page 219. • If Asset should still target the endpoint, make sure that the Asset action group includes the endpoint, and make sure Asset targets the endpoint in any expected configurations or profiles. Then, either wait for the manifest to update and then review the results again, or follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest.
Installation Blocker: `Unmet Dependencies: [ Tool name ]`	If no **Failure Message** or **Failure Step** appears, the endpoint might be waiting for the dependencies to install. Wait to see if the condition resolves on its own. If this condition remains for an extended period, ask the question again and review any error information in other columns, especially the **Failing Dependency** column.
`Failing Dependency:[ Tool name ]`	Ask the question: `Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains [Tool name] from all machines with Endpoint Configuration - Tools Status:Tool Name contains [Tool name]` Investigate further errors with the tool. If the dependency has not been installed on an endpoint, ask the question: `Get Endpoint Configuration - Tools Retry Status from all machines`

©2026 Tanium Inc. All Rights Reserved

Error Condition	Possible Resolution
	`with Computer Name equals Computer_Name` to review the retry status for the tool installation. For more information, see Review tool installations that are scheduled for a retry .
Manually Blocked: `blocked`	The tool was previously blocked, either manually or during a previous uninstallation. Unblock the tool. For more information, see Block or unblock tools from installing on an endpoint .

5. Review the Extensions logs on the endpoint. Take note of entries that include `fail` or `error`. For more information, see Review the Extensions log for an endpoint on page 219.

Next steps

For additional help, collect all logs for Asset, and contact Tanium Support on page 222.

Review the Extensions log for an endpoint

About this task

Use Client Management to directly connect to an endpoint and view and download extension logs.

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Direct Connect** search box, enter all or part of an IP address or a computer name. Matching results are displayed after the search completes.
4. From the search results, click the computer name to connect to the endpoint.
5. Click the **Logs** tab, and select an extensions[#].log file.
6. (Optional) To download the log, click **Download**.

Next steps

For additional help, collect all logs for Asset, and contact Tanium Support on page 222.

Remove Asset tools from endpoints

©2026 Tanium Inc. All Rights Reserved

About this task

You can deploy an action to remove Asset tools from an endpoint or computer group. Separate actions are available for Windows and non-Windows endpoints.

1. In Interact, target the endpoints from which you want to remove the tools. For example, ask a question that targets a specific operating system:`Get Endpoint Configuration - Tools Status from all machines with Is Windows equals true`
2. In the results, select the row for Asset, drill down as necessary, and select the targets from which you want to remove Asset tools. For more information, see Tanium Interact User Guide: Drill Down.
3. Click **Deploy Action**.
4. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
5. For **Tool Name**, select Asset.
6. (Optional) By default, after the tools are removed they cannot be reinstalled. To allow tools to be automatically reinstalled, clear the selection for **Block reinstallation**. Re-installation occurs almost immediately.

   Note:

   If reinstallation is blocked, you must unblock it manually:

   - To allow Asset to reinstall tools, deploy the **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]** package (depending on the targeted endpoints).
   - If you reinstall tools manually, select **Unblock Tool** when you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package.
7. (Optional) To remove all Asset databases and logs from the endpoints, clear the selection for **Soft uninstall**.

©2026 Tanium Inc. All Rights Reserved

> **CAUTION:** When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

8. (Optional) To also remove any tools that were dependencies of the Asset tools that are not dependencies for tools from other solutions, select **Remove unreferenced dependencies**.
9. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   > **Tip:** If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

10. Click **Show preview to continue**.
11. A results grid appears at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

    > **Note:** If you have enabled Endpoint Configuration approval, tool removal must be approved in Endpoint Configuration before tools are removed from endpoints.

Uninstall SBOM

1. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.
2. In the **Content** section, select the **SBOM** row.
3. Click Delete Selected and then click **Uninstall** to complete the process.

Use saved questions to populate Asset database

About this task

By default, Asset collects data from sensors registered with Tanium Data Service to populate information about endpoints in the Asset database. In releases prior to 1.31, Asset ran scheduled saved questions in Tanium to populate information about endpoints in the Asset database. If you upgraded from a version of Asset prior to 1.31 and want to continue using saved questions to

©2026 Tanium Inc. All Rights Reserved

populate the Asset database, Contact Tanium Support on page 222.

Uninstall Asset

1. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.
2. Select Asset and click **Uninstall**. Click **Yes** to complete the process.
3. Remove Asset Tools from your endpoints. For more information, see Remove Asset tools from endpoints on page 219.
4. A backup asset-files folder gets created as part of the uninstall process. You can keep or delete this folder. If any other Asset artifacts remain on your Module Server, Contact Tanium Support on page 222.
5. Remove Asset scheduled actions. Delete the Asset `Deploy Collect Active Directory Info` scheduled action that is created by the service account and running the Asset `Collect Active Directory Info` package.
6. Remove Asset action group. After the action group is empty, you can delete the `Tanium` Asset action group.

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

Reference: Cron syntax

A quick reference to cron syntax follows. You can use Crontab to build a cron expression.

```
┌──────────── minute
│ ┌────────── hour
│ │ ┌──────── day of month
│ │ │ ┌────── month
│ │ │ │ ┌──── day of week
│ │ │ │ │
│ │ │ │ │
* * * * *
```

Each asterisk is a field that must be included in the cron expression. The field value can either be an asterisk (any value) or one of the following values:

Valid values for cron fields

Field	Value
minute	0-59
hour	0-23
day of month	1-31
month	1-12
day of week (Sunday is 0 and 7)	0-7

Note: Cron expressions that specify both a day of week and day of month match days that meet either criteria. For example, the cron expression `* * 1 * 1` matches the first day of the month and every Monday.

©2026 Tanium Inc. All Rights Reserved

Reference: ServiceNow mappings

The following table describes how Asset attributes are mapped to ServiceNow attributes. The attributes are available on all Tanium Client supported operating systems, unless otherwise indicated.

For more information about exporting Asset data to ServiceNow, see ServiceNow: Tanium Asset integration on page 149.

ServiceNow attribute mappings

Category	ServiceNow Attribute	Asset Attribute	Comments
Computer	Computer Name	Computer Name	Filter-normalized
	Serial Number	Computer Serial Number	
	Operating System	Operating System	
	OS Version	Asset OS Version	
	OS Service Pack	Service Pack	Not available on macOS, Linux, and Solaris
	Manufacturer	Manufacturer	Not available on Solaris and AIX. Lookup to core_company
	Model	Model	Lookup to cmdb_model
	OS Domain	Domain Name	Filter-normalized
	DNS Domain	Domain	

©2026 Tanium Inc. All Rights Reserved

Category	ServiceNow Attribute	Asset Attribute	Comments
		Name	
	RAM	RAM	Normalized
	Virtual	Is Virtual	
	IP Address	Tanium Client IP Address	
	CPU Name	CPU Details > CPU	
	CPU Manufacturer	CPU Manufacturer	Not available on AIX
	CPU Speed	CPU Details > CPU Speed	Normalized
	CPU Count	CPU Details > Total Physical Processors	
	CPU Core Count	CPU Details > Total Cores	
	CPU Type	CPU Manufacturer	
Storage Device	Name	Physical Disk > Name	
	Device ID	Physical Disk > Device ID	
	Serial Number	Physical Disk	

©2026 Tanium Inc. All Rights Reserved

Category	ServiceNow Attribute	Asset Attribute	Comments
		> Serial Number	
	Manufacturer	Physical Disk > Manufacturer	Lookup to core_company.
	Model ID	Physical Disk > Model	Lookup to cmdb_model.
	Storage Type	Physical Disk > Storage Type	Filter-convert to ServiceNow values.
	Device Interface	Physical Disk > Device Interface	Filter-convert to ServiceNow values.
	Size	Physical Disk > Size	Normalized.
File System	Name	Logical Disk > Name	Not available on Solaris and AIX.
	Mount Point	Logical Disk > Mount Point	Not available on Solaris and AIX.
	Label	Logical Disk > Label	Not available on Solaris and AIX.
	Size	Logical Disk > Size	Not available on Solaris and AIX. Normalized.
	Free Space	Logical Disk > Free Space	Not available on Solaris and AIX. Normalized.

©2026 Tanium Inc. All Rights Reserved

Category	ServiceNow Attribute	Asset Attribute	Comments
	Media Type	Logical Disk > Media Type	Not available on Solaris and AIX. Convert to ServiceNow values.
	File System	Logical Disk > File System	Not available on Solaris and AIX. Convert to ServiceNow values.
Network Adapter	Name	Asset Network Adapter > Name	
	IP Address	Asset Network Adapter > IPv4 Address	
	Netmask	Asset Network Adapter > Subnet Mask	
	MAC Address	Asset Network Adapter > MAC Address	
	MAC Manufacturer	Asset Network Adapter > Manufacturer	Lookup to core_company.
	DHCP Enabled	Asset Network Adapter > DHCP Enabled	

©2026 Tanium Inc. All Rights Reserved

Category	ServiceNow Attribute	Asset Attribute	Comments
Software Package	Manufacturer	Asset Installed Applications > Vendor	If you have the SAM Pro feature, the attribute maps to Publisher.
	Name	Asset Installed Applications > Name	If you have the SAM Pro feature, the attribute maps to Display_Name.
	ServiceNow Software Identifier (Key)	Asset Installed Applications > Key	Filter-convert to ServiceNow values. This attribute is derived from the Manufacturer, Name, and Version attributes. This is not the license key and is only used by ServiceNow. If you have the SAM Pro feature, the attribute is not mapped.
	Version	Asset Installed Applications > Version	

Additional Service Graph Connector attributes

In addition to the fields listed above, you can add the following attributes to any Service Graph Connector destination. For more information about how to configure Service Graph Connector destinations, see ServiceNow: Service Graph Connector on page 157.

Service Graph Connector attribute mappings

Category	Asset Attribute	Comments
Asset	Asset System > Last Seen	Date and time the endpoint last responded to Tanium
Network Adapter	Asset Network Adapter > Model	
SIU Product Usage	Asset SIU Product Usage > Last Used Date	

©2026 Tanium Inc. All Rights Reserved

Category	Asset Attribute	Comments
	Asset SIU Product Usage > Name	
	Asset SIU Product Usage > Schema Version	Internal to Tanium (not the product version)
	Asset SIU Product Usage > Usage	Bucketed usage based on tracking settings
	Asset SIU Product Usage > Vendor	

©2026 Tanium Inc. All Rights Reserved

Reference: Source field mapping options

Important: The option to map additional fields is a beta feature. By default, field mapping is available to legacy versions of the Import API source. To enable field mapping for AWS, Microsoft Azure, Microsoft Intune, and Google sources, Contact Tanium Support on page 222.

In addition to the default field mappings for each custom source, you can configure additional field mappings. Each field mapping must specify how to map attributes in the source to attributes in the Asset database. Use this reference to understand the available options when you configure field mappings.

Note: Consider the data type when you map fields. In most cases, data is converted automatically to the appropriate data type before adding it to the Asset database. If Asset cannot convert data into the selected data type, the data is ignored. For example, if you attempt to map a string field in the source with a value of `Hello World` to an integer field in the Asset database, the incoming data is ignored.

Map additional fields for a source

In addition to the default field mappings for each custom source, you can configure custom field mappings.

Before you begin

- You must first create the source before you configure additional field mappings.
- To map a source field to an Asset entity, the field must exist in the source and the entity must exist in Asset. For more information about how to configure custom entities and attributes in Asset, see Configure additional Tanium entities and attributes on page 111.

©2026 Tanium Inc. All Rights Reserved

- To map an array of values in the source schema to an entity in Asset, use a multiple-row Asset entity. To map a single field in the source schema, use a single-row Asset entity. You must have a role with the **Asset Configuration Item write** permission to edit sources. Users assigned the **Asset Operator** and **Asset Administrator** reserved roles have this permission.
- You must have access to the field schema from the source, and you should understand how to navigate the schema using dot-notation syntax. For more information about how to use dot-notation when mapping fields, see Dot-notation syntax on page 235.

Steps

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Sources**.
2. In the row of the source that you want to edit, click Edit .
3. Go to the **Field Mappings** section and click **Add Entity Field Mapping**.

   The **Field Mappings** section contains the default field mappings for the source in addition to any custom field mappings. The section only appears when you edit the source.
4. From the **Add Entity Field Mapping** dialog, select the Asset entity to which you want to map a field from the source.
5. If you selected an entity that contains multiple rows per endpoint, enter the path to the array in the source schema in the **Source Array Path** field, and then select the **Attribute to Edit**.

   Tip: To reset any configuration settings for **Source** and **Convert Operations**, click Delete next to **Attribute to Edit**.
6. To map the value in the schema to the Asset attribute, enter the path to the field in the schema in the **Source** field and ensure **Path** is selected. If you selected an entity with multiple rows per endpoint, you only need to enter the path starting from the path specified in the **Source Array Path** field. Specify paths in dot-notation format. For more information, see Dot-notation syntax on page 235.

©2026 Tanium Inc. All Rights Reserved

> **Note:** You can also choose to map a constant value to the Asset attribute. Enter the value in the **Source** field and then select **Static Value**.

7. For the **Source** field, choose one of the following:

   - To map the value in the schema to the Asset attribute, select **Path** and then enter the path to the field in the schema in the **Source** field. If you selected an entity with multiple rows per endpoint, you only need to enter the path starting from the path specified in the **Source Array Path** field.
   - To map a constant value to the Asset attribute, select **Static Value** and enter the value in the **Source** field.

8. (Optional) To augment the data from the source, add convert operations.

   > **Note:** The option to add convert operations is not available if you select **Static Value** for the **Source** field.

   a. Click **Add Convert Operation**.

   b. Select the type of convert operation and then enter a value for the operation.

Convert Operation	Description
Append	Enter a value to append to the data.
Array Length	When the field that you specified in the **Source** field is an array, returns the length of the array
Lowercase	Convert all characters in the data to lowercase.
Replace	Match a regular expression in the data and then enter the replacement value.
Prefix	Enter a value to prepend to the data.

   For more information about these convert operations, see Convert operations on page 233.

©2026 Tanium Inc. All Rights Reserved

c. Repeat to add any additional convert operations.

d. (Optional) If you add multiple operations, drag the operations to change the order in which the operations occur.

9. When finished, click **Save Changes**.

The field mapping is immediately applied to the source; you do not need to save the source to save the new field mapping.

Tip: If you map a field to an attribute in a custom entity, and you later want to delete the attribute or custom entity, you must first remove the field mapping from the source. When you attempt to delete an attribute, Asset shows a list of references to the attribute from all reports, views, permissions, sources, and ServiceNow destinations. For more information about how to delete attributes, see Delete attributes on page 213.

What to do next

Import the source to verify the field mapping performs as expected. For more information, see Test field mappings on page 236.

Convert operations

The following convert operations are available when you configure additional field mapping. Convert operations are only available when the **Source** value contains a path. For more information, see Map additional fields for a source on page 230.

Note: Some convert operations are limited by the data type of the Asset field. For example, if the Asset field is an integer, you can only prefix or append numbers to the incoming data.

©2026 Tanium Inc. All Rights Reserved

Tip: You can add multiple convert operations to a single field mapping, and you can customize the order of the convert operations. When using any convert operations, consider using test data to verify the data is converted as intended.

Append

Enter a value to append to the data.

For example, if you select to append `GB` to the data (with a preceding space), a value of `10` is converted to `10 GB`.

Array Length

Return the length of the array specified in the **Source** field.

For example, consider the following schema from the source:

```
{
   "level1": {
      "level2": [
         {
            "value1": "something"
         },
         {
            "value2": "something"
         }
      }
   }
}
```

If you select to return the array length of the `level1.level2` array, the data is converted to `2`.

Note: If the field that you specify is not an array, the data converts to null.

Lowercase

Convert all characters in the data to lowercase.

©2026 Tanium Inc. All Rights Reserved

For example, if you select the **Lowercase** convert operation, a value of `ABC123def789GHI` is converted to `abc123def789ghi`.

Replace

Match a string or regular expression in the data with a replacement value.

For example, if you enter a **Match** value of `([^\\s]+).*` (anything other than a space character at the start of a string) and select a **Replace** value of `$1`, a value of `My Company` is converted to `My`.

Tip: The replace operation accepts the same regular expressions as the JavaScript replace function. For more information about acceptable patterns, see Specifying a string as the replacement.

Prefix

Enter a value to prepend to the data.

For example, if you select to prepend `SN_` to the data, a value of `123456789` is converted to `SN_123456789`.

Dot-notation syntax

Paths use standard JavaScript dot-notation syntax to navigate through a JSON object. Consider the following JSON example:

```
{
   "level1": {
      "level2": {
         "value": "something",
      }
   }
}
```

To map the data in `"value"` the path would be `level1.level2.value` and the returned value is

©2026 Tanium Inc. All Rights Reserved

`"something"`.

The path also supports arrays, where bracket parentheses index within the array.

```
{
   "level1": [
      {
         "value": "something1",
      },
      {
         "value": "something2".
      }
   ]
}
```

Use the zero-based index within the array for mapping. For example, `level1[0].value` maps to `"something1"`.

Arrays also support negative indexes to index from the bottom of the array. For example, `level1[-1].value` maps to `"something2"`.

Test field mappings

To view field mappings for a source, you can manually import the source from the **Schedules** page or wait until the next scheduled import.

To manually import the source, perform the following:

1. From the Main menu, go to **Modules** > **Asset** > **Inventory Management > Schedules**.
2. In the row of the source that you want to import on the **Import Schedules** tab, click Run Now .

©2026 Tanium Inc. All Rights Reserved

Reference: Gateway examples for Asset

Tanium Gateway provides a GraphQL API integration point for Tanium solutions, including Asset. Asset requests retrieve Asset products or endpoints based on Asset products, update Asset product tracking, and import assets to update or create assets.

Asset requests have the following feature-specific dependencies at the specified minimum versions:

- Asset 1.23.8 or later is required to submit a mutation request to import assets (`mutation.assetsImport`).
- Asset 1.24.76 or later is required to submit a request that retrieves Asset products (`query.assetProducts`) or endpoints based on installed Asset products (`query.assetProductEndpoints`).
- Asset 1.33.181 or later is required to submit a request that upserts (creates or updates by ID) endpoints (`mutation.assetUpsertEndpoints`), update endpoints based on Asset source (`mutation.assetUpdateEndpoints`), or update endpoints based endpoint ID (`query.assetUpdateEndpointsUsingEid`).

For additional Gateway example syntax, see Tanium Gateway User Guide: Reference: Filter syntax and Tanium Gateway User Guide: Reference: Gateway examples.

Asset query filter syntax

Filter Asset queries when retrieving Asset products (`query.assetProducts`) or endpoints (`query.assetProductEndpoints`).

Asset product queries (`assetProducts`) support the following filter fields:

- `search`
- `states`

©2026 Tanium Inc. All Rights Reserved

- `vendors`

For more information on syntax, see `assetProductsFilter` in the **Documentation Explorer** pane of the query explorer.

Endpoint queries using `assetProductEndpoints` support the following filter fields:

- `name`
- `vendor`
- `version`
- `usage`

For more information on syntax, see `assetProductEndpointsFilter` in the **Documentation Explorer** pane of the query explorer.

Asset products

You can retrieve Asset products and filter based on product metadata. Define a filter object using the syntax:

```
filter {
  vendors: [
    "vendor-name-1",
    "vendor-name-2",
    "vendor-name-n..."
  ],
  search: "search-string",
  states: [Cataloged | Ignored | Tracked]
}
```

For example, the following request retrieves only Asset products with a vendor name of `Example vendor`, an Asset state of `Cataloged`, and the search string `Product` in either the vendor name or product name:

```
query exampleGetAssetProductsFiltered($first: Int, $vendor: String!, $search: String,
$states: AssetProductState!) {
  assetProducts(
    first: $first, filter: {
      vendors: [$vendor],
      search: $search,
      states: [$states]
    }
  ) {
    edges {
      node {
```

©2026 Tanium Inc. All Rights Reserved

```
        vendor
        name
        installation {
          installedCount
          usedCount
          unusedCount
          pendingUsage
        }
        usage {
          usageNotDetected
          notInstalled
          baselining
          limited
          normal
          high
        }
        tracking {
          state
          reportingPeriodDays
          normalMinutesUsedPerDay
          highMinutesUsedPerDay
          baselinePeriodDays
        }
        versions {
          version
          installs
        }
      }
    }
  }
}
```

Include the filter variables in the **Variables** panel:

```
{
  "first": 2,
  "vendor": "Example vendor",
  "search": "Product",
  "states": "Cataloged"
}
```

Endpoints based on Asset products

You can retrieve endpoints and filter the returned endpoints based on Asset product information. Define a filter object using the syntax:

```
filter {
  vendors: [
    "vendor-name-1",
    "vendor-name-2",
    "vendor-name-n..."
  ],
  name: "name-string",
  version: "version-string"
}
```

For example, the following request retrieves only endpoints that have installed the `Example name`

©2026 Tanium Inc. All Rights Reserved

product, with a vendor of `Example vendor` and version of `1.2.3`:

```
query exampleGetEndpointsAssetProduct($first: Int, $vendor: String, $name: String, $version:
String) {
  assetProductEndpoints(
    first: $first
    filter: {vendor: $vendor, name: $name, version: $version, usage: Normal}
  ) {
    edges {
      node {
        id
        eid
        computerName
        computerId
        serialNumber
        osPlatform
        operatingSystem
        servicePack
        manufacturer
        ipAddress
        userName
        createdAt
        updatedAt
      }
    }
  }
}
```

Include the filter variables in the **Variables** panel:

```
{
  "first": 2,
  "vendor": "Example vendor",
  "name": "Example name",
  "version": "1.2.3"
}
```

Get Asset products

query.assetProducts

About this task

The following query requires Asset 1.24.76 or later and retrieves Asset products:

```
query exampleGetAssetProducts($first: Int) {
  assetProducts(
    first: $first
  ) {
    edges {
      node {
        vendor
        name
        installation {
          installedCount
          usedCount
```

©2026 Tanium Inc. All Rights Reserved

```
          unusedCount
          pendingUsage
        }
        usage {
          usageNotDetected
          notInstalled
          baselining
          limited
          normal
          high
        }
        tracking {
          state
          reportingPeriodDays
          normalMinutesUsedPerDay
          highMinutesUsedPerDay
          baselinePeriodDays
        }
        versions {
          version
          installs
        }
      }
    }
  }
}
```

Include the cursor variable in the **Variables** panel or in your variables dictionary:

```
{
  "first": 2
}
```

Example response:

```
{
  "data": {
    "assetProducts": {
      "edges": [
        {
          "node": {
            "vendor": "Example vendor",
            "name": "Example product",
            "installation": {
              "installedCount": 8,
              "usedCount": 0,
              "unusedCount": 0,
              "pendingUsage": null
            },
            "usage": {
              "usageNotDetected": 0,
              "notInstalled": 0,
              "baselining": 0,
              "limited": 0,
              "normal": 0,
              "high": 0
            },
            "tracking": {
              "state": "Cataloged",
              "reportingPeriodDays": 90,
              "normalMinutesUsedPerDay": 60,
```

©2026 Tanium Inc. All Rights Reserved

```
              "highMinutesUsedPerDay": 240,
              "baselinePeriodDays": 7
            },
            "versions": [
              {
                "version": "1.2.3",
                "installs": 2
              },
              {
                "version": "1.2.4",
                "installs": 2
              }
            ]
          }
        },
        {
          "node": {
            "vendor": "Example vendor 2",
            "name": "Example product 2",
            "installation": {
              "installedCount": 1,
              "usedCount": 0,
              "unusedCount": 0,
              "pendingUsage": null
            },
            "usage": {
              "usageNotDetected": 0,
              "notInstalled": 0,
              "baselining": 0,
              "limited": 0,
              "normal": 0,
              "high": 0
            },
            "tracking": {
              "state": "Cataloged",
              "reportingPeriodDays": 90,
              "normalMinutesUsedPerDay": 60,
              "highMinutesUsedPerDay": 240,
              "baselinePeriodDays": 7
            },
            "versions": [
              {
                "version": "0.1.2",
                "installs": 1
              }
            ]
          }
        }
      ]
    }
  }
}
```

The following query request filters and retrieves only Asset products with a vendor name of `Example vendor`, an Asset state of `Cataloged`, and the search string `Product` in either the vendor name or product name:

```
query exampleGetAssetProductsFiltered($first: Int, $vendor: String!, $search: String,
$states: AssetProductState!) {
  assetProducts(
    first: $first, filter: {
```

©2026 Tanium Inc. All Rights Reserved

```
      vendors: [$vendor],
      search: $search,
      states: [$states]
    }
  ) {
    edges {
      node {
        vendor
        name
        installation {
          installedCount
          usedCount
          unusedCount
          pendingUsage
        }
        usage {
          usageNotDetected
          notInstalled
          baselining
          limited
          normal
          high
        }
        tracking {
          state
          reportingPeriodDays
          normalMinutesUsedPerDay
          highMinutesUsedPerDay
          baselinePeriodDays
        }
        versions {
          version
          installs
        }
      }
    }
  }
}
```

Include the cursor and filter variables in the **Variables** panel or in your variables dictionary:

```
{
  "first": 2,
  "vendor": "Example vendor",
  "search": "Product",
  "states": "Cataloged"
}
```

Example response:

```
{
  "data": {
    "assetProducts": {
      "edges": [
        {
          "node": {
            "vendor": "Example vendor",
            "name": "Example product",
            "installation": {
              "installedCount": 8,
              "usedCount": 0,
```

©2026 Tanium Inc. All Rights Reserved

```
            "unusedCount": 0,
            "pendingUsage": null
          },
          "usage": {
            "usageNotDetected": 0,
            "notInstalled": 0,
            "baselining": 0,
            "limited": 0,
            "normal": 0,
            "high": 0
          },
          "tracking": {
            "state": "Cataloged",
            "reportingPeriodDays": 90,
            "normalMinutesUsedPerDay": 60,
            "highMinutesUsedPerDay": 240,
            "baselinePeriodDays": 7
          },
          "versions": [
            {
              "version": "0.1.2",
              "installs": 2
            },
            {
              "version": "3.4.5",
              "installs": 2
            }
          ]
        }
      },
      {
        "node": {
          "vendor": "Example vendor",
          "name": "Product example",
          "installation": {
            "installedCount": 1,
            "usedCount": 0,
            "unusedCount": 0,
            "pendingUsage": null
          },
          "usage": {
            "usageNotDetected": 0,
            "notInstalled": 0,
            "baselining": 0,
            "limited": 0,
            "normal": 0,
            "high": 0
          },
          "tracking": {
            "state": "Cataloged",
            "reportingPeriodDays": 90,
            "normalMinutesUsedPerDay": 60,
            "highMinutesUsedPerDay": 240,
            "baselinePeriodDays": 7
          },
          "versions": [
            {
              "version": "6.7.8",
              "installs": 1
            }
          ]
        }
      }
    ]
```


©2026 Tanium Inc. All Rights Reserved

```
    }
  }
}
```

Get endpoints based on Asset products

query.assetProductEndpoints

About this task

The following query requires Asset 1.24.76 or later and retrieves the first 2 endpoints with the `Example name` product installed, associated with the `Example vendor` vendor and version `1.2.3`:

```
query exampleGetEndpointsAssetProduct($first: Int, $vendor: String, $name: String, $version:
String) {
  assetProductEndpoints(
    first: $first
    filter: {vendor: $vendor, name: $name, version: $version}
  ) {
    edges {
      node {
        id
        eid
        computerName
        computerId
        serialNumber
        osPlatform
        operatingSystem
        servicePack
        manufacturer
        ipAddress
        userName
        createdAt
        updatedAt
      }
    }
  }
}
```

Include the cursor and filtering variables in the **Variables** panel or in your variables dictionary:

```
{
  "first": 2,
  "vendor": "Example vendor",
  "name": "Example name",
  "version": "1.2.3"
}
```

Example response:

```
{
  "data": {
    "assetProductEndpoints": {
      "edges": [
```

©2026 Tanium Inc. All Rights Reserved

```
        {
          "node": {
            "id": 123,
            "eid": 456789,
            "computerName": "example-host-1",
            "computerId": "123456789",
            "serialNumber": "1234567890abcdef",
            "osPlatform": "Windows",
            "operatingSystem": "Windows 10 Enterprise",
            "servicePack": "No Service Pack found",
            "manufacturer": "VMware, Inc.",
            "ipAddress": "192.0.2.10",
            "userName": "example-user",
            "createdAt": "2022-09-29T07:00:16.000Z",
            "updatedAt": "2022-11-10T23:00:06.000Z"
          }
        },
        {
          "node": {
            "id": 456,
            "eid": 789012,
            "computerName": "example-host-2",
            "computerId": "987654321",
            "serialNumber": "fedcba0987654321",
            "osPlatform": "Windows",
            "operatingSystem": "Windows 10 Enterprise",
            "servicePack": "No Service Pack found",
            "manufacturer": "VMware, Inc.",
            "ipAddress": "192.0.2.20",
            "userName": "example-user",
            "createdAt": "2022-09-29T07:00:16.000Z",
            "updatedAt": "2022-10-31T14:00:05.000Z"
          }
        }
      ]
    }
  }
}
```


Update Asset endpoints based on source

mutation.assetUpdateEndpoints

About this task

Stability: 1.2 - Experimental (Release Candidate)

The following mutation requires Asset 1.33.181 or later and updates the endpoint record based on the default Tanium source. If reconciliation keys are included, asset reconciliation is used. If no endpoints match the keys, the response returns an error.

©2026 Tanium Inc. All Rights Reserved

Note: To update an endpoint in the Tanium source, you must specify the `Computer Name`, `Computer ID`, and `Endpoint Fingerprint` keys. Asset finds the endpoint if at least two of the keys match.

Note: After you submit a successful request, it can take up to two import cycles, or approximately 20 minutes, for attributes to appear in Asset and in reports.

```
mutation exampleAssetUpdateEndpointsTaniumSource($input: AssetUpdateEndpointsInput!) {
  assetUpdateEndpoints(
    input: $input
  ) {
    assets {
      eid
      source {
        namespace
        id
        name
      }
      status
      error
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "sourceName": "Tanium",
    "entityNames": [
      "Computer Name",
      "Computer ID",
      "Endpoint Fingerprint",
      "Asset Custom: custom_entity_1"
    ],
    "assets": [
      {
        "entities": [
          {
            "entityName": "Computer Name",
            "entityRowItems": [
              {
                "attributes": [
                  {
                    "attributeName": "Computer Name",
                    "value": "computer1"
                  }
                ]
              }
            ]
          },
          {
            "entityName": "Computer ID",
            "entityRowItems": [
```

```
              {
                "attributes": [
                  {
                    "attributeName": "Computer ID",
                    "value": "1234567890"
                  }
                ]
              }
            ]
          },
          {
            "entityName": "Endpoint Fingerprint",
            "entityRowItems": [
              {
                "attributes": [
                  {
                    "attributeName": "Endpoint Fingerprint",
                    "value":
"1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef"
                  }
                ]
              }
            ]
          },
          {
            "entityName": "Asset Custom: custom_entity_1",
            "entityRowItems": [
              {
                "attributes": [
                  {
                    "attributeName": "Asset Custom: custom_entity_1",
                    "value": "example_value"
                  }
                ]
              }
            ]
          }
        ]
      }
    ]
  }
}
```

Example response:

```
{
  "data": {
    "assetUpdateEndpoints": {
      "assets": [
        {
          "eid": "12345",
          "source": {
            "namespace": "Asset: Tanium",
            "id": "1",
            "name": "Tanium"
          },
          "status": "Updated",
          "error": null
        }
      ]
    }
  }
```

©2026 Tanium Inc. All Rights Reserved

```
}
```

The following mutation updates the endpoint record based on a Microsoft Azure source:

Note: To update an endpoint in the Tanium source, you must specify the `Computer Name`, `Computer ID`, and `Endpoint Fingerprint` keys. Asset finds the endpoint if at least two of the keys match. For an example, see Update Asset endpoint by Asset source on page 246.

```
mutation exampleAssetUpdateEndpointsMicrosoftAzureSource($input: AssetUpdateEndpointsInput!)
{
  assetUpdateEndpoints(
    input: $input
  ) {
    assets {
      eid
      source {
        namespace
        id
        name
      }
      status
      error
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "sourceName": "example Microsoft Azure source",
    "entityNames": [
      "Cloud Instance ID",
      "Asset Custom: custom_entity_1"
    ],
    "assets": [
      {
        "entities": [
          {
            "entityName": "Cloud Instance ID",
            "entityRowItems": [
              {
                "attributes": [
                  {
                    "attributeName": "Cloud Instance ID",
                    "value": "12345678-90ab-cdef-1234-567890abcdef"
                  }
                ]
              }
            ]
          },
          {
            "entityName": "Asset Custom: custom_entity_1",
            "entityRowItems": [
              {
                "attributes": [
```

©2026 Tanium Inc. All Rights Reserved

```
                {
                  "attributeName": "Asset Custom: custom_entity_1",
                  "value": "Test 1"
                }
              ]
            }
          ]
        }
      ]
    }
  }
}
```

Example response:

```
{
  "data": {
    "assetUpdateEndpoints": {
      "assets": [
        {
          "eid": "149157",
          "source": {
            "namespace": "Asset: example Microsoft Azure source",
            "id": "102",
            "name": "example Microsoft Azure source"
          },
          "status": "Updated",
          "error": null
        }
      ]
    }
  }
}
```

Update Asset endpoints based on endpoint ID (EID)

mutation.assetUpdateEndpointsUsingEid

About this task

Stability: 1.2 - Experimental (Release Candidate)

The following mutation requires Asset 1.33.181 or later and updates the endpoint record for an Asset source that matches the endpoint ID (EID). If reconciliation keys are included, asset reconciliation is used. If no endpoints match the keys, the response returns an error.

Note: To update an endpoint in the Tanium source, you must specify the `Computer Name`, `Computer ID`, and `Endpoint Fingerprint` keys. Asset finds the endpoint if at least two of the keys match. For an example, see Update Asset endpoint by Asset source on page 246.

©2026 Tanium Inc. All Rights Reserved

Note: After you submit a successful request, it can take up to two import cycles, or approximately 20 minutes, for attributes to appear in Asset and in reports.

```
mutation exampleAssetUpdateEndpointsEID($input: AssetUpdateEndpointsUsingEidInput!) {
  assetUpdateEndpointsUsingEid(input: $input) {
    assets {
      eid
      source {
        namespace
        id
        name
      }
      status
      error
    }
  }
}
```

Include the input variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "sourceName": "example_source",
    "entityNames": [
      "Asset Custom: custom_entity_1"
    ],
    "assets": [
      {
        "eid": "12345",
        "entities": [
          {
            "entityName": "Asset Custom: custom_entity_1",
            "entityRowItems": [
              {
                "attributes": [
                  {
                    "attributeName": "Asset Custom: custom_entity_1",
                    "value": "example_test"
                  }
                ]
              }
            ]
          }
        ]
      }
    ]
  }
}
```

Example response:

```
{
  "data": {
    "assetUpdateEndpointsUsingEid": {
      "assets": [
        {
          "eid": "12345",
          "source": {
```

©2026 Tanium Inc. All Rights Reserved

```
            "namespace": "Asset: example_source",
            "id": "123",
            "name": "example_source"
          },
          "status": "Updated",
          "error": null
        }
      ]
    }
  }
}
```

Upsert (create or update by ID) Asset endpoint

mutation.assetUpsertEndpoints

About this task

Stability: 1.2 - Experimental (Release Candidate)

The `assetUpsertEndpoints` mutation requires Asset 1.33.181 or later and either creates a new endpoint record or updates an existing endpoint record using the defined `sourceName` for Import API sources. Asset creation or update is based on comparing key field values. If reconciliation keys are included, asset reconciliation is used. To determine whether an existing asset updates, or a new asset is created:

1. If an imported asset key matches an existing asset key imported using the `sourceName` Import API source, that existing asset updates. The status in the response equals `Updated`.

2. If an imported asset key matches an existing asset reconciliation key imported using the Tanium source only, that existing asset is reconciled, and then updates. The status in the response equals `Reconciled`.

3. Otherwise, if no existing asset matches the imported asset, the asset is imported as a new asset using the `sourceName` Import API source. The status in the response is equal to `Created`.

Note: If the request is structurally and syntactically valid, each asset object imports separately. A failed asset import does not prevent other valid asset objects in that request from importing.

©2026 Tanium Inc. All Rights Reserved

Note: After you submit a successful request, it can take up to two import cycles, or approximately 20 minutes, for attributes to appear in Asset and in reports.

The following mutation request creates an asset, if no existing asset in the `example_source` Import API source matches on the `Computer Name` key field, and updates a single `attributeName` value:

```
mutation exampleAssetUpsertEndpoints($input: AssetUpsertEndpointsInput!) {
  assetUpsertEndpoints(input: $input) {
    assets {
      eid
      source {
        namespace
        id
        name
      }
      status
      error
    }
  }
}
```

Include the variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "sourceName": "example_source",
    "entityNames": [
      "Computer Name",
      "Asset Custom: custom_entity_1"
    ],
    "assets": [
      {
        "entities": [
          {
            "entityName": "Computer Name",
            "entityRowItems": [
              {
                "attributes": [
                  {
                    "attributeName": "Computer Name",
                    "value": "computer1"
                  }
                ]
              }
            ]
          },
          {
            "entityName": "Asset Custom: custom_entity_1",
            "entityRowItems": [
              {
                "attributes": [
                  {
                    "attributeName": "Asset Custom: custom_entity_1",
                    "value": "Test 1"
                  }
```

©2026 Tanium Inc. All Rights Reserved

```
                ]
              }
            ]
          }
        ]
      }
    ]
  }
}
```

As the request is evaluated, the asset object defines a value for the `computerName` key field, matching the key field defined for the `example_source` source, and is imported using that source. The example response shows a status of `Created`:

```
{
  "data": {
    "assetUpsertEndpoints": {
      "assets": [
        {
          "eid": "12345",
          "source": {
            "namespace": "Asset: example_source",
            "id": "123",
            "name": "example_source"
          },
          "status": "Created",
          "error": null
        }
      ]
    }
  }
}
```

The following mutation request updates an asset if an asset in the `example_source` Import API source matches on the `Computer Name` key field, and updates two `attributeName` values:

```
mutation exampleAssetUpsertEndpointsMultiColumn($input: AssetUpsertEndpointsInput!) {
  assetUpsertEndpoints(input: $input) {
    assets {
      eid
      source {
        namespace
        id
        name
      }
      status
      error
    }
  }
}
```

Include the variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "sourceName": "example_source",
    "entityNames": [
```

©2026 Tanium Inc. All Rights Reserved

```
      "Computer Name",
      "Asset Custom: custom_entity_2"
    ],
    "assets": [
      {
        "entities": [
          {
            "entityName": "Computer Name",
            "entityRowItems": [
              {
                "attributes": [
                  {
                    "attributeName": "Computer Name",
                    "value": "computer1"
                  }
                ]
              }
            ]
          },
          {
            "entityName": "Asset Custom: custom_entity_2",
            "entityRowItems": [
              {
                "attributes": [
                  {
                    "attributeName": "column_1",
                    "value": "column_1_test"
                  },
                  {
                    "attributeName": "column_2",
                    "value": "column_2_test"
                  }
                ]
              }
            ]
          }
        ]
      }
    ]
  }
}
```

As the request is evaluated, the asset object defines a value for the `computerName` key field, matching the key field defined for the `example_source` Import API source, and is imported using that source. The example response shows a status of `Updated`:

```
{
  "data": {
    "assetUpsertEndpoints": {
      "assets": [
        {
          "eid": "12345",
          "source": {
            "namespace": "Asset: example_source",
            "id": "123",
            "name": "example_source"
          },
          "status": "Updated",
          "error": null
        }
      ]
```

©2026 Tanium Inc. All Rights Reserved

```
    }
  }
}
```

The following mutation request updates an asset if an asset in the `example_source` Import API source matches on the `Computer Name` key field, and updates two rows with two `attributeName` values:

```
mutation exampleAssetUpsertEndpointsMultiRow($input: AssetUpsertEndpointsInput!) {
  assetUpsertEndpoints(input: $input) {
    assets {
      eid
      source {
        namespace
        id
        name
      }
      status
      error
    }
  }
}
```

Include the variables in the **Variables** panel or in your variables dictionary:

```
{
  "input": {
    "sourceName": "ktai_example_custom_source",
    "entityNames": [
      "Computer Name",
      "Asset Custom: ktai_custom_entity_3"
    ],
    "assets": [
      {
        "entities": [
          {
            "entityName": "Computer Name",
            "entityRowItems": [
              {
                "attributes": [
                  {
                    "attributeName": "Computer Name",
                    "value": "computer1"
                  }
                ]
              }
            ]
          },
          {
            "entityName": "Asset Custom: ktai_custom_entity_3",
            "entityRowItems": [
              {
                "attributes": [
                  {
                    "attributeName": "multi_row_1",
                    "value": "row_1_column_1_test"
                  },
                  {
                    "attributeName": "multi_row_2",
                    "value": "row_1_column_2_test"
```

©2026 Tanium Inc. All Rights Reserved

```
                }
              ]
            },
            {
              "attributes": [
                {
                  "attributeName": "multi_row_1",
                  "value": "row_2_column_1_test"
                },
                {
                  "attributeName": "multi_row_2",
                  "value": "row_2_column_2_test"
                }
              ]
            }
          ]
        }
      ]
    }
  }
}
```

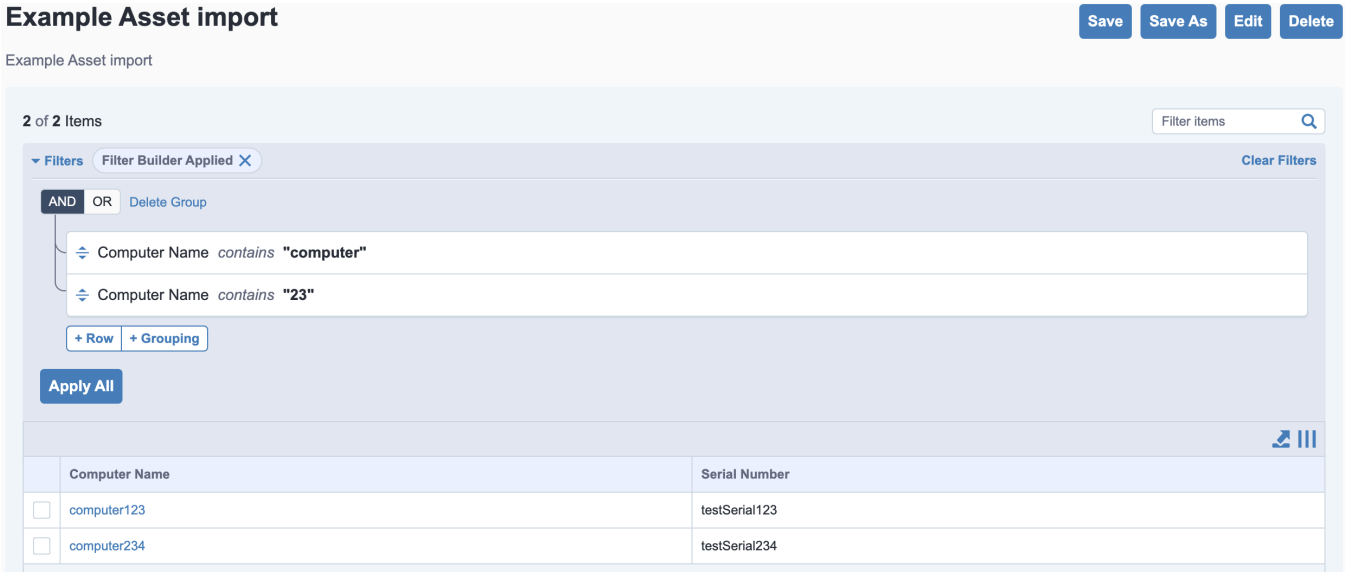
As the request is evaluated, the asset object defines a value for the `computerName` key field, matching the key field defined for the `example_source` Import API source, and is imported using that source. The example response shows a status of `Updated`:

```
{
  "data": {
    "assetUpsertEndpoints": {
      "assets": [
        {
          "eid": "12345",
          "source": {
            "namespace": "Asset: example_source",
            "id": "123",
            "name": "example_source"
          },
          "status": "Updated",
          "error": null
        }
      ]
    }
  }
}
```

To verify the import, create a report based on the custom source definition, and filter the report to search for imported assets. For example, creating a report with **Computer Name** and **Serial Number** as columns, then filtering **Computer Name** for values containing `computer` and `23` returns the imported assets.

Figure 15. Example Asset import report

©2026 Tanium Inc. All Rights Reserved



Note: You can also add the Asset source ID to view only assets from that source.

For more information, see Tanium Asset User Guide: Create a report.

Import assets

mutation.assetsImport

About this task

Stability: 0 - Deprecated

Note: This is deprecated in favor of `mutation.assetUpsertEndpoints`. For more information, see the example syntax on page 252.

Note: Before you submit this mutation request, you must configure an Asset custom source. For more information and an example workflow, see Tanium Asset User Guide: Create an Import API source.

©2026 Tanium Inc. All Rights Reserved

Note: After you submit a successful request, it can take up to two import cycles, or approximately 20 minutes, for attributes to appear in Asset and in reports.

The `assetsImport` mutation requires Asset 1.23.8 and imports assets defined in the request `json` variable value, using the defined `sourceName` custom source. To determine whether an existing asset updates, or a new asset is created:

1. If an imported asset key matches an existing asset key imported using the `sourceName` custom source, that existing asset updates.
2. If no existing asset from the configured source matches, but values in the imported asset match an existing asset key imported using a source different from the `sourceName` custom source, and the other source allows the `sourceName` custom source to update, the existing asset from the other source updates.
3. Otherwise, if no existing asset matches the imported asset, the asset is imported as a new asset using the `sourceName` custom source.

Note: If the request is structurally and syntactically valid, each asset object imports separately. A failed asset import does not prevent other valid asset objects in that request from importing.

Define the `json` attribute as a JSON object array, with each object corresponding to an asset. Ensure that the Asset custom source passes the JSON object array according to the following guidelines:

- Use the backslash escape character with each quotation mark (`\"`) in the JSON array.
- You must define key field values for each object. If you do not define the key field values, the object does not import and the response returns `ErrorMissingKey` status for that object.
- You can define source field mappings to destination fields for each object. If you do not define a source field mapping, values from those source fields are imported as `null` values for that object.
- Field values are defined per object; you cannot globally define a single field value in the request to apply to every imported asset object.
- You can define up to 5000 asset objects per array, and by extension, per request.

©2026 Tanium Inc. All Rights Reserved

The following example Asset custom source, named `test-name`, defines two field mappings for `computer_name` and `serial_number` and defines `computer_name` as a key field.

```
{
  "keys": [
    "computer_name"
  ],
  "fieldMaps": [
    {
      "destination": "computer_name",
      "source": "computerName"
    },
    {
      "destination": "serial_number",
      "source": "serialNumber"
    }
  ]
}
```

The following mutation request imports assets based on the variables definition:

```
mutation exampleImportAssets($source: String!, $json: String!) {
  assetsImport(input: {sourceName: $source, json: $json}) {
    assets {
      id
      index
      status
    }
  }
}
```

Include the variables in the **Variables** panel or in your variables dictionary.

The following variables manually define the `test-name` source for importing and two asset objects in the JSON object array. Each object has a value for the key field (`computerName`) and for the `serialNumber` field mapping.

```
{
  "source": "test-name",
  "json": "[{\"computerName\": \"computer123\", \"serialNumber\": \"testSerial123\"},
{\"computerName\": \"computer234\", \"serialNumber\": \"testSerial234\"}]"
}
```

As the request is evaluated, each asset object defines a value for the `computerName` key field, matching the key field defined for the `test-name` custom source, and both are imported using that source. The example response shows both objects with a status of `Created`:

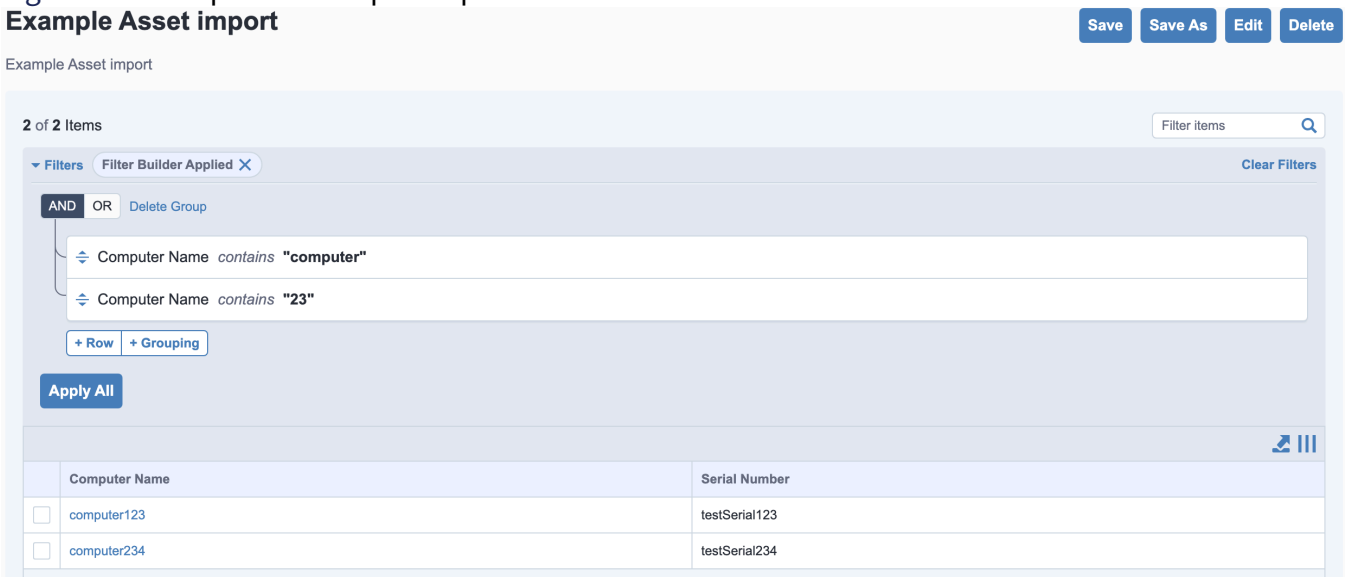
```
{
  "data": {
    "assetsImport": {
      "assets": [
        {
          "id": 6,
          "index": 0,
```

©2026 Tanium Inc. All Rights Reserved

```
          "status": "Created"
        },
        {
          "id": 7,
          "index": 1,
          "status": "Created"
        }
      ]
    }
  }
}
```


To verify the import, create a report based on the custom source definition, and filter the report to search for imported assets. For example, creating a report with **Computer Name** and **Serial Number** as columns, then filtering **Computer Name** for values containing `computer` and `23` returns the imported assets.

Figure 16. Example Asset import report



For more information, see Tanium Asset User Guide: Create a report.

©2026 Tanium Inc. All Rights Reserved

Reference: Export data through the Asset REST API

To retrieve data from Asset, use an Asset view and send the data in JSON format through the Asset REST API.

Tip: This reference includes a scenario to retrieve data through a ServiceNow view. You can adapt these steps to retrieve data through any view in Asset.

Before you begin

- These steps require Tanium Gateway to manage API tokens. For more information, see Asset requirements on page 26.
- To create a view in Asset, you require a role with the **Asset Report write** permission. The predefined **Asset Administrator**, **Asset Operator**, and **Asset User** roles contain this permission.
- The steps use cURL to test the API from a local machine. To follow these steps verbatim, ensure that cURL is installed and available on your Windows, Linux, or macOS machine. You can also use your preferred API tool to access the API.
- These steps require you to create a new Asset API user in Tanium Console. Ensure the user account exists in your IdP. For more information, see Tanium Console User Guide: User authentication.

Create a dedicated ServiceNow view

Create a view to filter endpoint data in Asset so that you only export attributes that you want.

©2026 Tanium Inc. All Rights Reserved

Note: These steps create a view for the ServiceNow Service Graph Connector pull integration. You can adapt these steps to create views for other integrations.

1. From the Main menu, go to **Modules** > **Asset** > **Views**.
2. If the **ServiceNow (reserved)** view does not appear in the grid, click **Create Views**, and select **Create ServiceNow View**.

   Asset creates the **ServiceNow (reserved)** view and updates the grid on the **Views** page.
3. In the row of the **ServiceNow (reserved)** view, click Create Copy.

   The **Create View** page loads with data prefilled from the **ServiceNow (reserved)** view.
4. Update the name of the view. For example, **ServiceNow SGC**.
5. In the **Select Columns from Asset Tables** section, select the columns that you want to include in the view. These example steps include the **Computer Name** and **OS Platform** columns.
6. Add any filters as desired.

   Note: Available filters depend on which columns you add to the view. For example, if you include the **SIU Product Usage** > **Usage** column, the **SIU Product Usage Filter** section appears. You can then add a filter in the **SIU Product Usage Filter** section to remove assets whose SIU product usage is not installed. To do so, select the **Usage** attribute, set the operator to **does not contain**, enter a value of **not installed**, and then click Apply.
7. Click **Submit** to save the view.

   Asset saves the view and loads the **Views** page.
8. Test the view. On the **Views** page, hover over a view and click Test View, which runs the view for a single asset. The resulting message states whether the view can run successfully or contains errors such as pending attributes.
9. Record the ID of the new view.

©2026 Tanium Inc. All Rights Reserved

a. From the grid on the **Views** page, click Edit in the row of the new view.

b. In the URL field of your browser, record the number that appears at the end of the URL.



Create a user account with the Asset API User role

Create a specific **Asset API User** account for which to retrieve data through the Asset API.

Best Practice: For continuity, create a service account that is not assigned to any particular person. The service account should have enough permissions to read data from Asset views and create and rotate tokens for Asset API access. Before you create a user account in Tanium Console, make sure an account exists in your IdP and any multifactor authentication is configured.

Note: Alternatively, you can use a persona to represent a restricted account. However, if the Tanium user account is deleted, any API tokens that are associated with the account are no longer valid. For more information about API tokens, see Tanium Console User Guide: Managing API tokens.

1. From the Main menu, go to **Administration** > **Permissions** > **Users** and click **New User**.
2. Specify a **User Name** that matches an account in your IdP.
3. Set the **Display Name** to **Asset API User**.
4. In the **Roles** section, click **Manage Roles**.
5. Select the **Asset Report Reader** and **Gateway User** roles, then click **Apply**.
6. Click **Save**.

Note: Do not assign any user groups or computer groups to the user.

©2026 Tanium Inc. All Rights Reserved

For more information about how to create user accounts in Tanium Console, see Tanium Console User Guide: Create a user.

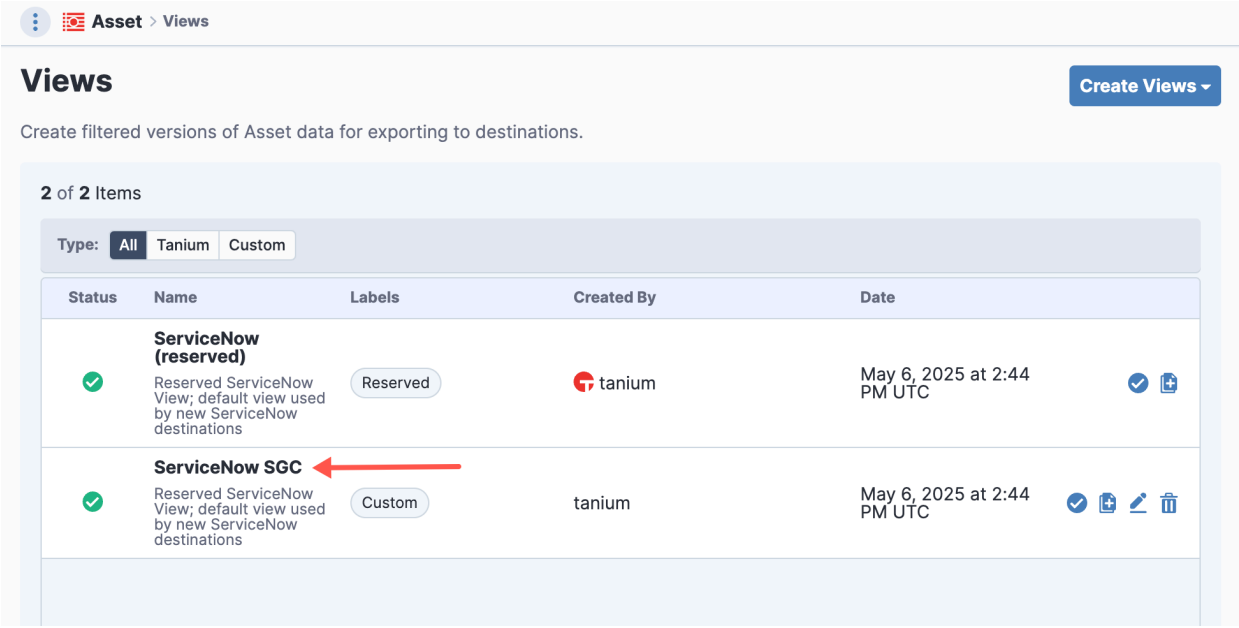
Verify permissions and create an API token

Sign in to Tanium Console with the new user account to verify that you can see views in Asset and generate API tokens.

1. Sign in to Console as **Asset API User**.
2. From the Main menu, go to **Modules** > **Asset** > **Views**.

   If you cannot access the page, verify the **Asset API User** role has the **Asset Report Reader** role.
3. Verify that you can see the view you created.

   If the view does not appear, sign in to Console as a user with the **Asset Report Reader** permission, create the view as described in Create a dedicated ServiceNow view on page 262, and then try this step again.



4. Generate an API token for use by the **Asset API User**. You require a single API token per ServiceNow environment for each integration.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Do not use a single token to establish sessions for multiple processes. When a token rotates for any process, that token stops working for any other processes that use the token. If you have three different environments for which you need to configure the Service Graph Connector, you can reuse the **Asset API User** account, but you need to create three API tokens, one for each environment.

a. From the Main menu, go to **Administration** > **Permissions** > **API Tokens** and click **New API Token**.

b. Enter **Service Graph Connector** or similar message for **Notes** and then specify an expiration time.

c. Leave **Persona** set to **Default**.

d. Enter the external IP addresses of the systems from which you will use this token to authenticate with the Tanium Server.

e. Click **Save**.

   The **View API Token** dialog appears.

f. Click Copy API Token to copy the token string to your clipboard, and then click **Close** to return to the **API Tokens** page.

   For more information about how to create API tokens, see Tanium Console User Guide: Managing API tokens.

Retrieve data

Retrieve data through the Asset API integration independent of any third-party applications or partner connections. The following steps use cURL to test the API integration from Windows, Linux, and macOS machines.

Best Practice: If your instance uses a ServiceNow MID Server or similar intermediary system, run these tests from that server.

©2026 Tanium Inc. All Rights Reserved

1. On a Windows machine, open an administrator command prompt. On Linux or macOS machines, open a Terminal window.

2. Run the following command to set a variable for the Tanium Server, where `<YourInstanceName>` is the domain name or IP address of the Tanium Server.

    - Windows:

      ```
      set TS=<YourInstanceName>
      ```

    - Linux / macOS:

      ```
      export TS=<YourInstanceName>
      ```

3. Run the following command to set the session token, where `<YourApiToken>` is the API token string that you copied to your clipboard.

    - Windows:

      ```
      set S=<YourApiToken>
      ```

    - Linux / macOS:

      ```
      export S=<YourApiToken>
      ```

    Tip: Include the entire token string, including the `token-` prefix. For example, `set S=token-744b6a6e9408c8fec82871c80ce0d8ec6d40c7c63b04d42325c4aea824`.

4. Run the following command to verify that you have the correct ID for the view that you created. Replace the ID at the end of the URL with the ID that you recorded.

    - Windows:

      ```
      curl -k -X GET -4 -H "tanium_server: %TS%" -H "Content-Type: application/json"
      -H "session: %S%" "https://%TS%/plugin/products/asset/v1/views/2"
      ```

    - Linux / macOS:

      ```
      curl -k -X GET -4 -H "tanium_server: ${TS}" -H "Content-Type: application/
      ```

©2026 Tanium Inc. All Rights Reserved

```
json" -H "session: $S" "https://${TS}/plugin/products/asset/v1/views/2"
```

A successful response contains the definition of the view in JSON format:

```
{
   "data":{
      "definition":{
         "attributes":[
            {
               "id":1,
               "entityId":1,
               "entityName":"Computer Name",
               "tableName":"ci_item",
               "displayName":"Computer Name",
               "fieldName":"computer_name",
               "dataType":"text"
            },
            {
               "id":3,
               "entityId":3,
               "entityName":"OS Platform",
               "tableName":"ci_item",
               "displayName":"OS Platform",
               "fieldName":"os_platform",
               "dataType":"text"
            }
         ],
         "filter":{
            "$or":[

            ]
         }
      },
      "id":2,
      "viewName":"ServiceNow SGC",
      "description":"Reserved ServiceNow View; default view used by new ServiceNow
destinations",
```

©2026 Tanium Inc. All Rights Reserved

```
      "reserved":false,
      "username":"tanium",
      "createdAt":"2025-05-23T15:33:28.212Z",
      "updatedAt":"2025-05-23T15:33:28.212Z",
      "status":"ready"
   }
}
```

5. Run the following command to retrieve and validate data from 100 endpoints. Replace the ID associated with the `viewId` with the ID of your **ServiceNow SCG** view.

   - Windows:

     ```
     curl -k -X GET -4 -H "tanium_server: %TS%" -H 'Content-Type: application/json' -H "session: %S%" "https://%TS%/plugin/products/asset/v1/assets?viewId=2&minimumAssetId=1&limit=100"
     ```

   - Linux / macOS:

     ```
     curl -k -X GET -4 -H "tanium_server: ${TS}" -H 'Content-Type: application/json' -H "session: $S" "https://${TS}/plugin/products/asset/v1/assets?viewId=2&minimumAssetId=1&limit=100"
     ```

   A successful response contains details for up to 100 endpoints in JSON format. truncated example:

```
{
   "meta":{
      "nextAssetId":101,
      "endOfReader":false
   },
   "data":[
      {
         "computer_name":"test001",
         "os_platform":"AIX"
      },
      {
         "computer_name":"test002",
```

©2026 Tanium Inc. All Rights Reserved

```
         "os_platform":"Linux"
      },
      {
         "computer_name":"test003",
         "os_platform":"Windows"
      }
   ]
}
```

The response includes two metadata properties to help paginate the data:

- `nextAssetId`: The ID of the next asset to retrieve. In terms of pagination, use this value as the cursor to start the next page of data. When `endOfReader` is `false`, the nextAssetId field is omitted from the response.
- `endOfReader`: A value of `false` indicates that more endpoint data is available. To retrieve all endpoint data, paginate until you reach the end of the results, indicated when `endOfReader` is `true`.

The `nextAssetId` and `endOfReader` properties appear in the `meta` section at the beginning of the response. For example:

```
{"meta":{"nextAssetId":101,"endOfReader":false},"data":[{...
```

6. Continue to run the GET command. In each command, set the `minimumAssetId` parameter to the value of the `nextAssetId` property that was returned in the previous response.
   - Windows:

     ```
     curl -k -X GET -4 -H "tanium_server: %TS%" -H 'Content-Type: application/json'
     -H "session: %S%" "https://%TS%/plugin/products/asset/v1/
     assets?viewId=2&minimumAssetId=101&limit=100"
     ```

   - Linux / macOS:

     ```
     curl -k -X GET -4 -H "tanium_server: ${TS}" -H 'Content-Type: application/
     json' -H "session: $S" "https://${TS}/plugin/products/asset/v1/
     assets?viewId=2&minimumAssetId=101&limit=100"
     ```

©2026 Tanium Inc. All Rights Reserved

When a response includes `endOfReader: true` and omits the `nextAssetId` property, there are no more assets to retrieve.

Note:

Large gaps in asset IDs might result in a 500 error and the `meta` section might still indicate more results and data is null. For example:

```
{"meta":{"nextAssetId":244,"message":{"code":"asset-additional-results-may-
exist-1","text":"Additional results may exist. Try again with a larger
minimumAssetId."},"endOfReader":false},"data":[]}
```

This can occur when the view uses filters to exclude endpoints that have no data for a specific column. If you encounter a 500 error, check to see if the response contains a `meta` section. If the `meta` section appears and `endOfReader` is `false`, try the request again with a larger `minimumAssetId` value.

©2026 Tanium Inc. All Rights Reserved

Reference: SBOM files and file types

For more information about Software Bill of Materials (SBOM), see Creating a Software Bill of Materials on page 159. SBOM supports scanning for the following files and file types:

Files and file types supported by SBOM

Ecosystem	Files and file types
Java	pom.xml , pom.properties , manifest.mf , JAR, WAR, PAR, EAR, SAR, HPI, JPI
JavaScript	package.json
Python	metadata, WHL
Ruby	GEMSPEC
PHP	installed.json
Go	Files with a magic number indicating that the file is an executable.*
Native library files	SO, A, DYLIB, DLL

* For more information about magic numbers, see Tanium Client Index Extension User Guide: Calculate magic number .

©2026 Tanium Inc. All Rights Reserved