Tanium Connect User Guide

2026H2 Semiannual Release

Version 5.56

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
- Connections 13
- Connection destinations 13
- Connection sources 14
- Connection schedules 19
- Tanium Autonomous IT Platform in Connect 19
- Interoperability with other Tanium products 19

Getting started 21

Gaining organizational effectiveness 22

Requirements 26
- Core platform dependencies 26
- Solution dependencies 26
  - Tanium recommended installation 26
  - Import specific solutions 27
  - Required dependencies 27
  - Feature-specific dependencies 27
- Tanium Module Server 28
- Endpoints 28
- Third-party software 28
- Host and network security requirements 29
  - Ports 29
  - Security exclusions 29
  - Internet URLs 30
- User role requirements 30

Installing 37
- Before you begin 37
- Import Connect with default settings 37

©2026 Tanium Inc. All Rights Reserved

Import Connect with custom settings 38
Manage solution dependencies 38
Upgrade Connect 39
Verify Connect version 39
Verify solution dependency versions 39

Configuring 41
Configure a file share mount 41
Configure Connect settings 41
Set up Connect users 42
Configure email server profile settings for Microsoft 365 44
Configure email server profile settings for SMTP 49
Configure Microsoft Azure cloud storage profile settings 51
Configure Google Cloud Storage cloud storage profile settings 53
Configure Oracle Cloud Infrastructure cloud storage profile settings 56
Configure AWS S3 cloud storage profile settings 59
Configure Tanium plugin for Security Copilot 60

Managing connections 62
View connection status 62
Filter connections list 63
View schedule for all connections 64
View connection metrics 65
Edit connections 65
Schedule connections 66
Update a connection schedule 66
Run connections 68
Update connection owner and persona 69
Update owner or persona for one or more connections 70
Manage connection limits 71
Export connections 71
Import connections 72
Use the same source for multiple destinations 74
Use the same destination in multiple connections 75
Clear New Items cache 76
Configure notifications for failed connection runs 76

©2026 Tanium Inc. All Rights Reserved

AWS S3 (Legacy) 78
Specify general connection information 78
Configure the connection source 80
Configure AWS S3 destination 81
Configure filters 84
Format data for AWS S3 84
Schedule the connection 85
Enable listening for an event 88
Save and verify connection 88

Cloud Storage 90
Prerequisites 91
Prerequisites for Microsoft Azure cloud storage destinations 91
Prerequisites for Google Cloud Storage cloud storage destinations 92
Prerequisites for OCI cloud storage destinations 93
Prerequisites for AWS cloud storage destinations 94
Specify general connection information 94
Configure the connection source 96
Configure the Cloud Storage destination 97
Configure filters 101
Format data for Cloud Storage 101
Schedule the connection 103
Enable listening for an event 105
Save and verify connection 105

Elasticsearch 107
Specify general connection information 107
Configure the connection source 109
Configure Elasticsearch destination 110
Configure filters 112
Format data for Elasticsearch 112
Schedule the connection 114
Enable listening for an event 117
Save and verify connection 117

Email 119

©2026 Tanium Inc. All Rights Reserved

Prerequisites for Microsoft 365 destinations 119
Prerequisites for SMTP destinations 121
Specify general connection information 122
Configure the connection source 124
Configure the email results destination 125
Configure filters 127
Format data for email 128
Schedule the connection 129
Enable listening for an event 132
Save and verify connection 132

Email (Legacy SMTP) 134
Prerequisites 134
Specify general connection information 134
Configure the connection source 136
Configure the Email (SMTP) results destination 137
Configure filters 141
Format data for email 141
Schedule the connection 142
Enable listening for an event 145
Save and verify connection 145

File 147
Configure the file destination 147
Format data for file 150

HTTP 151
Configure a receiver 151
Node.js example 151
Python example 152
Ruby example 152
Specify general connection information 152
Configure the connection source 154
Configure the HTTP destination 155
Configure filters 159
Format data for HTTP 160
Schedule the connection 161

©2026 Tanium Inc. All Rights Reserved

Enable listening for an event 164
Save and verify connection 164

Microsoft Azure Monitor 166
Microsoft Azure requirements 166
Specify general connection information 167
Configure the connection source 169
Configure the Microsoft Azure Monitor destination 170
Configure filters 173
Format data for Microsoft Azure Monitor 173
Schedule the connection 175
Enable listening for an event 177
Save and verify connection 177

Microsoft Log Analytics 179
Microsoft Azure requirements 179
Specify general connection information 179
Configure the connection source 181
Configure the Microsoft Log Analytics destination 182
Configure filters 185
Format data for Microsoft Log Analytics 185
Schedule the connection 187
Enable listening for an event 189
Save and verify connection 189

SMB file share 191
Prerequisites 191
Specify general connection information 191
Configure the connection source 193
Configure the SMB file share destination 194
Configure filters 196
Format data for SMB file share 196
Schedule the connection 197
Enable listening for an event 200
Save and verify connection 200

Socket (SIEM) 202

©2026 Tanium Inc. All Rights Reserved

Specify general connection information 202
Configure the connection source 204
Configure the SIEM destination 205
Configure filters 207
Format data 207
Schedule the connection 209
Enable listening for an event 212
Save and verify connection 212

SQL Server 214
System requirements 214
Set up the database 214
Sample SQL Script for creating stored procedures 215
Specify general connection information 217
Configure the connection source 219
Configure SQL Server destination 220
Configure filters 225
Map database table columns 225
Schedule the connection 227
Enable listening for an event 229
Save and verify connection 229

Maintaining 231
Review and remediate connection issues 231
Review and remediate connection schedules 232
Review and update connection owners 232
Review and remediate destination issues 233

Troubleshooting 234
Collect logs 234
Upgrading to Connect 5.18 or later 234
Configure per-connection log level 235
Collect a trace log for a connection 236
Configure general log settings 236
Adjust log expiration 236
Adjust log level 237
View logs 237

©2026 Tanium Inc. All Rights Reserved

Service logs 237
Connection run logs 237
Connect configuration state 237
Test connections 238
Troubleshoot issues 240
Issue: Cannot connect to Connect service 240
Issue: Connection fails 241
Connection reached memory ceiling 241
Issue: <no value> in Tanium Data Service (TDS) output 242
Issue: Connection does not export all intended data 242
Issue: Columns are missing from the Microsoft Azure Monitor table 242
Issue: Scheduled connection owned by a deleted user no longer runs 243
Issue: Tanium Audit Source connection fails with MaxNumberOfAuditEntriesPerCacheExceeded error 244
Issue: Emails to Microsoft 365 destinations fail to send 244
Issue: Imported connections to Microsoft 365 destinations do not run 245
Issue: Created connection does not allow editing of source or destination type 245
Issue: Cannot authenticate connection to Splunk instance using HTTP destination 245
Uninstall Connect 246
Uninstall Connect so data is restored on reinstall 246
Uninstall Connect so you start fresh when you reinstall 246
Contact Tanium Support 247

Reference: Column customizations 248
Replace data that matches a regular expression 248
Send custom columns to the destination 250
Customize the source columns sent to the destination 251

Reference: Cron syntax for Connect 253

Reference: Deprecated connection migration 254
Migrating Tanium Trends connections to Tanium Reporting connections 254

Reference: Filtering options 257
New Items 257
Continue Learning options 258
Using the New Items filter with time-windowed sources 259

©2026 Tanium Inc. All Rights Reserved

Regular Expression 259
Valid regular expression example 260
Invalid regular expression example 260
Numeric Operator 261

Reference: Format types 262
CEF 263
CSV 263
Delimiter separated values 264
Elasticsearch 265
HTML 266
JSON 266
LEEF 268
SQL server 269
Syslog RFC 5424 269

Reference: Gateway examples for Connect 271
Connect REST API replacement 271
Get a connection by ID 272
Get a connection run by ID 273
Get connection runs 274
Get connections 275
Get multiple Connect connections by ID 277
Get multiple Connect connections by description 278
Get Connect connection by ID and displayName 279
Get SQL Server stored procedures 280
Get SQL Server stored procedures through a satellite 282
Start connection run 284
Stop the active run for a Connect connection 284
Stop a specific connection run 285
Start multiple connection runs 286
Stop multiple in-progress connection runs 287
Enable multiple connections 288
Disable multiple connections 289
Delete multiple connections 290
Transfer ownership of multiple connections 291

©2026 Tanium Inc. All Rights Reserved

Change the persona of multiple connections 292

Reference: Microsoft Security Copilot integration with Tanium skills 294

Reference: Variables 295

Connection variables 295

Time stamp variables 297

Reference: Tanium Audit Source data 301

Supported audit types 301

General audit table columns 313

Authentication audit table columns 314

©2026 Tanium Inc. All Rights Reserved

Connect overview

With Connect, you can integrate Tanium with a SIEM, log analytics tools, threat feeds, or send email notifications.

Connections

A connection is the link between a *connection source* and a *connection destination*. The connection source might be data that Tanium is creating, like an answer or a log message. The connection destination is something outside of Tanium that you are integrating with, like a security information and event management (SIEM) tool.

Connection destinations

Connect includes templates for many common SIEM tools, file, log, and email formats. You can use these templates to integrate with configuration management databases (CMDB), trouble ticketing systems, and proprietary IT systems.

- Configuring cloud storage destinations on page 90
- Configuring Elasticsearch destinations on page 107
- Configuring email destinations on page 119
- Configuring file destinations on page 147
- Configuring HTTP destinations on page 151
- Configuring Microsoft Azure Monitor destinations on page 166
- Configuring Socket (SIEM) destinations on page 202
- Configuring SMB file share destinations on page 191
- Configuring SQL Server destinations on page 214

©2026 Tanium Inc. All Rights Reserved

- Configuring Tanium™ Reputation destinations: Tanium Reputation User Guide: Send data to the reputation service

Connection sources

Action History

The action history is a record of all actions issued by console operators. To view this record in Tanium, go to **Administration** > **Actions** > **Action History**. Connections configured with this source export the available action history on the first run. On subsequent runs, they export only action history that was generated after the previous connection run. For more information, see Tanium™ Console User Guide: Manage actions that are completed or in progress.

Client Status

Client Status, previously named System Status, includes the state of all the endpoints, including some useful information about the endpoint like IP Address, position in the network, and the last time it registered with the Tanium Server. For more information about the Client Status data, see Tanium Console User Guide: View the status of Tanium™ Client registration and communication.

Event

Tanium solutions, like Tanium™ Discover and Tanium™ Threat Response, can forward events to Connect as a data source. These events can then be used as a connection source in a connection and sent to any of the available connection destinations. For more information, see Tanium Discover User Guide: Create connection for event notifications and Tanium Threat Response User Guide: Exporting audit data.

Question History

The question history log is a history of every question that has been asked. When you are using the question log as a data source in Connect, you can filter the log in several ways to reduce the total volume of data being sent. Connections configured with this source export the available question history on the first run. On subsequent runs, they export only question history that was generated after the previous connection run. For more information, see Tanium Console User Guide: Question history.

Saved Question

©2026 Tanium Inc. All Rights Reserved

A saved question is a Tanium question that you want to ask on a repeated basis. For more information about saved questions, see Tanium™ Interact User Guide: Managing saved questions in Interact.

Note: When you select a saved question as a source, **Computer Group** defaults to **No Filter**, which does not filter the saved question with a computer group. Select **No Filter** if you want to send recent saved question results from all endpoints to the destination. The endpoint results are subject to the computer group management rights of the user configuring the connection, and might not match the endpoint membership of the **All Computers** computer group. Select the **All Computers** computer group if you want to explicitly filter the saved question on the **All Computers** computer group.

You can use the following settings for saved question sources:

Settings for saved questions sources in Tanium Connect

Setting	Description
Flatten Results	You might want to enable the **Flatten Results** setting to process results as individual records. For example, you might want to get notified when you see a new MD5 hash on a machine. Without the **Flatten Results** setting enabled, the entire data set that is retrieved by the saved question from a machine, such as all MD5 hashes, is considered to be a single record. Any change that is made to this data set shows up in the destination. By enabling the **Flatten Results** setting, Connect processes the new hashes on an individual basis (one MD5 hash from one machine) instead of all hashes from a machine as a single record.
Hide Errors	If the saved question returns an error, you can use the **Hide Errors** setting to prevent the error results from getting sent to the destination.
Hide No Results	If the saved question returns `[No results]`, you can use the **Hide No Results** setting to prevent this result from being sent to the destination.
Include Recent Answers	If you want to include results from machines that are offline, select **Include Recent Answers**, which returns the most recent answer to the saved question for the offline endpoint. **Note:** If you select **Include Recent Answers**, for the best results, you should also select **No Filter** from **Computer Group**.
Answer Complete Percent	Results are returned when the saved question returns the configured complete percent value. Any results that come in after the configured percent value has passed are not sent to the destination. If you find that the data returned from

©2026 Tanium Inc. All Rights Reserved

Setting	Description
	the saved question is incomplete in your destination, you can disable this setting by setting it to 0. If disabled, all data is returned after the timeout passes.
Timeout	Minutes to wait for clients to reply before returning processed results when **Answer Complete Percent** is set to 0. If the **Answer Complete Percent** value is not met at the end of the time limit, then the connection run is marked as a failure. The maximum timeout is 10 minutes.
Batchsize	Number of rows that are returned for the saved question results at one time. This setting might vary depending on your destination.

Server Information Source

Use the server information in the following location as a connection source: `https://<tanium_server>/info.json`.

Tanium™ Asset

Tanium Asset comes with a set of predefined reports to help you prepare for audit and inventory activities. You can also create your own custom reports and views. For each report or view, you can create a connection that specifies a report or view as a data source. Currently supported destinations include Email, File, HTTP, Socket Receiver, Splunk, and SQL Server. For more information, see Tanium Asset User Guide: Asset overview.

Tanium™ Audit Source

Tanium Server keeps detailed audit logs for server configuration and settings changes. However, accessing these logs requires direct access to the Tanium database. To access the audit logs, you can set them up as a data source in Connect.

For information about data available with the Tanium Audit Source, see Reference: Tanium Audit Source data on page 301.

Tanium™ Comply

Tanium Comply enables you to export compliance and vulnerability findings to help support enterprise compliance goals. Use the **Tanium Comply (Findings)** source to export all compliance and all vulnerability findings. For more information, see Tanium Comply User Guide: Exporting

©2026 Tanium Inc. All Rights Reserved

findings and assessments.

> **Important:** Exporting vulnerability assessments through Tanium Connect is a deprecated feature, which means it is available but is no longer receiving updates, or active development. Instead, use **Tanium Comply (Findings)** as a source.

Tanium™ Data Service (TDS)

TDS enables you to see stored sensor results for endpoints that are offline at the moment you issue a saved question. For more information, see Tanium Interact User Guide: Managing Tanium Data Service.

Tanium™ Direct Connect

Tanium Direct Connect enables other Tanium modules to establish sessions with endpoints. You can create a connection that generates an audit report of Direct Connect sessions and actions that users performed on endpoints during Direct Connect sessions. For more information, see Tanium Direct Connect User Guide: Exporting an audit log.

Tanium™ Discover

Tanium Discover contains reports that maintain an inventory of interfaces in your environment. For each report, you can create a connection that specifies a report as a data source. For more information, see Tanium Discover User Guide: Discover overview.

Tanium™ Endpoint Configuration

Tanium Endpoint Configuration enables you to deliver configuration information to endpoints consistently for all Tanium solutions that are available in an environment. You can create a connection that generates an audit report of all Endpoint Configuration management actions, manifest actions, and configuration changes. For more information, see Tanium Endpoint Configuration User Guide: Exporting an audit log.

Tanium™ Impact

Tanium Impact identifies the users, groups, and endpoints that have the highest potential impact in your organization if compromised, based on the impact rating. You can create a connection that specifies all users, groups, or endpoints with the highest impact as a data source. For more information, see Tanium Impact User Guide: Impact overview.

©2026 Tanium Inc. All Rights Reserved

Tanium™ Integrity Monitor

Tanium Integrity Monitor enables you to define watchlists of files, directories, and Windows registry paths that you want to monitor for changes. Use the **Tanium Integrity Monitor** source to export watchlist data. For more information, see Tanium Integrity Monitor User Guide: Integrity Monitor overview.

Tanium™ Jump Gate

Use Tanium Jump Gate to provide secure, controlled just-in-time access to critical systems and data in your environment. With Jump Gate, you can grant temporary role-based access to controlled infrastructure endpoints managed by Tanium Client, only when needed. With Connect, you can create connections to export audit, session, and recording data.

- The **Tanium Jump Gate Audit** source sends audit data for Jump Gate.
- The **Tanium Jump Gate Sessions** source sends session data and recordings from Jump Gate.

Tanium™ Reporting

Use Tanium Reporting to create custom reports and dashboards from data that TDS collects. You can create a connection to export report data or a dashboard. For more information, see Tanium Reporting User Guide: Export dashboards through Tanium Connect.

- The **Tanium Reporting (Source Data)** source sends raw source data and supports all destinations.
- The **Tanium Reporting (Reports and Dashboards)** source sends HTML files to destinations. Valid destinations include AWS S3, Email, File, or SMB File Share.

Tanium™ Reputation

Tanium Reputation is an aggregated repository of reputation data from various sources, including Palo Alto Networks WildFire, ReversingLabs, and VirusTotal. You can choose which type of status to include, such as only malicious or suspicious content. You can choose to include the full report, which includes detailed information from the reputation source, not just the status of the reputation item. You must have one or more reputation sources configured to get information from this connection source. For more information, see Tanium Reputation User Guide: Reputation overview.

Tanium™ Threat Response

©2026 Tanium Inc. All Rights Reserved

Tanium Threat Response contains audit reports for actions that were performed in Threat Response. For each report, you can create a connection that specifies a report as a data source. For more information, see Tanium Threat Response User Guide: Threat Response overview.

Tanium™ Trends

Tanium Trends provides data visualization panels from saved questions or module sources. You can create boards that organize one or more panels. For each board, you can create a connection that specifies a board as a data source in HTML format. Valid destinations include AWS S3, Email, or File. For more information, see Tanium Trends User Guide: Trends overview.

Important: Exporting Trends boards through Tanium Connect is a deprecated feature, which means it is available but is no longer receiving updates, or active development. Instead, migrate your Trends boards to Reporting, and then use Tanium Reporting as a source. For more information, see Tanium Trends User Guide: Migrating Trends boards to Reporting.

Connection schedules

A *connection run* is a single iteration of sending data from a connection source to a connection destination. Use cron schedules to adjust the timing of each connection run. You can have connections run at different combinations of on the minute, hour, day, week, or month. You can see when connections are running and how much data is being sent with the schedule view. For more information about schedules, see Schedule connections on page 66.

Tanium Autonomous IT Platform in Connect

Tanium Autonomous IT Platform comprises a set of interrelated features across multiple Tanium solutions. The Autonomous IT Platform provides guided initial configuration for solutions, proactively collects intelligence about conditions in Tanium environments, provides guidance based on those conditions, and enables automated workflows to address issues. For more information, see Tanium Console User Guide: Working with the Autonomous IT Platform.

Interoperability with other Tanium products

In addition to connection source data from other Tanium products, Connect works with other Tanium products to provide additional features and reporting of related data.

©2026 Tanium Inc. All Rights Reserved

Tanium™ Automate

From the Automate **Run a Tanium Connection** step, you can run a Connect connection as part of a playbook. For more information, see Tanium Automate User Guide: Reference: Steps.

Tanium™ Gateway

Use Gateway to access the Connect API. For more information, see Reference: Gateway examples for Connect on page 271.

Reputation

If you want to pre-populate reputation data with hashes from your environment, you can send data to Tanium Reputation from Connect. When this content is pre-populated, the reputation service can start querying about the status of the items from the reputation sources. For more information, see Tanium Reputation User Guide: Send data to the reputation service.

Trends

Connect features Trends charts that provide data visualization of Connect concepts. These boards are available in Trends and also appear on the Connect **Overview** page.

The **Connect** charts contain how much data is sent to all destinations each day, and the number of total connections that are initiated and scheduled each hour. The charts include data for both failed and successful connection runs. The following panels are in the **Connect** board that appears both in Trends and on the **Connect Overview** page:

- Bytes sent per day
- Data sent per day
- Connection runs per hour
- Scheduled connections per hour

For more information about how to import the Trends boards that are provided by Connect, see Tanium Trends User Guide: Importing the initial gallery.

©2026 Tanium Inc. All Rights Reserved

Getting started with Connect

Step 1: Install and configure Connect

Install and configure Tanium Connect.

For more information, see Installing Tanium Connect on page 37. If you upgrade from a previous version, see Upgrade Connect on page 39.

Step 2: Create connections

Connections consist of a source and destination.

For more information, see Connection sources on page 14 and Connection destinations on page 13.

Step 3: Manage connections

When you have multiple connections, you can view a list of all the connections and the connection schedule.

For more information, see Managing connections on page 62.

©2026 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Connect

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

- Develop a dedicated change management process. For more information, see Change management on page 22.
- Track operational maturity. For more information, see Operational metrics on page 23.
- Validate cross-functional alignment. For more information, see Organizational alignment on page 25.

Change management

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

- Update SLAs with elevated expectations, including connection configuration and maintenance.
- Identify key resources in the organization to review and approve changes to connection requirements to ensure minimal unexpected or unapproved changes.
- Identify internal and external dependencies for connections from Tanium sources to destinations (example: creating or updating database tables before sending data to a database).
- Identify maintenance windows for various connection management scenarios to maximize connection uptime.
- Create a Tanium steering group (TSG) for connection activities, to expedite reviews and approvals of processes that align with SLAs.

©2026 Tanium Inc. All Rights Reserved

Operational metrics

Connect maturity

Managing a program to export data from Tanium sources to destinations successfully includes operationalization of the technology and measuring success through key benchmarking metrics. The four key processes to measure and guide operational maturity of your Tanium Connect program are as follows:

Processes to measure Tanium Connect maturity

Process	Description
Usage	how and when Tanium Connect is used in your organization
Automation	how automated Tanium Connect is
Functional Integration	how integrated Tanium Connect is, across IT security, IT operations, and IT risk/compliance teams
Reporting	how automated Tanium Connect is and who the audience of connection reporting is

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

Benchmark metrics for Tanium Connect maturity

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Tanium Core Platform and Connect installed	Basic connections configured and running, such as sending data to an Email or SMB destination	Configuration fine-tuned, such as memory consumption or memory usage	• Events forwarded from Tanium modules • Data filters configured to send new items, or data matching	Advanced connections configured and running, such as integrations with third-party applications (Splunk, ITSM solution, SQL Server)

©2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
					numeric values or regular expressions, to destination	
	Automation	Manual	Manual	Scheduled connections	Scheduled connections listening to event-based sources	End-to-end workflow established to take action, such as alerting or remediation to a third-party application
	Functional integration	Unused	AWS S3 or SMB destination configured, for example	• Scheduled exports to third-party IT systems, such as data lakes and SIEMs • Email destination configured • Tanium Threat Response or Tanium Reputation sources configured, for example	Using integrated event forwarding and emails	Connect integrated with a third-party application (Splunk, ITSM solution, SQL Server)
	Reporting	Unused	Ad hoc; Reporting tailored to	Consistent; Reporting tailored to	Automated; Reporting tailored to stakeholders	Automated; Reporting tailored to stakeholders ranging

©2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
			stakeholders at request	stakeholders on cadence	ranging from Operator to Executive	from Operator to Executive

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 improve patch management.

©2026 Tanium Inc. All Rights Reserved

Connect requirements

Review the requirements before you install and use Connect.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Connect. For more information about how to get Connect, see Tanium Solutions & Bundles.
- Tanium™ Core Platform servers
- Tanium™ Client: No client requirements.

Solution dependencies

Other Tanium solutions are required for Connect to function (required dependencies) or for specific Connect 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 Connect 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 Connect requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Connect, 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.

©2026 Tanium Inc. All Rights Reserved

Import specific solutions

If you select only Connect 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 Connect, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Connect has the following required dependencies:

- Tanium™ Email Service
- Tanium™ RDB Service
- Tanium™ Secrets Service

Feature-specific dependencies

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

- Tanium Asset and Feature-specific dependencies for the Tanium Asset source
- Tanium™ Blob Service for the External Storage (Blob) destination
- Tanium Comply and Feature-specific dependencies for the Tanium Comply source
- Tanium Data Service (TDS) for the Tanium Data Service source
- Tanium Direct Connect and Feature-specific dependencies for the Tanium Direct Connect source
- Tanium Discover and Feature-specific dependencies for the Tanium Discover or Event sources
- Tanium Endpoint Configuration and Feature-specific dependencies for the Tanium Endpoint Configuration source

©2026 Tanium Inc. All Rights Reserved

    - 2.5.89 or later to send data to an on-premises destination that is not accessible from the external internet

- Tanium Impact and Feature-specific dependencies for the Tanium Impact source
- Tanium Integrity Monitor for the Tanium Integrity Monitor or Event sources
- Tanium Interact to view charts on the **Connect Overview** page
- Tanium Reporting and Feature-specific dependencies for the Tanium Reporting source
- Tanium Reputation for the Tanium Reputation source
- Tanium Threat Response and Feature-specific dependencies for the Tanium Threat Response source
- Tanium Trends and Feature-specific dependencies for the Tanium Trends source and to view charts on the **Connect Overview** page

Tanium Module Server

Connect installs and runs as a service on the Module Server host computer. The impact on the Module Server depends on usage.

Endpoints

Connect does not deploy packages to endpoints. For more information about Tanium Client operating system support, see Tanium™ Client Management User Guide: Client version and operating system requirements.

Third-party software

With Connect, you can integrate with several different kinds of third-party software or cloud providers. If no specific version is listed, there are no version requirements for that software.

- Amazon Web Services S3
- Google Cloud Storage

©2026 Tanium Inc. All Rights Reserved

- Microsoft Azure Blob Storage
- Microsoft Azure Monitor
- Microsoft O365 email
- Microsoft SQL Server 2008, 2012, or 2014
- Elasticsearch:
    - Elasticsearch destination: Elasticsearch 8.7 or earlier.
    - Socket Receiver destination: Elasticsearch 8.8 or later.
- SMTP email servers
- Security information and event management (SIEM) products and services including: HP ArcSight, IBM QRadar, LogRhythm, McAfee SIEM, and Splunk.

Host and network security requirements

Specific ports and processes are needed to run Connect.

Ports

The following ports are required for Connect communication.

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

©2026 Tanium Inc. All Rights Reserved

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.

Internet URLs

If security software is deployed in the environment to monitor and block unknown URLs, your security administrator might need to allow access to the following internet URLs on the Tanium Module Server to use the Email (O365) destination:

- graph.microsoft.com:443
- login.microsoftonline.com:443
- graph.microsoft.us:443
- dod-graph.microsoft.us:443

  for DoD tenants
- login.microsoftonline.us:443
- outlook.office.com:443

  if you assign the `Mail.ReadWrite` permission to the Microsoft Entra ID application

User role requirements

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

- Connect solution permissions on page 31

©2026 Tanium Inc. All Rights Reserved

- Tanium™ Email Service user role permissions on page 33
- Connect administration, platform content, and global permissions on page 34: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Connect users on page 42.

Table 8. Optional roles for Connect on page 35 are required to enable optional Connect functionality.

Some Connect 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 Connect. If you create custom roles for Connect users, be sure to assign all the solution permissions and content set permissions that are required for Connect 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 **Connect Service Account**, **Email Service Account**, or **Email Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

Note: For the best results, do not assign the **Connect Write (All)** permission to a custom role. A user with this permission might edit a connection that they otherwise would not have the proper permission to access, and send unintended source data to a destination. Instead, if you want to edit a connection, take ownership, then make updates.

Connect solution permissions

Permission	Connect Administrator [1,2]	Connect Operator [1,2]	Connect User [1,2]
Connect OPERATOR: Operator access to Connect READ: Read own	✓	✓	✓

©2026 Tanium Inc. All Rights Reserved

Permission	Connect Administrator [1,2]	Connect Operator [1,2]	Connect User [1,2]
connections RUN: Run own connections SHOW: View the Connect workbench WRITE: Write own connections	READ RUN SHOW WRITE	OPERATOR READ RUN SHOW WRITE	READ RUN SHOW WRITE
Connect Administrator Administrative-level access to Connect. Provides the **User** read permission	✓ ADMINISTER	✗	✗
Connect Event Write access to events through the Connect API	✓ WRITE	✓ WRITE	✓ WRITE
Connect Eventschema Read and write access to event schemas through the Connect API	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE
Connect Owner Write access to take ownership of connections owned by other users	✓ WRITE	✓ WRITE	✗
Connect Plugin For internal purposes only	✗	✗	✗
Connect Read View all connections	✓ ALL	✓ ALL	✗
Connect Run Run all connections. Provides the **User** read permission	✓ ALL	✓ ALL	✗
Connect Write Create, view, edit, or delete any connection. Provides the **User** read permission.	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Connect Administrator [1,2]	Connect Operator [1,2]	Connect User [1,2]
Connect Service Account Access to module service accounts to read and write data	✗	✗	✗

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

[2] Users with this role can reuse a configured destination that they own, but cannot modify destinations owned by other users.

Blob Service user role permissions

Permission	Connect Administrator	Connect Operator	Connect User
Blob External Storage Config Read and write access to blob external storage configuration	✓ READ WRITE	✓ READ WRITE	✗
External Blob Send blob data to external destinations	✓ WRITE	✓ WRITE	✓ WRITE

Tanium™ Email Service user role permissions

Permission	Connect Administrator	Connect Operator	Connect User
Email Send emails using the Email (O365) destination	✓ SEND	✓ SEND	✓ SEND
Email Config Read and write access to O365 email server configuration	✓ READ WRITE	✓ READ WRITE	✗
Email Support Bundle Read access to the email (O365) support bundle	✓ WRITE	✗	✗

©2026 Tanium Inc. All Rights Reserved

Connect administration, platform content, and global permissions

Permission	Permission Type	Connect Administrator	Connect Operator	Connect User
Action Group	Administration	✓ READ	✓ READ	✓ READ
Token - Use	Administration	✓ SPECIAL	✓ SPECIAL	✓ SPECIAL
User	Administration	✓ READ	✗	✗
Action	Platform Content	✓ READ WRITE	✓ READ WRITE	✗
Filter Group	Platform Content	✓ READ	✓ READ	✓ READ
Own Action	Platform Content	✓ READ	✓ READ	✗
Package	Platform Content	✓ READ	✓ READ	✗
Plugin	Platform Content	✓ EXECUTE READ	✓ EXECUTE READ	✓ EXECUTE READ
Saved Question	Platform Content	✓ READ	✓ READ	✗
Sensor	Platform Content	✓ READ	✓ READ	✓ READ

©2026 Tanium Inc. All Rights Reserved

Permission	Permission Type	Connect Administrator	Connect Operator	Connect User

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

[1] Denotes a permission when Trends 2.4 or later is installed.

Important: Connections are hidden from the Connections list view if the authenticated user does not have the required permissions for the data source. Examples that could limit the view of an authenticated user include RBAC access to a saved question or computer group, or System Administrator access to the various types of audit logs that are available from the Tanium Platform. See the following table for required permissions for specific sources.

Optional roles for Connect

Role	Enables
A custom role that includes the **Action read** platform content permission	Access to the **Action History** source. For more information, see Tanium Console User Guide: Configure a custom role .
A custom role that includes the **Audit read** administration permission	Access to the **Tanium Audit Source** source. For more information, see Tanium Console User Guide: Configure a custom role .
A custom role that includes the **Client Status read** administration permission	Access to the **Client Status** source. For more information, see Tanium Console User Guide: Configure a custom role .
A custom role that includes the **Data Collection Registration write** Interact permission	Access to the **Tanium Data Service** source. For more information, see Tanium Console User Guide: Configure a custom role .
A custom role that includes the **Question History read** administration permission	Access to the **Question History** source. For more information, see Tanium Console User Guide: Configure a custom role .
A custom role that includes the **System Status read** administration permission	Access to the **Server Information Source** source. For more information, see Tanium Console User Guide:

©2026 Tanium Inc. All Rights Reserved

Role	Enables
	Configure a custom role .

Note: Connections use the owner's role permissions to access content. If the connection owner has insufficient permission for content that a connection requires, such as inability to view a computer group, the connection might not fully export the data that you intend to export. For more information and descriptions of content sets and permissions, see Tanium Console User Guide: RBAC overview.

©2026 Tanium Inc. All Rights Reserved

Installing Tanium Connect

Use the Tanium Console **Solutions** page to install Connect and choose either automatic or manual configuration:

- Automatic configuration with default settings: Connect is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information about the automatic configuration for Connect, see Import Connect with default settings on page 37.
- Manual configuration with custom settings: After installing Connect, you must manually configure required settings. Select this option only if Connect requires settings that differ from the recommended default settings. For more information, see Import Connect with custom settings on page 38.

Before you begin

- Read the .
- Review the Connect requirements on page 26.
- If you are upgrading from a previous version, see Upgrade Connect on page 39.
- Review the User role requirements on page 30. and assign the correct roles to Connect users. For more information, see Tanium Console User Guide: Managing roles.
    - To import the Connect solution, you must be assigned the Administrator reserved role.

Import Connect with default settings

Use default settings to get started with installing Connect without extra configuration steps.

You can set the Connect action group to target the **No Computers** filter group by enabling restricted targeting before importing Connect. This option enables you to control Connect tools deployment

©2026 Tanium Inc. All Rights Reserved

through scheduled actions that are created during the import and that target the Connect tools action group. For example, you might want to test Connect tools on a subset of endpoints before deploying the Connect tools to all endpoints. In this case, you can manually deploy the Connect 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.

To import Connect 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 Connect version on page 39.

Import Connect with custom settings

To import Connect without automatically configuring default settings, be sure to deselect the **Apply All Tanium recommended configurations** checkbox while performing the steps in Tanium Console User Guide: Import or update specific solutions. To verify that the correct version is installed after the import, see Verify Connect version on page 39.

To configure settings, see Configure Connect settings on page 41.

Manage solution dependencies

About this task

When you start the Connect workbench for the first time, the Tanium Server checks whether all the Tanium modules and shared services (solutions) that are required for Connect are installed at the required versions. The Connect workbench cannot load unless all required dependencies are installed. If you selected **Tanium Recommended Installation** when you imported Connect , the Tanium Server automatically imported all your licensed solutions at the same time. Otherwise, if you manually imported Connect and did not import all its dependencies, Tanium Console displays a banner that lists the dependencies and the required versions.

Perform the following steps if a banner indicates any Connect dependencies are not installed:

1. Install the dependencies as described in Tanium Console User Guide: Import or update specific solutions.
2. From the Main menu, go to **Modules** > **Connect** to open the **Overview** page. to open the Connect **Overview** page and verify that Console no longer displays a banner to list missing

©2026 Tanium Inc. All Rights Reserved

dependencies.

Upgrade Connect

Important: Before you upgrade Connect, you must back up your <Module Server>\services\connect-files\config\connect.db file in case you need to revert to a previous version of Connect. The support package is the easiest way to obtain a backup of the Connect database. For more information, see Collect logs on page 234.

To upgrade Connect, see Tanium Console User Guide: Managing Tanium solutions. To verify that the correct version is installed after the upgrade, see Verify Connect version on page 39.

Verify Connect version

After you import or upgrade Connect , verify that the correct version is installed.

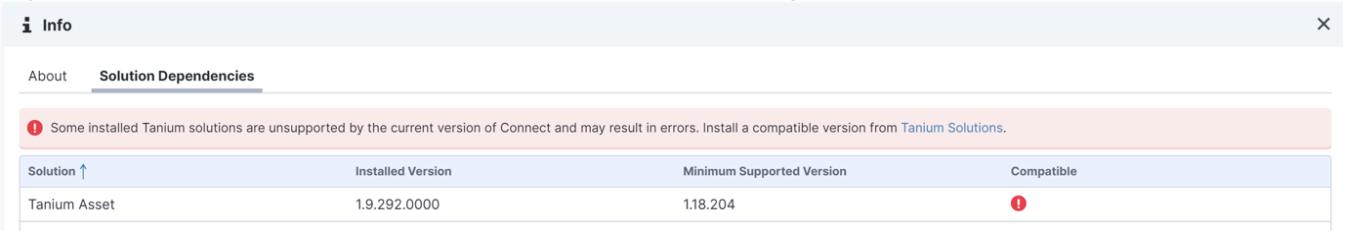
1. Refresh your browser.
2. From the Main menu, go to **Modules** > **Connect** to open the **Overview** page.
3. To show version information, click Info .

Verify solution dependency versions

About this task

Verify that installed solution dependencies are at the minimum required version or later. The Solution Dependencies table lists only out-of-date solutions that are configured as a source for at least one connection.

Figure 1. Solution Dependencies table in the Connect settings



©2026 Tanium Inc. All Rights Reserved

Note: Only Tanium administrators can view the Solution Dependencies table.

1. Refresh your browser.
2. From the Main menu, go to **Modules** > **Connect** to open the **Connect Overview** page.
3. Click Info and then click **Solution Dependencies** to show installed solutions and version information. If all solutions are at the minimum required version or later, the table does not list any solutions.
   If a Tanium solution or source shows Critical, the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

©2026 Tanium Inc. All Rights Reserved

Configuring Connect

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

No default settings are configured for Connect.

Configure a file share mount

Connect can write consumable files to disk. You can configure the Module Server to copy these files to a Common Internet File System (CIFS) or Network File System (NFS) share on a file server, or to an *internal share* on a Tanium™ Appliance. An internal share is a directory that the `tancopy` user can access using SFTP. For more information about how to configure a file share, see Tanium Appliance User Guide: Configure solution module file share mounts.

Configure Connect settings

To configure the following settings, from the Main menu, go to **Modules** > **Connect** > **Overview**, click Settings , and then go to the **Configuration** tab.

Connect settings

Setting	Description
Connection Run Log Expiration	Number of days before connection run logs are removed.
Connect Service Log Level	Log level for the Connect service logs.
Internal IPs	Select this to allow anyone to run connections to IP addresses in the following internal subnets, or clear this to allow only administrator users to run connections to IP addresses in the following internal subnets: • `10.0.0.0/8`

©2026 Tanium Inc. All Rights Reserved

Setting	Description
	• `127.0.0.0/8` • `169.254.0.0/16` • `172.16.0.0/12` • `192.168.0.0/16` For more information, see Test connections on page 238 .
Memory Ceiling	The global maximum sum of memory (GB) for all simultaneously running connections. This defaults to 8 GB. The per-connection Memory Ceiling (by default, 1 GB) cannot exceed the global Memory Ceiling. Increase this setting when you have one or more demanding connections that frequently exhibit out of memory errors while running. **Note:** If the sum of simultaneously scheduled connection **Memory Ceiling** values exceed the global **Memory Ceiling** , connections run until the global **Memory Ceiling** is reached, then any remaining connections enter a waiting queue if you select the **Queue Connections** configuration setting, or fail if you clear the **Queue Connections** configuration setting.
Process Count Limit	Specify the number of scheduled connections that can run simultaneously, each with its own dedicated background process. This setting gives you better control over how many simultaneously running connections you want to allow in your environment. Set to `0` to allow unlimited simultaneous connections.
Queue Connections	Option to queue additional scheduled connections when the maximum memory or process counts is reached. If this setting is not enabled, any connections beyond the specified maximum values that attempt to run result in failures.

Set up Connect users

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

To review specific permissions for each role, see User role requirements on page 30.

Important: On installation, Connect creates a Connect user to automatically manage the Connect service account. Do not edit or delete the Connect user.

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

©2026 Tanium Inc. All Rights Reserved

Tip: To provide just-in-time access or scalable standing access to Connect functionality, you can use SCIM provisioning combined with Tanium user groups. This approach lets you manage user access at scale or ad hoc through your identity provider, without creating users individually in Tanium. For more information, see Provision users into Tanium user groups with SCIM.

Connect Administrator

Assign the **Connect Administrator** role to users who manage the configuration of Connect. This role can perform the following tasks:

- Configure Connect settings, including resource allocation and logging
- View, run, and create connections
- Take ownership of connections owned by other users
- Edit and delete owned connections
- Access the Connect REST API

Connect Operator

Assign the **Connect Operator** role to users who manage the configuration of Connect. This role can perform the following tasks:

- Configure some Connect settings, including resource allocation and logging
- View, run, and create connections
- Take ownership of connections owned by other users
- Edit and delete owned connections
- Access the Connect REST API

Connect User

Assign the **Connect User** role to users who work with connections. This role can perform the following tasks:

- Create connections

©2026 Tanium Inc. All Rights Reserved

- View, run, edit, and delete owned connections

> **Note:** Do not assign the **Connect Service Account**, **Email Service Account**, or **Email Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

Configure email server profile settings for Microsoft 365

About this task

If you want to configure a connection destination to send email using Microsoft 365, you must first configure an email server profile.

> **Note:** Microsoft 365 was previously known as Office 365 (O365).

Note the following settings:

- For a walkthrough of configuration prerequisites, Microsoft Azure configuration, email server profile configuration, and connection configuration, see Tanium Community: Use Tanium Connect to Send Microsoft Office 365 Emails using Modern Authentication.
- You must have a Microsoft 365 Outlook email address associated with a Microsoft Entra ID (formerly Azure Active Directory) user.
- You must create a Microsoft Entra ID application and service principal, and assign the **Mail.Send** and **User.Read** permissions to the application, to send an email with an attachment up to a total of 3 MB (this includes the body of the email plus the attachment). If you want to limit the application scope, create an application access policy and associate it with a mail-enabled security group containing at least one user. For more information, see Microsoft Entra documentation: Create a Microsoft Entra application and service principal that can access resources and Microsoft Graph documentation: Configure ApplicationAccessPolicy.
    - You must also generate a Microsoft Entra ID application client secret. For more information, see Microsoft Entra documentation: Option 3: Create a new client secret.
    - You must also assign the **Mail.Send** and **User.Read** permissions to the application to

©2026 Tanium Inc. All Rights Reserved

send emails with attachments up to a total of 3 MB. For more information, see Microsoft Entra documentation: Assign a role to the application.

> **Note:** If a connection run generates no data, no email is sent. However, if you select a saved question source and clear **Hide No Results**, an email is sent per connection run, regardless of whether data is available.

- If you want to enable sending emails with attachments greater than 3 MB and up to 150 MB (subject to your Microsoft 365 attachment settings), you can assign the **Mail.ReadWrite** permission to the Microsoft Entra ID application. If you assign this permission, you must allow traffic to **outlook.office.com** over port 443/TCP and **outlook.office365.com** over port 443/TCP.

  > **Important:** Attachments larger than 3 MB are not supported for email sent through GCC M365, including FedRAMP M365. Connect uses the Microsoft **createUploadSession** API to manage attachments for Microsoft 365 email uploads. The API has a known issue with attachments larger than 3 MB in GCC M365 environments. This limitation applies to any customer whose Microsoft 365 environment is GCC M365, independent of the Tanium environment. Customers who try to send an email with an attachment larger than 3 MB through a GCC M365 environment might receive a **MS_GRAPH_STATUS_CODE 401 large_attachment** response that contains an error message similar to **caused by unexpected status code 401 from ms-graph**. For more information about the **createUploadSession** API and the known issue, see Microsoft Graph documentation: attachment: createUploadSession.

  > **Note:** The **Mail.ReadWrite** permission only permits a larger attachment size; the body of the email must never exceed 3 MB.

  > **Note:** For the best results, if you assign the **Mail.ReadWrite** permission, create an access policy and limit Microsoft Entra ID application access to one user. For more information, see Microsoft Graph documentation: Limiting application permissions to specific Exchange Online mailboxes.

- The **Email (O365 & SMTP)** destination requires an email server profile on the Tanium Server. You can configure an email server profile through the Connect workbench in Tanium

©2026 Tanium Inc. All Rights Reserved

Console.

- To configure an email server profile in Tanium Console, you must have a role with the Tanium **Email Config write** permission. The predefined **Connect Operator** and **Connect Administrator** roles in Connect have this permission. Sending an email requires the user that configures the connection to have permission to the content set to which you assign the email server profile. For more information about predefined roles in Connect, see User role requirements on page 30. For information about configuring custom roles, see Tanium Console User Guide: Managing roles

> **Note:** If you delete an email server profile configuration that is referenced by a scheduled connection, future scheduled instances of that connection fail. For more information, see Issue: Emails to Microsoft 365 destinations fail to send on page 244.

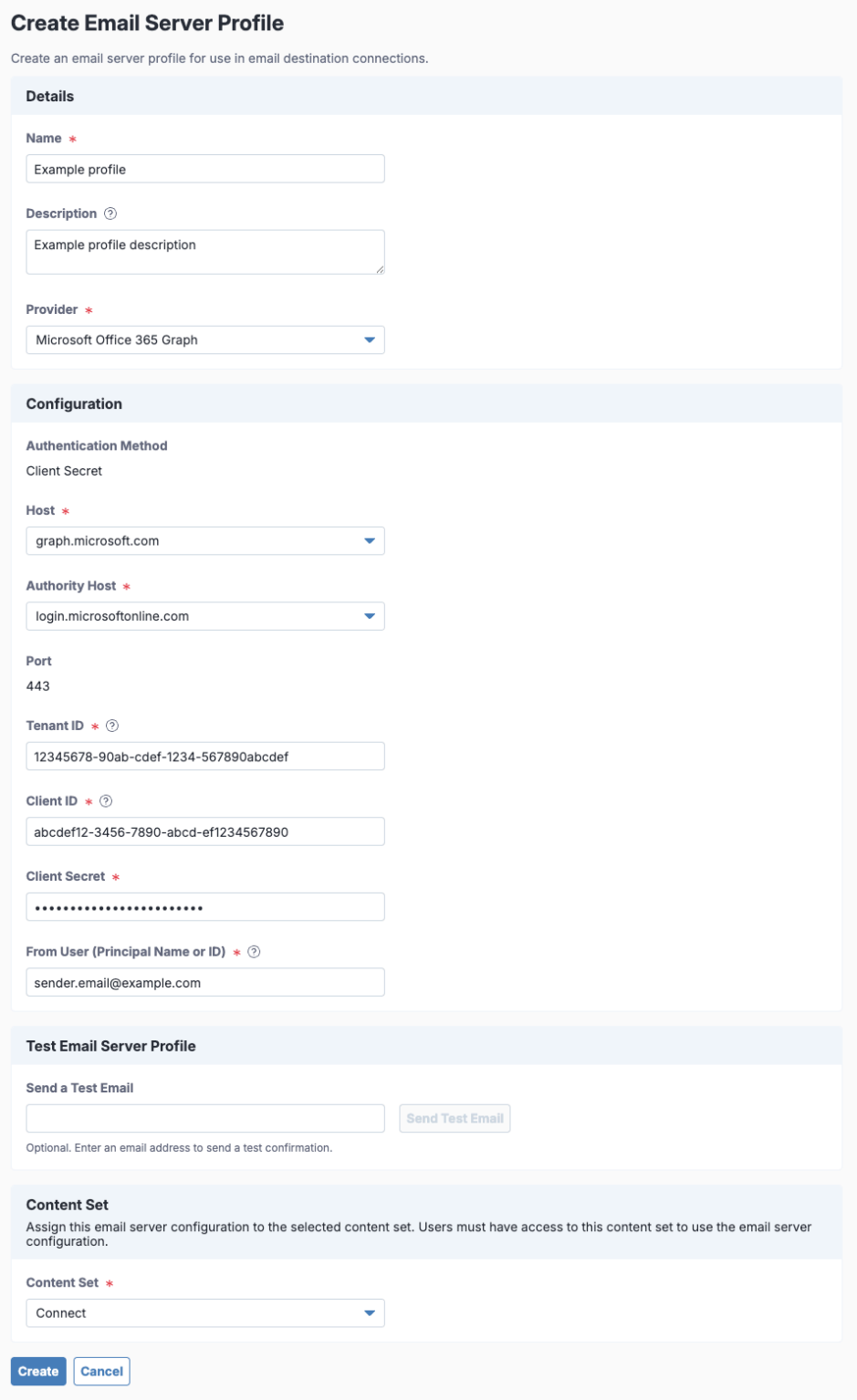
- The email server profile uses the **Authority Host** that you select for authentication to the **Host** that you select, over port 443/TCP.
- Configure your network allow list to allow traffic outbound from your Tanium Module Server to the following Microsoft 365 URLs and enable access for Microsoft 365 mail resources:
  - **graph.microsoft.com:443**
  - **login.microsoftonline.com:443**
  - **graph.microsoft.us:443**
  - **dod-graph.microsoft.us:443** for DoD tenants
  - **login.microsoftonline.us:443**
  - **outlook.office.com:443** and **outlook.office365.com:443** if you assign the **Mail.ReadWrite** permission to the Microsoft Entra ID application. For more information, see Microsoft 365 documentation: Office 365 URLs and IP address ranges.

For more information, see Configuring email destinations on page 119.

1. From the Main menu, go to **Modules** > **Connect** > **Overview**.
2. Click Settings and go to the **Email Server** tab.

©2026 Tanium Inc. All Rights Reserved

3. Click **Create Email Profile**.



4. Enter a profile **Name** and **Description**.
5. For the **Provider**, select **Microsoft Office 365 Graph**.
6. Select the **Host** and **Authority Host** of the destination.

©2026 Tanium Inc. All Rights Reserved

The **Authentication Method** and **Port** are predefined.

For the available **Host** and **Authority Host** values, see the list of email server profile settings at the beginning of this task.

7. Enter the Microsoft Azure **Tenant ID** in hexadecimal UUID format. For more information, see Microsoft Azure documentation: How to find your Azure Active Directory tenant ID.
8. Enter the Microsoft Azure application **Client ID** in hexadecimal UUID format. For more information, see Microsoft Azure documentation: Sign in to the application.
9. Enter the Microsoft Azure application **Client Secret**. For more information, see Microsoft Azure documentation: Option 2: Create a new application secret.
10. Enter a Microsoft Entra ID (formerly Azure Active Directory) user User Principal Name attribute or Object ID as the **From User (Principal Name or ID)**. Emails sent using this email server profile show this user in the **From** field. For more information, see Microsoft Azure documentation: Add or update a user's profile information and settings.
11. To verify your configuration, enter an email address in the **Send a Test Email** field, then click **Send Test Email**. An email from the configured **From User** with the subject `Tanium Connection Test` is sent to this email address. If you receive this email in the email address inbox within the next few minutes, continue to the next step. Otherwise, check the following:
    - Check the recipient email address spam folder and deleted items folder to see if a rule redirected the email from the inbox.
    - Check the sender email address sent email folder to verify that the email was generated and sent.
    - Check that your email server profile settings are correct, including the **Tenant ID**, **Client ID**, and **Client Secret**.
    - Verify that your network allow list contains properly configured rules for graph.microsoft.com (or graph.microsoft.us for GCC High tenants, dod-graph.microsoft.us for DoD tenants), login.microsoftonline.com (or login.microsoftonline.us for GCC High and DoD tenants), outlook.office.com, and outlook.office365.com.
12. Assign a **Content Set** to this email server profile.

Tip: Ensure that users who configure connections with this email server profile are able to access this content set.

©2026 Tanium Inc. All Rights Reserved

13. Click **Create**.

Configure email server profile settings for SMTP

About this task

If you want to configure a connection destination to send email through an SMTP server, you must first configure an email server profile.

Note the following settings:

- The **Email (O365 & SMTP)** destination requires an email server profile on the Tanium Server. You can configure an email server profile through the Connect workbench in Tanium Console.
    - To configure an email server profile in Tanium Console, you must have a role with the Tanium **Email Config write** permission. The predefined **Connect Operator** and **Connect Administrator** roles in Connect have this permission. Sending an email requires the user that configures the connection to have permission to the content set to which you assign the email server profile. For more information about predefined roles in Connect, see User role requirements on page 30. For information about configuring custom roles, see Tanium Console User Guide: Managing roles

    Note: If you delete an email server profile configuration that is referenced by a scheduled connection, future scheduled instances of that connection fail.

- Configure your network allow list to allow traffic outbound from your Tanium Module Server to the SMTP server.
    - To use Google Mail as an SMTP server, allow traffic to `smtp.google.com`.
- You must have email addresses to send and receive email results.
- Gather information about your mail server, including host, port, certificate, user name, password.

©2026 Tanium Inc. All Rights Reserved

Note: Standard TCP ports for secure email using SMTP include 465 and 587. Do not send unencrypted data over TCP port 25 outbound.

For more information, see Configuring email destinations on page 119.

1. From the Main menu, go to **Modules** > **Connect** > **Overview**.
2. Click Settings and go to the **Email Server** tab.
3. Click **Create Email Profile**.
4. Enter a profile **Name** and **Description**.
5. For the **Provider**, select **SMTP**.
6. In the **Configuration** section, click **Secure** to secure the connection with TLS.

   Note: If you do not select **Secure**, authentication information is encrypted at rest, but passed unencrypted to the destination.
7. (Optional) If you have a certificate, you can upload the certificate to provide additional security. Click **Upload Certificate**, select the certificate, and then click **Import**. Certificates must be uploaded in PEM format.
8. Enter the **Host** and **Port** of the SMTP server.
9. To authenticate with the SMTP server, click **Use Authentication**, and then enter the **User Name** and **Password** to sign into the SMTP server.
10. Enter a connection **Timeout** (in seconds), and then enter an email address for the **From User**.
    Emails sent using this email server profile show this user in the **From** field.
11. To verify your configuration, enter a destination email address in the **Send a Test Email** field, then click **Send Test Email**. An email from the configured **From User** with the subject **Tanium Connection Test** is sent to this email address. If you receive this email in the email address inbox within the next few minutes, continue to the next step. Otherwise, check the following:
    - Check the recipient email address spam folder and deleted items folder to see if a rule redirected the email from the inbox.
    - Check the sender email address sent email folder to verify that the email was

©2026 Tanium Inc. All Rights Reserved

generated and sent.
- Check that the email server profile settings are correct.
- Check that your network egress allow list contains properly configured rules for the SMTP server.

12. Assign a **Content Set** to this email server profile.

Tip: Ensure that users who configure connections with this email server profile are able to access this content set.

13. Click **Create**.

Configure Microsoft Azure cloud storage profile settings

About this task

If you want to send a file to Microsoft Azure Cloud Storage, you must first configure a cloud storage profile. Note the following settings:

- You must configure a Microsoft Azure blob storage account with the following settings:
  - **Performance**: select **Standard** for a general-purpose v2 account type, or **Premium** for block blobs or page blobs account type.



Note: General-purpose v1 accounts are not supported.

  - **Enable storage account key access**: select this to enable Shared Key authorization. The External Storage (Blob) destination does not support shared access signature (SAS) authorization or Entra ID authorization.
  - **Endpoint type**: select **Standard** endpoint (in the format https://<storage-account-name>.blob.core.windows.net). The External Storage (Blob) destination does not support Microsoft Azure DNS zone endpoints (in the format https://<storage-account-name>.z[00-50].blob.storage.azure.net).



Note: Compressed and uncompressed blob files created with this destination are limited to a maximum of 200 GB.

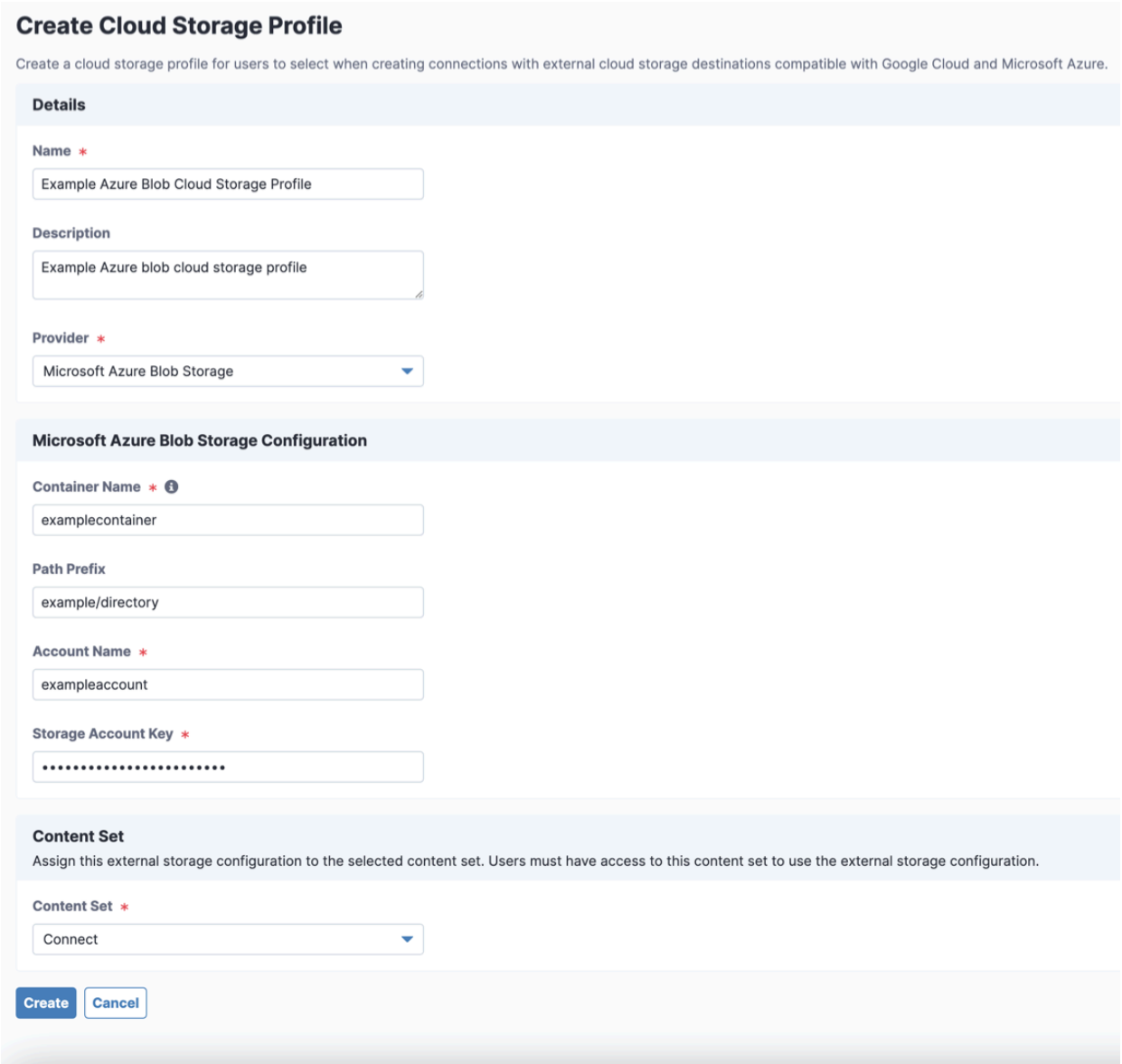
©2026 Tanium Inc. All Rights Reserved

For more information about Microsoft Azure storage accounts, see Microsoft Azure Blob storage documentation: Storage account overview.

- You must configure at least one storage account container to store blobs.

For more information, see Configuring cloud storage destinations on page 90.

1. From the Main menu, go to **Modules** > **Connect** > **Overview**.
2. Click Settings and go to the **Cloud Storage** tab.
3. Click **Create Cloud Storage Profile**.



4. Enter a profile **Name** and **Description**.
5. Select **Azure Blob** from **Provider**.

©2026 Tanium Inc. All Rights Reserved

6. Enter the Microsoft Azure storage account **Container Name**.
7. Enter a blob **Path Prefix** to define the directory path to store the blob, based on your bucket configuration. Use the format of /<directory-name-1>/<directory-name-2>/<directory-names-n...> to define path prefixes. If you configure a cloud storage profile with a **Path Prefix**, select this cloud storage profile for a Cloud Storage destination, and also configure a destination **Path Prefix**, the generated endpoint contains both Path Prefix values. The cloud storage profile **Path Prefix** value precedes the destination **Path Prefix** value, such as https://myaccount.blob.core.windows.net/container-name/<profile-path-prefix>/<destination-path-prefix>/blob-file-name.

   > **Note:** Directory names and the directory path must conform to Microsoft Azure storage account directory rules and blob name virtual directory rules. For more information, see Microsoft Azure documentation: Directory Names and Microsoft Azure documentation: Blob Names.

8. Enter the Microsoft Azure storage **Account Name**.
9. Enter the **Storage Account Key** associated with the storage account.
10. Assign the cloud storage profile to a **Content Set**.

    > **Tip:** Ensure that Tanium operators who configure connections with this cloud storage profile have the **Blob External Storage write** permission for this content set.

11. Click **Create**.

Configure Google Cloud Storage cloud storage profile settings

About this task

If you want to send a file to Google Cloud Storage, you must first configure a cloud storage profile. Note the following settings:

- You must configure a Google Cloud Storage bucket with the following settings:
  - Enter a globally unique name in the namespace that complies with bucket name restrictions. For more information, see Google Cloud Storage documentation: Bucket names.

©2026 Tanium Inc. All Rights Reserved

- Select a `STANDARD` data storage class.
- If you want to create a folder structure to store objects, select **Enable Hierarchical namespace on this bucket**. For more information, see Google Cloud Storage documentation: Hierarchical Namespace.

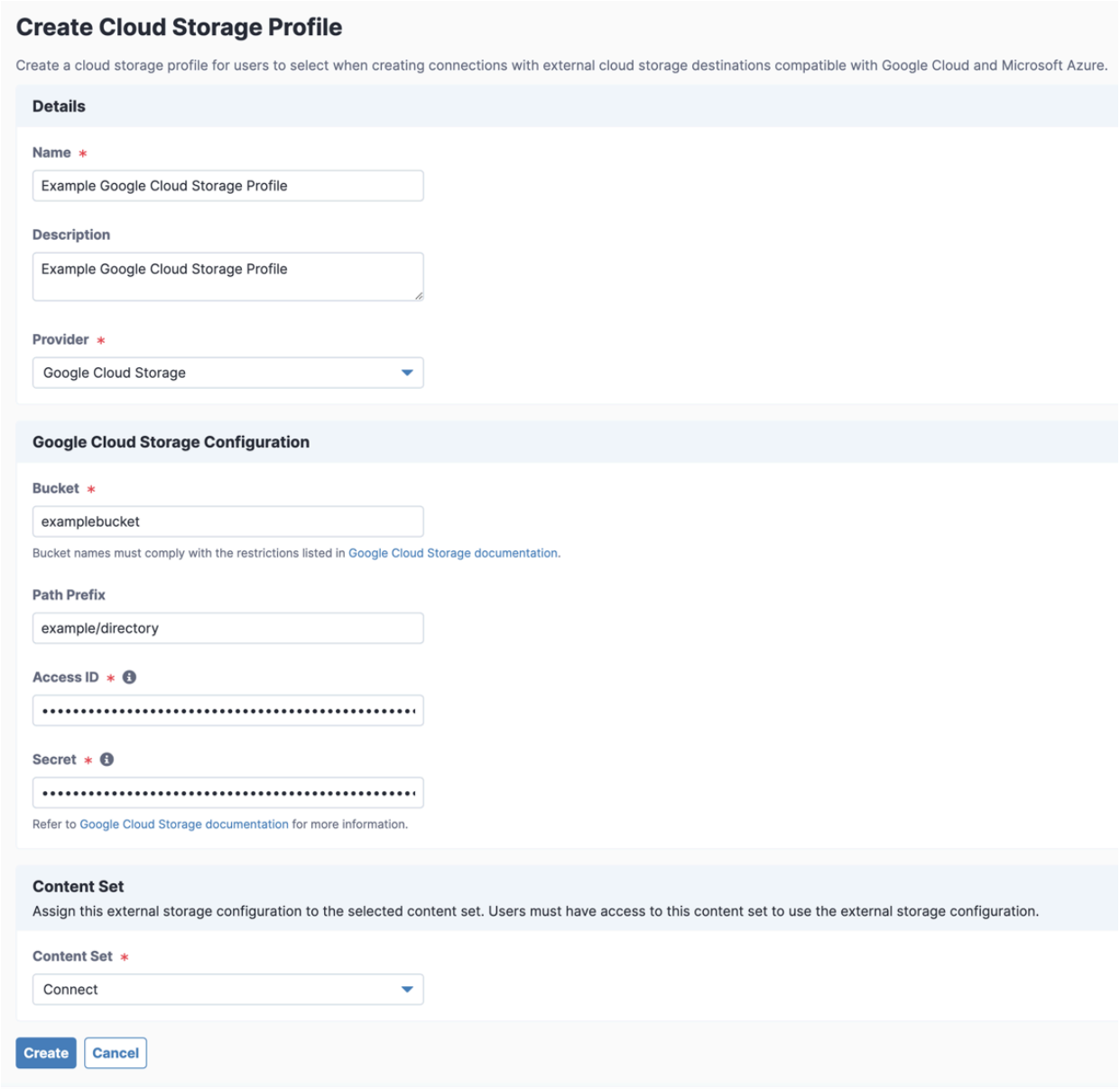
> **Note:** Compressed and uncompressed blob files created with this destination are limited to a maximum of 200 GB.

- You must configure a Google Cloud Storage service or user account with the following bucket permissions: **storage.objects.create**, **storage.objects.delete**, **storage.objects.get**, **storage.objects.list**.
- You must configure hash-based message authentication code (HMAC) keys for Google Cloud Storage authentication to enable blob upload to the bucket. The HMAC key access ID and secret must be associated with the Google Cloud Storage service or user account assigned the bucket permissions. For more information, see Google Cloud Storage documentation: HMAC keys.

For more information, see Configuring cloud storage destinations on page 90.

1. From the Main menu, go to **Modules** > **Connect** > **Overview**.
2. Click Settings and go to the **Cloud Storage** tab.
3. Click **Create Cloud Storage Profile**.

©2026 Tanium Inc. All Rights Reserved



4. Enter a profile **Name** and **Description**.
5. Select **Google Cloud Storage** from **Provider**.
6. Enter the Google Cloud Storage **Bucket** name.
7. Enter a blob **Path Prefix** to define the folder path to store the blob, based on your bucket configuration. Use the format of /<folder-name-1>/<folder-name-2>/<folder-names-n...> to define path prefixes. If you configure a cloud storage profile with a **Path Prefix**, select this cloud storage profile for a Cloud Storage destination, and also configure a destination **Path Prefix**, the generated endpoint contains both Path Prefix values. The cloud storage profile **Path Prefix** value precedes the destination **Path Prefix** value, such as https://storage.googleapis.com/bucket_name/profile-path-prefix/destination-path-prefix/

©2026 Tanium Inc. All Rights Reserved

blob-file-name.

8. Enter the HMAC key **Access ID**. This HMAC key must be associated with the Google Cloud Storage service or user account that is assigned bucket permissions.
9. Enter the HMAC key **Secret**. This HMAC key must be associated with the Google Cloud Storage service or user account that is assigned bucket permissions.
10. Assign the cloud storage profile to a **Content Set**.

    Tip: Ensure that Tanium operators who configure connections with this cloud storage profile have the **Blob External Storage write** permission for this content set.

11. Click **Create**.

Configure Oracle Cloud Infrastructure cloud storage profile settings

About this task

If you want to send a file to Oracle Cloud Infrastructure (OCI), you must first configure a cloud storage profile. Note the following settings:

- You must configure an OCI bucket with the following settings:
  - Enter a globally unique name in the compartment that complies with bucket name restrictions. For more information, see Oracle Cloud Infrastructure documentation: Object Storage Buckets.
  - Select a `STANDARD` default storage tier.

  Note: Compressed and uncompressed blob files created with this destination are limited to a maximum of 200 GB.

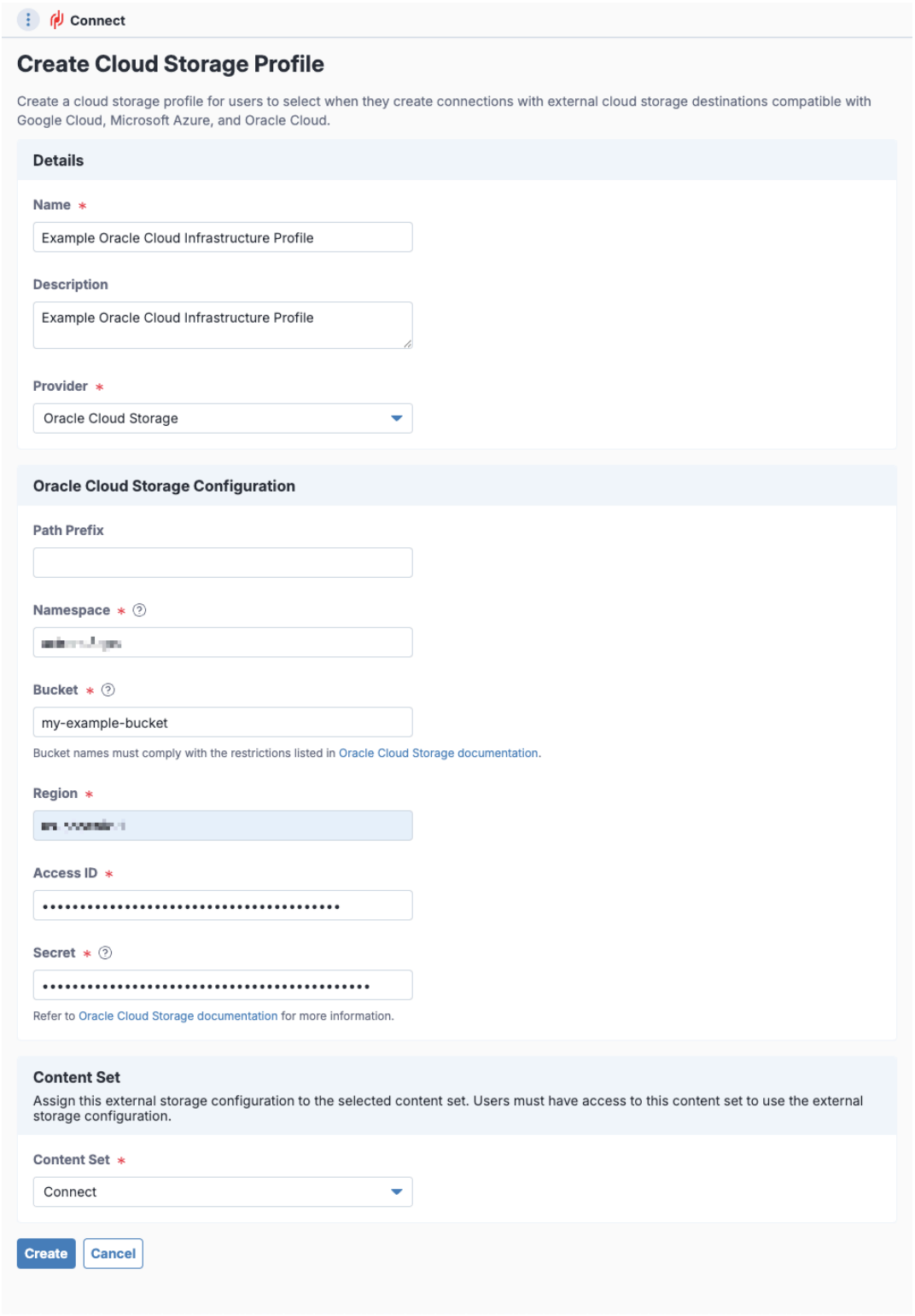
- You must configure customer secret keys for OCI authentication to enable blob uploads to the bucket. The access key and secret key must be associated with the OCI service or user account that is assigned the bucket permissions. For more information, see Oracle Cloud Infrastructure documentation: Creating a Customer Secret Key.

©2026 Tanium Inc. All Rights Reserved

For more information, see Configuring cloud storage destinations on page 90.

1. From the Main menu, go to **Modules** > **Connect** > **Overview**.
2. Click Settings and go to the **Cloud Storage** tab.
3. Click **Create Cloud Storage Profile**.

©2026 Tanium Inc. All Rights Reserved



4. Enter a profile **Name** and **Description**.
5. Select **Oracle Cloud Storage** from **Provider**.
6. (Optional) Enter a blob **Path Prefix** to define the folder path to store the blob, based on your bucket configuration. Use the format of /<folder-name-1>/<folder-name-2>/<folder-names-

©2026 Tanium Inc. All Rights Reserved

n...> to define path prefixes. If you configure a cloud storage profile with a **Path Prefix**, select this cloud storage profile for a Cloud Storage destination, and also configure a destination **Path Prefix**, the generated endpoint contains both **Path Prefix** values. The cloud storage profile **Path Prefix** value precedes the destination **Path Prefix** value in the object path. For more information about OCI object paths, see Oracle Cloud Infrastructure documentation: Downloading an Object Storage Object from a Bucket.

7. Enter the **Namespace** of the top-level container for all buckets and objects.
8. Enter the OCI **Bucket** name.
9. Enter the **Region** of the cloud storage destination
10. Enter the **Access ID**. The ID must be associated with the OCI service or user account that is assigned bucket permissions.
11. Enter the **Secret**. This secret must be associated with the OCI service or user account that is assigned bucket permissions.
12. Assign the cloud storage profile to a **Content Set**.

    Note: Ensure that Tanium operators who configure connections with this cloud storage profile have the **Blob External Storage write** permission for this content set.

13. Click **Create**.

Configure AWS S3 cloud storage profile settings

About this task

If you want to send a file to AWS S3 cloud storage, you must first configure a cloud storage profile. For information about required AWS S3 bucket permissions, see Prerequisites for AWS cloud storage destinations on page 94.

For more information, see Configuring cloud storage destinations on page 90.

1. From the Main menu, go to **Modules** > **Connect** > **Overview**.
2. Click Settings and go to the **Cloud Storage** tab.
3. Click **Create Cloud Storage Profile**.
4. Enter a profile **Name** and **Description**.

©2026 Tanium Inc. All Rights Reserved

5. Select **AWS S3 Storage** from **Provider**.
6. Enter the **Access Key** for the AWS Identity and Access Management (IAM) user or role that is assigned bucket permissions.
7. Enter the **AWS Secret Access Key** for the IAM user or role that is assigned bucket permissions. For more information, see AWS documentation: Amazon S3 API Reference.
8. (Optional) Enter a **Path Prefix** to define the directory path to store the file, based on your bucket configuration. Use the format of /<directory-name-1>/<directory-name-2>/<directory-names-n...> to define path prefixes. If you configure a cloud storage profile with a **Path Prefix**, select this cloud storage profile for a Cloud Storage destination, and also configure a destination **Path Prefix**, the generated endpoint contains both **Path Prefix** values. The cloud storage profile **Path Prefix** value precedes the destination **Path Prefix** value.
9. Enter the **S3 Bucket Name**. For more information, see AWS documentation: General purpose bucket naming rules.
10. Enter the **AWS Region** of the S3 bucket.
11. Select a **Server-Side Encryption** option. **Amazon S3 managed keys (SSE-S3)** is the only available option.
12. (Optional) Enter a **Custom AWS Endpoint** to use an endpoint other than the default endpoint associated with your AWS credentials.
13. If you have a proxy configured for your Tanium Module Server, select **Module Server Proxy**.
14. Assign the cloud storage profile to a **Content Set**.

    Tip: Ensure that Tanium operators who configure connections with this cloud storage profile have the **Blob External Storage write** permission for this content set.
15. Click **Create**.

Configure Tanium plugin for Security Copilot

©2026 Tanium Inc. All Rights Reserved

Important: The Microsoft Security Copilot integration is available in Tanium Integrations Gallery. For more information, see Tanium Integrations Gallery User Guide: Managing the Microsoft Security Copilot integration.

©2026 Tanium Inc. All Rights Reserved

Managing connections

You can view status, edit, import, and export connections.

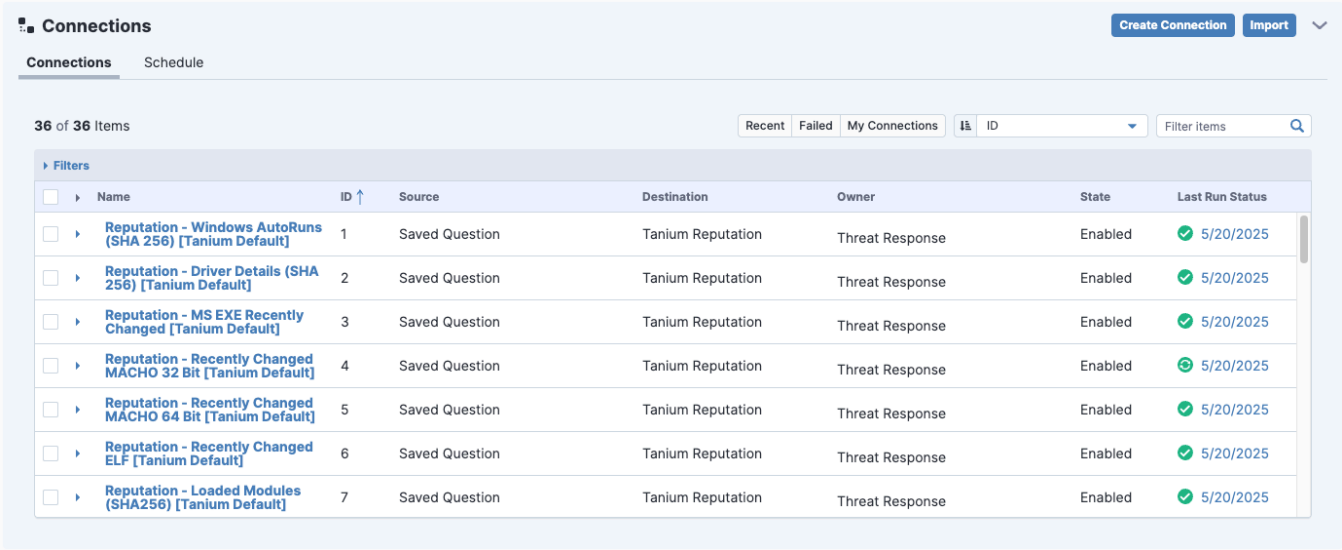
View connection status

To view the status of your connections, choose one of the following options:

- From the Main menu, go to **Modules** > **Connect** > **Overview** and then go to the **Connections** section.
- From the Main menu, go to **Modules** > **Connect** > **Connections**.

A list of your connections appears with status information.

Figure 2. Connections tab that appears on the Connections page



©2026 Tanium Inc. All Rights Reserved

Note:
If a **Last Run Status** value contains Critical , the most recent connection run failed. Review the connection log information for previous runs to troubleshoot.

If a Tanium solution or source shows Critical , the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

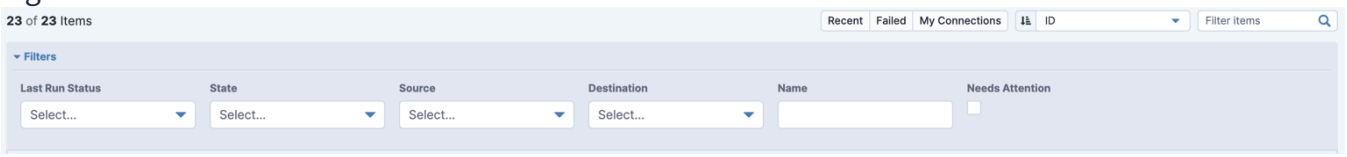
- Click to expand any row to show additional details for the connection, such as source and schedule.
- Click any connection to view details for the connection, including associated persona, statistics about the amount of data, connection runs, schedule, and logs for previous runs.

Tip: The **Connections** section also has a dedicated page. To access, go to **Modules** > **Connect** > **Connections** from the Main menu.

Filter connections list

If you have many connections, you can filter or order the list.

Figure 3. Connection filters



- To filter on a specific connection, enter a string in the **Filter items** field. The list updates with any connection names that contain matching text in the **Name**, **ID**, **Source**, **Destination**, or **Owner** columns. To clear the filter, click **X** in the **Filter items** field.
- To filter on a specific column, expand **Filters** and specify any filters for the **Last Run Status**, **State**, **Source**, **Destination**, or **Name** columns. Connections must match all filters to appear.
- To show connections that have configuration issues, expand **Filters** and select **Needs Attention**. Possible issues include:

©2026 Tanium Inc. All Rights Reserved

- The connection contained a scheduling issue that Connect resolved. Review the configured schedule to verify the connection runs as intended.
- Certificates on TCP connections that have the **Trust on First Use** option selected are now pinned regardless of the certificate derivation from a trusted Certificate Authority. Disable **Trust on First Use** in the connection configuration if connection runs result in a certificate error.

- Click a column header to sort the connections by the data in the column in descending order. Click the column header again to sort the list in ascending order. To clear the sort, click the column header a third time.

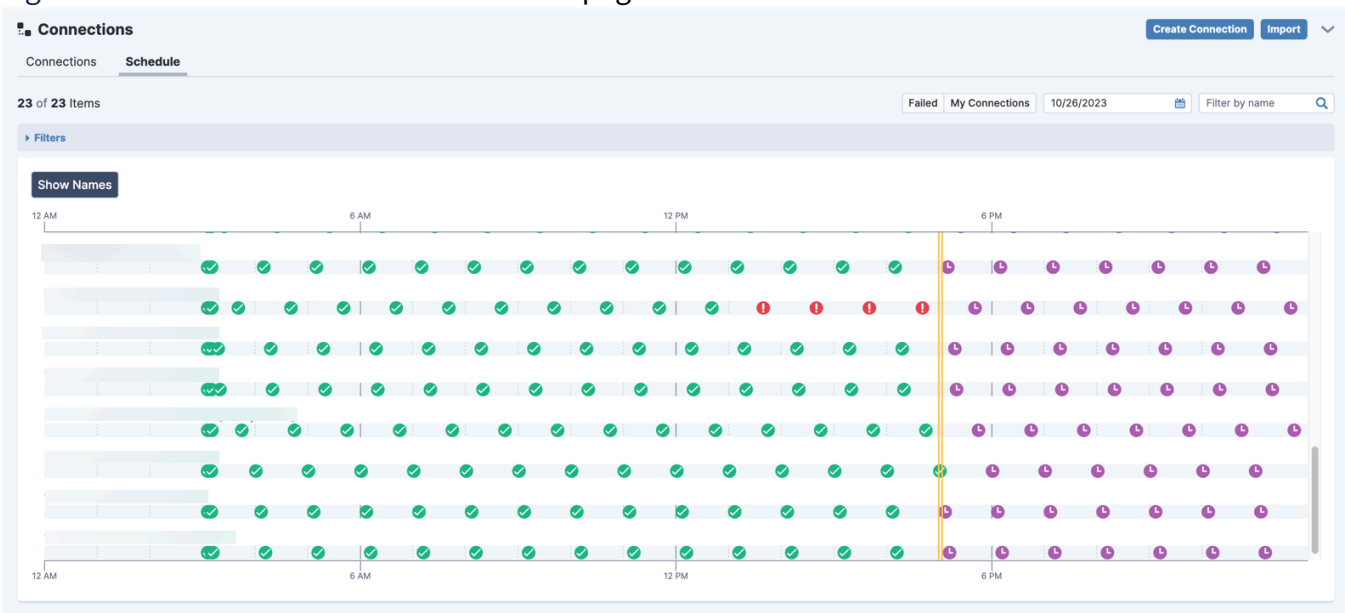
View schedule for all connections

To view the schedule for each connection in relation to all of the other connections, choose one of the following options:

- From the Connect menu, click **Schedule**.
- From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click **Schedule**.

The default view shows the connection runs for the current day, in the time zone of your browser.

Figure 4. Schedules tab on the Connections page



- To view details about a connection, click the connection name or click a run icon for the

©2026 Tanium Inc. All Rights Reserved

connection. If the run icon is for a failed run, click the run icon to open the specific run log.

- To view all connections that happened on a specific date, select the date in the calendar field above the schedule.
- To filter the connections that appear in the schedule, type a name into the **Filter by name** field. The list of connections automatically updates. To clear the filter, click **X** in the **Filter by name** field.
- To view the run log for a specific connection run, click the run icon in the schedule.

View connection metrics

Use the charts in the **Summary** section to view overall connection metrics.

- To track how many connections have run for each hour over the past seven days, use the **Connection Runs Per Hour** and **Scheduled Connections Per Hour** charts.
- To track how much data is sent by all connections over the past seven days, use the **Rows Sent Per Day** and **Bytes Sent Per Day** charts.

Edit connections

To edit a connection, from the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section, click the connection, and click **Edit**. You can change the connection source configuration, destination configuration, filters, formats, and schedule in the configuration screen.

After you create a connection, you cannot update the connection source type or destination type, only the source configuration or destination configuration. If you want to change the source type or destination type, create a new connection.



Note: Users that are members of predefined roles can only edit owned connections. For more information about connection ownership, see Update connection owner and persona on page 69.

You can reference the documentation for the destination type for more information.

- Some destinations use specific destination names. When you edit a named destination, the

©2026 Tanium Inc. All Rights Reserved

changes affect all connections where that specific **Destination Name** is used.

- Some connections use passwords for the destination. If you change settings for a destination, you must re-enter the password.

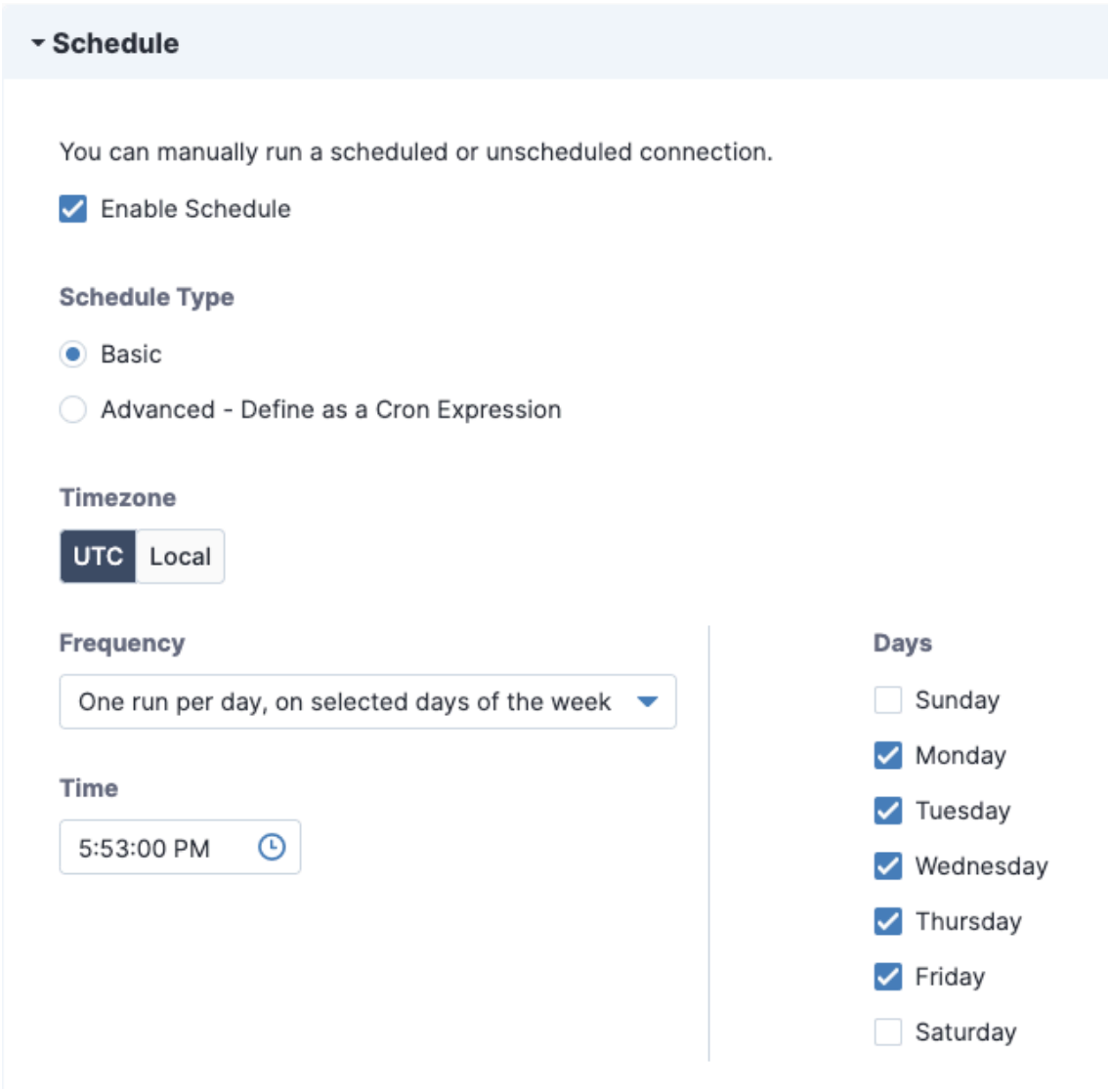
Schedule connections

Schedule connections to run at specific time intervals. Then, you can view the schedule status of all your connections in the schedule view.

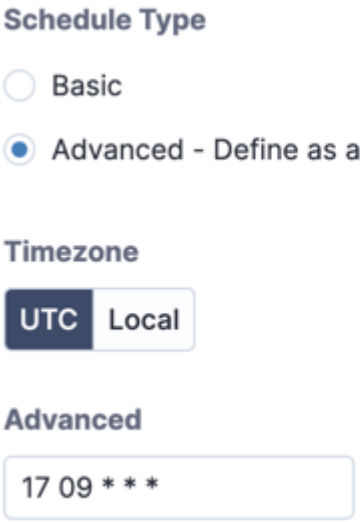
Update a connection schedule

1. Edit the connection. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click the connection.
2. Use the **Schedule** section to update the schedule.
    - Select **Enable schedule**.
    - In the **Schedule Type**, select **Basic** to build a schedule with the provided controls.

©2026 Tanium Inc. All Rights Reserved



- To view or edit the cron expression directly, select **Advanced - Define as a Cron Expression**, and use the **Advanced** field to edit the cron expression.



©2026 Tanium Inc. All Rights Reserved

> **Note:** If a user that owns a scheduled connection is deleted, future scheduled instances of that connection do not run. For more information, see Issue: Scheduled connection owned by a deleted user no longer runs on page 243.

3. Go to the bottom of the page and click **Save**.

Result

> **Note:** To run a connection, Connect creates an API token for the user or persona who runs or schedules the connection. These API tokens appear on the **API Tokens** page in Tanium Console with descriptions of **System Use Only for Connect**. Connect manages these API tokens automatically. To avoid disruptions, do not delete or manually rotate these API tokens, and do not delete the user or persona who initiated the connection.

Run connections

In addition to scheduling a connection, you can manually run a connection. There are multiple options throughout Connect to manually run a connection:

- From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section, select the checkbox next to the connection, and click **Run Now**.
- From the Connect menu, click **Connections** to open the **Connections** page. Select the checkbox next to the connection and click **Run Now**.
- From either the Connect **Overview** page or the **Connections** page, click the connection to view details for the connection. From this page, click **Run**.
- When you edit a connection, click **Run** at the top of the page to run the connection. Note that if you click **Run**, any changes you made are not saved. If you make changes to the connection and want to run the connection with the updated settings, go to the bottom of the page and click **Save and Run**.

> **Tip:** If a connection is already running, the option to run the connection is replaced with a **Stop** button.

©2026 Tanium Inc. All Rights Reserved



Note: To run a connection, Connect creates an API token for the user or persona who runs or schedules the connection. These API tokens appear on the **API Tokens** page in Tanium Console with descriptions of **System Use Only for Connect**. Connect manages these API tokens automatically. To avoid disruptions, do not delete or manually rotate these API tokens, and do not delete the user or persona who initiated the connection.

Update connection owner and persona

Each connection is associated with a user account that owns the connection, and an optional persona for that user account. Only data that the owner user and associated persona can access is sent from a source to a connection destination.

Connections contain one of the following **Owner** values:

- A user name if a user owns the connection
- **Unassigned** if no user owns the connection

Connections contain one of several **Run as Persona** values:

- a persona name if a persona is associated with the connection and the active session user either has the persona or otherwise has rights to view the persona
- a persona ID if a persona is associated with the connection, but the active session user does not have the persona nor rights to view the persona
- **Default Persona** if no persona is associated with the connection
- **Unknown** while an existing connection is migrated to an updated Connect version, or in other rare cases. For more information, see Troubleshooting on page 234.

The user that creates a connection is the initial owner, and that user's active persona at creation time is the initial persona associated with the connection. If the user selects the default persona during connection creation, no persona is associated with the connection.

You can update a connection owner or associated persona. For example, if a connection owner leaves a department or otherwise changes responsibilities, you can update the connection owner to another user to maintain the connections and data output. Alternatively, if you add a new computer group and new persona, you can update the persona associated with the connection to the new

©2026 Tanium Inc. All Rights Reserved

persona, and include data from the new endpoints in a connection run.

Note: Verify that a new owner user or persona can access intended content before you update connection ownership or associated persona, to ensure that a connection runs as expected. For example, if the updated permission set does not have the right to access a computer group, endpoint members of that computer group might not be included in the data. Alternatively, if the updated permission set does not have the right to access a saved question, a connection that uses that saved question as a source might fail.

You can only update the persona associated with a connection if your user is the owner. The personas available to a connection are limited to the personas assigned to your user account. You can update connection ownership or associated persona for one or more connections at a time.

Update owner or persona for one or more connections

1. Change your active persona to a persona you want to associate with a connection. If you use the default persona, no persona is associated with a connection. For more information about how to select a persona, see Tanium Console User Guide: Select a persona for your Console session.
2. Choose one of the following options:
   - From the Main menu, go to **Modules** > **Connect** > **Overview** and then go to the **Connections** section.
   - From the Connect menu, click **Connections**.
3. Choose one of the following options:
   - To update the owner and persona to your active user and persona, select the checkbox next to one or more connections, then click **Actions** > **Edit Ownership**. Click **Save**.

     The connection ownership updates to the active session user and persona.

   - To update the persona on connections that your user owns, select the checkbox next to one or more connections, then click **Actions** > **Change persona**. Click **Change Persona**.

     The connection persona updates to the active session user persona.

©2026 Tanium Inc. All Rights Reserved

> **Note:** If you select multiple connections to update ownership, and your user account is already the owner of some connections, your user remains the owner of those connections. Similarly, if the active persona is already associated with some of the selected connections, the persona remains associated with those connections.

Manage connection limits

Connect contains options to limit the CPU and memory resources that are available for connections. Connect settings are available in the **Configuration** tab of the **Settings** page.

- Use the **Memory Ceiling** option to set a maximum sum of memory (GB) for all simultaneously running connections.
- Use the **Process Count Limit** option to limit the number of connections that can run simultaneously.

If you update these settings, make sure the settings account for how much average and maximum data is sent on the connection runs. For example, if **Process Count Limit** is set to 4 and **Memory Ceiling** is set to 8 GB, the maximum average data available per connection is 2 GB. If your connections send an average of 4 GB for each connection run, and the **Process Count Limit** is set to 4, then the default **Memory Ceiling** setting of 8 GB is not enough to simultaneously run four connections in your environment. In this case, you can increase the **Memory Ceiling** to 16 GB, decrease the **Process Count Limit** to 2, or reschedule connections to reduce the number of simultaneously running connections.

For more information about Connect settings, see Installing Tanium Connect on page 37.

> **Best Practice:** When scheduling connections, you should stagger connection start times to reduce the number of connections that run simultaneously. For information about how to see the schedule for all connections, see View schedule for all connections on page 64.

Export connections

About this task

©2026 Tanium Inc. All Rights Reserved

If you want to back up or move connections between environments, you can export a connection. Both Tanium environments where you intend to export from or import to must run the same Connect version.

Note: Do not manually update a connection export JSON file, because the updated JSON file might not import properly to another environment.

Note: Connections that use profiles do not export with the profile configuration. After you import the connection, re-configure a profile for the connection.

1. From the Main menu, go to **Modules** > **Connect** > **Overview** and then go to the **Connections** section.
2. Select the connections that you want to export, click **Actions** > **Export**, and confirm the export. The connections are saved to your download folder as a JSON file.

Import connections

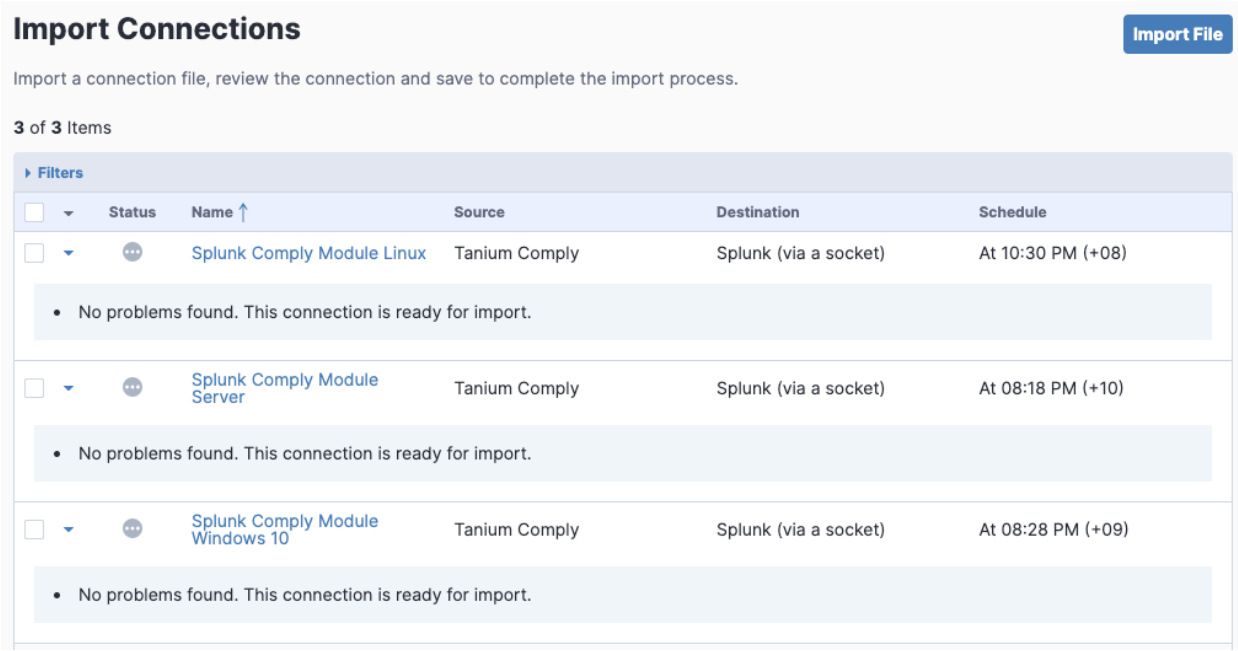
About this task

You can import connections from JSON files that have been exported from Connect. Both Tanium environments where you intend to export from or import to must run the same Connect version.

Note: Imported connections are initially disabled. To ensure proper connection functionality and performance, update the connection configuration, including the connection owner and active persona, before enabling the connection. For more information about how to update the connection owner and active persona, see Update connection owner and persona on page 69.

1. From the Main menu, go to **Modules** > **Connect** > **Overview** and then go to the **Connections** section.
2. Click **Import** and then click **Import File**. Select the JSON file from which you want to import connections.
3. Expand each row to review the messages for each connection that you are importing.

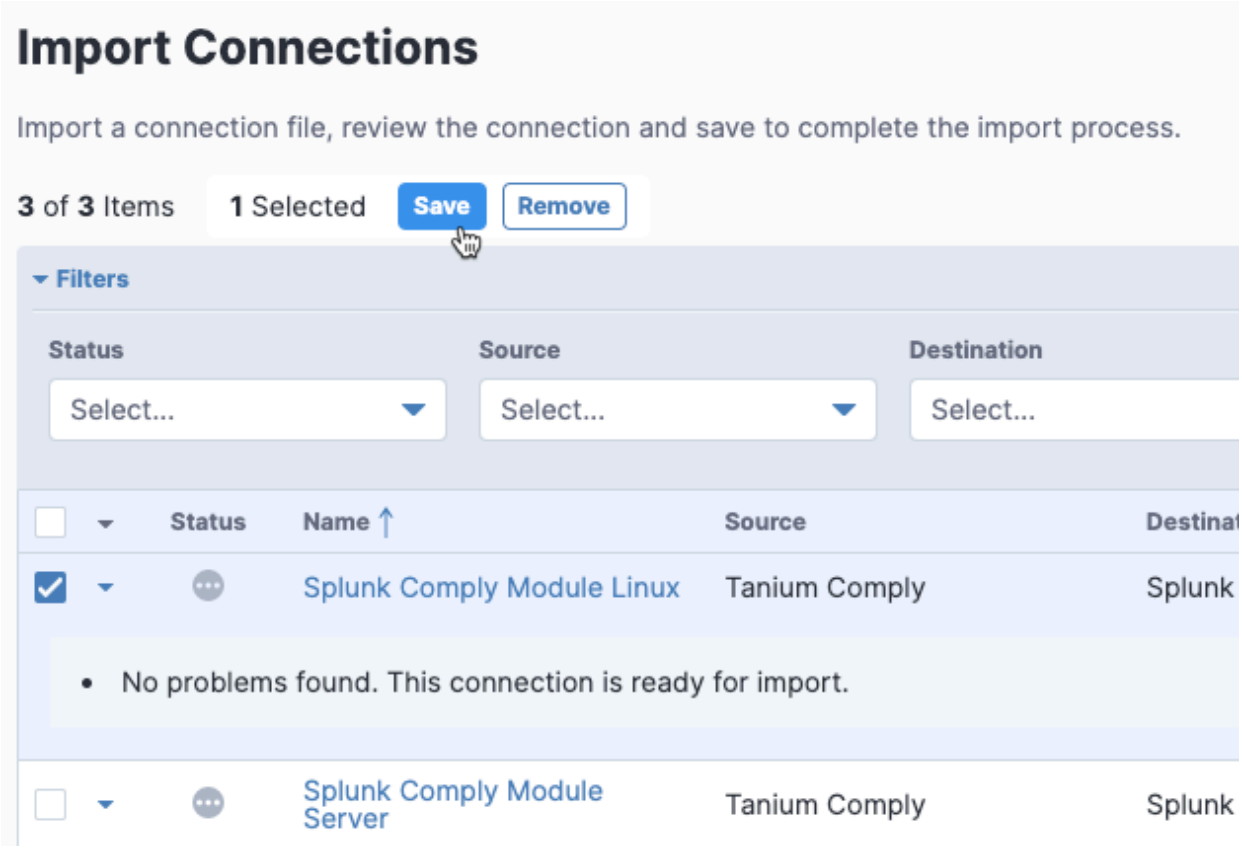
©2026 Tanium Inc. All Rights Reserved



Tip: You can filter the list of connections by the connection status, source, or destination.

4. When you are ready to import one or more connections, select the connections and click **Save**.

©2026 Tanium Inc. All Rights Reserved



5. If any of the connections have errors or warnings, resolve the issues before you import the connection.
    a. Click the name of the connection that you want to import that has import errors.
    b. Edit the settings in the connection to resolve the issues.
    c. Click **Import Connection**.
6. (Optional) If a connection is on the list that you do not want to import or review, select the connection and click **Remove**.

Use the same source for multiple destinations

For **Event**, **Saved Question**, and **Tanium Data Service** (TDS) sources, you can send data from one source to multiple destinations by creating multiple connections that run at the same time, or within the question expiration period.

For example, you might want the output of a single saved question to send data to Splunk and also send an email. You can create two connections that both use the same source, but are each configured to use different destinations. If you configure both connections to run at the same time, or within the question expiration period, the environment is queried only once and the data is sent to

©2026 Tanium Inc. All Rights Reserved

both destinations.

For more information about the question expiration period, see Tanium Console User Guide: Question expiration.

Use the same destination in multiple connections

You can reuse a destination in multiple connections. An existing destination is a specific instance of a destination that has specific details of the data target specified. These details vary for each destination type, but might include information such as the target IP address and port number, user name and password information, and destination paths.

After you create a destination, you can use the destination again in another connection.

Figure 5. Select an existing destination to reuse



To reuse a destination, choose an existing destination for the **Destination Name**.

For example, you might create a Splunk connection by setting the host name and port of the Splunk indexer and the format of the data to send. You can use this configured Splunk destination with multiple connections to send multiple data sources to your single Splunk configuration.

Note: Configure a unique destination per connection. If you edit the settings for a shared destination for one connection, any other connections that use the shared destination are affected, and connection runs might fail. Alternatively, you can copy the settings of an existing destination, then update the **Destination Name** to create a unique destination.

©2026 Tanium Inc. All Rights Reserved

Clear New Items cache

About this task

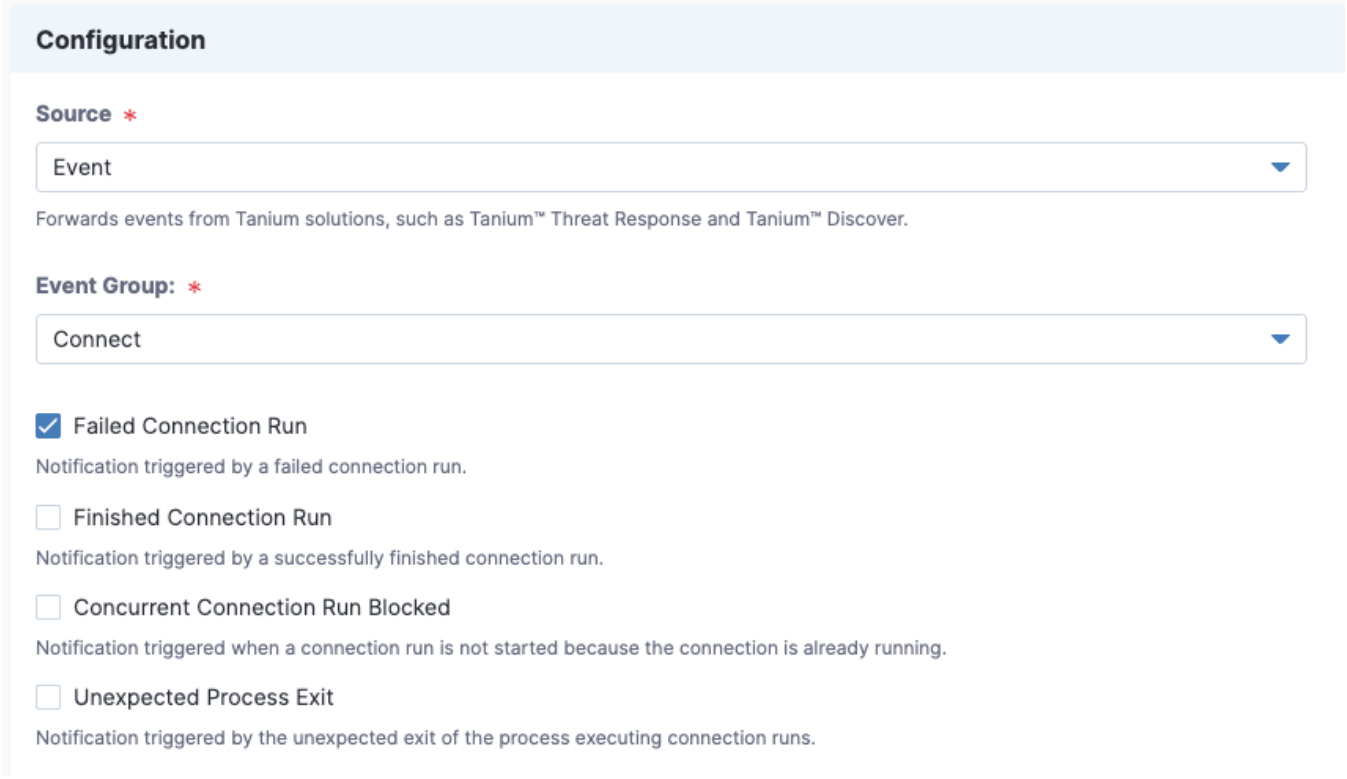
If you are using the New Items filter, you can clear the new items cache in an existing connection.

1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click the connection.
2. Click **Edit**.
3. Expand the **Configure Output** > **Filters** > **Learning Settings** section.
4. Click **Clear Learned Items Cache** and then click **Confirm** to remove all items in the baseline data. To remove all items in the baseline data and restart the learning period, click **Restart learning**.

Configure notifications for failed connection runs

If you use the **Connect** > **Failed Connection Run** event group, you can choose to send a notification for a failed connection run.

Figure 6. Select Failed Connection Run to trigger notifications on failures



©2026 Tanium Inc. All Rights Reserved

This type of connection runs only once. If this connection fails, it does not reattempt the notification, so it prevents the connection from repeatedly running in the event that something in the connection fails.

©2026 Tanium Inc. All Rights Reserved

Configuring AWS S3 destinations

About this task

With Amazon Web Services (AWS) S3, you can store and retrieve data in real time from almost any type of structured and unstructured data source. With Connect, Tanium can write data directly to AWS S3.

Note: This destination appears in Connect as **AWS S3 (Legacy)**. You can still create and edit connections with this legacy destination. For new connections, use the Cloud Storage destination with an AWS S3 profile instead. For more information, see Configuring cloud storage destinations on page 90.

Important: The AWS S3 destination is tested for compatibility with only the AWS cloud provider, and does not support cloud providers that offer S3 API-compatible storage solutions. Destination updates are tested against only AWS S3, not other S3 API-compatible storage solutions.

Note:

Configure a network egress allow list rule for each of the following FQDNs of your S3 bucket:

- my-bucket-name.s3.amazonaws.com
- my-bucket-name.s3.region.amazonaws.com

Assign the minimum required S3 bucket access permissions (**s3:GetObject**, **s3:PutObject**, and **s3:ListBucket**) before you configure an S3 bucket as a destination.

Specify general connection information

1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section

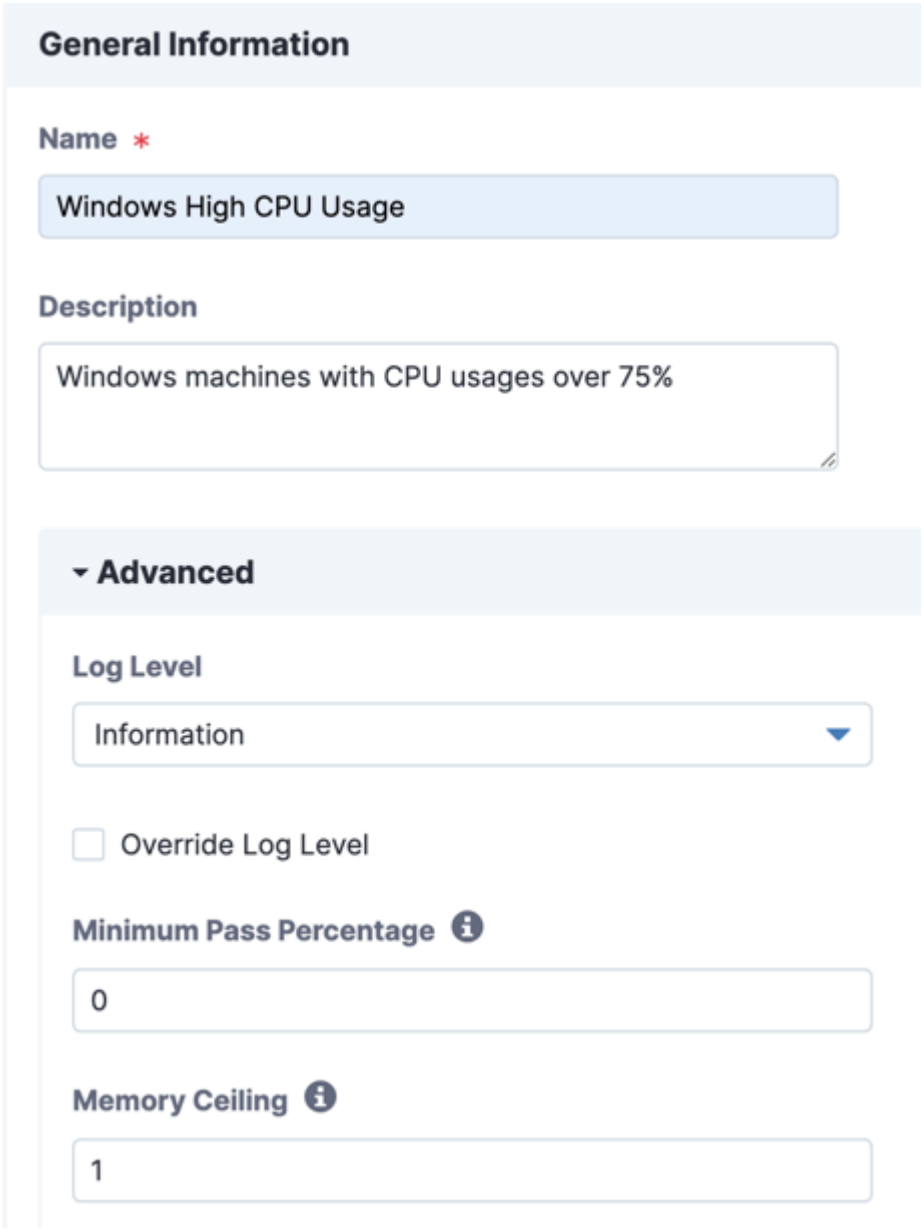
©2026 Tanium Inc. All Rights Reserved

and click **Create Connection**.

2. Enter a name and description for the connection.
3. (Optional) In the **General Information** section, expand **Advanced** to configure the following settings:

   Log Level

   By default, **Log Level** is set to **Information**. To reduce the amount of logging, you can set **Log Level** to **Warning**, **Error**, or **Fatal**.



   Override Log Level

   If you are debugging the connection, select **Override Log Level** to set a **Temporary Log**

©2026 Tanium Inc. All Rights Reserved

Level (such as **Trace** or **Debug**) on this connection for a selected **Number of Runs** (up to **24**). A scheduled or manual connection run, once started, counts towards the number of runs, regardless of the connection status. After the number of runs elapses, the logging for this connection returns to the **Log Level** you selected to prevent finer-grained logging from consuming additional resources for an indefinite number of runs.

Minimum Pass Percentage
: Minimum percentage of the expected rows that must be processed for the connection to succeed.

Memory Ceiling (GB)
: Maximum memory for the node process to run the connection. This defaults to 1 GB per connection, and cannot exceed the global maximum sum of memory for all running connections (by default, 8 GB). Increase this setting if a connection frequently exhibits out of memory errors while running.

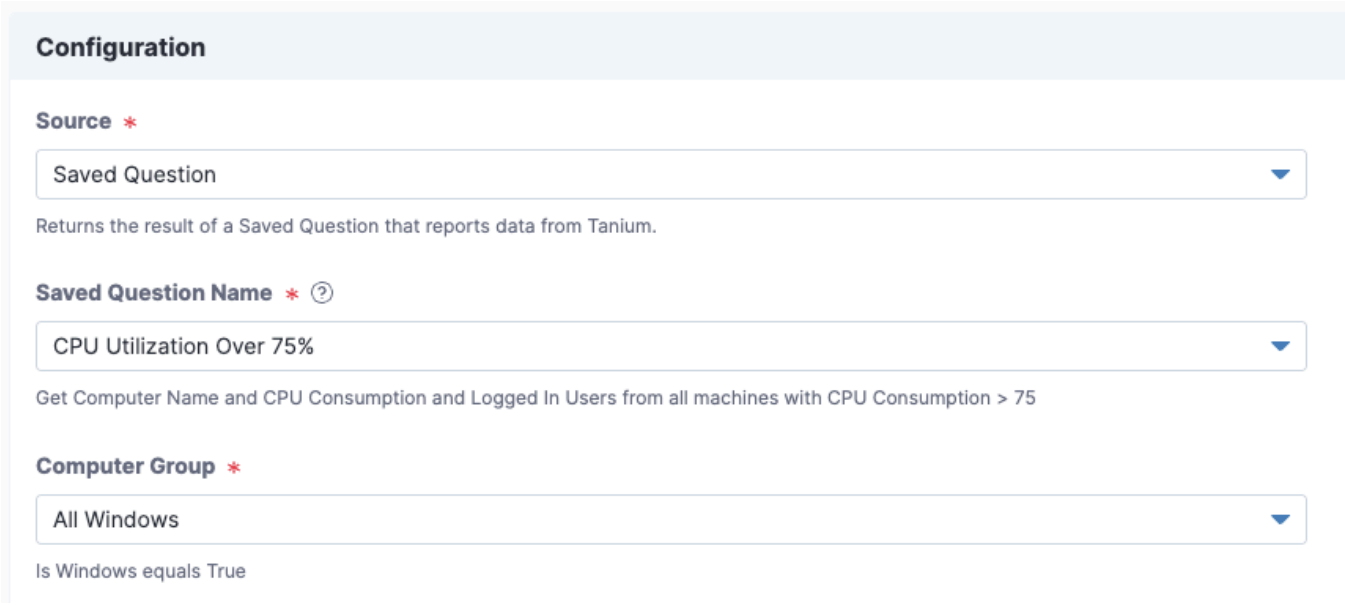
> **Note:** If the sum of simultaneously scheduled connection **Memory Ceiling** values exceed the global **Memory Ceiling**, connections run until the global **Memory Ceiling** is reached, then any remaining connections enter a waiting queue if you select the **Queue Connections** configuration setting, or fail if you clear the **Queue Connections** configuration setting.

Configure the connection source

The connection source determines what data you are sending to the destination. This data is usually information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

Figure 7. Connection source settings

©2026 Tanium Inc. All Rights Reserved



Note:

If a Tanium solution or source shows Critical, the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

Note: After you create a connection, you cannot update the connection source type, only the source configuration. If you want to change the source type, create a new connection.

For more information about available connection sources, see Connection sources on page 14.

Configure AWS S3 destination

About this task

Note: After you create a connection, you cannot update the connection destination type, only the destination configuration. If you want to change the destination, create a new connection.

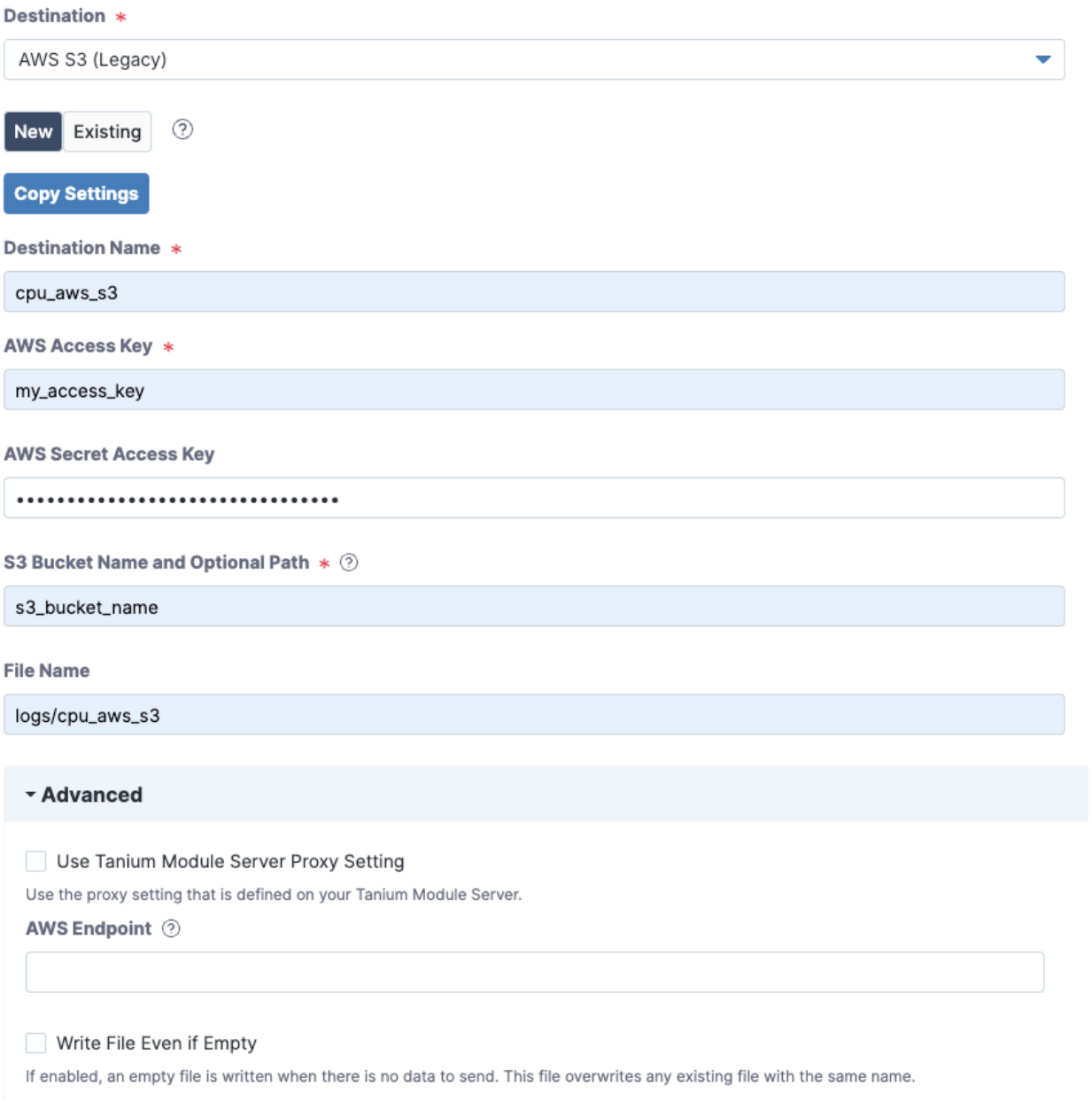
©2026 Tanium Inc. All Rights Reserved

1. Select **AWS S3 (Legacy)** for the destination and provide a destination name. Do one of the following:
    - Create a new destination: Specify a unique name to save the configuration information as a new destination. Select **New** and then enter a **Destination Name**
    - Copy an existing destination: Select **New**, and then click **Copy Settings**. Select a destination, click **Apply**, and update the **Destination Name**.
    - Reuse an existing destination: Select **Existing**, and then select a **Destination Name**.

    > **Note:** Configure a unique destination per connection. If you edit the settings for a shared destination for one connection, any other connections that use the shared destination are affected, and connection runs might fail.

2. Specify authentication credentials, including AWS access key, secret access key, bucket name, AWS region, and file name. You can use a variable for both the bucket name and the file name, as listed in Reference: Variables on page 295.

©2026 Tanium Inc. All Rights Reserved



3. (Optional) Configure advanced settings. In the **Configuration** section, under the destination settings, expand **Advanced**.
    a. If you have a proxy configured for your Tanium Module Server, select **Use Tanium Module Server Proxy Setting**.
    b. To use an endpoint other than the default endpoint that is associated with your AWS credentials, provide the host.

    > **Note:** If you specify an AWS Virtual Private Cloud (VPC) endpoint, enable private DNS and private DNS names for the endpoint. You cannot upload files larger than 20 MB if the VPC does not have private DNS and private DNS names enabled.

©2026 Tanium Inc. All Rights Reserved

c. To control the chunk size of multipart uploads, enter a **Part Size (MB)**. By default, the field is empty but defaults to 5 MB. The accepted range is 5–100 MB.

> **Note:** The maximum exportable object size is the part size multiplied by 10,000. For example, a 100 MB part size supports objects up to approximately 976 GB. If an export exceeds this limit, the run log contains an error similar to **Export exceeded the <integer> GB limit (part size x 10,000 parts). Increase the AWS S3 destination's part size setting or split the export**.

Configure filters

(Optional) In the **Configure Output** > **Filters** section, you can specify filters to modify the data that you are getting from your connection source before it is sent to the destination.

For more information about the types of filters you can configure, see Reference: Filtering options on page 257.

Format data for AWS S3

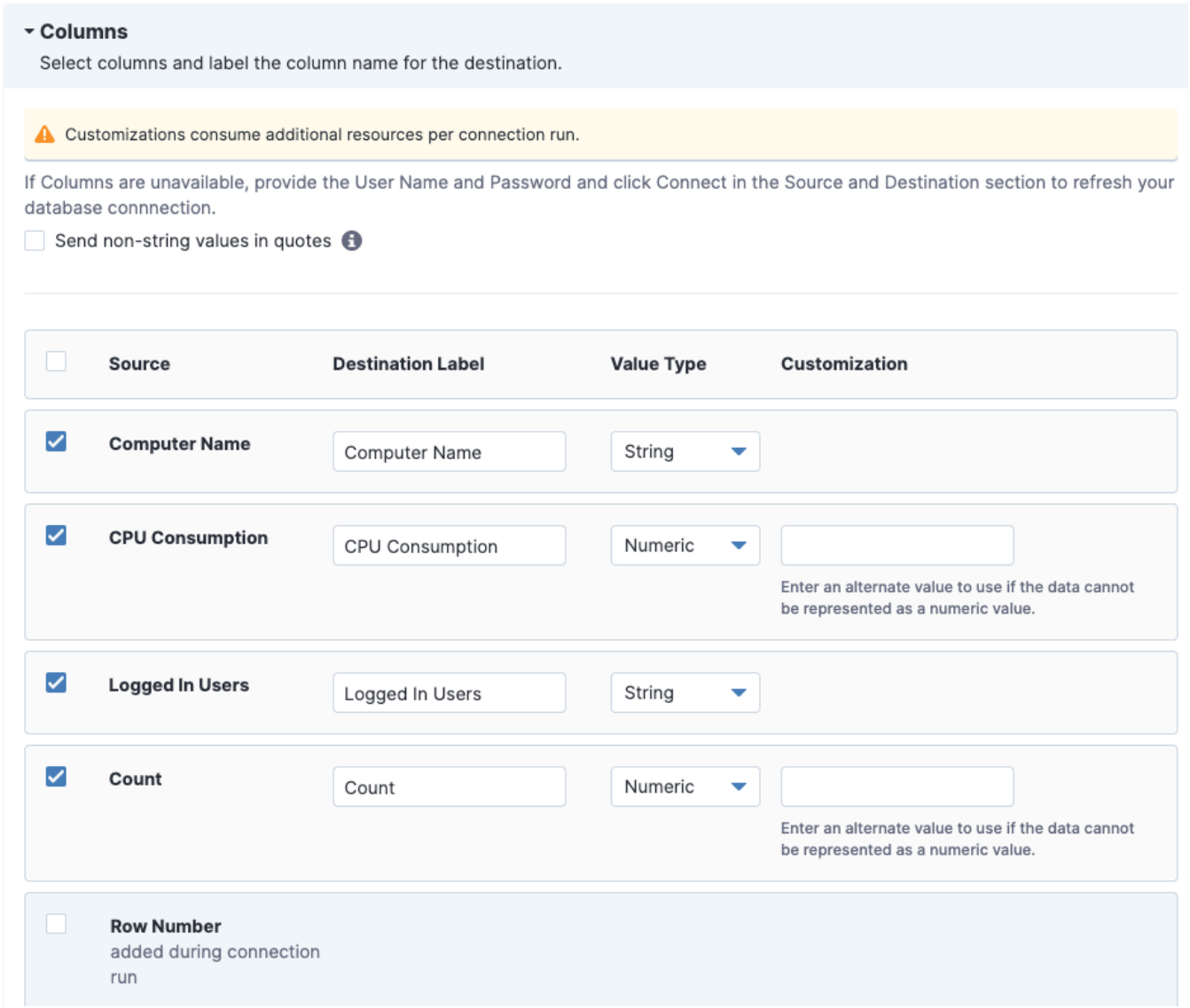
In the **Configure Output** > **Format** section, you can choose to save your data in all available formats, as listed in Reference: Format types on page 262. Each format has slightly different configuration options, but all allow you to choose which column data to save.

> **Note:** If the data format supports row delimiter characters, update the characters to ensure that individual rows are sent in a format that the destination can parse. You can define one or more of `\n` (new line), `\r` (carriage return), and `\t` (tab).

In the **Configure Output** > **Columns** section, you can change the **Destination Label** of each column and **Value Type** to force the column to be a String, Numeric, or Date/Time value.

Figure 8. Columns section with Destination Label and Value Type fields

©2026 Tanium Inc. All Rights Reserved



If you choose **Numeric** for the value, you can specify a default value that is used if the data cannot be coerced into a numeric value. You can specify any negative or positive number.

If you choose **Date/Time** for the value, specify the format that you want to use for the column. For more information about how to use a variable, see Time stamp variables on page 297.

For more information about column customizations, see Reference: Column customizations on page 248.

Schedule the connection

Connections can run at a highly configurable time interval, such as multiple times per hour, day, week, or month.

©2026 Tanium Inc. All Rights Reserved

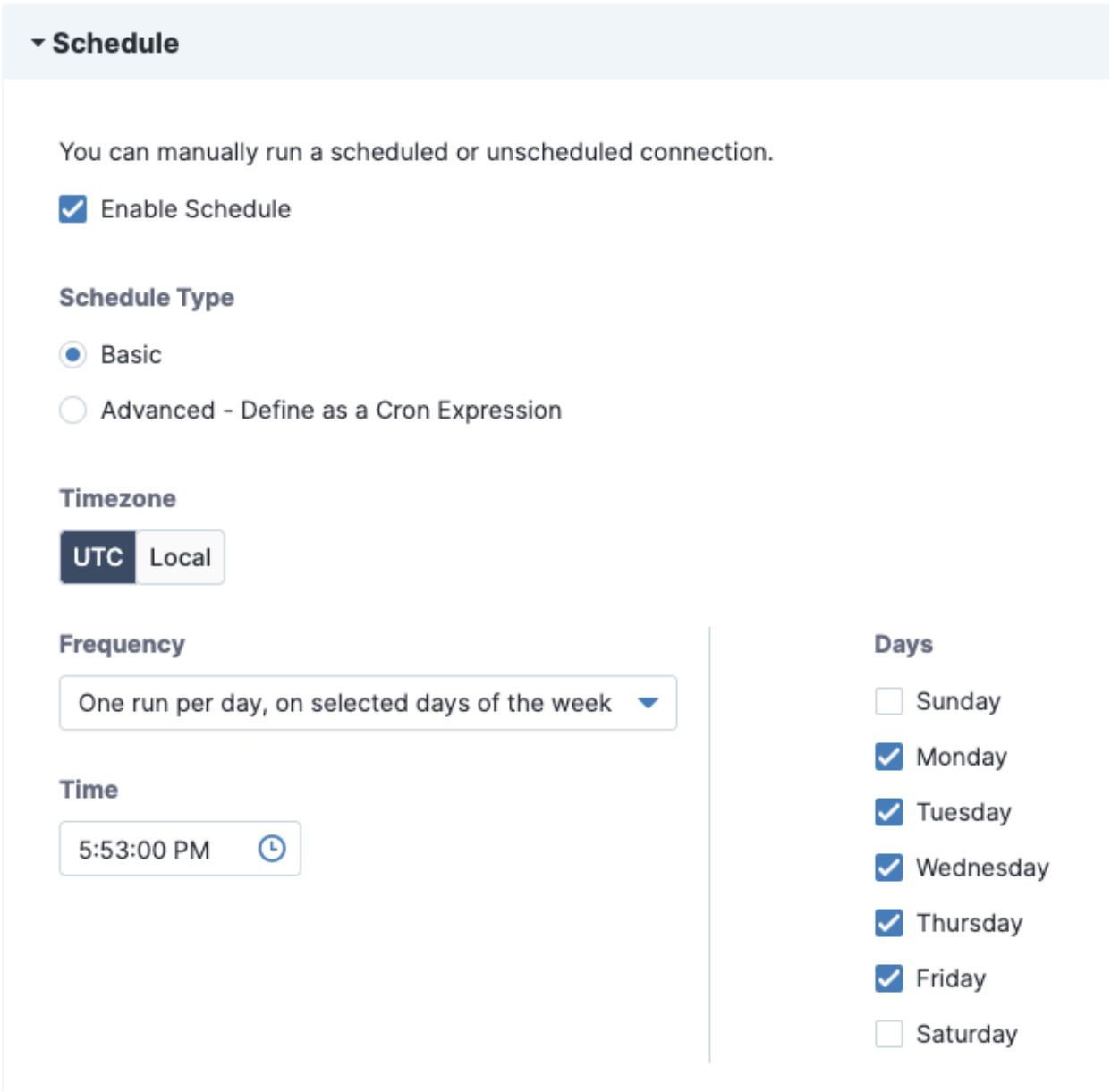
Important: Connections scheduled to run during an upgrade of Connect, or any Tanium solution configured as a connection source, might be interrupted or fail. Schedule your connections to run at a different time than your Tanium upgrades.

Note: If you do not enable the schedule, the connection only runs when you manually run it, unless you configure an **Event** source. Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Schedule** section to update the schedule:

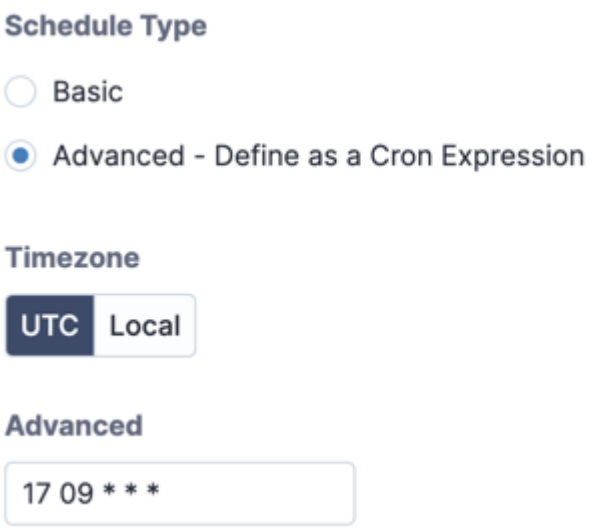
- Select **Enable schedule**.
- In the **Schedule Type**, select **Basic** to build a schedule with the provided controls.

©2026 Tanium Inc. All Rights Reserved



- To view or edit the cron expression directly, select **Advanced - Define as a Cron Expression**, and use the **Advanced** field to edit the cron expression.

©2026 Tanium Inc. All Rights Reserved



Note: If a user that owns a scheduled connection is deleted, future scheduled instances of that connection do not run. For more information, see Issue: Scheduled connection owned by a deleted user no longer runs on page 243.

For more information about cron syntax, see Reference: Cron syntax for Connect on page 253.

Enable listening for an event

Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Enablement** section to send data when a configured event is detected:

- Select **Listen for this Event**.

Save and verify connection

1. After you enter the details for the connection, click **Save**.

   Tip: To save the connection and immediately run the connection, click **Run and Save**.

   If needed, resolve any errors or missing information. After the connection creates successfully, the connection details appear.

©2026 Tanium Inc. All Rights Reserved

2. To view details when the connection runs, click the **Logs** tab.
3. To view an individual run log, expand the row table. For more information about how to resolve errors, see Troubleshooting on page 234.

©2026 Tanium Inc. All Rights Reserved

Configuring cloud storage destinations

You can send data from Connect to cloud storage providers, such as Microsoft Azure, Google Cloud Storage, or Oracle Cloud Infrastructure (OCI), and save the data as a file.

Note:

Configure a network allow list rule to the cloud storage provider over port 443 for HTTPS traffic:

- Microsoft Azure storage account standard endpoint FQDN in the format <storage-account-name>.blob.core.windows.net/<container-name>
- Google Cloud Storage bucket FQDN in the format <bucket-name>.storage.googleapis.com/<profile-directory-value>/<destination-directory-value>
- OCI bucket endpoint FQDN in the format <namespace>.compat.objectstorage.<region>.oraclecloud.com

HTTPS connections from this destination to a cloud provider use TLS 1.2. For more information about how to view details for a connection, see View connection status on page 62.

©2026 Tanium Inc. All Rights Reserved

Best Practice:

Connect might send data in multipart uploads to cloud storage destinations. When this occurs, there is the possibility that a connection might end prematurely, creating orphan upload files on the cloud storage provider. Connect cloud storage connections only upload data and do not delete any data on behalf of the user. By default, Microsoft Azure keeps orphaned multipart upload files for seven days, while AWS and OCI and Google Cloud Platform keep orphaned multipart upload files indefinitely. Review the retention policy for your cloud storage provider to set up a lifecycle policy.

- Microsoft Azure: Microsoft Azure documentation: Invalid blob or block content, or invalid block list
- AWS: AWS documentation: Uploading and copying objects using multipart upload in Amazon S3. To set up a lifecycle policy, see AWS documentation: Discovering and Deleting Incomplete Multipart Uploads to Lower Amazon S3 Costs.
- Google Cloud Platform: Google Cloud Storage documentation: Object Lifecycle Management
- OCI: Oracle Cloud Infrastructure documentation: Object Storage Multipart Uploads and Oracle Cloud Infrastructure documentation: Object Storage Object Lifecycle Management

Prerequisites

If you want to configure a connection destination to send a file to a cloud storage provider, you must first configure a cloud storage profile. For more information, see the following:

- Configure Microsoft Azure cloud storage profile settings on page 51
- Configure Google Cloud Storage cloud storage profile settings on page 53
- Configure Oracle Cloud Infrastructure cloud storage profile settings on page 56
- Configure AWS S3 cloud storage profile settings on page 59

Prerequisites for Microsoft Azure cloud storage destinations

©2026 Tanium Inc. All Rights Reserved

If you want to send a file to Microsoft Azure cloud storage, note the following settings:

- You must configure a Microsoft Azure blob storage account with the following settings:
    - **Performance**: select **Standard** for a general-purpose v2 account type, or **Premium** for block blobs or page blobs account type.

      Note: General-purpose v1 accounts are not supported.

    - **Enable storage account key access**: select this to enable Shared Key authorization. The External Storage (Blob) destination does not support shared access signature (SAS) authorization or Entra ID authorization.
    - **Endpoint type**: select **Standard** endpoint (in the format https://<storage-account-name>.blob.core.windows.net). The External Storage (Blob) destination does not support Microsoft Azure DNS zone endpoints (in the format https://<storage-account-name>.z[00-50].blob.storage.azure.net).

  Note: Compressed and uncompressed blob files created with this destination are limited to a maximum of 200 GB.

  For more information about Microsoft Azure storage accounts, see Microsoft Azure Blob storage documentation: Storage account overview.

- You must configure at least one storage account container to store blobs.

Note: Configuration requires the Azure storage account name, storage account container name, and storage account access key. For more information, see Microsoft Azure Blob Storage documentation: Get storage account configuration information.

Prerequisites for Google Cloud Storage cloud storage destinations

If you want to send a file to Google Cloud Storage, note the following settings:

- You must configure a Google Cloud Storage bucket with the following settings:

©2026 Tanium Inc. All Rights Reserved

- Enter a globally unique name in the namespace that complies with bucket name restrictions. For more information, see Google Cloud Storage documentation: Bucket names.
- Select a `STANDARD` data storage class.
- If you want to create a folder structure to store objects, select **Enable Hierarchical namespace on this bucket**. For more information, see Google Cloud Storage documentation: Hierarchical Namespace.

> **Note:** Compressed and uncompressed blob files created with this destination are limited to a maximum of 200 GB.

- You must configure a Google Cloud Storage service or user account with the following bucket permissions: **storage.objects.create**, **storage.objects.delete**, **storage.objects.get**, **storage.objects.list**.
- You must configure hash-based message authentication code (HMAC) keys for Google Cloud Storage authentication to enable blob upload to the bucket. The HMAC key access ID and secret must be associated with the Google Cloud Storage service or user account assigned the bucket permissions. For more information, see Google Cloud Storage documentation: HMAC keys.

> **Note:** Configuration requires the Google Cloud Storage bucket name, service or user account name, and HMAC key access ID and secret.

Prerequisites for OCI cloud storage destinations

If you want to send a file to OCI cloud storage, note the following settings:

- You must configure an OCI bucket with the following settings:
  - Enter a globally unique name in the compartment that complies with bucket name restrictions. For more information, see Oracle Cloud Infrastructure documentation: Object Storage Buckets.
  - Select a `STANDARD` default storage tier.

©2026 Tanium Inc. All Rights Reserved

> **Note:** Compressed and uncompressed blob files created with this destination are limited to a maximum of 200 GB.

- You must configure customer secret keys for OCI authentication to enable blob uploads to the bucket. The access key and secret key must be associated with the OCI service or user account that is assigned the bucket permissions. For more information, see Oracle Cloud Infrastructure documentation: Creating a Customer Secret Key.

Prerequisites for AWS cloud storage destinations

If you want to send a file to AWS cloud storage, note the following settings:

- You must configure an AWS S3 bucket. Assign the minimum required access permissions (**s3:GetObject**, **s3:PutObject**, and **s3:ListBucket**) before you configure the AWS S3 bucket as a destination.

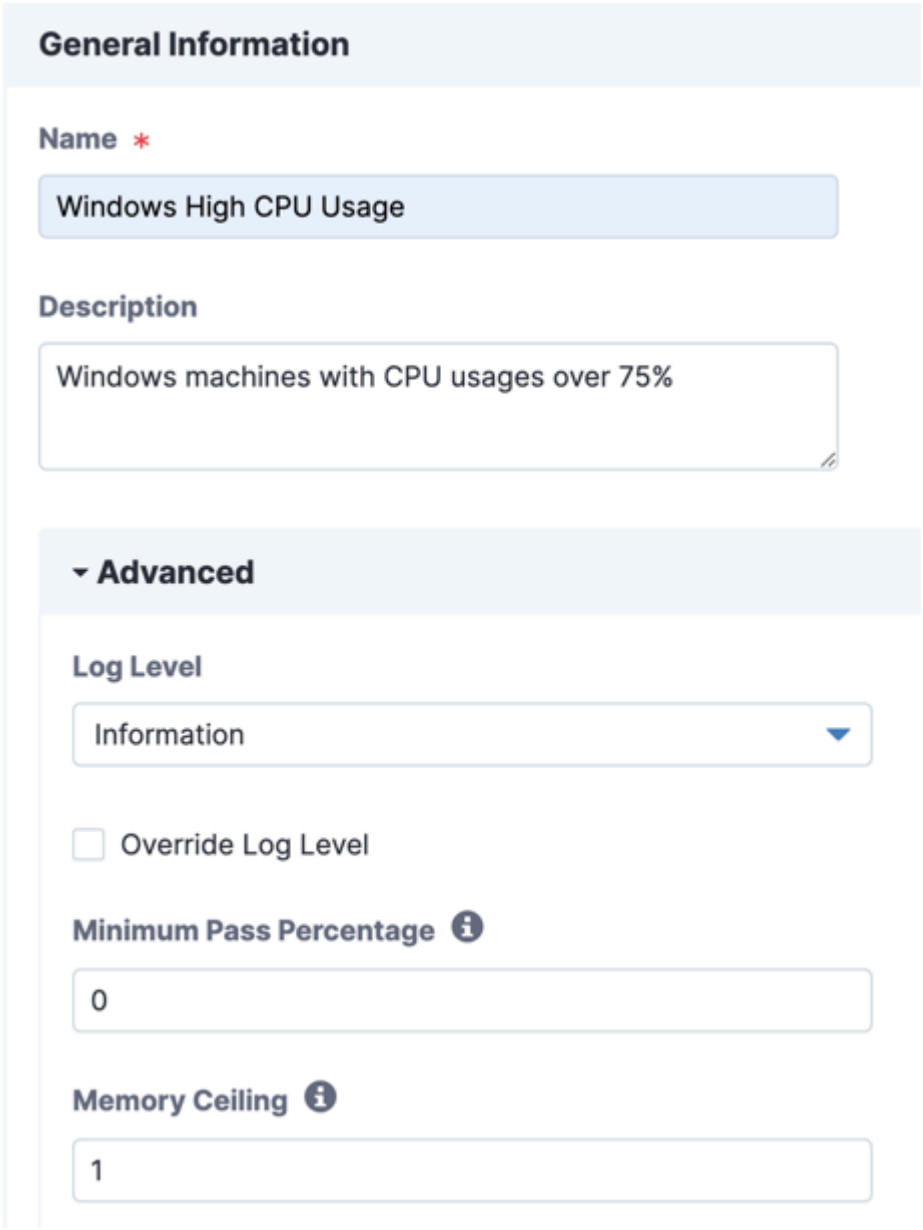
Specify general connection information

1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click **Create Connection**.
2. Enter a name and description for the connection.
3. (Optional) In the **General Information** section, expand **Advanced** to configure the following settings:

   Log Level

   By default, **Log Level** is set to **Information**. To reduce the amount of logging, you can set **Log Level** to **Warning**, **Error**, or **Fatal**.

©2026 Tanium Inc. All Rights Reserved



Override Log Level

If you are debugging the connection, select **Override Log Level** to set a **Temporary Log Level** (such as **Trace** or **Debug**) on this connection for a selected **Number of Runs** (up to **24**). A scheduled or manual connection run, once started, counts towards the number of runs, regardless of the connection status. After the number of runs elapses, the logging for this connection returns to the **Log Level** you selected to prevent finer-grained logging from consuming additional resources for an indefinite number of runs.

Minimum Pass Percentage

Minimum percentage of the expected rows that must be processed for the connection to succeed.

©2026 Tanium Inc. All Rights Reserved

Memory Ceiling (GB)

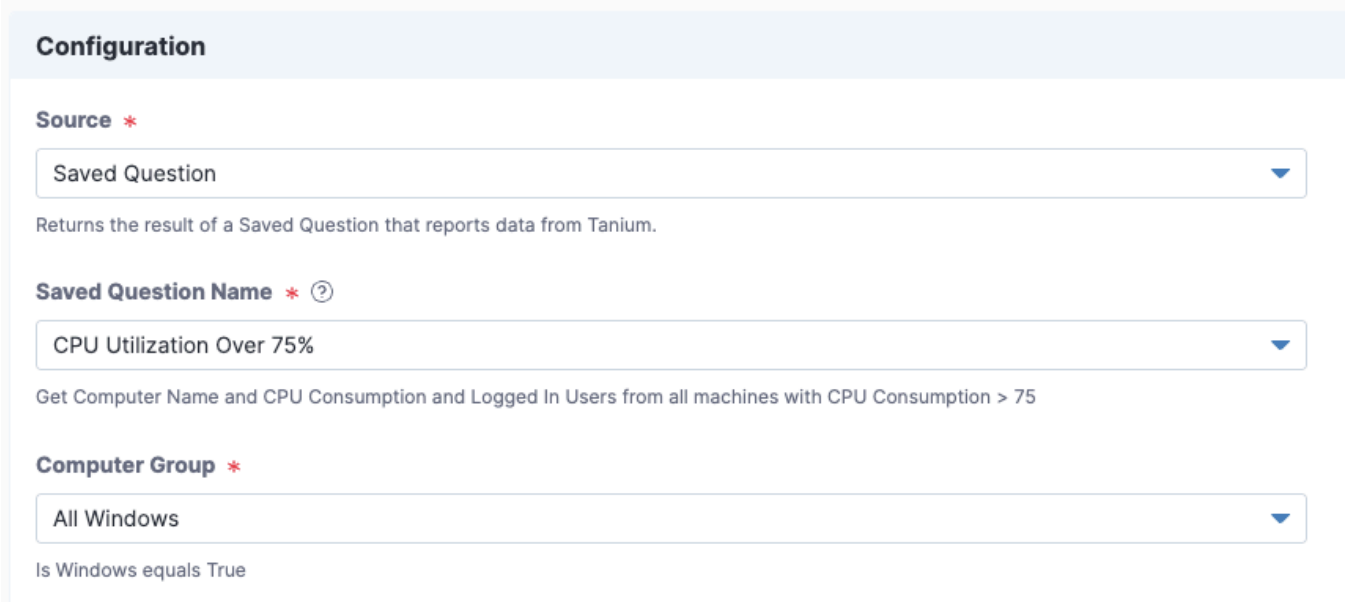
Maximum memory for the node process to run the connection. This defaults to 1 GB per connection, and cannot exceed the global maximum sum of memory for all running connections (by default, 8 GB). Increase this setting if a connection frequently exhibits out of memory errors while running.

> **Note:** If the sum of simultaneously scheduled connection **Memory Ceiling** values exceed the global **Memory Ceiling**, connections run until the global **Memory Ceiling** is reached, then any remaining connections enter a waiting queue if you select the **Queue Connections** configuration setting, or fail if you clear the **Queue Connections** configuration setting.

Configure the connection source

The connection source determines what data you are sending to the destination. This data is usually information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

Figure 9. Connection source settings



©2026 Tanium Inc. All Rights Reserved

Note:

If a Tanium solution or source shows Critical, the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

Note: After you create a connection, you cannot update the connection source type, only the source configuration. If you want to change the source type, create a new connection.

For more information about available connection sources, see Connection sources on page 14.

Configure the Cloud Storage destination

About this task

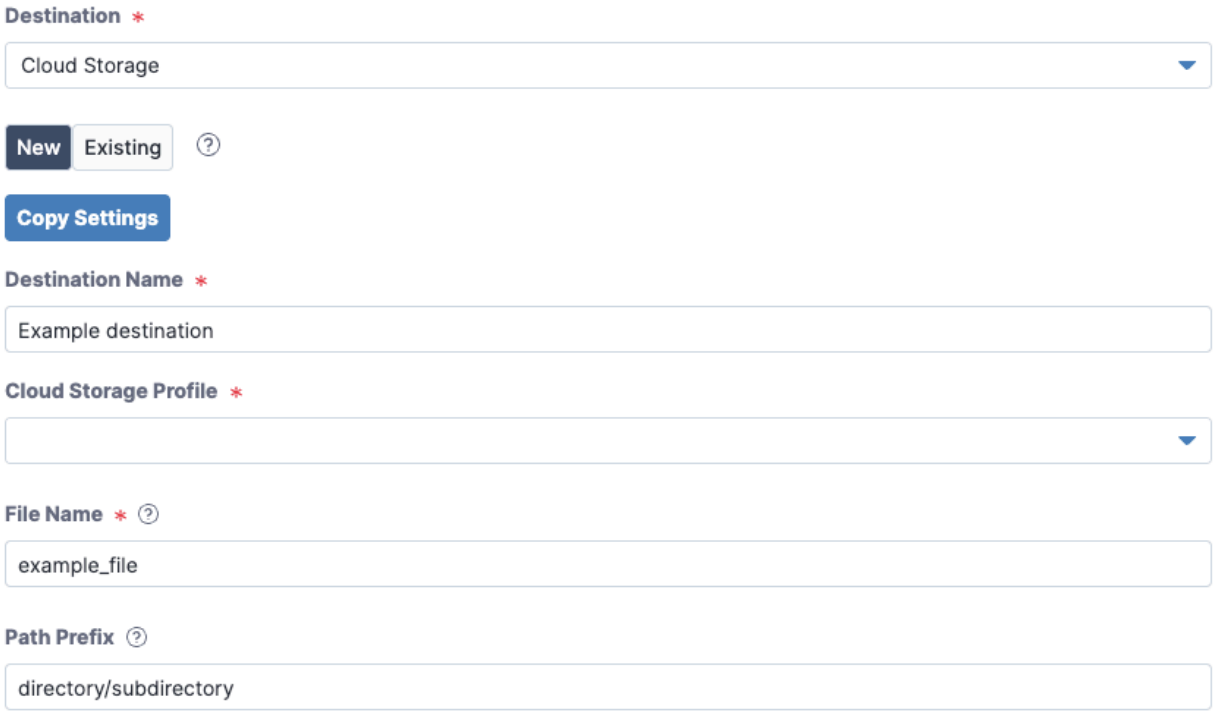
Note: After you create a connection, you cannot update the connection destination type, only the destination configuration. If you want to change the destination, create a new connection.

Specify a cloud storage profile, file name and optional timestamp format, file path prefix, and file compression type.

1. Select **Cloud Storage** for the destination and then provide a name for the destination. You have the following options:
    - Create a new destination: Specify a unique name to save the configuration information as a new destination. Select **New** and then enter a **Destination Name**
    - Copy an existing destination: Select **New**, and then click **Copy Settings**. Select a destination, click **Apply**, and update the **Destination Name**.
    - Reuse an existing destination: Select **Existing**, and then select a **Destination Name**.

©2026 Tanium Inc. All Rights Reserved

Note: Configure a unique destination per connection. If you edit the settings for a shared destination for one connection, any other connections that use the shared destination are affected, and connection runs might fail.



2. Select a **Cloud Storage Profile**. For more information about how to configure a cloud storage profile, see the following:
   - Configure Microsoft Azure cloud storage profile settings on page 51
   - Configure Google Cloud Storage cloud storage profile settings on page 53
   - Configure Oracle Cloud Infrastructure cloud storage profile settings on page 56
   - Configure AWS S3 cloud storage profile settings on page 59
3. Enter the **File Name**.

Note: If your cloud storage profile is configured for Microsoft Azure, file names must conform to Microsoft Azure blob name rules. Do not define a file name that exceeds 1024 characters. If you define connection variables in the file name or select a **File Name Timestamp Format**, the file name might exceed the 1024 character limit after character substitution, even if the configured file name does not exceed this limit when you save the connection. For more information, see Microsoft Azure documentation: Blob Names.

©2026 Tanium Inc. All Rights Reserved

Note:

If your cloud storage profile is configured for Google Cloud Storage, file names must conform to Google Cloud Storage object name rules.

- If your bucket is in a flat namespace, do not define a file name that exceeds 1024 characters.
- If your bucket has Hierarchical namespace enabled, do not define a file name that exceeds 512 characters.

If you define connection variables in the file name or select a **File Name Timestamp Format**, the file name might exceed the character limit after character substitution, even if the configured file name does not exceed this limit when you save the connection. For more information, see Google Cloud Storage documentation: About Cloud Storage objects.

Note: If your cloud storage profile is configured for OCI, file names must conform to OCI object name rules. Do not define a file name that exceeds 1024 characters. If you define connection variables in the file name or select a **File Name Timestamp Format**, the file name might exceed the 1024 character limit after character substitution, even if the configured file name does not exceed this limit when you save the connection. For more information, see Oracle Cloud Infrastructure documentation: Object Names.

4. Enter a file **Path Prefix** to define the storage account container directory path to store the file, based on your storage account configuration. Use the format of /<directory-name-1>/<directory-name-2>/directory-names-n... to define path prefixes. If you configure a cloud storage profile with a **Path Prefix**, select this cloud storage profile for a Cloud Storage destination, and also configure a destination **Path Prefix**, the generated endpoint contains both Path Prefix values. The cloud storage profile **Path Prefix** value precedes the destination **Path Prefix** value, such as https://myaccount.blob.core.windows.net/container-name/profile-path-prefix/destination-path-prefix/file-name.

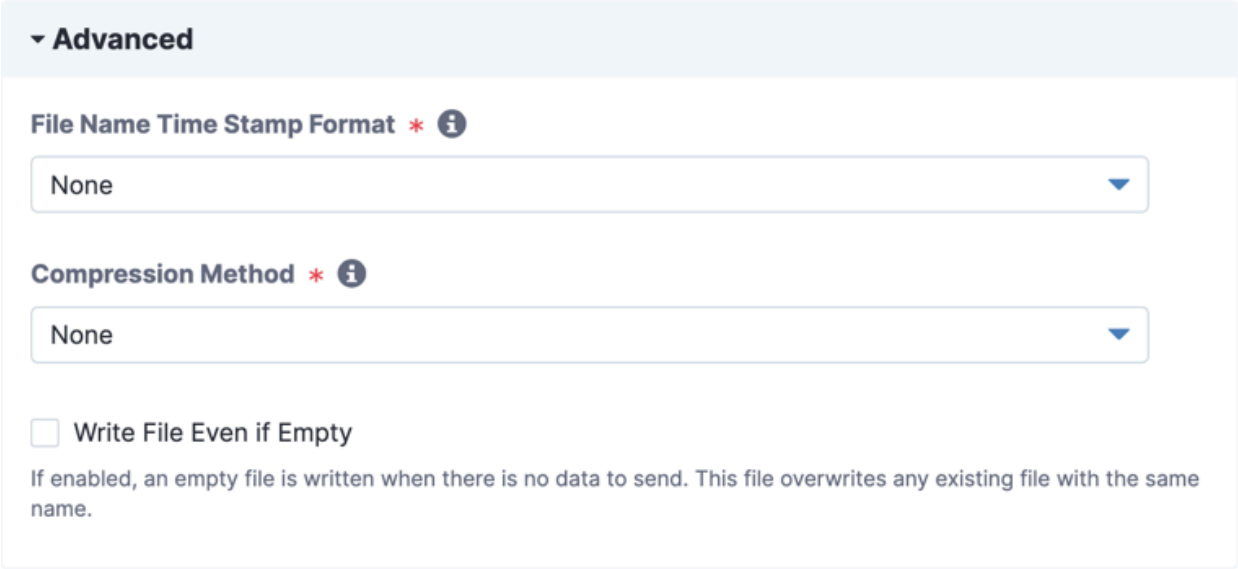
   Note: If your cloud storage profile is configured for Microsoft Azure, directory names and the directory path must conform to Microsoft Azure storage account directory rules and blob name virtual directory rules. For more information, see Microsoft Azure documentation: Directory Names and Microsoft Azure documentation: Blob Names.

©2026 Tanium Inc. All Rights Reserved

> **Note:** If your cloud storage profile is configured for Google Cloud Storage, and your bucket has Hierarchical namespace enabled, folder names and the folder path must conform to Google Cloud Storage hierarchical namespace rules. For more information, see Google Cloud Storage documentation: Hierarchical Namespace.

> **Note:** If your cloud storage profile is configured for OCI, OCI buckets and objects exist in a flat structure. To simulate a directory structure, you can add a prefix string that includes one or more forward slash characters (/) to an object name. For more information, see Oracle Cloud Infrastructure documentation: Object Naming Using Prefixes and Hierarchies.

5. If you need to configure a path prefix, file name timestamp format, file compression, or file behavior when no data is available to send, expand **Advanced**.



   - Select a **File Name Time Stamp Format** to append a time stamp to the file name.

     > **Note:** Use connection time stamp variables if you want to add a timestamp to a file name other than at the end.

   - Select a file **Compression Type** to generate a **GZip** or **Zip** file. Select **None** to generate an uncompressed file.

     > **Note:** Compressed and uncompressed files created with this destination are limited to a maximum of 200 GB.

   - Select **Write File Even if Empty** to generate a file even if no data is available when

©2026 Tanium Inc. All Rights Reserved

the connection runs. Clear **Write File Even if Empty** to generate a file only when data is available when the connection runs.

> **Note:** If you configure the connection to add a time stamp to the file name, this option does not overwrite existing files. The connection generates a new file with the time stamp in the file name each time that it runs.

Configure filters

(Optional) In the **Configure Output** > **Filters** section, you can specify filters to modify the data that you are getting from your connection source before it is sent to the destination.

For more information about the types of filters you can configure, see Reference: Filtering options on page 257.

Format data for Cloud Storage

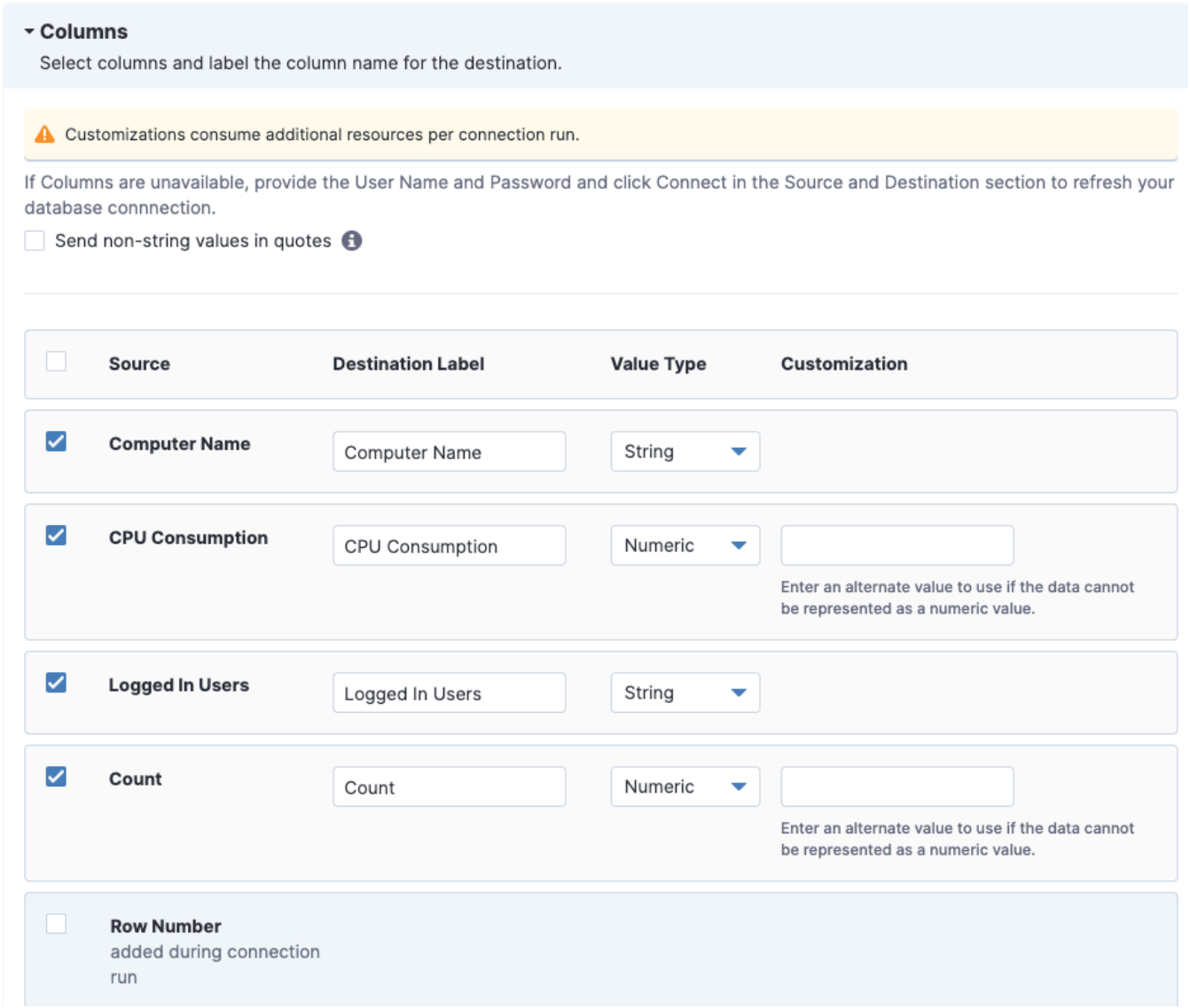
> **Important:** If you want to send a file in JSON file format, select **Generate Document** and clear **Wrap data with source** to properly structure the JSON file for Microsoft Azure. Connection runs fail if you do not properly structure the JSON file.

> **Note:** If the data format supports row delimiter characters, update the characters to ensure that individual rows are sent in a format that the destination can parse. You can define one or more of `\n` (new line), `\r` (carriage return), and `\t` (tab).

In the **Configure Output** > **Columns** section, you can change the **Destination Label** of each column and **Value Type** to force the column to be a String, Numeric, or Date/Time value.

Figure 10. Columns section with Destination Label and Value Type fields

©2026 Tanium Inc. All Rights Reserved



If you choose **Numeric** for the value, you can specify a default value that is used if the data cannot be coerced into a numeric value. You can specify any negative or positive number.

If you choose **Date/Time** for the value, specify the format that you want to use for the column. For more information about how to use a variable, see Time stamp variables on page 297.

For more information about column customizations, see Reference: Column customizations on page 248.

Note: After a connection run successfully completes, it may take several minutes or more for the cloud storage provider to populate the destination table with the data.

©2026 Tanium Inc. All Rights Reserved

Schedule the connection

Connections can run at a highly configurable time interval, such as multiple times per hour, day, week, or month.

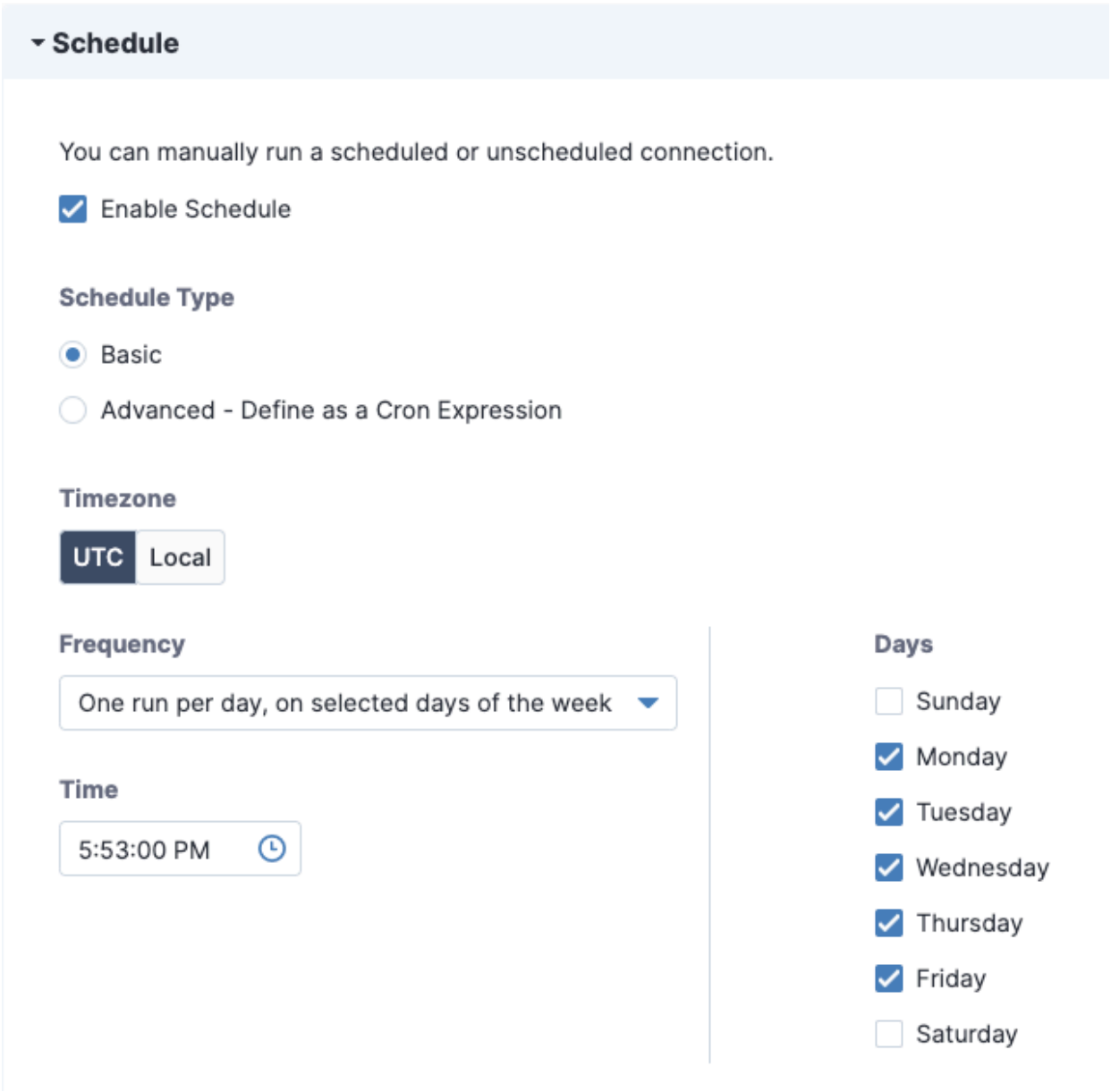
Important: Connections scheduled to run during an upgrade of Connect, or any Tanium solution configured as a connection source, might be interrupted or fail. Schedule your connections to run at a different time than your Tanium upgrades.

Note: If you do not enable the schedule, the connection only runs when you manually run it, unless you configure an **Event** source. Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Schedule** section to update the schedule:

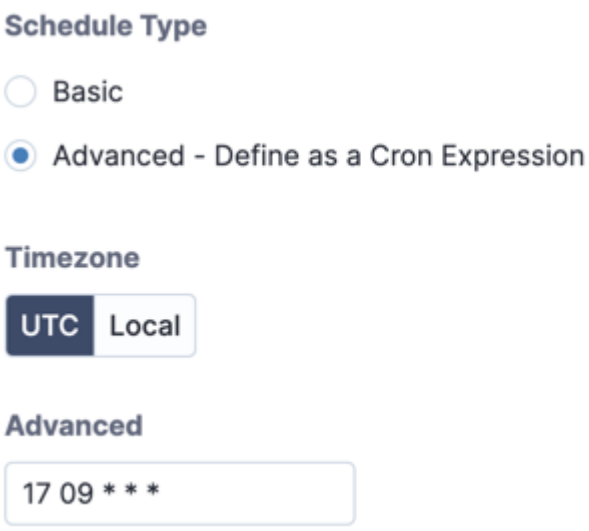
- Select **Enable schedule**.
- In the **Schedule Type**, select **Basic** to build a schedule with the provided controls.

©2026 Tanium Inc. All Rights Reserved



- To view or edit the cron expression directly, select **Advanced - Define as a Cron Expression**, and use the **Advanced** field to edit the cron expression.

©2026 Tanium Inc. All Rights Reserved



Note: If a user that owns a scheduled connection is deleted, future scheduled instances of that connection do not run. For more information, see Issue: Scheduled connection owned by a deleted user no longer runs on page 243.

For more information about cron syntax, see Reference: Cron syntax for Connect on page 253.

Enable listening for an event

Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Enablement** section to send data when a configured event is detected:

- Select **Listen for this Event**.

Save and verify connection

1. After you enter the details for the connection, click **Save**.

   Tip: To save the connection and immediately run the connection, click **Run and Save**.

   If needed, resolve any errors or missing information. After the connection creates successfully, the connection details appear.

©2026 Tanium Inc. All Rights Reserved

2. To view details when the connection runs, click the **Logs** tab.
3. To view an individual run log, expand the row table. For more information about how to resolve errors, see Troubleshooting on page 234.

©2026 Tanium Inc. All Rights Reserved

Configuring Elasticsearch destinations

With Elasticsearch, you can search, analyze, and get actionable insights in real time from almost any type of structured and unstructured data source. With Connect, Tanium can write data directly to Elasticsearch.

Note: The Elasticsearch destination supports Elasticsearch 8.7 or earlier. If you want to send data to a later Elasticsearch version, use the Socket Receiver destination. For more information about how to configure the Socket Receiver destination, see Configuring Socket (SIEM) destinations on page 202.

Note: If you want to use nested JSON for your Elasticsearch data, deselect the **Flatten Results** setting in the **Advanced** section for the source. If you leave the data flattened, a single JSON item with all of the rows is returned.

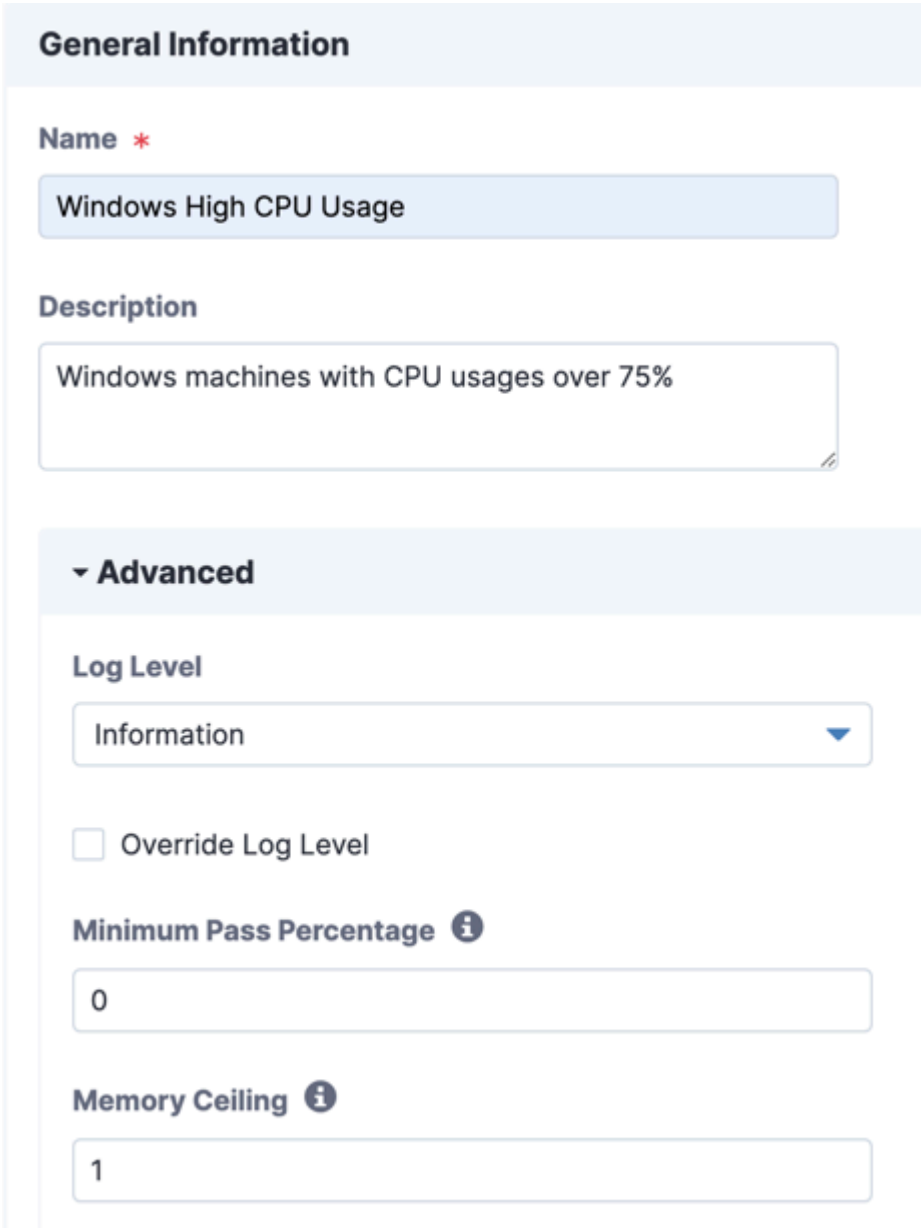
Specify general connection information

1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click **Create Connection**.
2. Enter a name and description for the connection.
3. (Optional) In the **General Information** section, expand **Advanced** to configure the following settings:

   Log Level

   By default, **Log Level** is set to **Information**. To reduce the amount of logging, you can set **Log Level** to **Warning**, **Error**, or **Fatal**.

©2026 Tanium Inc. All Rights Reserved



Override Log Level

If you are debugging the connection, select **Override Log Level** to set a **Temporary Log Level** (such as **Trace** or **Debug**) on this connection for a selected **Number of Runs** (up to **24**). A scheduled or manual connection run, once started, counts towards the number of runs, regardless of the connection status. After the number of runs elapses, the logging for this connection returns to the **Log Level** you selected to prevent finer-grained logging from consuming additional resources for an indefinite number of runs.

Minimum Pass Percentage

Minimum percentage of the expected rows that must be processed for the connection to succeed.

©2026 Tanium Inc. All Rights Reserved

Memory Ceiling (GB)

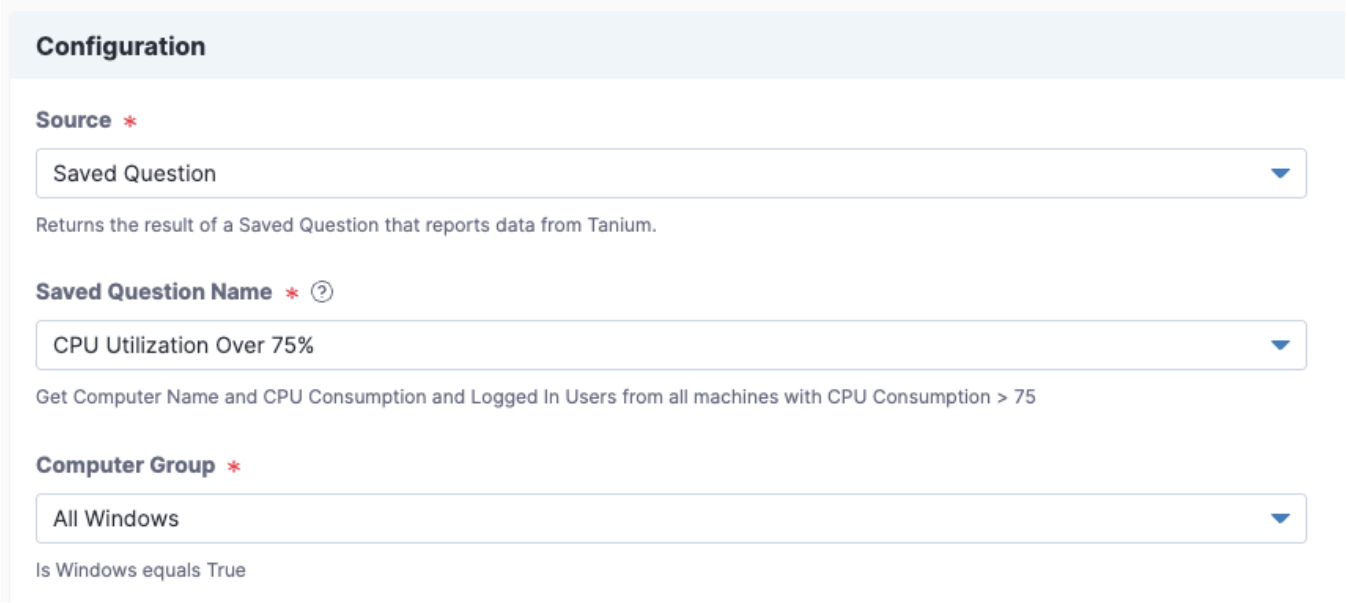
Maximum memory for the node process to run the connection. This defaults to 1 GB per connection, and cannot exceed the global maximum sum of memory for all running connections (by default, 8 GB). Increase this setting if a connection frequently exhibits out of memory errors while running.

> **Note:** If the sum of simultaneously scheduled connection **Memory Ceiling** values exceed the global **Memory Ceiling**, connections run until the global **Memory Ceiling** is reached, then any remaining connections enter a waiting queue if you select the **Queue Connections** configuration setting, or fail if you clear the **Queue Connections** configuration setting.

Configure the connection source

The connection source determines what data you are sending to the destination. This data is usually information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

Figure 11. Connection source settings



©2026 Tanium Inc. All Rights Reserved

Note:

If a Tanium solution or source shows Critical, the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

Note: After you create a connection, you cannot update the connection source type, only the source configuration. If you want to change the source type, create a new connection.

For more information about available connection sources, see Connection sources on page 14.

Configure Elasticsearch destination

About this task

Note: After you create a connection, you cannot update the connection destination type, only the destination configuration. If you want to change the destination, create a new connection.

1. In the **Configuration** section, provide a name for the destination.
   - Create a new destination: Specify a unique name to save the configuration information as a new destination. Select **New** and then enter a **Destination Name**
   - Copy an existing destination: Select **New**, and then click **Copy Settings**. Select a destination, click **Apply**, and update the **Destination Name**.
   - Reuse an existing destination: Select **Existing**, and then select a **Destination Name**.

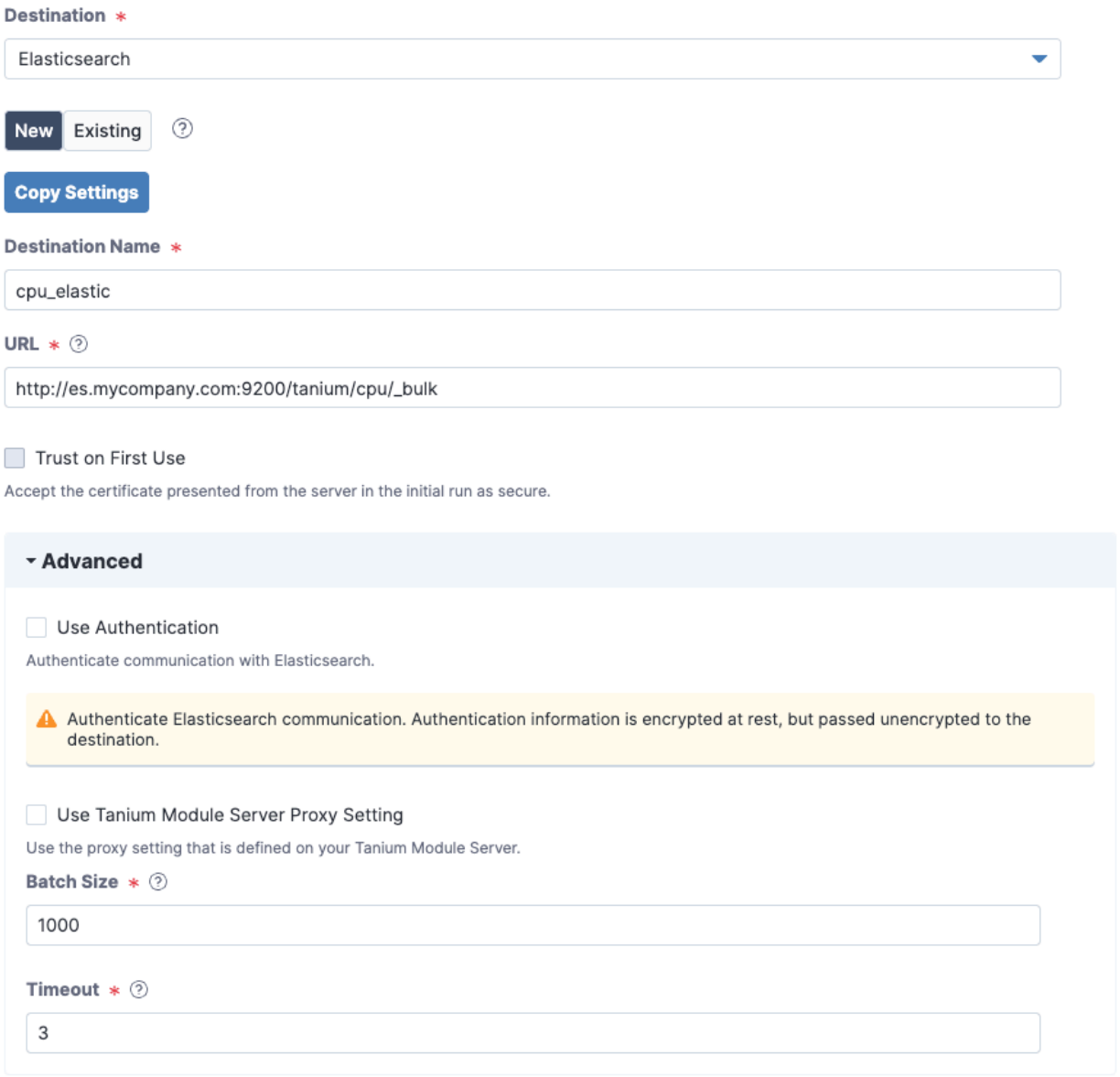
     Note: Configure a unique destination per connection. If you edit the settings for a shared destination for one connection, any other connections that use the shared destination are affected, and connection runs might fail.
2. Define a URL to access the Elasticsearch API.
   You can use a variable for the URL, as listed in Reference: Variables on page 295. The URL is in

©2026 Tanium Inc. All Rights Reserved

the following format:

`<protocol>://<elasticSearchHost>:<elasticSearchPort>/<index>/_bulk`

where:



protocol

Specifies the protocol for accessing the Elasticsearch server (`http` or `https`). If you specify `https` for the URL, the connection validates the Transport Layer Security (TLS) certificate. You can also select **Trust on First Use** to accept the certificate presented from the server and trust only that certificate for future connection runs.

elasticSearchHost

Specifies the fully qualified domain name (FQDN) or IP of the Elasticsearch server.

©2026 Tanium Inc. All Rights Reserved

elasticSearchPort
: Specifies the port on which the Elasticsearch server is listening. The default is: `9200`.

index
: Specifies the unique identifier for this API request. The common format for this identifier is: `{name}-{0:yyyy.MM.dd}`. This date format creates a unique index each day.

3. In the **Advanced** section for the destination, select **Use Authentication** if you want to use authentication with Elasticsearch, then enter a **User Name** and **Password**.

   > **Note:** If you specify `http` for the URL, authentication information is encrypted at rest, but passed unencrypted to the destination.

4. In the **Advanced** section, define the **Batch Size**, which determines the number of messages to batch before sending data to Elasticsearch, and the connection **Timeout** in seconds.

5. If you have a proxy configured for your Tanium Module Server, select **Use Tanium Module Server Proxy Setting**. When selected, the proxy makes the outbound connection to the specified Elasticsearch instance provided in the URL.

Configure filters

(Optional) In the **Configure Output** > **Filters** section, you can specify filters to modify the data that you are getting from your connection source before it is sent to the destination.

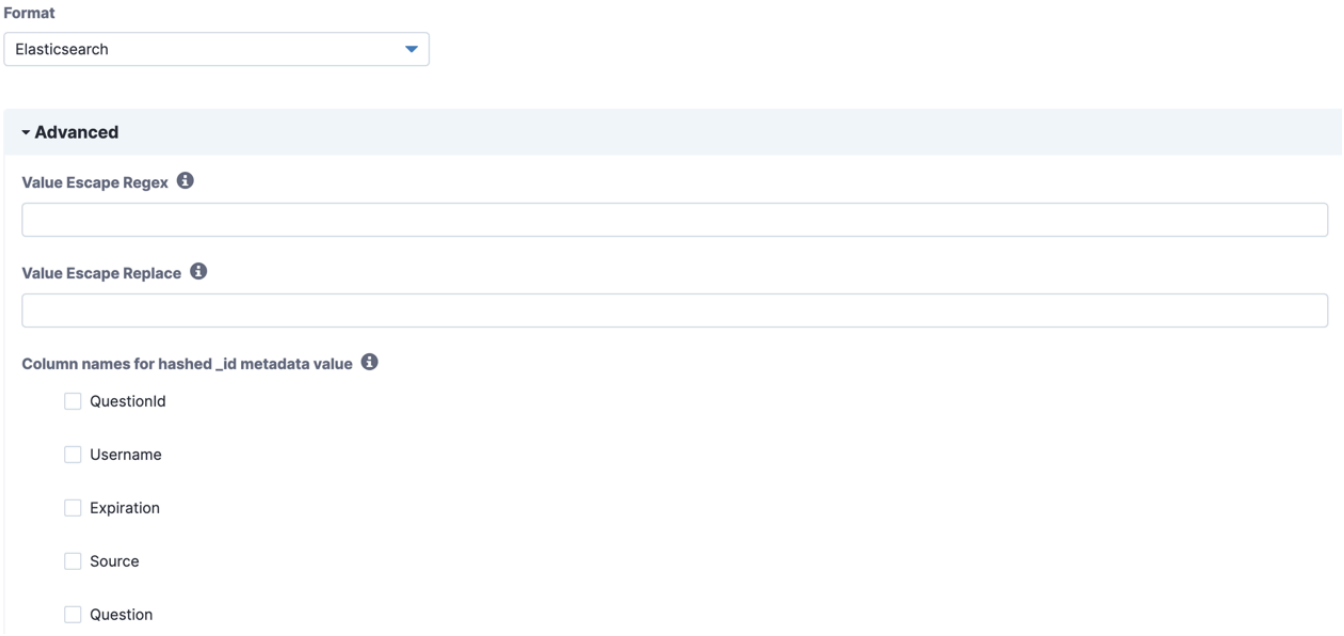
For more information about the types of filters you can configure, see Reference: Filtering options on page 257.

Format data for Elasticsearch

In the **Configure Output** > **Format** > **Advanced** section, choose the columns that you want to use as an **_id** metadata value in Elasticsearch. The **_id** value is a hash value generated from the combination of the selected column values, before applying any configured **Value Escape Regex** regular expressions and **Value Escape Replace** value substitutions. If you select at least one column, the connection data includes an additional column (**id**) which also contains the **_id** hash value. If you do not select any columns, Elasticsearch generates a unique **_id** value.

Figure 12. Advanced format options for Elasticsearch destinations

©2026 Tanium Inc. All Rights Reserved



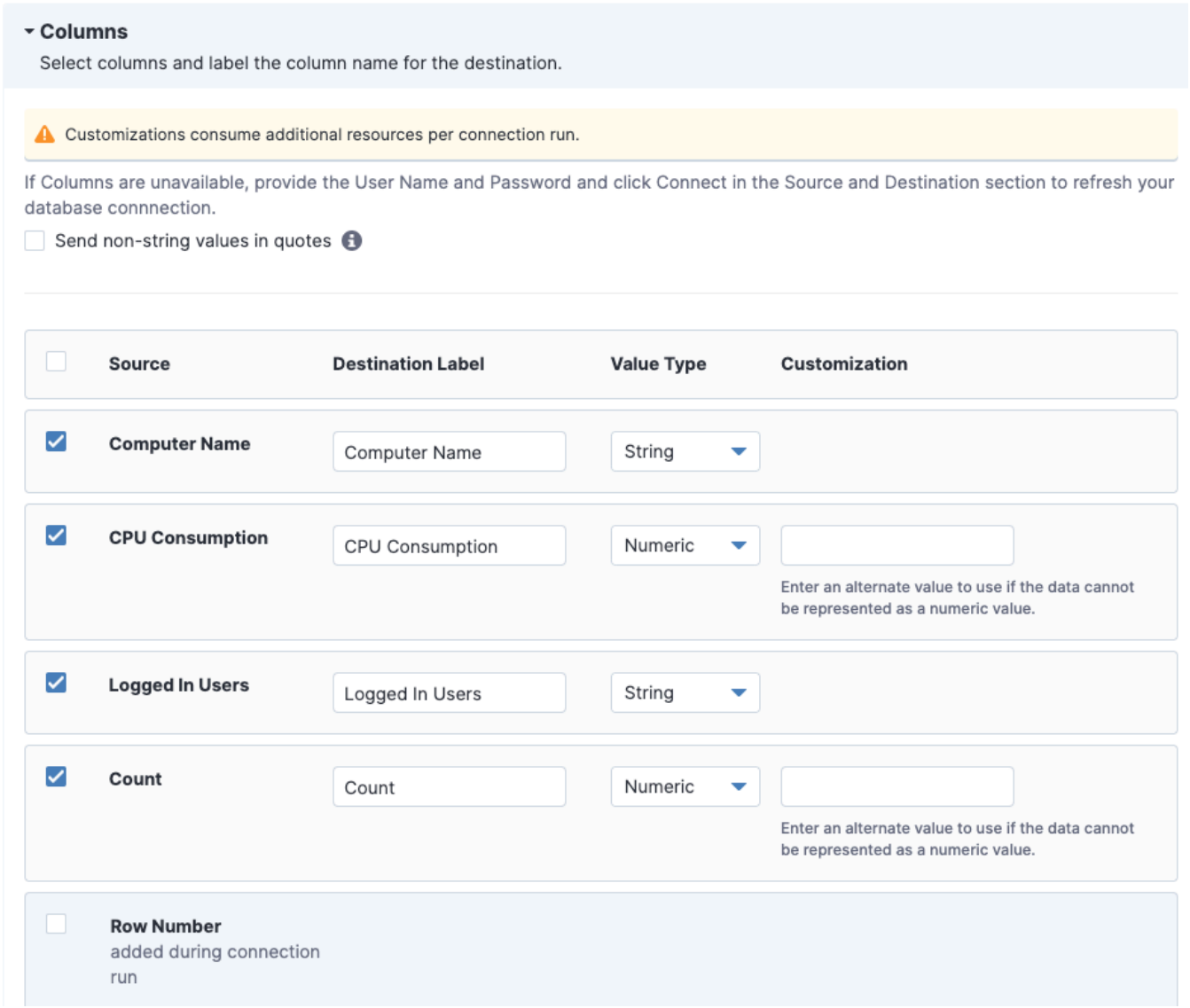
Note: Select columns whose values generally remain static, such as **ComputerId**, **ComputerName**, or **ComputerSerialNumber**.

If a saved question is selected as a source, select **Group columns by sensor** to return the results as an array of objects instead of an array of simple value types. You cannot customize the columns with this option.

In the **Configure Output** > **Columns** section, you can change the **Destination Label** of each column and **Value Type** to force the column to be a String, Numeric, or Date/Time value.

Figure 13. Columns section with Destination Label and Value Type fields

©2026 Tanium Inc. All Rights Reserved



If you choose **Numeric** for the value, you can specify a default value that is used if the data cannot be coerced into a numeric value. You can specify any negative or positive number.

If you choose **Date/Time** for the value, specify the format that you want to use for the column. For more information about how to use a variable, see Time stamp variables on page 297.

For more information about column customizations, see Reference: Column customizations on page 248.

Schedule the connection

Connections can run at a highly configurable time interval, such as multiple times per hour, day, week, or month.

©2026 Tanium Inc. All Rights Reserved

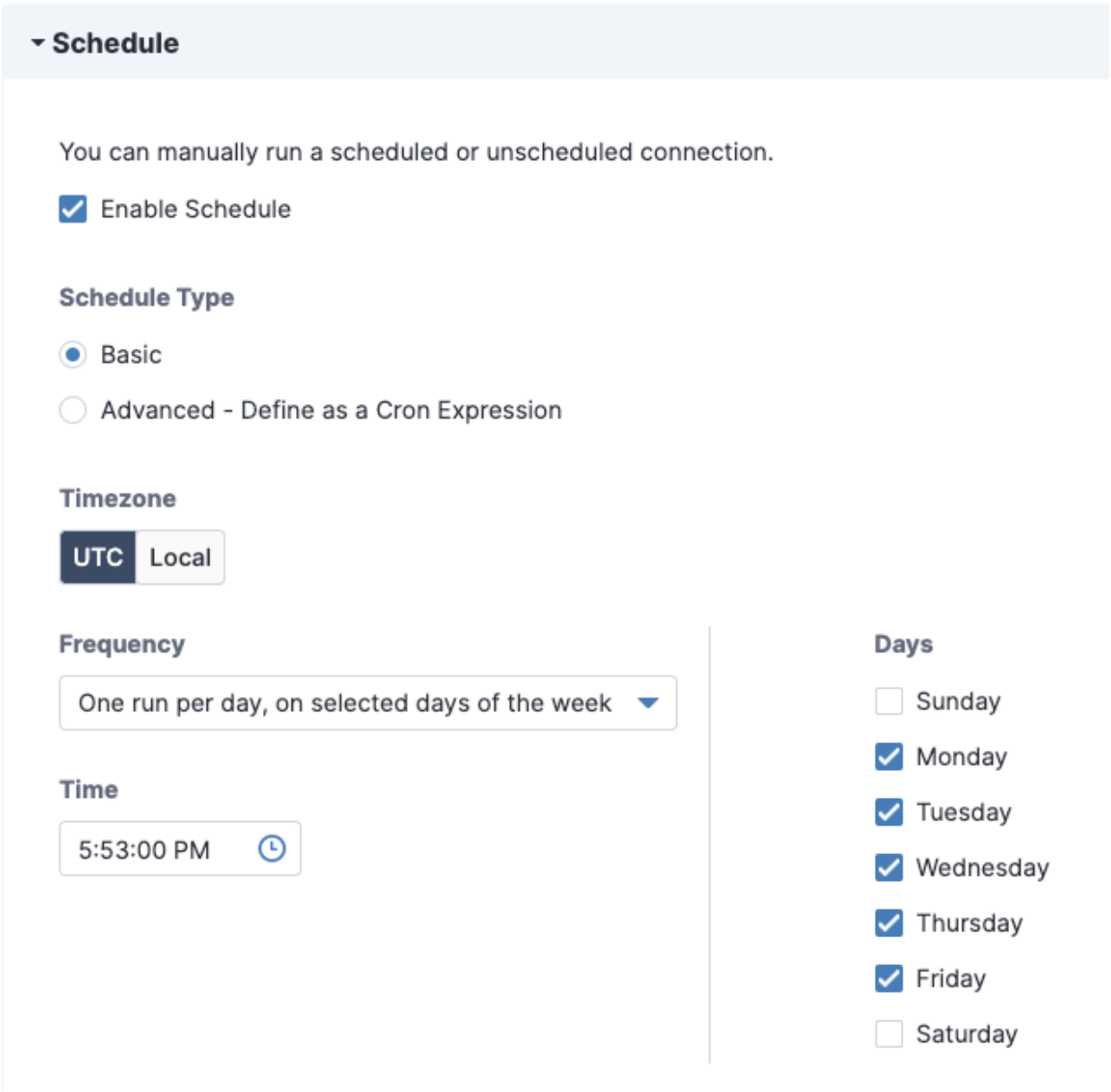
Important: Connections scheduled to run during an upgrade of Connect, or any Tanium solution configured as a connection source, might be interrupted or fail. Schedule your connections to run at a different time than your Tanium upgrades.

Note: If you do not enable the schedule, the connection only runs when you manually run it, unless you configure an **Event** source. Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Schedule** section to update the schedule:

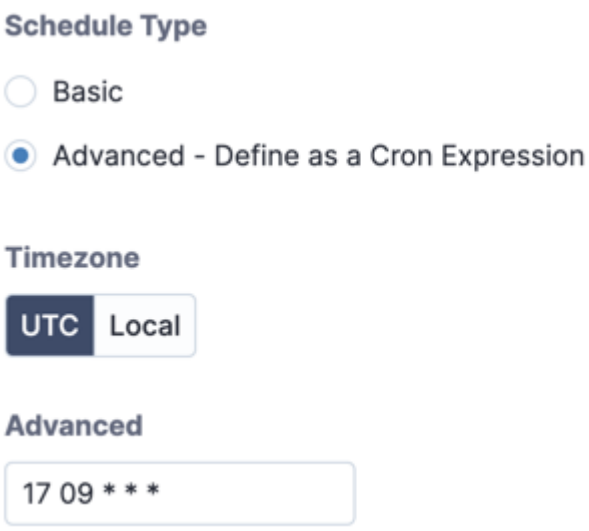
- Select **Enable schedule**.
- In the **Schedule Type**, select **Basic** to build a schedule with the provided controls.

©2026 Tanium Inc. All Rights Reserved



- To view or edit the cron expression directly, select **Advanced - Define as a Cron Expression**, and use the **Advanced** field to edit the cron expression.

©2026 Tanium Inc. All Rights Reserved



Note: If a user that owns a scheduled connection is deleted, future scheduled instances of that connection do not run. For more information, see Issue: Scheduled connection owned by a deleted user no longer runs on page 243.

For more information about cron syntax, see Reference: Cron syntax for Connect on page 253.

Enable listening for an event

Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Enablement** section to send data when a configured event is detected:

- Select **Listen for this Event**.

Save and verify connection

1. After you enter the details for the connection, click **Save**.

   Tip: To save the connection and immediately run the connection, click **Run and Save**.

   If needed, resolve any errors or missing information. After the connection creates successfully, the connection details appear.

©2026 Tanium Inc. All Rights Reserved

2. To view details when the connection runs, click the **Logs** tab.
3. To view an individual run log, expand the row table. For more information about how to resolve errors, see Troubleshooting on page 234.

©2026 Tanium Inc. All Rights Reserved

Configuring email destinations

You can send information from a connection source to a set of email addresses using Microsoft 365 email resources or through an SMTP server. You can either include the results in the email body, or create an attachment.



Note: Microsoft 365 was previously known as Office 365 (O365).

Prerequisites for Microsoft 365 destinations

To configure a connection destination to send email through Microsoft 365, ensure you complete the following prerequisites:

- For a walkthrough of configuration prerequisites, Microsoft Azure configuration, email server profile configuration, and connection configuration, see Tanium Community: Use Tanium Connect to Send Microsoft Office 365 Emails using Modern Authentication.
- You must have a Microsoft 365 Outlook email address associated with a Microsoft Entra ID (formerly Azure Active Directory) user.
- You must create a Microsoft Entra ID application and service principal, and assign the **Mail.Send** and **User.Read** permissions to the application, to send an email with an attachment up to a total of 3 MB (this includes the body of the email plus the attachment). If you want to limit the application scope, create an application access policy and associate it with a mail-enabled security group containing at least one user. For more information, see Microsoft Entra documentation: Create a Microsoft Entra application and service principal that can access resources and Microsoft Graph documentation: Configure ApplicationAccessPolicy.
    - You must also generate a Microsoft Entra ID application client secret. For more information, see Microsoft Entra documentation: Option 3: Create a new client secret.
    - You must also assign the **Mail.Send** and **User.Read** permissions to the application to send emails with attachments up to a total of 3 MB. For more information, see

©2026 Tanium Inc. All Rights Reserved

Microsoft Entra documentation: Assign a role to the application.

> **Note:** If a connection run generates no data, no email is sent. However, if you select a saved question source and clear **Hide No Results**, an email is sent per connection run, regardless of whether data is available.

- If you want to enable sending emails with attachments greater than 3 MB and up to 150 MB (subject to your Microsoft 365 attachment settings), you can assign the **Mail.ReadWrite** permission to the Microsoft Entra ID application. If you assign this permission, you must allow traffic to **outlook.office.com** over port 443/TCP and **outlook.office365.com** over port 443/TCP.

  > **Important:** Attachments larger than 3 MB are not supported for email sent through GCC M365, including FedRAMP M365. Connect uses the Microsoft **createUploadSession** API to manage attachments for Microsoft 365 email uploads. The API has a known issue with attachments larger than 3 MB in GCC M365 environments. This limitation applies to any customer whose Microsoft 365 environment is GCC M365, independent of the Tanium environment. Customers who try to send an email with an attachment larger than 3 MB through a GCC M365 environment might receive a **MS_GRAPH_STATUS_CODE 401 large_attachment** response that contains an error message similar to **caused by unexpected status code 401 from ms-graph**. For more information about the **createUploadSession** API and the known issue, see Microsoft Graph documentation: attachment: createUploadSession.

  > **Note:** The **Mail.ReadWrite** permission only permits a larger attachment size; the body of the email must never exceed 3 MB.

  > **Note:** For the best results, if you assign the **Mail.ReadWrite** permission, create an access policy and limit Microsoft Entra ID application access to one user. For more information, see Microsoft Graph documentation: Limiting application permissions to specific Exchange Online mailboxes.

- The **Email (O365 & SMTP)** destination requires an email server profile on the Tanium Server. You can configure an email server profile through the Connect workbench in Tanium Console.

©2026 Tanium Inc. All Rights Reserved

- To configure an email server profile in Tanium Console, you must have a role with the Tanium **Email Config write** permission. The predefined **Connect Operator** and **Connect Administrator** roles in Connect have this permission. Sending an email requires the user that configures the connection to have permission to the content set to which you assign the email server profile. For more information about predefined roles in Connect, see User role requirements on page 30. For information about configuring custom roles, see Tanium Console User Guide: Managing roles



Note: If you delete an email server profile configuration that is referenced by a scheduled connection, future scheduled instances of that connection fail. For more information, see Issue: Emails to Microsoft 365 destinations fail to send on page 244.

- The email server profile uses the **Authority Host** that you select for authentication to the **Host** that you select, over port 443/TCP.
- Configure your network allow list to allow traffic outbound from your Tanium Module Server to the following Microsoft 365 URLs and enable access for Microsoft 365 mail resources:
  - **graph.microsoft.com:443**
  - **login.microsoftonline.com:443**
  - **graph.microsoft.us:443**
  - **dod-graph.microsoft.us:443** for DoD tenants
  - **login.microsoftonline.us:443**
  - **outlook.office.com:443** and **outlook.office365.com:443** if you assign the **Mail.ReadWrite** permission to the Microsoft Entra ID application. For more information, see Microsoft 365 documentation: Office 365 URLs and IP address ranges.

For more information about how to configure an email server profile, see Configure email server profile settings for Microsoft 365 on page 44.

Prerequisites for SMTP destinations

©2026 Tanium Inc. All Rights Reserved

- The **Email (O365 & SMTP)** destination requires an email server profile on the Tanium Server. You can configure an email server profile through the Connect workbench in Tanium Console.

    - To configure an email server profile in Tanium Console, you must have a role with the Tanium **Email Config write** permission. The predefined **Connect Operator** and **Connect Administrator** roles in Connect have this permission. Sending an email requires the user that configures the connection to have permission to the content set to which you assign the email server profile. For more information about predefined roles in Connect, see User role requirements on page 30. For information about configuring custom roles, see Tanium Console User Guide: Managing roles

  Note: If you delete an email server profile configuration that is referenced by a scheduled connection, future scheduled instances of that connection fail.

- Configure your network allow list to allow traffic outbound from your Tanium Module Server to the SMTP server.

    - To use Google Mail as an SMTP server, allow traffic to `smtp.google.com`.

- You must have email addresses to send and receive email results.

- Gather information about your mail server, including host, port, certificate, user name, password.

Note: Standard TCP ports for secure email using SMTP include 465 and 587. Do not send unencrypted data over TCP port 25 outbound.

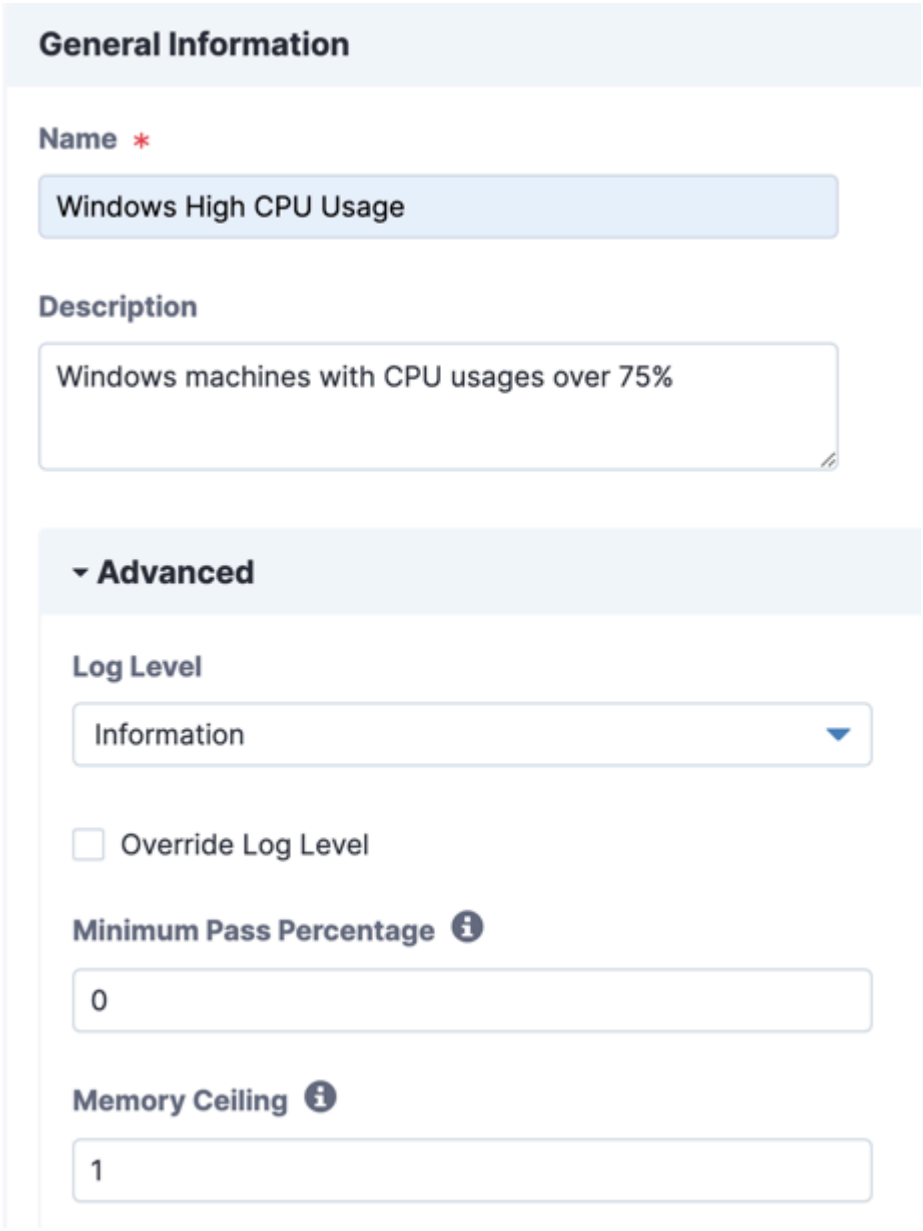
Specify general connection information

1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click **Create Connection**.
2. Enter a name and description for the connection.
3. (Optional) In the **General Information** section, expand **Advanced** to configure the following settings:

©2026 Tanium Inc. All Rights Reserved

Log Level

By default, **Log Level** is set to **Information**. To reduce the amount of logging, you can set **Log Level** to **Warning**, **Error**, or **Fatal**.



Override Log Level

If you are debugging the connection, select **Override Log Level** to set a **Temporary Log Level** (such as **Trace** or **Debug**) on this connection for a selected **Number of Runs** (up to **24**). A scheduled or manual connection run, once started, counts towards the number of runs, regardless of the connection status. After the number of runs elapses, the logging for this connection returns to the **Log Level** you selected to prevent finer-grained logging from consuming additional resources for an indefinite number of runs.

©2026 Tanium Inc. All Rights Reserved

Minimum Pass Percentage

Minimum percentage of the expected rows that must be processed for the connection to succeed.

Memory Ceiling (GB)

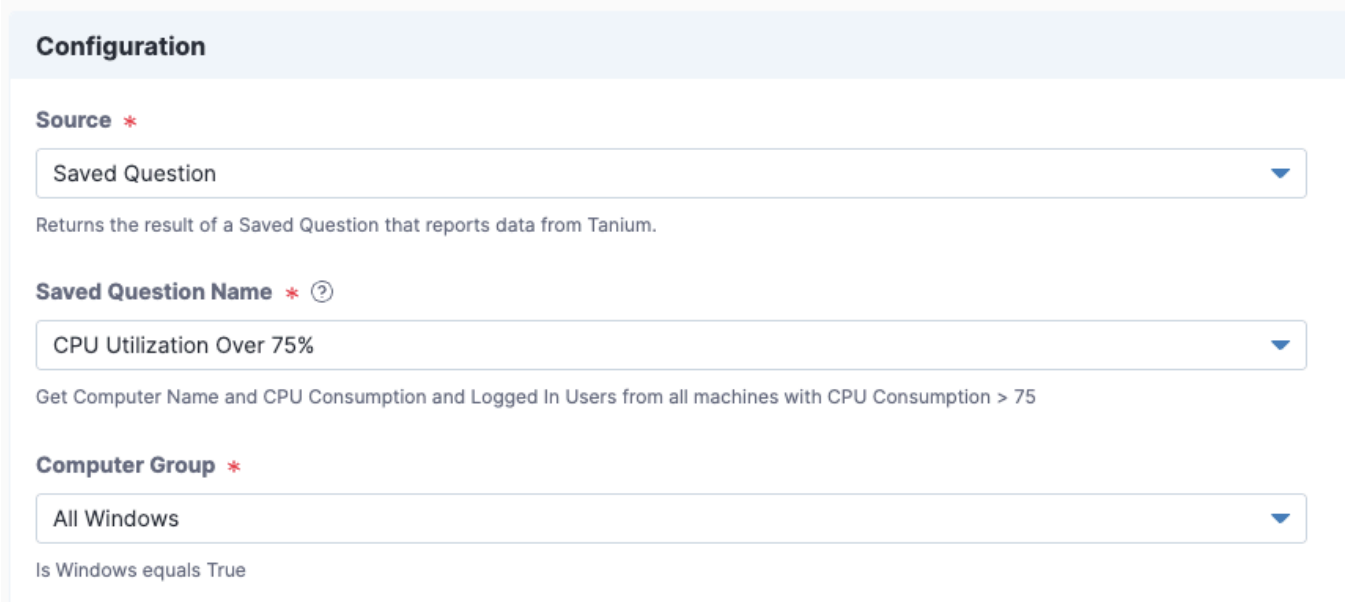
Maximum memory for the node process to run the connection. This defaults to 1 GB per connection, and cannot exceed the global maximum sum of memory for all running connections (by default, 8 GB). Increase this setting if a connection frequently exhibits out of memory errors while running.

> **Note:** If the sum of simultaneously scheduled connection **Memory Ceiling** values exceed the global **Memory Ceiling**, connections run until the global **Memory Ceiling** is reached, then any remaining connections enter a waiting queue if you select the **Queue Connections** configuration setting, or fail if you clear the **Queue Connections** configuration setting.

Configure the connection source

The connection source determines what data you are sending to the destination. This data is usually information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

Figure 14. Connection source settings



©2026 Tanium Inc. All Rights Reserved

Note:

If a Tanium solution or source shows Critical, the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

Note: After you create a connection, you cannot update the connection source type, only the source configuration. If you want to change the source type, create a new connection.

For more information about available connection sources, see Connection sources on page 14.

Configure the email results destination

About this task

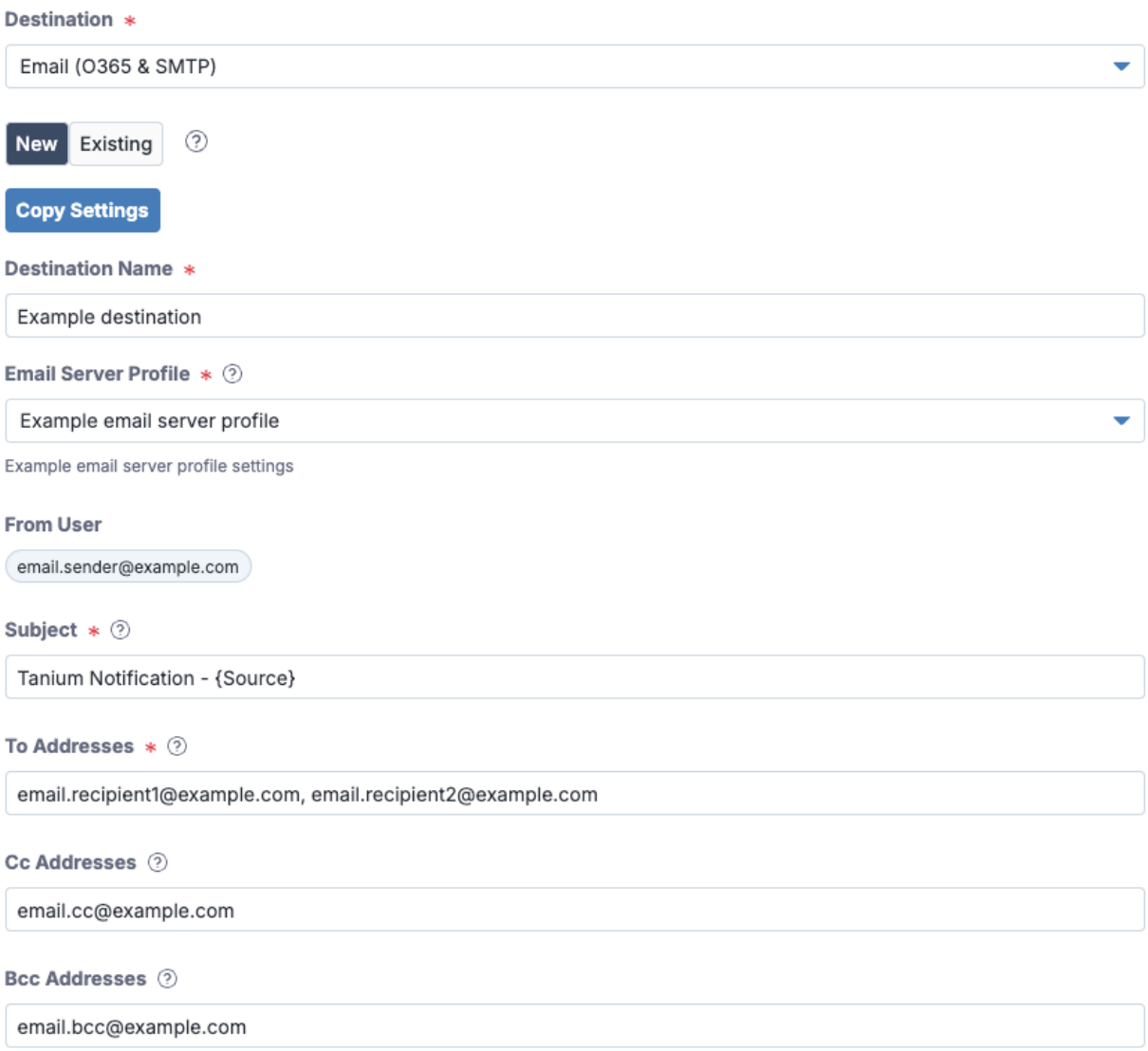
Note: After you create a connection, you cannot update the connection destination type, only the destination configuration. If you want to change the destination, create a new connection.

1. For **Destination**, select **Email (O365 & SMTP)**.
2. Provide a name for the destination. Options include:
   - Create a new destination: Specify a unique name to save the configuration information as a new destination. Select **New** and then enter a **Destination Name**
   - Copy an existing destination: Select **New**, and then click **Copy Settings**. Select a destination, click **Apply**, and update the **Destination Name**.
   - Reuse an existing destination: Select **Existing**, and then select a **Destination Name**.

     Note: Configure a unique destination per connection. If you edit the settings for a shared destination for one connection, any other connections that use the shared destination are affected, and connection runs might fail.

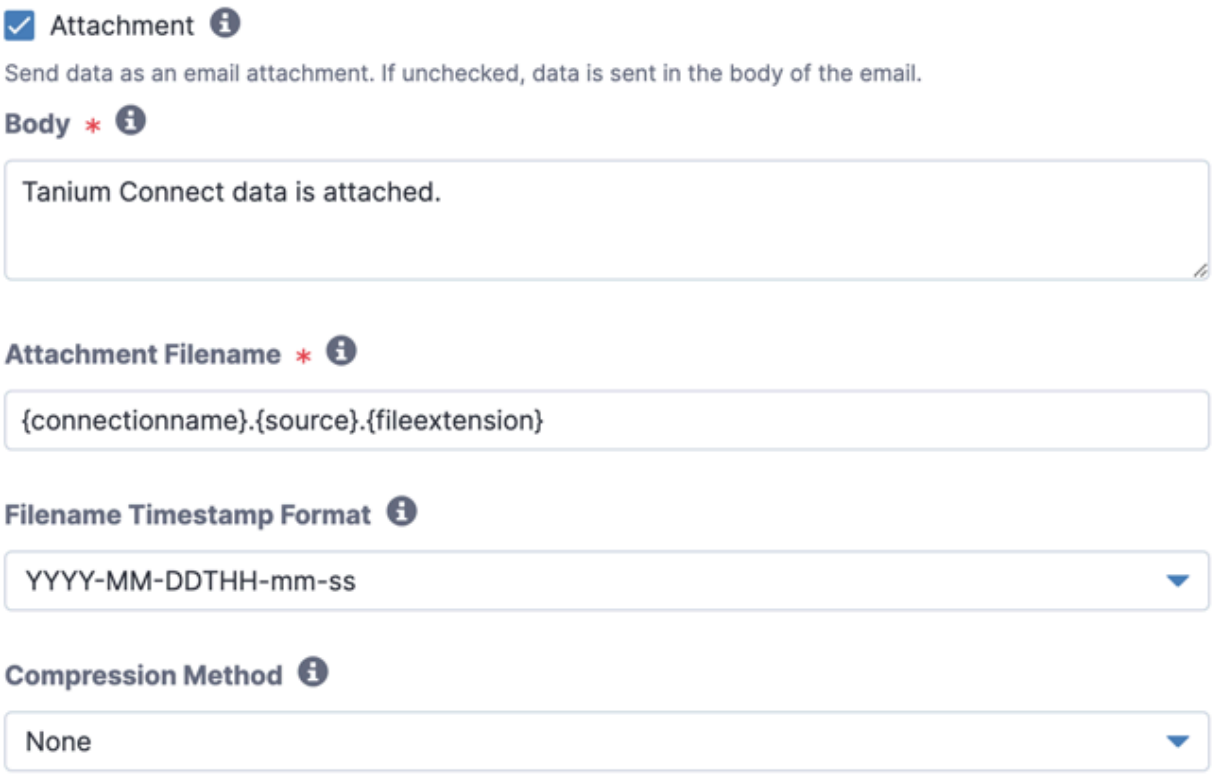
©2026 Tanium Inc. All Rights Reserved

3. Select an **Email Server Profile** from the drop-down list.
    - To configure an email server profile for Microsoft 365, see Configure email server profile settings for Microsoft 365 on page 44.
    - To configure an email server profile for an SMTP server, see Configure email server profile settings for SMTP on page 49.
4. Provide information about the email **Subject**, **To Addresses**, **Cc Addresses**, and **Bcc Addresses**.
   The **Subject** field supports variable substitution, as listed in Reference: Variables on page 295.



5. (Optional) Specify attachment settings.
   The **Attachment Filename** field supports variable substitution, as listed in Reference: Variables on page 295.

©2026 Tanium Inc. All Rights Reserved



- **Attachment** is selected by default. Enter up to 5000 characters of email **Body** text included with each email. Specify a file name and file extension in the **Attachment Filename**. The file extension does not need to match the format option you select in the **Format** section. Note the option that you select in the **Format** section does not add or change the file extension. Select a **Filename Timestamp Format** if you want to append a timestamp to the file name.

  > **Note:** The Tanium Reporting source requires selecting **Attachment**.

- You can compress the attachment into a zip or gzip file. If you select a compression method, the file extension for the compression method is automatically added to the end of the file name.

Configure filters

(Optional) In the **Configure Output** > **Filters** section, you can specify filters to modify the data that you are getting from your connection source before it is sent to the destination.

For more information about the types of filters you can configure, see Reference: Filtering options on page 257.

©2026 Tanium Inc. All Rights Reserved

Format data for email

You can choose from any of the available formats for your email. The data is sent in an email attachment by default.

If you want to have the data in the body of the email instead of attaching a file to the email, edit the email destination settings to clear **Attachment**.

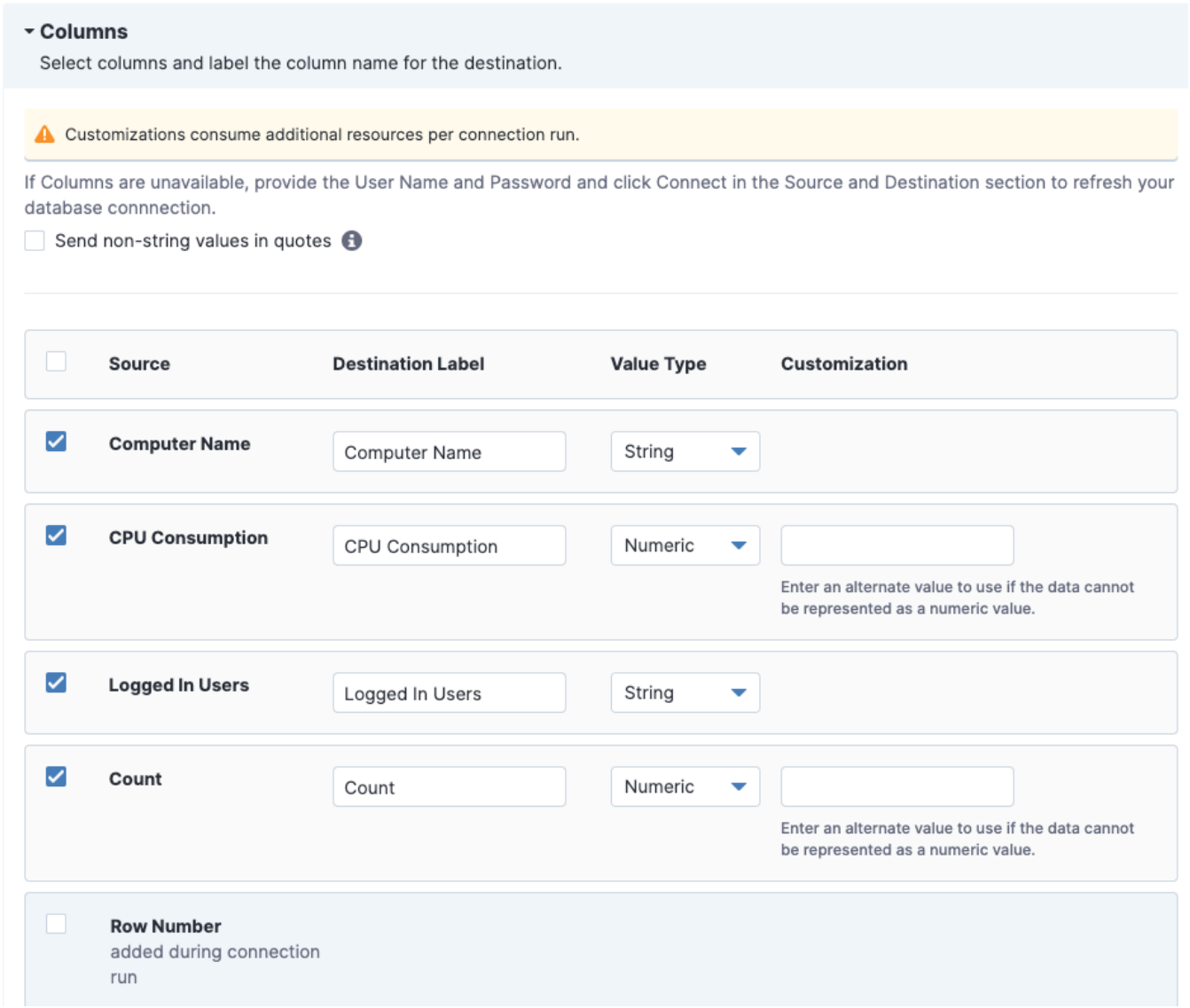
You can choose the columns that appear in the resulting email.

> **Note:** If the data format supports row delimiter characters, update the characters to ensure that individual rows are sent in a format that the destination can parse. You can define one or more of `\n` (new line), `\r` (carriage return), and `\t` (tab).

In the **Configure Output** > **Columns** section, you can change the **Destination Label** of each column and **Value Type** to force the column to be a String, Numeric, or Date/Time value.

Figure 15. Columns section with Destination Label and Value Type fields

©2026 Tanium Inc. All Rights Reserved



If you choose **Numeric** for the value, you can specify a default value that is used if the data cannot be coerced into a numeric value. You can specify any negative or positive number.

If you choose **Date/Time** for the value, specify the format that you want to use for the column. For more information about how to use a variable, see Time stamp variables on page 297.

For more information about column customizations, see Reference: Column customizations on page 248.

Schedule the connection

Connections can run at a highly configurable time interval, such as multiple times per hour, day, week, or month.

©2026 Tanium Inc. All Rights Reserved

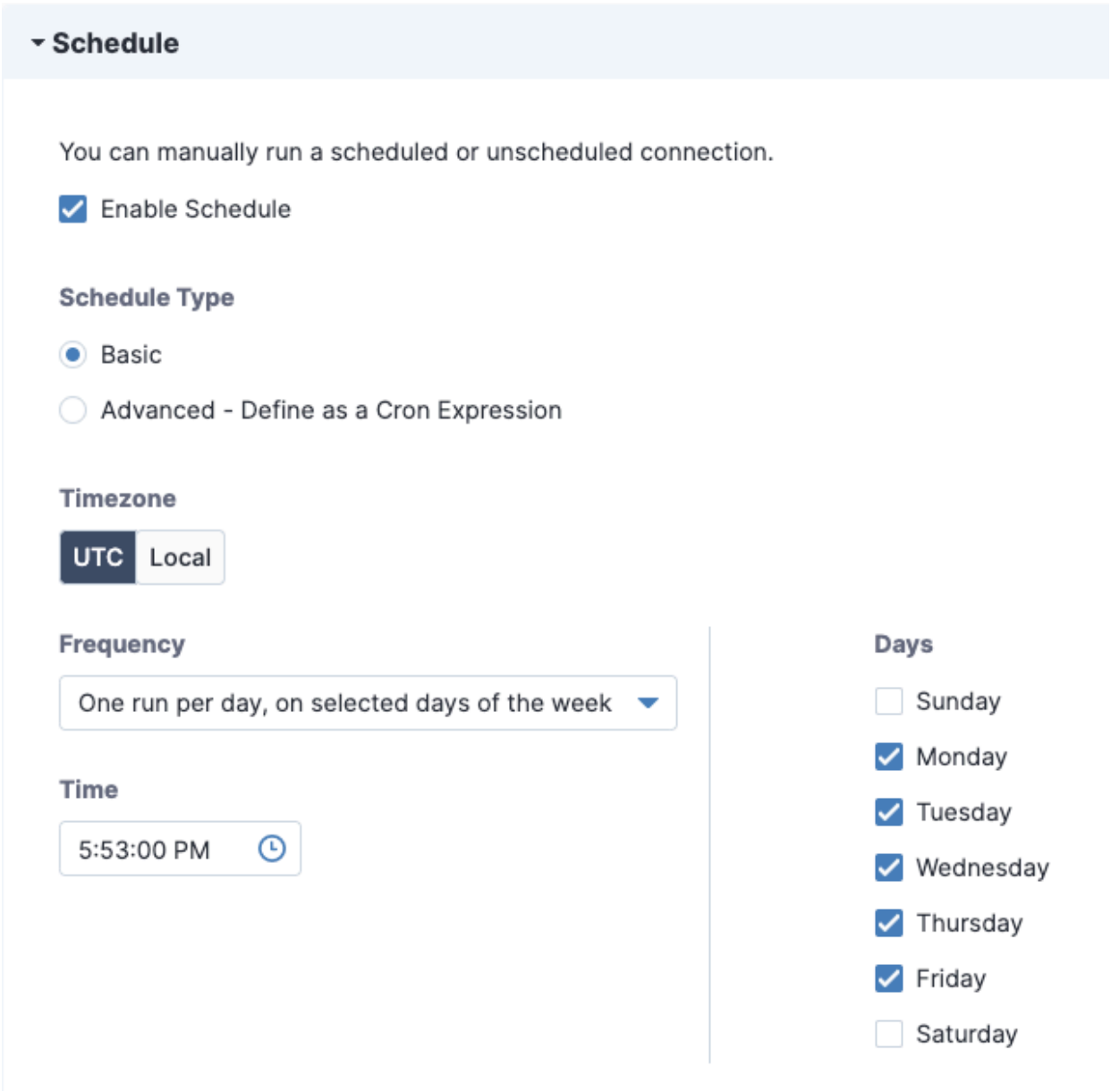
Important: Connections scheduled to run during an upgrade of Connect, or any Tanium solution configured as a connection source, might be interrupted or fail. Schedule your connections to run at a different time than your Tanium upgrades.

Note: If you do not enable the schedule, the connection only runs when you manually run it, unless you configure an **Event** source. Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Schedule** section to update the schedule:

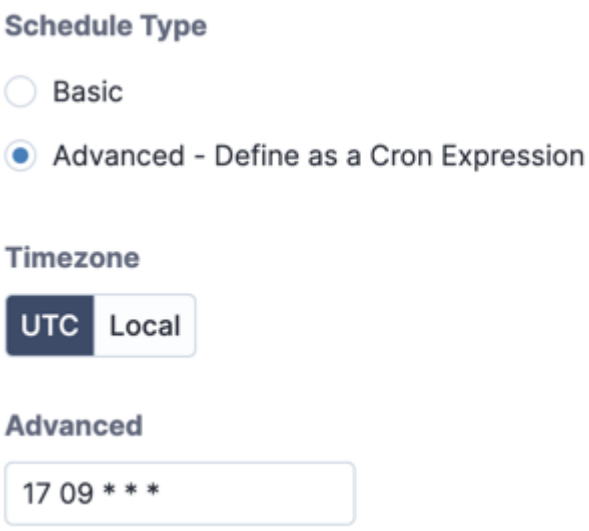
- Select **Enable schedule**.
- In the **Schedule Type**, select **Basic** to build a schedule with the provided controls.

©2026 Tanium Inc. All Rights Reserved



- To view or edit the cron expression directly, select **Advanced - Define as a Cron Expression**, and use the **Advanced** field to edit the cron expression.

©2026 Tanium Inc. All Rights Reserved



Note: If a user that owns a scheduled connection is deleted, future scheduled instances of that connection do not run. For more information, see Issue: Scheduled connection owned by a deleted user no longer runs on page 243.

For more information about cron syntax, see Reference: Cron syntax for Connect on page 253.

Enable listening for an event

Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Enablement** section to send data when a configured event is detected:

- Select **Listen for this Event**.

Save and verify connection

1. After you enter the details for the connection, click **Save**.

   Tip: To save the connection and immediately run the connection, click **Run and Save**.

   If needed, resolve any errors or missing information. After the connection creates successfully, the connection details appear.

©2026 Tanium Inc. All Rights Reserved

2. To view details when the connection runs, click the **Logs** tab.
3. To view an individual run log, expand the row table. For more information about how to resolve errors, see Troubleshooting on page 234.

©2026 Tanium Inc. All Rights Reserved

Configuring SMTP email destinations

Important: The email (SMTP) destination described in this chapter is deprecated and will be removed in a future release. The destination appears in Connect as **Email (Legacy SMTP)**. Support for SMTP servers continues through the **Email (O365 & SMTP)** destination and email server profiles. For more information, see Configuring email destinations on page 119 and Configure email server profile settings for SMTP on page 49.

You can send information from a connection source to a set of email addresses using SMTP servers. You can either include the results in the email body, or create an attachment.

Prerequisites

- Email addresses for sending and receiving email results.
- Information about your mail server, including host, port, user name, password, and authentication information.

Note: Standard TCP ports for secure email using SMTP include 465 and 587. Do not send unencrypted data over TCP port 25 outbound.

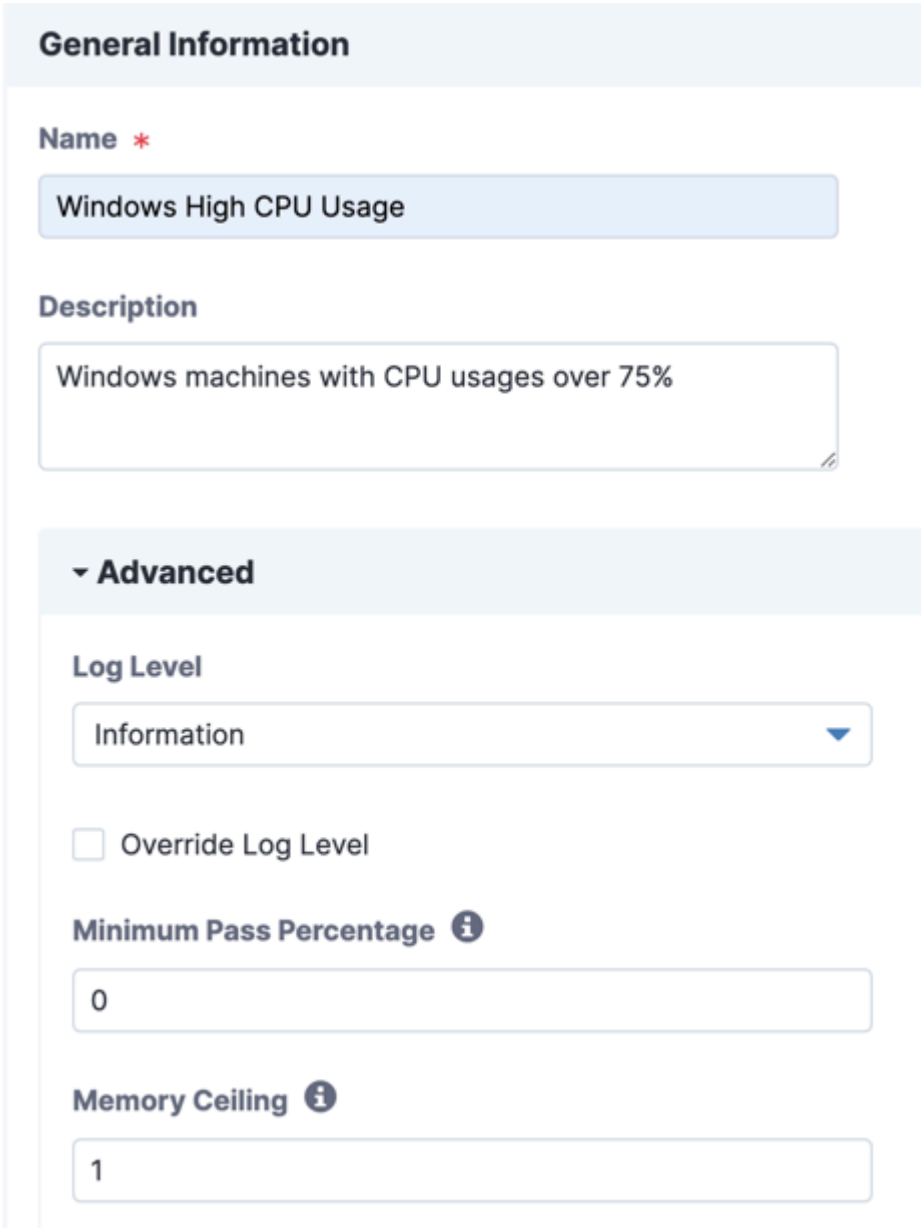
Specify general connection information

1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click **Create Connection**.
2. Enter a name and description for the connection.
3. (Optional) In the **General Information** section, expand **Advanced** to configure the following settings:

   Log Level

   By default, **Log Level** is set to **Information**. To reduce the amount of logging, you can set **Log Level** to **Warning**, **Error**, or **Fatal**.

©2026 Tanium Inc. All Rights Reserved



Override Log Level

If you are debugging the connection, select **Override Log Level** to set a **Temporary Log Level** (such as **Trace** or **Debug**) on this connection for a selected **Number of Runs** (up to **24**). A scheduled or manual connection run, once started, counts towards the number of runs, regardless of the connection status. After the number of runs elapses, the logging for this connection returns to the **Log Level** you selected to prevent finer-grained logging from consuming additional resources for an indefinite number of runs.

Minimum Pass Percentage

Minimum percentage of the expected rows that must be processed for the connection to succeed.

©2026 Tanium Inc. All Rights Reserved

Memory Ceiling (GB)

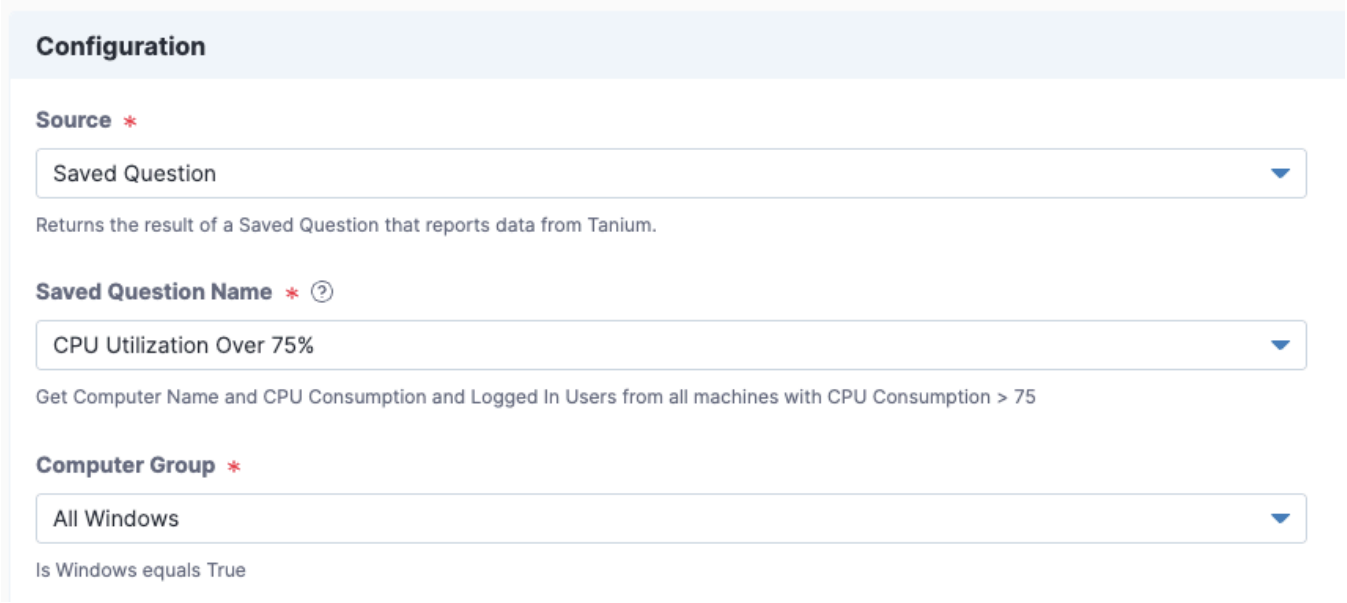
Maximum memory for the node process to run the connection. This defaults to 1 GB per connection, and cannot exceed the global maximum sum of memory for all running connections (by default, 8 GB). Increase this setting if a connection frequently exhibits out of memory errors while running.

> **Note:** If the sum of simultaneously scheduled connection **Memory Ceiling** values exceed the global **Memory Ceiling**, connections run until the global **Memory Ceiling** is reached, then any remaining connections enter a waiting queue if you select the **Queue Connections** configuration setting, or fail if you clear the **Queue Connections** configuration setting.

Configure the connection source

The connection source determines what data you are sending to the destination. This data is usually information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

Figure 16. Connection source settings



©2026 Tanium Inc. All Rights Reserved

Note:

If a Tanium solution or source shows Critical, the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

Note: After you create a connection, you cannot update the connection source type, only the source configuration. If you want to change the source type, create a new connection.

For more information about available connection sources, see Connection sources on page 14.

Configure the Email (SMTP) results destination

About this task

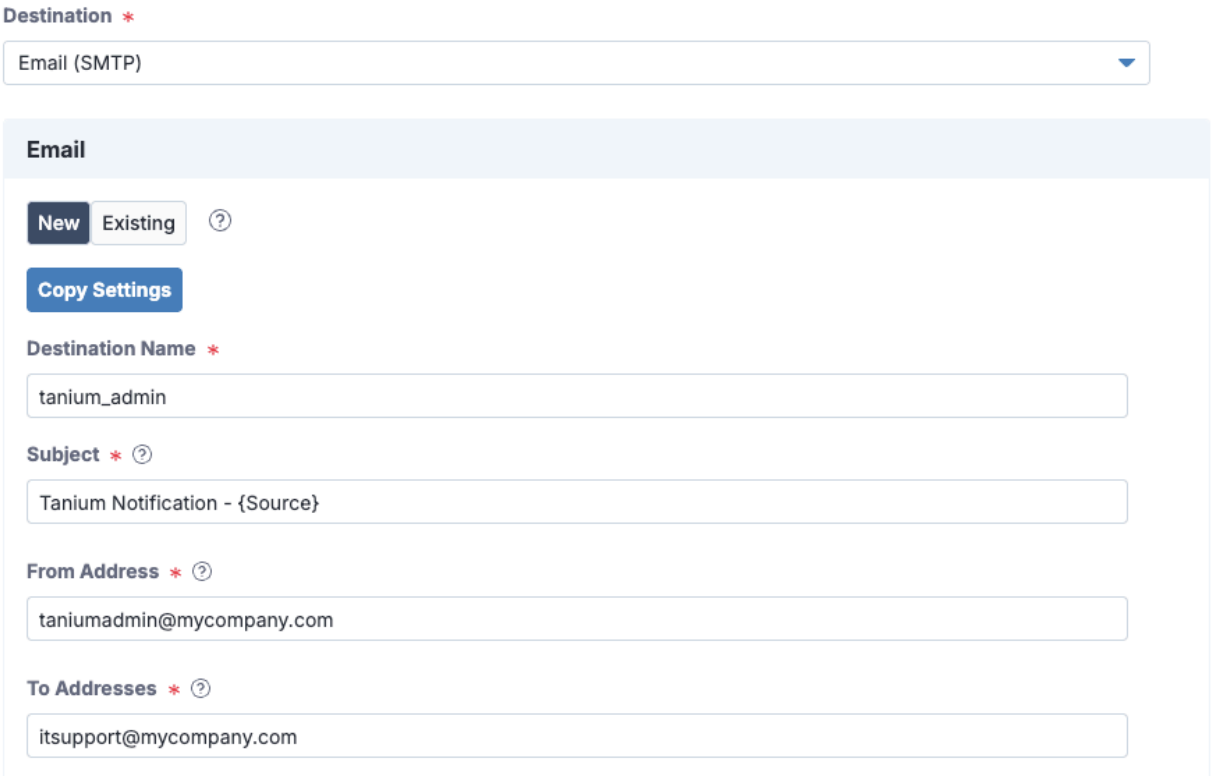
Note: After you create a connection, you cannot update the connection destination type, only the destination configuration. If you want to change the destination, create a new connection.

1. In the **Email** section for the Email (SMTP) destination, provide a name for the destination.
   - Create a new destination: Specify a unique name to save the configuration information as a new destination. Select **New** and then enter a **Destination Name**
   - Copy an existing destination: Select **New**, and then click **Copy Settings**. Select a destination, click **Apply**, and update the **Destination Name**.
   - Reuse an existing destination: Select **Existing**, and then select a **Destination Name**.

     Note: Configure a unique destination per connection. If you edit the settings for a shared destination for one connection, any other connections that use the shared destination are affected, and connection runs might fail.
2. In the **Email** section, provide information about the email **Subject**, **From Address**, and **To Address** sections.

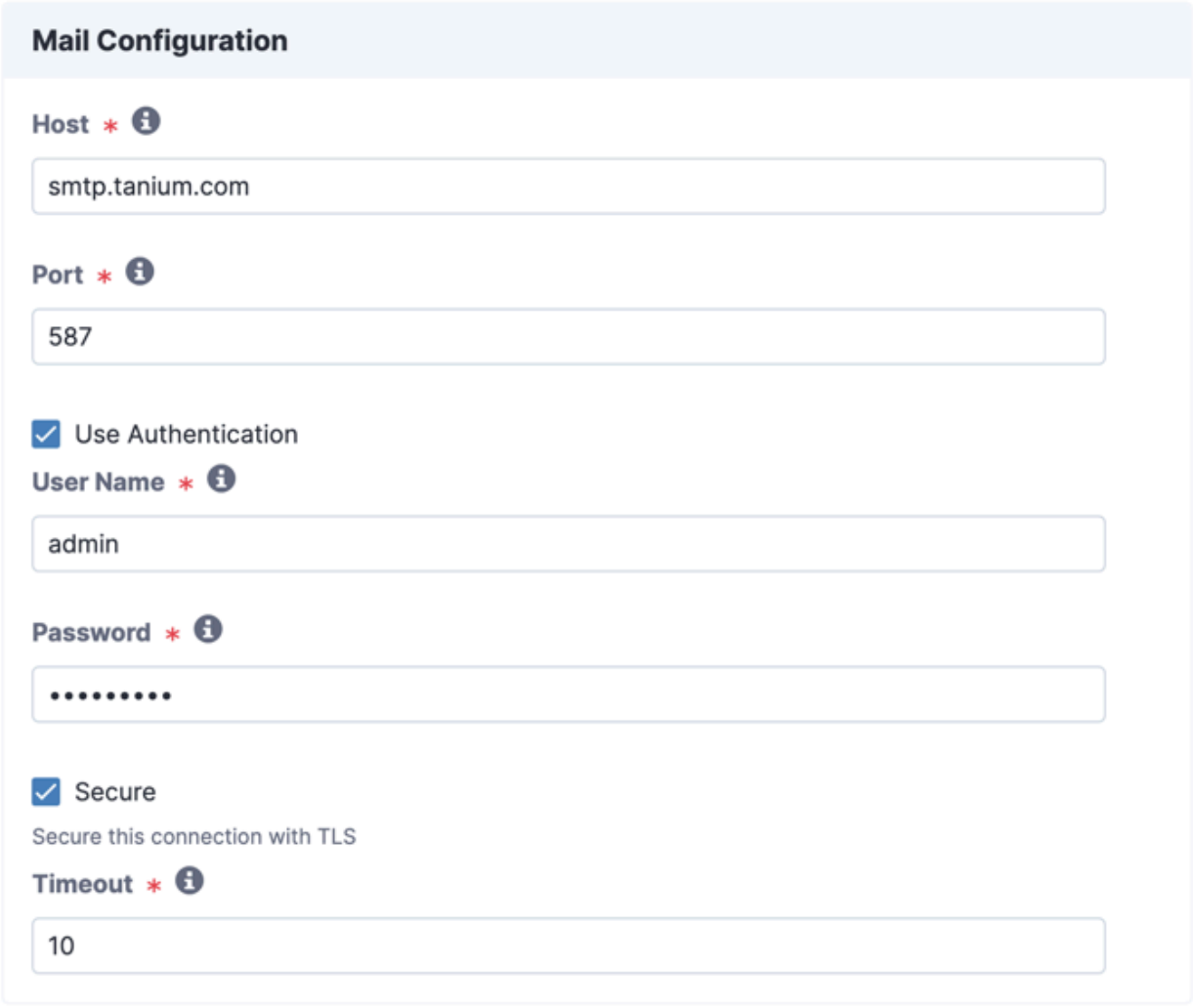
©2026 Tanium Inc. All Rights Reserved

Some fields also support variable substitution, as listed in Reference: Variables on page 295.



3. Specify information about the mail server in the **Mail Configuration** section:

©2026 Tanium Inc. All Rights Reserved



- Provide the host name, port, user name, and password.

  Important: Google Workspace ends support for logins with a Google username and password on September 30, 2024. Update your connections to Google Workspace email destinations with an app password before this date. For more information about how to use an app password, see Gmail Help: Sign in with app passwords.

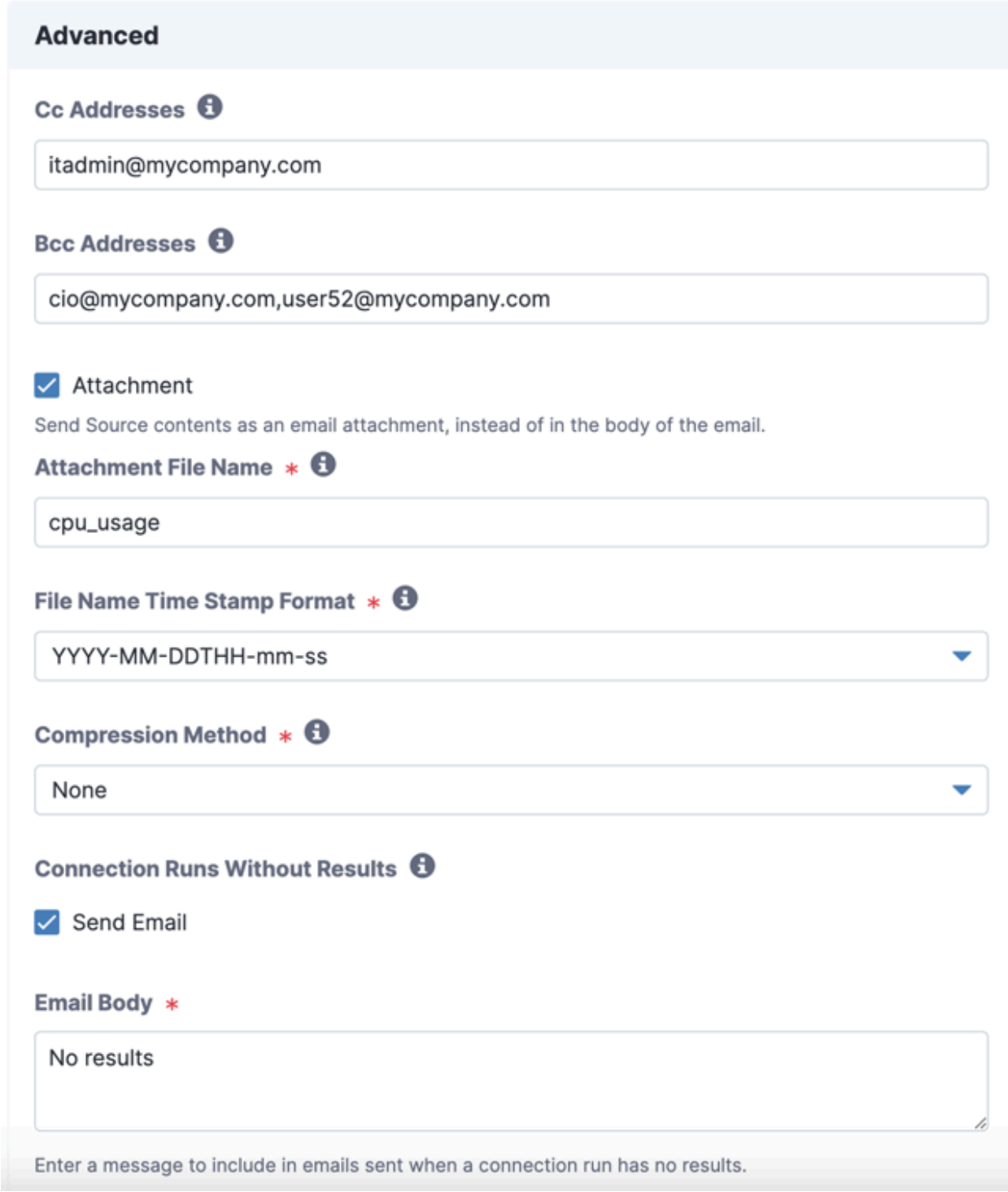
- Select **Secure** if the connection with the SMTP server is authenticated and uses TLS encryption.

  Note: If you do not select **Secure**, authentication information is encrypted at rest, but passed unencrypted to the destination.

- Specify a **Timeout** value for sending the message. The default is 0, which means that there is no timeout. A recommended timeout value is 10 seconds.

©2026 Tanium Inc. All Rights Reserved

4. (Optional) Specify advanced settings.
   Some fields also support variable substitution, as listed in Reference: Variables on page 295.



   - You can configure CC and BCC addresses for the email and specify the settings for the email attachment.
   - **Attachment** is selected by default. Specify a file name and file extension in the

©2026 Tanium Inc. All Rights Reserved

Attachment File Name. The file extension does not need to match the format option you select in the **Format** section. Note the option that you select in the **Format** section does not add or change the file extension.

- You can compress the attachment into a zip or gzip file. If you select a compression method, the file extension for the compression method is automatically added to the end of the file name.
- Under **Connection Runs Without Results**, select **Send Email** to send an email if the connection run generates no results. Enter a message in the **Email Body** field to include in the email body.

Configure filters

(Optional) In the **Configure Output** > **Filters** section, you can specify filters to modify the data that you are getting from your connection source before it is sent to the destination.

For more information about the types of filters you can configure, see Reference: Filtering options on page 257.

Format data for email

You can choose from any of the available formats for your email. The data is sent in the body of the email by default.

If you want to attach a file to the email instead of having the data in the body of the email, edit the **Advanced** settings for the Email destination and select **Attachment**. Specify a file name and whether the file should be compressed.

The data format for email destinations is HTML by default. You can choose the columns that appear in the resulting email.

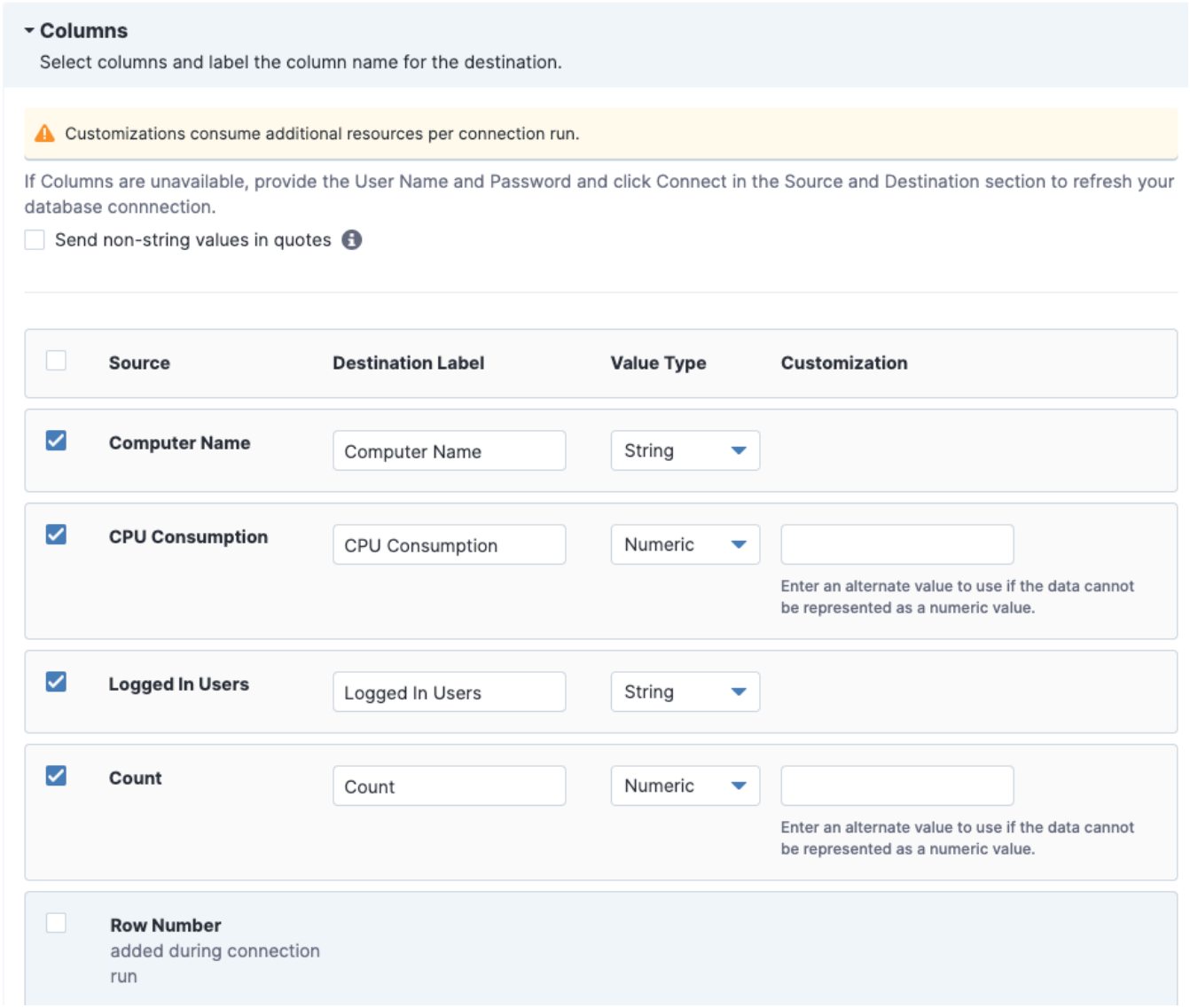
Note: If the data format supports row delimiter characters, update the characters to ensure that individual rows are sent in a format that the destination can parse. You can define one or more of `\n` (new line), `\r` (carriage return), and `\t` (tab).

In the **Configure Output** > **Columns** section, you can change the **Destination Label** of each column

©2026 Tanium Inc. All Rights Reserved

and **Value Type** to force the column to be a String, Numeric, or Date/Time value.

Figure 17. Columns section with Destination Label and Value Type fields



If you choose **Numeric** for the value, you can specify a default value that is used if the data cannot be coerced into a numeric value. You can specify any negative or positive number.

If you choose **Date/Time** for the value, specify the format that you want to use for the column. For more information about how to use a variable, see Time stamp variables on page 297.

For more information about column customizations, see Reference: Column customizations on page 248.

Schedule the connection

©2026 Tanium Inc. All Rights Reserved

Connections can run at a highly configurable time interval, such as multiple times per hour, day, week, or month.

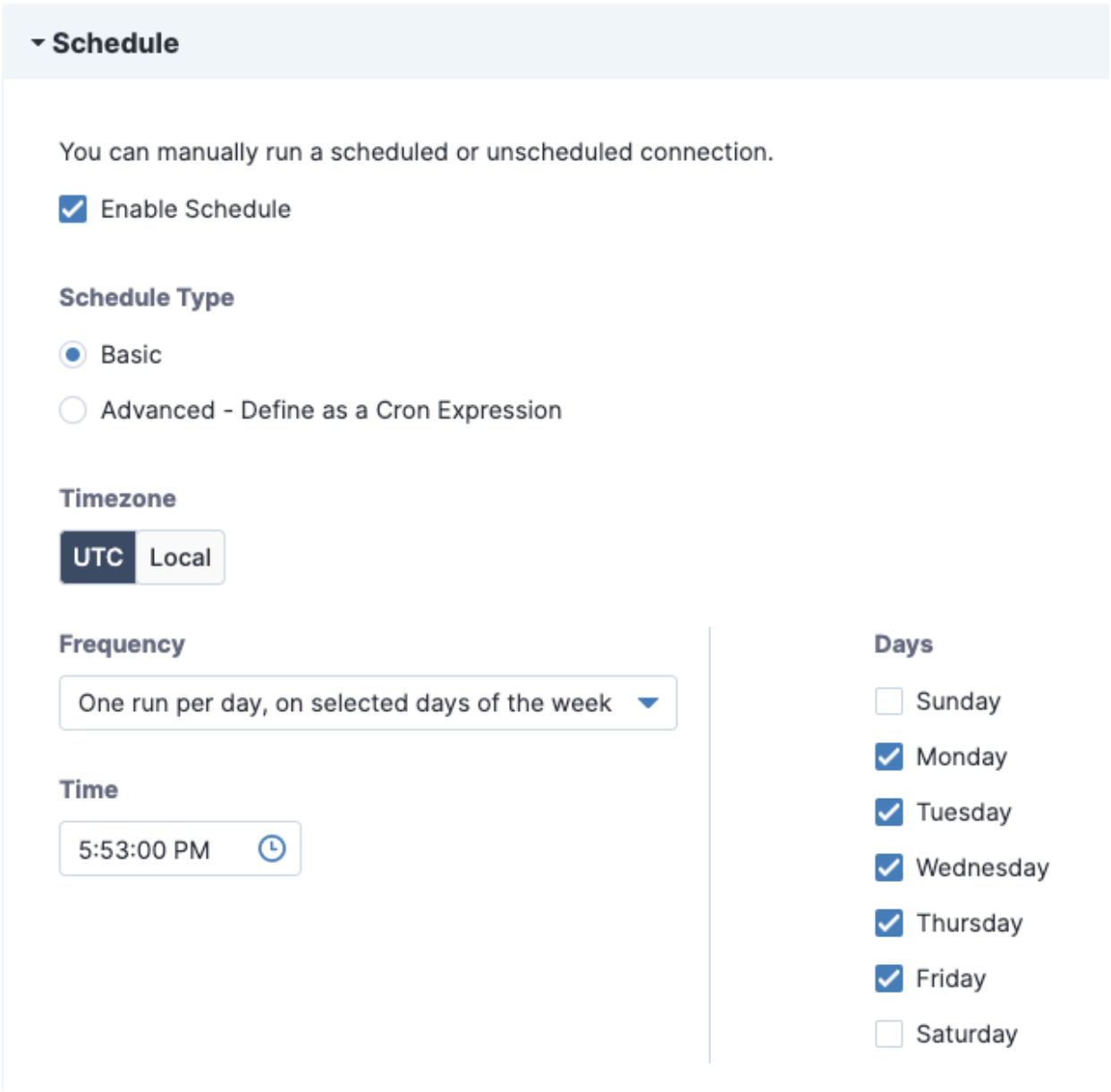
Important: Connections scheduled to run during an upgrade of Connect, or any Tanium solution configured as a connection source, might be interrupted or fail. Schedule your connections to run at a different time than your Tanium upgrades.

Note: If you do not enable the schedule, the connection only runs when you manually run it, unless you configure an **Event** source. Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Schedule** section to update the schedule:

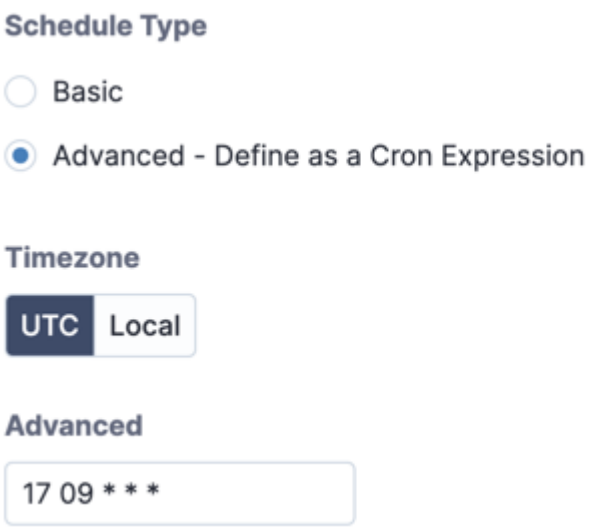
- Select **Enable schedule**.
- In the **Schedule Type**, select **Basic** to build a schedule with the provided controls.

©2026 Tanium Inc. All Rights Reserved



- To view or edit the cron expression directly, select **Advanced - Define as a Cron Expression**, and use the **Advanced** field to edit the cron expression.

©2026 Tanium Inc. All Rights Reserved



Note: If a user that owns a scheduled connection is deleted, future scheduled instances of that connection do not run. For more information, see Issue: Scheduled connection owned by a deleted user no longer runs on page 243.

For more information about cron syntax, see Reference: Cron syntax for Connect on page 253.

Enable listening for an event

Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Enablement** section to send data when a configured event is detected:

- Select **Listen for this Event**.

Save and verify connection

1. After you enter the details for the connection, click **Save**.

   Tip: To save the connection and immediately run the connection, click **Run and Save**.

   If needed, resolve any errors or missing information. After the connection creates successfully, the connection details appear.

©2026 Tanium Inc. All Rights Reserved

2. To view details when the connection runs, click the **Logs** tab.
3. To view an individual run log, expand the row table. For more information about how to resolve errors, see Troubleshooting on page 234.

©2026 Tanium Inc. All Rights Reserved

Configuring file destinations

You can configure flat text or JSON files as your connection destination. By default, files are written to /opt/mounts/connect/ on a Tanium™ Appliance, or you can specify a file share mount for Connect. For more information, see Tanium Appliance User Guide: Configure solution module file share mounts. In a Windows environment, files are written to the \Program Files\Tanium\Tanium Module Server\services\connect-files\output directory by default.

Configure the file destination

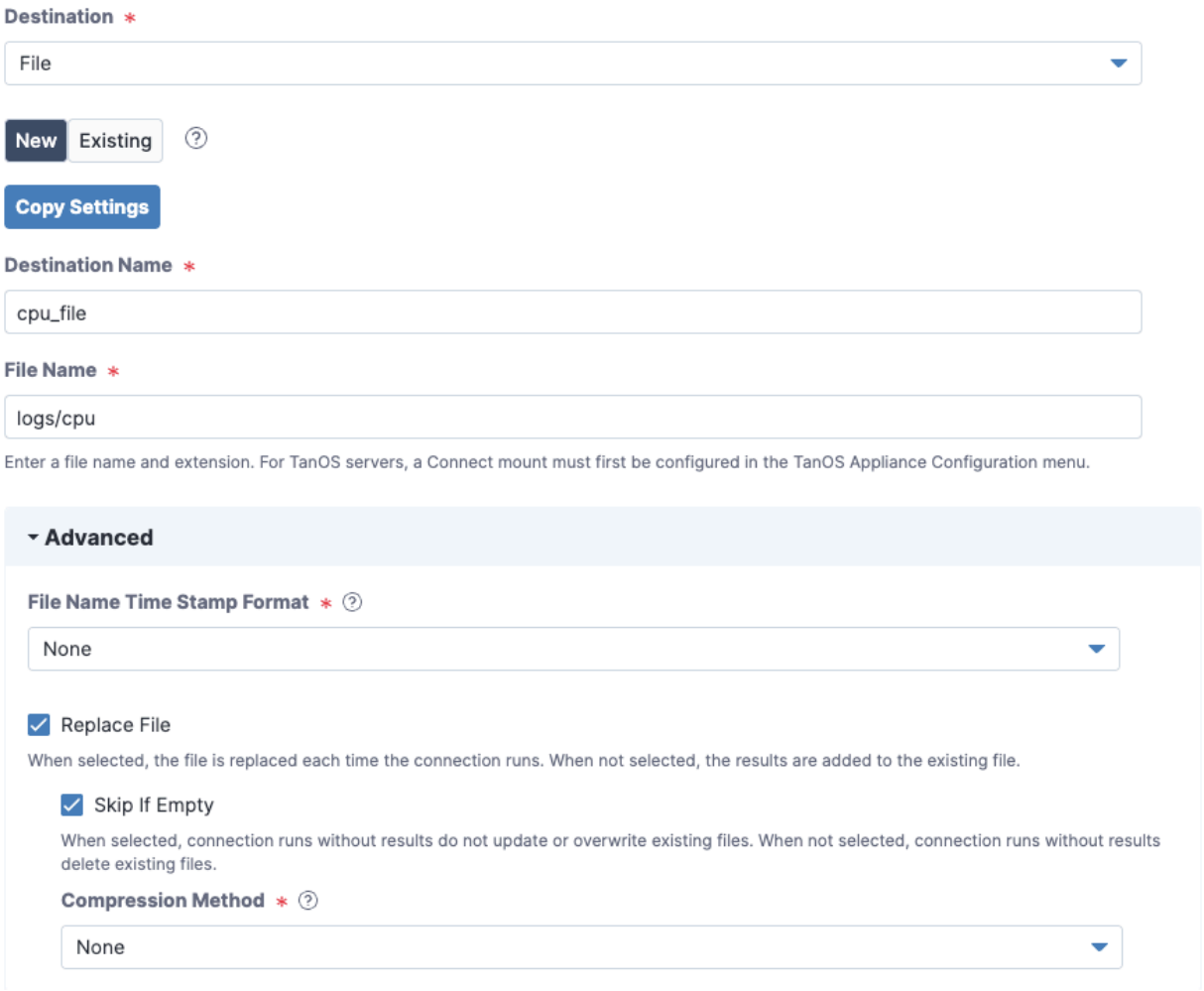
About this task

Specify details about the file that you want Connect to create, including the file name and how you want to save the file.

1. Name the destination.
    - Create a new destination: Specify a unique name to save the configuration information as a new destination. Select **New** and then enter a **Destination Name**
    - Copy an existing destination: Select **New**, and then click **Copy Settings**. Select a destination, click **Apply**, and update the **Destination Name**.
    - Reuse an existing destination: Select **Existing**, and then select a **Destination Name**.

      Note: Configure a unique destination per connection. If you edit the settings for a shared destination for one connection, any other connections that use the shared destination are affected, and connection runs might fail.

©2026 Tanium Inc. All Rights Reserved



2. Enter the file name with extension, or use a variable as listed in Reference: Variables on page 295. On a Tanium Appliance, files are written to /opt/mounts/connect by default, or you can specify a file share mount for Connect. For more information, see Tanium Appliance User Guide: Configure solution module file share mounts. On Windows, files are written to the \Program Files\Tanium\Tanium Module Server\services\connect-files\output directory.
    - The file name can include a subdirectory to create in the \Program Files\Tanium\Tanium Module Server\services\connect-files\output directory, or just the file name. For example, if you specify high_cpu_results\cpu_results.txt, the file is written to: \Program Files\Tanium\Tanium Module Server\services\connect-files\output\high_cpu_results\cpu_results.txt.

    - If you want to point to the file directory on the Module Server from another location, create a symbolic link with the mklink command. For example, if you wanted a symbolic link from the c:\logs\mylogs directory to the Connect logs directory, you might run:

©2026 Tanium Inc. All Rights Reserved

```
mklink /d "c:\logs\mylogs" "c:\Program Files\Tanium\Tanium Module Server\
services\connect-files\output\logs\mylogs"
```

- Include a file extension with the file name. The file extension does not need to match the format option you select in the **Format** section. Note the option that you select in the **Format** section does not add or change the file extension.

- You can choose to compress the resulting file as a GZIP or ZIP file. If you select a compression method, the file extension for the compression method is automatically added to the end of the file name.

3. (Optional) In the **Advanced** section, add a time stamp to the file name. Each time that the connection runs, it generates a new file with the time stamp in the file name. You can choose from the formats that are available, or enter your own time stamp format in ISO 8601 format.

4. (Optional) Replace or compress files, or remove empty files.
   Choose whether you want to replace the contents of the file when the connection runs, or if you want to append to the file contents. If you choose to replace the file contents, you can also compress the resulting file in zip or gzip format. You can also choose whether to create an empty file if the connection run generates no results and no file exists, based on the following configuration:

   - In all cases, create a new file if none exists and the connection run generated results.

   - If you clear **Replace File**, append to the existing file if the connection run generated results, or do nothing to the existing file if the connection run generated no results.

   - If you select **Replace File** and clear **Skip If Empty**, overwrite the existing file if the connection run generated results, or delete the existing file if the connection run generated no results.

   - If you select **Replace File** and select **Skip If Empty**, do nothing to the existing file, whether the connection run generated results or generated no results.

   > **Note:** If you configure the connection to add a time stamp to the file name, the **Replace File** option has no effect. The connection generates a new file with the time stamp in the file name each time that it runs.

Result

©2026 Tanium Inc. All Rights Reserved

Format data for file

You can choose to save your file in any of the available formats, as listed in Reference: Format types on page 262. Each format has slightly different configuration options, but all allow you to choose which column data to save.

©2026 Tanium Inc. All Rights Reserved

Configuring HTTP destinations

You can send data from Connect to a REST API. You can choose to send all the data to the REST API in a single batch or in multiple segments. Form data is not supported.

Configure a receiver

You must have a script on your server that can receive the HTTP request from Tanium.



Note: The following examples use a service that only accepts JSON format.

Node.js example

```
'use strict';
const restify = require('restify');
const fs = require('fs');
const server = restify.createServer({ name: 'File Receiver' });

let file = 0;
const dir = 'files';
if (!fs.existsSync(dir)) {
    fs.mkdirSync('files');
}

function postFile(req, res, next) {
    const fileName = `files/testing${file++}.txt`;
    const fileData = JSON.stringify(req.body);
    fs.writeFile(fileName, fileData, err => {
        if (err) {
            console.error('err', err);
            res.send(500, err);
        } else {
            console.log(`wrote to file ${fileName}`);
            res.send(200);
        }
        next();
    });
}

server.post('/post', postFile);
server.listen(17800, '0.0.0.0', () => {
    console.log(`${server.name} listening at ${server.url}`);
});
```

©2026 Tanium Inc. All Rights Reserved

Python example

```
from flask import Flask, request, Response
import os
import json
app = Flask(__name__)

file = 0
dir = 'files'
os.makedirs(dir, exist_ok=True)

@app.route("/post", methods=['POST'])
def connection_handle():
    global file
    file_data = json.dumps(request.get_json())
    file_name = f"{dir}/testing{file}.txt"
    file += 1
    try:
        file_handle = open(file_name, mode="w", encoding="utf-8")
        file_handle.write(file_data)
        file_handle.close()
    except:
        return Response('err', status=500, mimetype='application/json')
    return 'done'

app.run(host = '0.0.0.0', port = 17800)
```

Ruby example

```
require "sinatra"
require "fileutils"

set :port, 17800
set :bind, "0.0.0.0"

file = 0
dir = "files"
FileUtils.mkdir_p dir

post "/post" do
  file_data = JSON.parse request.body.read
  file_name = "#{dir}/testing#{file}.txt"
  file += 1
  begin
    File.write file_name, file_data.to_json
    puts "wrote to file #{file_name}"
    return
  rescue Exception => e
    status 500
    "err #{e}"
  end
end
```

Specify general connection information

1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section

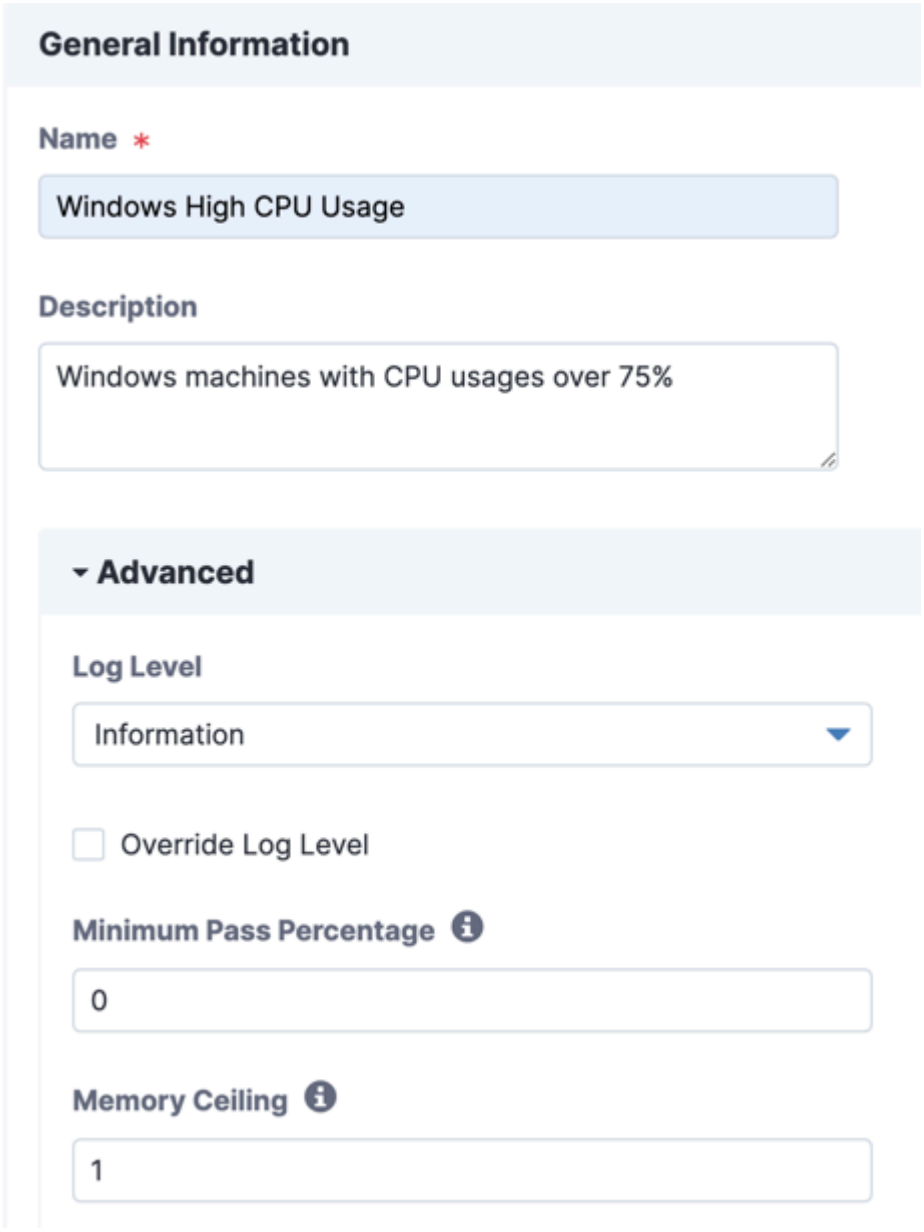
©2026 Tanium Inc. All Rights Reserved

and click **Create Connection**.

2. Enter a name and description for the connection.
3. (Optional) In the **General Information** section, expand **Advanced** to configure the following settings:

   Log Level

   By default, **Log Level** is set to **Information**. To reduce the amount of logging, you can set **Log Level** to **Warning**, **Error**, or **Fatal**.



   Override Log Level

   If you are debugging the connection, select **Override Log Level** to set a **Temporary Log**

©2026 Tanium Inc. All Rights Reserved

Level (such as **Trace** or **Debug**) on this connection for a selected **Number of Runs** (up to **24**). A scheduled or manual connection run, once started, counts towards the number of runs, regardless of the connection status. After the number of runs elapses, the logging for this connection returns to the **Log Level** you selected to prevent finer-grained logging from consuming additional resources for an indefinite number of runs.

Minimum Pass Percentage
: Minimum percentage of the expected rows that must be processed for the connection to succeed.

Memory Ceiling (GB)
: Maximum memory for the node process to run the connection. This defaults to 1 GB per connection, and cannot exceed the global maximum sum of memory for all running connections (by default, 8 GB). Increase this setting if a connection frequently exhibits out of memory errors while running.

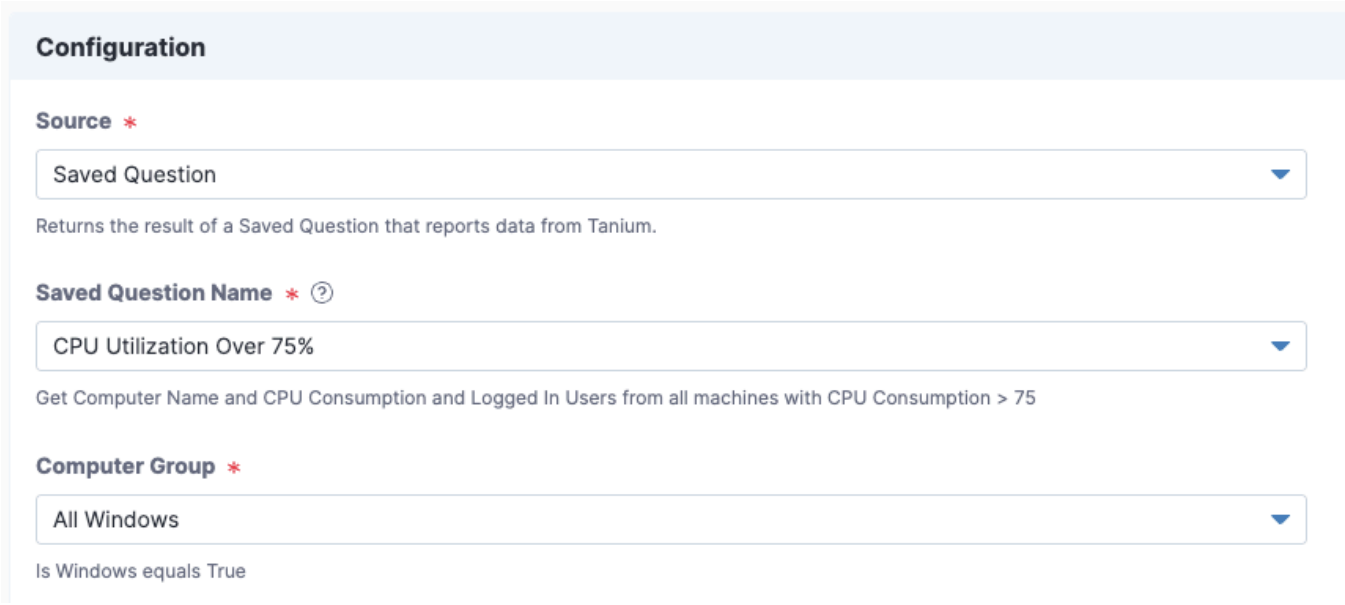
> **Note:** If the sum of simultaneously scheduled connection **Memory Ceiling** values exceed the global **Memory Ceiling**, connections run until the global **Memory Ceiling** is reached, then any remaining connections enter a waiting queue if you select the **Queue Connections** configuration setting, or fail if you clear the **Queue Connections** configuration setting.

Configure the connection source

The connection source determines what data you are sending to the destination. This data is usually information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

Figure 18. Connection source settings

©2026 Tanium Inc. All Rights Reserved



Note:

If a Tanium solution or source shows Critical, the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

Note: After you create a connection, you cannot update the connection source type, only the source configuration. If you want to change the source type, create a new connection.

For more information about available connection sources, see Connection sources on page 14.

Configure the HTTP destination

About this task

Specify the URL, method, and headers for the destination to which you want to send data.

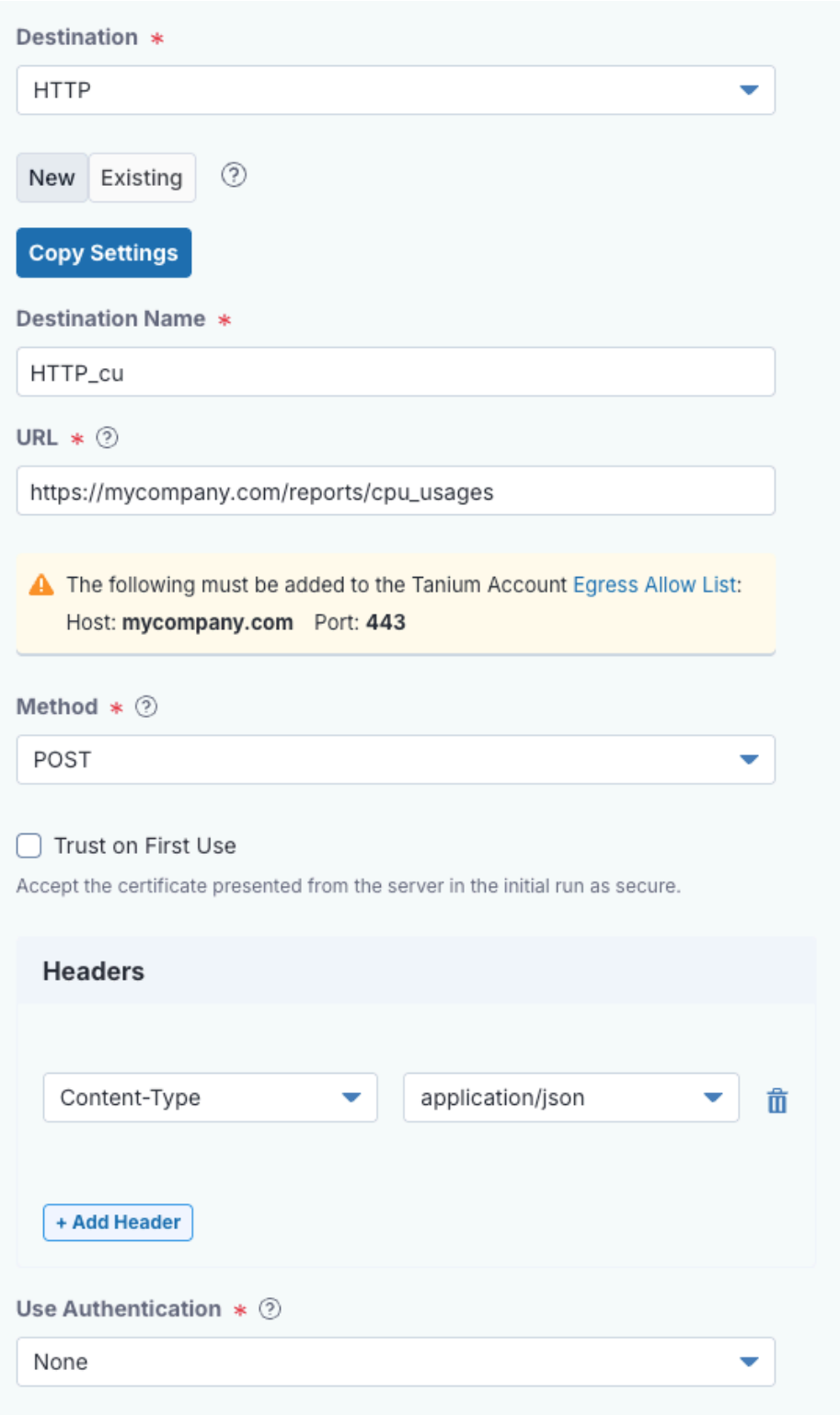
©2026 Tanium Inc. All Rights Reserved

Note: After you create a connection, you cannot update the connection destination type, only the destination configuration. If you want to change the destination, create a new connection.

1. Select HTTP for the destination and then provide a name for the destination.
    - Create a new destination: Specify a unique name to save the configuration information as a new destination. Select **New** and then enter a **Destination Name**
    - Copy an existing destination: Select **New**, and then click **Copy Settings**. Select a destination, click **Apply**, and update the **Destination Name**.
    - Reuse an existing destination: Select **Existing**, and then select a **Destination Name**.

      Note: Configure a unique destination per connection. If you edit the settings for a shared destination for one connection, any other connections that use the shared destination are affected, and connection runs might fail.

©2026 Tanium Inc. All Rights Reserved



2. Specify an HTTP or HTTPS URL for the REST API to which you want to send the data and the HTTP method that you want to use for the request. If you specify `https` for the URL, the connection validates the Transport Layer Security (TLS) certificate. You can select **Trust on First Use** to accept the certificate presented from the server and trust only that certificate for future connection runs.

©2026 Tanium Inc. All Rights Reserved

Tip: When you change certificates, you can edit the connection to remove the previous trusted certificate. This option is available after the connection runs and trusts the certificate.

3. Add any required headers. To specify multiple headers, click **+ Add Header**.



Note: Google is deprecating the legacy Backstory Ingestion API key authentication method for Google Security Operations (SecOps), formerly named Chronicle. Google requires OAuth2 or a Service Account JSON file for the direct Ingestion API. Connect does not support that authentication format. To send data to SecOps, set the destination **URL** to the endpoint URL from the SecOps Webhook Feed and add two headers to the destination: `X-goog-api-key` with an API key restricted to Chronicle and `X-Webhook-Access-Key` with the Webhook Feed secret. For the current deprecation timeline, see Google Cloud: Chronicle deprecations.

4. Select an authentication method from **Use Authentication**. Configure one of the following:
   - **None** - Do not authenticate against the HTTP destination.
   - **Basic Authentication** - Authenticate against the HTTP destination with a **User Name** and **Password**.
   - **OAuth2 Client Credentials** - Authenticate against the HTTP resource OAuth2.0 authorization server with a **Client ID**, **Secret** password, and **Authentication URL**. Do not add an Authorization header if you select **OAuth2 Client Credentials**.
   - **Header Authentication** - Authenticate against the HTTP destination using an HTTP Authorization request header containing the **Auth Header Name** and **Secret** value.

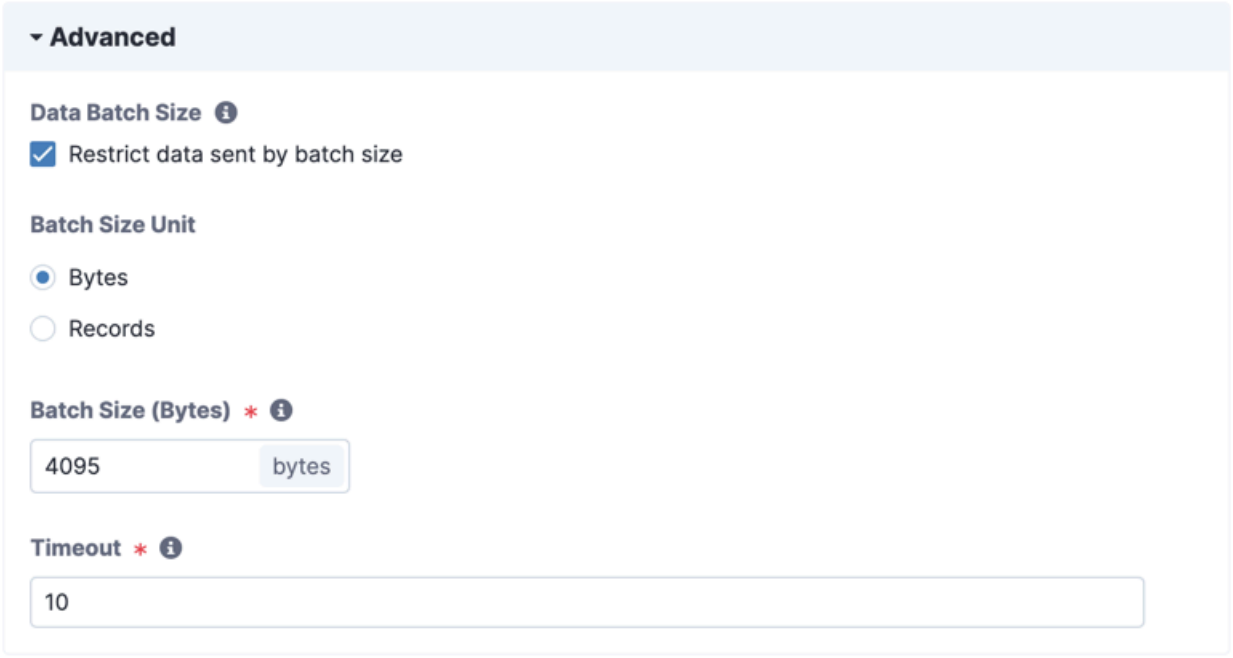
     Note: For connections to Splunk instances that use the HTTP destination, enter `Authorization` for **Auth Header Name** and use the format `Splunk <token-string>` for the **Secret** value. Replace `<token-string>` with the token string from Splunk.
   - **IBM Cloud IAM - API Key** - Authenticate against an IBM Cloud HTTP destination with an IAM token generated from the **Secret** API key you enter.

©2026 Tanium Inc. All Rights Reserved

> **Note:** Click **Test Authentication** for the **OAuth2 Client Credentials** or **IBM Cloud IAM - API Key** authentication methods to confirm that you entered the proper authentication information.

> **Note:** If you specify `http` for the URL, authentication information is encrypted at rest, but passed unencrypted to the destination.

5. If you need to configure the batch size or the timeout, expand **Advanced**.



   - Select **Restrict data sent by batch size** to configure a **Batch Size Unit** in number of **Bytes** or number of **Records**. Configuring a batch size creates multiple POST requests when data is sent to the destination. Each request contains up to the configured number of records, or up to the configured number of bytes, until all data is sent. If the **Batch Size** is `0`, all records are sent in one POST request to the destination.

     > **Note:** If you configure a **Batch Size** in number of **Bytes**, a POST request can exceed this if a single record is larger than the configured number of bytes.

   - Configure a connection **Timeout** in number of seconds.

Configure filters

©2026 Tanium Inc. All Rights Reserved

(Optional) In the **Configure Output** > **Filters** section, you can specify filters to modify the data that you are getting from your connection source before it is sent to the destination.

For more information about the types of filters you can configure, see Reference: Filtering options on page 257.

Format data for HTTP

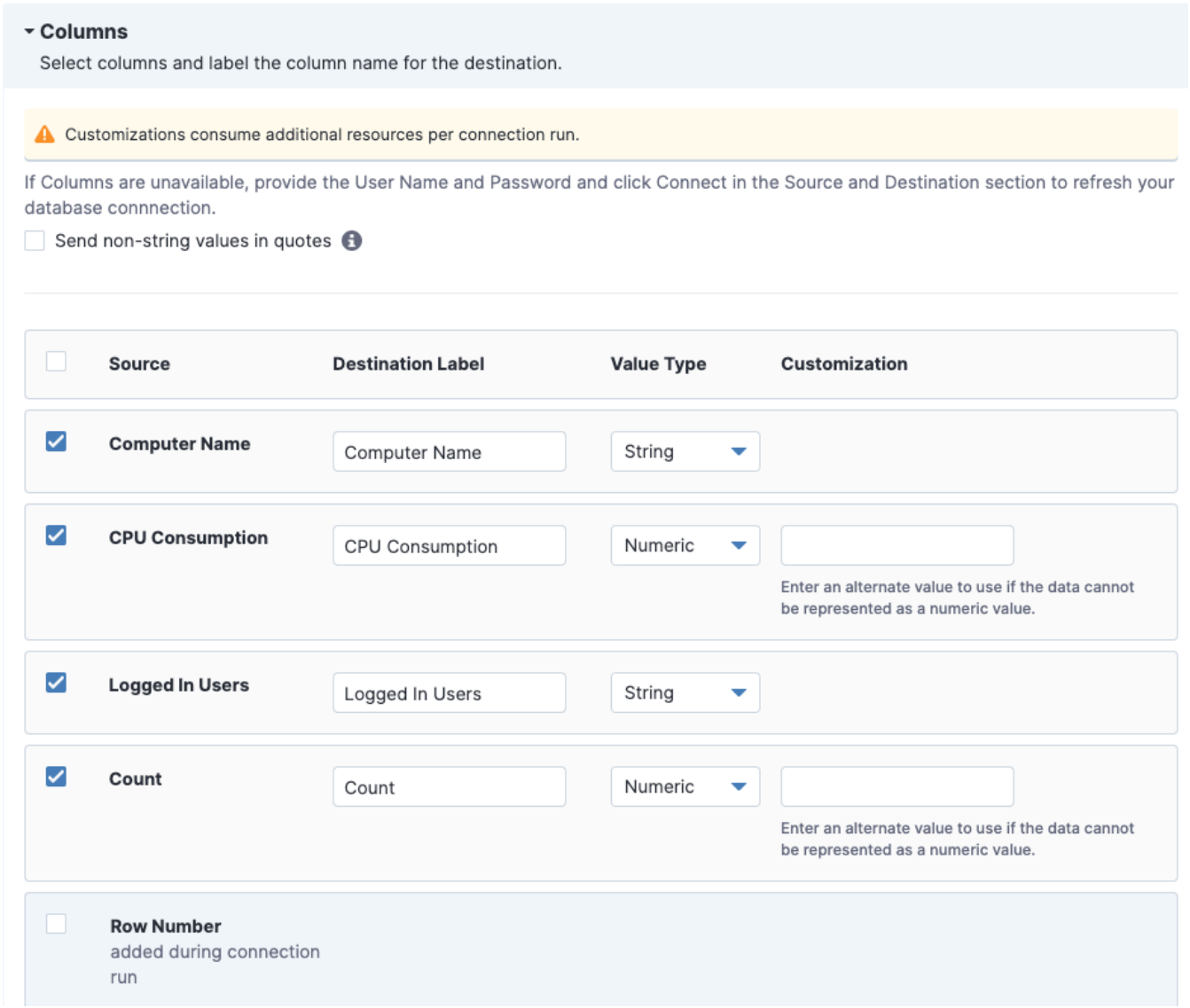
You can choose to save your file in all of the available formats, as listed in Reference: Format types on page 262. The default format is JSON. Each format has slightly different configuration options, but all allow you to choose which column data to save.

> **Note:** If the data format supports row delimiter characters, update the characters to ensure that individual rows are sent in a format that the destination can parse. You can define one or more of `\n` (new line), `\r` (carriage return), and `\t` (tab).

In the **Configure Output** > **Columns** section, you can change the **Destination Label** of each column and **Value Type** to force the column to be a String, Numeric, or Date/Time value.

Figure 19. Columns section with Destination Label and Value Type fields

©2026 Tanium Inc. All Rights Reserved



If you choose **Numeric** for the value, you can specify a default value that is used if the data cannot be coerced into a numeric value. You can specify any negative or positive number.

If you choose **Date/Time** for the value, specify the format that you want to use for the column. For more information about how to use a variable, see Time stamp variables on page 297.

For more information about column customizations, see Reference: Column customizations on page 248.

Schedule the connection

Connections can run at a highly configurable time interval, such as multiple times per hour, day, week, or month.

©2026 Tanium Inc. All Rights Reserved

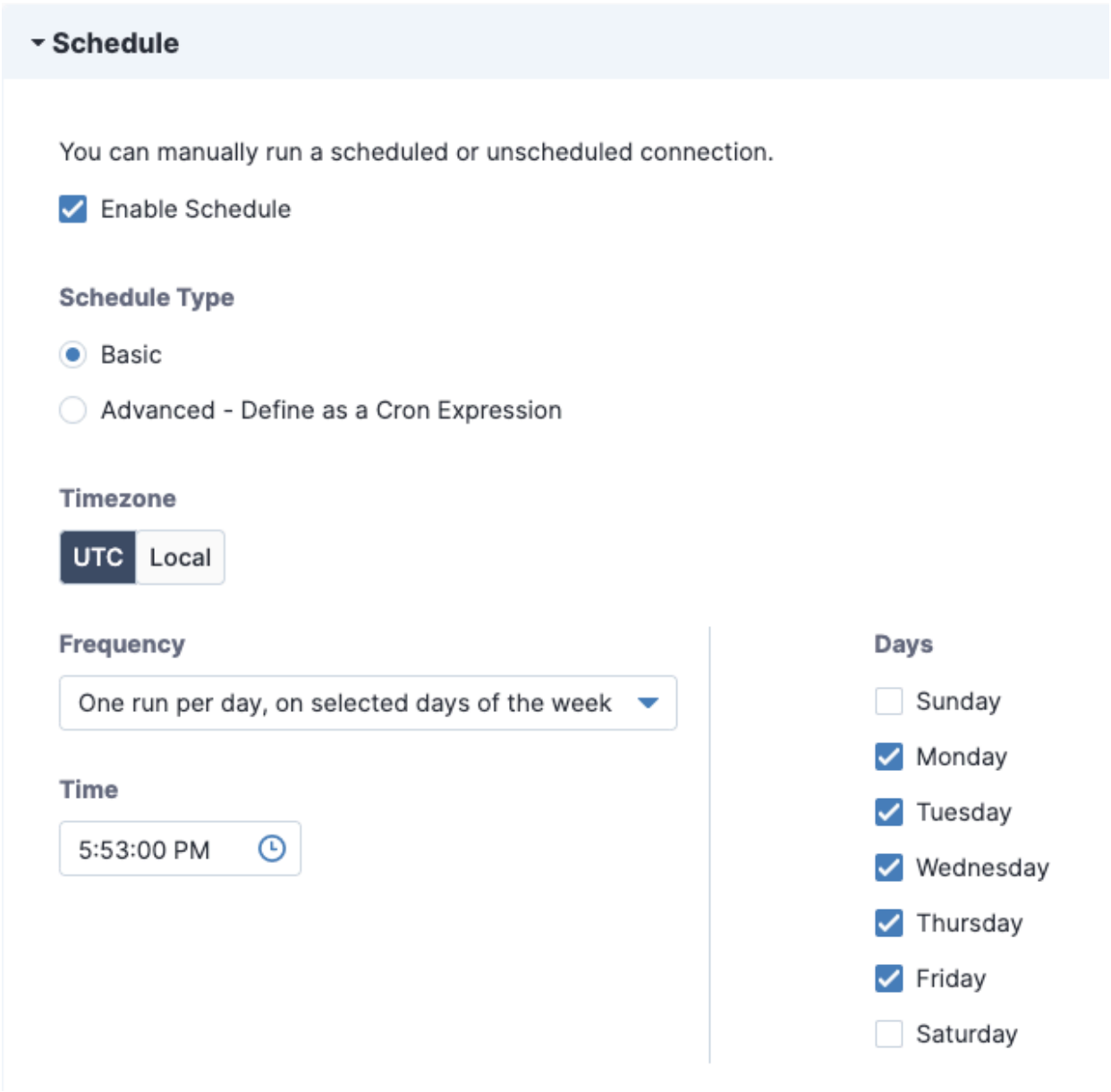
Important: Connections scheduled to run during an upgrade of Connect, or any Tanium solution configured as a connection source, might be interrupted or fail. Schedule your connections to run at a different time than your Tanium upgrades.

Note: If you do not enable the schedule, the connection only runs when you manually run it, unless you configure an **Event** source. Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Schedule** section to update the schedule:

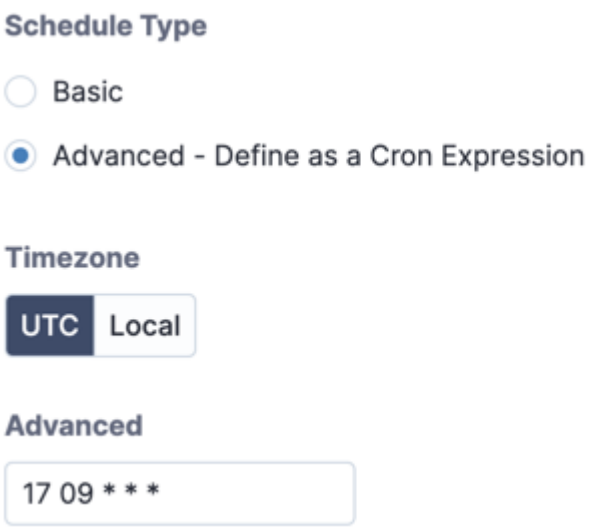
- Select **Enable schedule**.
- In the **Schedule Type**, select **Basic** to build a schedule with the provided controls.

©2026 Tanium Inc. All Rights Reserved



- To view or edit the cron expression directly, select **Advanced - Define as a Cron Expression**, and use the **Advanced** field to edit the cron expression.

©2026 Tanium Inc. All Rights Reserved



Note: If a user that owns a scheduled connection is deleted, future scheduled instances of that connection do not run. For more information, see Issue: Scheduled connection owned by a deleted user no longer runs on page 243.

For more information about cron syntax, see Reference: Cron syntax for Connect on page 253.

Enable listening for an event

Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Enablement** section to send data when a configured event is detected:

- Select **Listen for this Event**.

Save and verify connection

1. After you enter the details for the connection, click **Save**.

   Tip: To save the connection and immediately run the connection, click **Run and Save**.

   If needed, resolve any errors or missing information. After the connection creates successfully, the connection details appear.

©2026 Tanium Inc. All Rights Reserved

2. To view details when the connection runs, click the **Logs** tab.
3. To view an individual run log, expand the row table. For more information about how to resolve errors, see Troubleshooting on page 234.

©2026 Tanium Inc. All Rights Reserved

Configuring Microsoft Azure Monitor destinations

You can send data from Connect to Microsoft Azure Monitor. The **Azure Monitor** destination uses the Logs Ingestion API found within Azure Monitor to send data to Log Analytics Workspace tables. You can choose to send all the data to Azure in a single batch or in multiple segments.

For more information, see Microsoft Azure documentation: Logs Ingestion API in Azure Monitor.

> **Note:** Configure a network allow list rule for the Ingestion Endpoint URL. To find the Logs Ingestion URL, open Azure Portal and go to **Azure Portal** > **Monitor** > **Data Collection Endpoints**.

> **Note:** The Azure Monitor destination also authenticates with Microsoft Entra using the Azure App Registration client credentials, which requires a network allow list rule for the Microsoft Entra token endpoint: login.microsoftonline.com:443 for commercial Azure tenants or login.microsoftonline.us:443 for Azure Government tenants.

Microsoft Azure requirements

- Microsoft Azure App Registration (Client ID, Client Secret, Tenant ID)
- Azure Monitor Logs Ingestion URL
- Data Collection Rule (DCR) with a custom stream

©2026 Tanium Inc. All Rights Reserved

Important: Contrary to the deprecated Configuring Microsoft Log Analytics destinations on page 179 destination, the Microsoft Azure destination does not automatically create columns from incoming data. The `streamDeclarations.columns` array in your DCR must include every column that Tanium Connect sends. This list must match the connection output configuration exactly. Before the transformation runs, Microsoft Azure silently drops any column that Tanium Connect sends that is not declared in `streamDeclarations.columns`. No error is logged on either side. The following example shows a valid `streamDeclarations` block that includes all Tanium Connect output columns:

```
"streamDeclarations": {
  "Custom-YourTableName_CL": {
    "columns": [
      { "name": "TimeGenerated", "type": "datetime" },
      { "name": "connection_name", "type": "string" },
      { "name": "timestamp", "type": "string" },
      { "name": "message", "type": "string" }
    ]
  }
}
```

Tip: Set `transformKql` to `source` for a passthrough transformation unless you have a specific reason to remap fields. If you use `source | project col1, col2`, Microsoft Azure drops any column not listed, even if it is declared in `streamDeclarations.columns`.

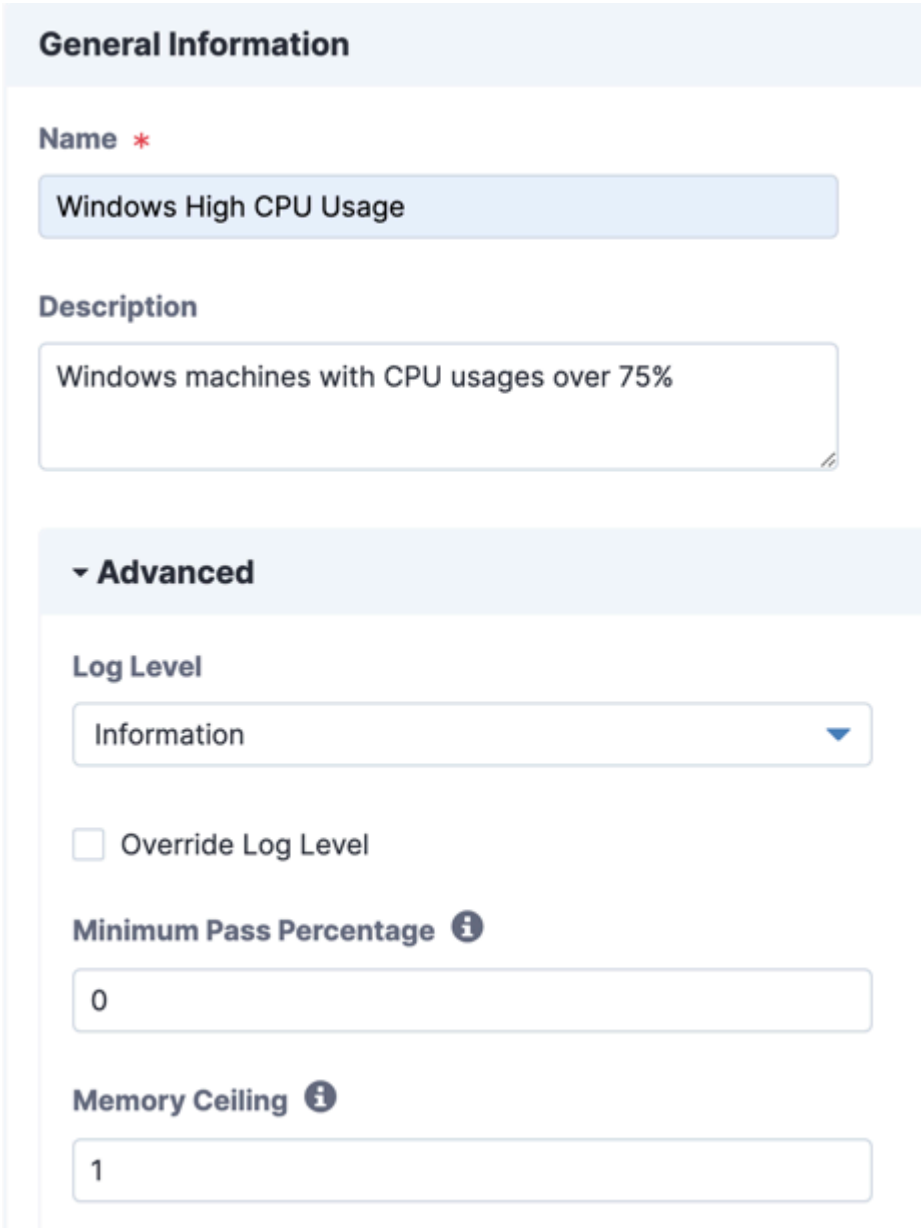
Specify general connection information

1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click **Create Connection**.
2. Enter a name and description for the connection.
3. (Optional) In the **General Information** section, expand **Advanced** to configure the following settings:

   Log Level

   By default, **Log Level** is set to **Information**. To reduce the amount of logging, you can set **Log Level** to **Warning**, **Error**, or **Fatal**.

©2026 Tanium Inc. All Rights Reserved



Override Log Level

If you are debugging the connection, select **Override Log Level** to set a **Temporary Log Level** (such as **Trace** or **Debug**) on this connection for a selected **Number of Runs** (up to **24**). A scheduled or manual connection run, once started, counts towards the number of runs, regardless of the connection status. After the number of runs elapses, the logging for this connection returns to the **Log Level** you selected to prevent finer-grained logging from consuming additional resources for an indefinite number of runs.

Minimum Pass Percentage

Minimum percentage of the expected rows that must be processed for the connection to succeed.

©2026 Tanium Inc. All Rights Reserved

Memory Ceiling (GB)

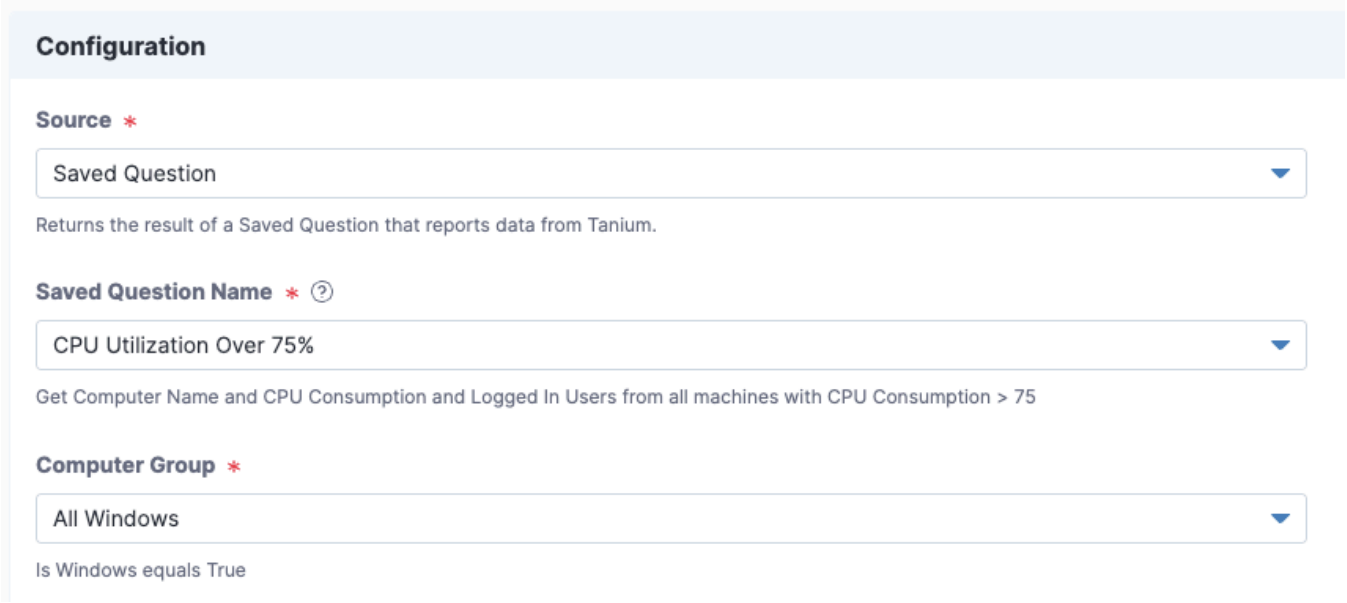
Maximum memory for the node process to run the connection. This defaults to 1 GB per connection, and cannot exceed the global maximum sum of memory for all running connections (by default, 8 GB). Increase this setting if a connection frequently exhibits out of memory errors while running.

> **Note:** If the sum of simultaneously scheduled connection **Memory Ceiling** values exceed the global **Memory Ceiling**, connections run until the global **Memory Ceiling** is reached, then any remaining connections enter a waiting queue if you select the **Queue Connections** configuration setting, or fail if you clear the **Queue Connections** configuration setting.

Configure the connection source

The connection source determines what data you are sending to the destination. This data is usually information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

Figure 20. Connection source settings



©2026 Tanium Inc. All Rights Reserved

Note:

If a Tanium solution or source shows Critical, the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

Note: After you create a connection, you cannot update the connection source type, only the source configuration. If you want to change the source type, create a new connection.

For more information about available connection sources, see Connection sources on page 14.

Configure the Microsoft Azure Monitor destination

About this task

Specify the Microsoft Azure Monitor settings for the Azure instance to which you want to send data.

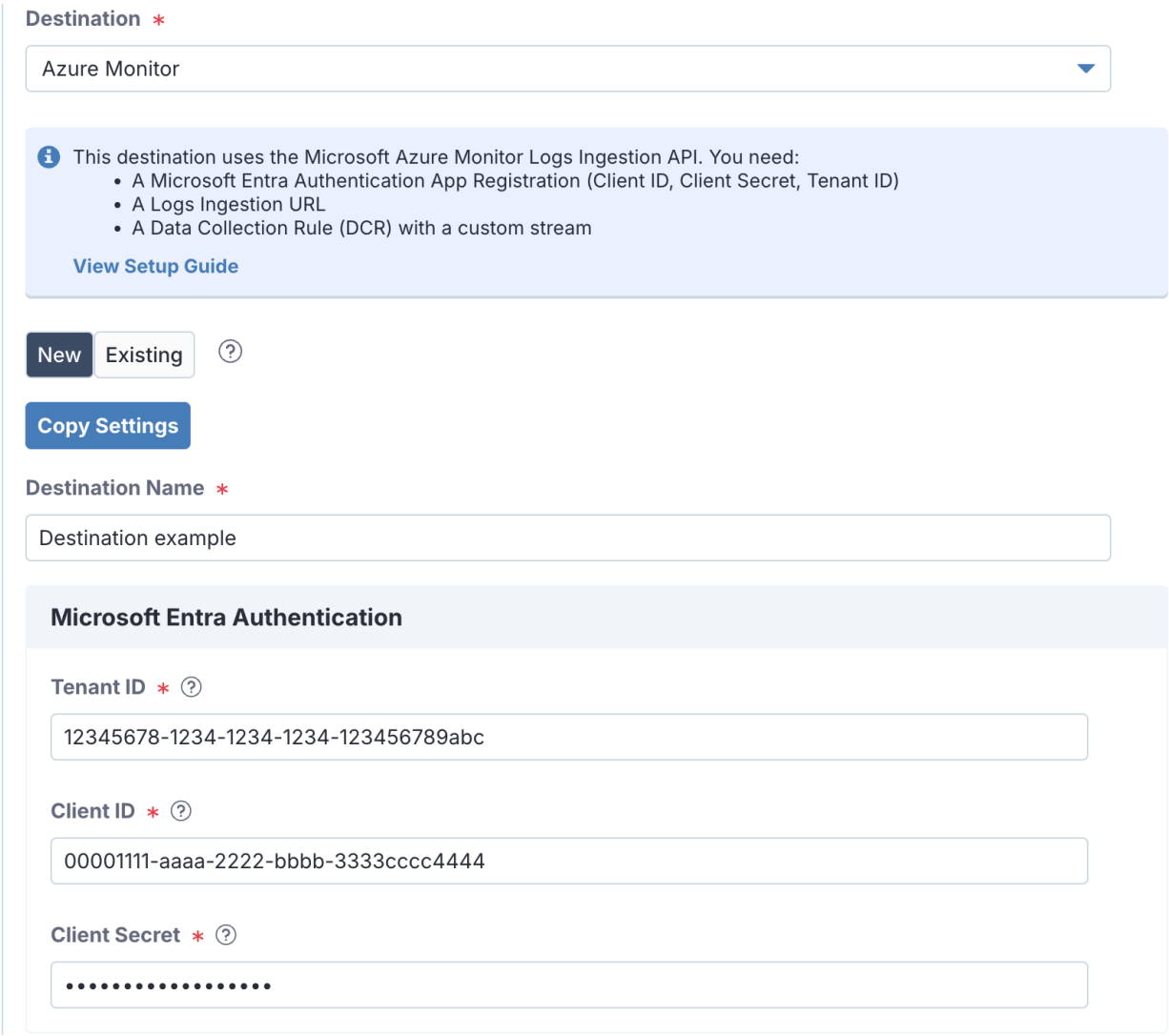
Note: After you create a connection, you cannot update the connection destination type, only the destination configuration. If you want to change the destination, create a new connection.

Note: Individual field values in a row are limited to 32 KB. Values exceeding that limit are truncated to 32 KB.

1. Select Azure Monitor for the destination and then provide a name for the destination.
    - Create a new destination: Specify a unique name to save the configuration information as a new destination. Select **New** and then enter a **Destination Name**
    - Copy an existing destination: Select **New**, and then click **Copy Settings**. Select a destination, click **Apply**, and update the **Destination Name**.
    - Reuse an existing destination: Select **Existing**, and then select a **Destination Name**.

©2026 Tanium Inc. All Rights Reserved

> **Note:** Configure a unique destination per connection. If you edit the settings for a shared destination for one connection, any other connections that use the shared destination are affected, and connection runs might fail.



2. Enter the Microsoft Azure App Registration Tenant ID in the **Tenant ID** field. For more information about how to find the 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.

3. Enter the Microsoft Azure App Registration (Client) ID in the **Client ID** field.
4. Enter the Microsoft Azure App Registration Client Secret in the **Client Secret** field.

©2026 Tanium Inc. All Rights Reserved

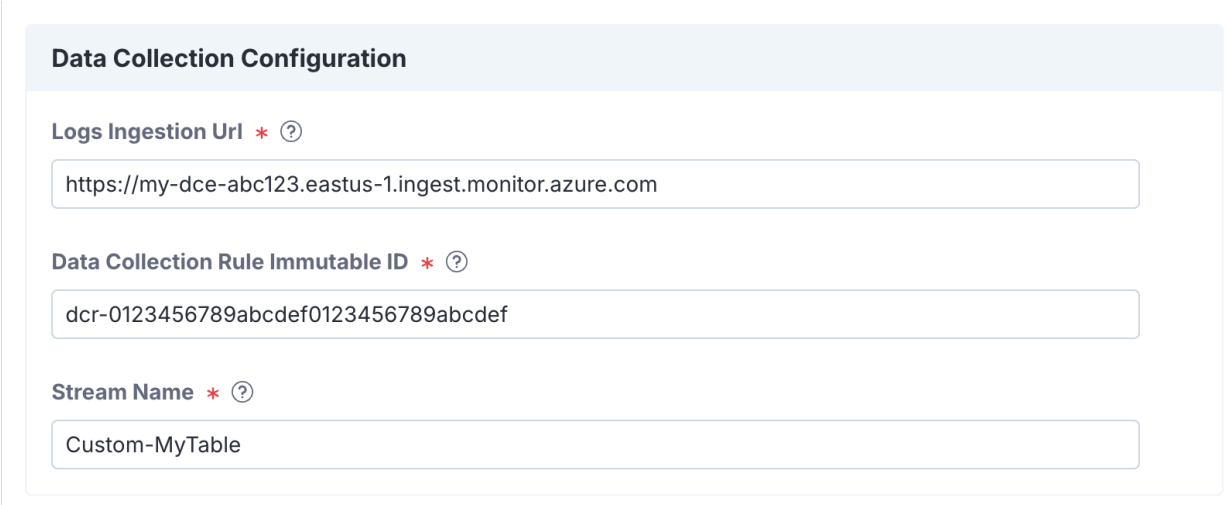
Important: Be sure to provide the *value* of the client secret, and not the ID. The value only appears when you add the secret in the Microsoft Entra admin center and does not appear again. For more information, see Microsoft Entra documentation: Add a client secret.

5. Specify **Data Collection Configuration** settings:
    a. Enter the Logs ingestion URL in the **Logs Ingestion URL** field. To find the Logs Ingestion URL, open Azure Portal and go to **Azure Portal** > **Monitor** > **Data Collection Endpoints**.
    b. Enter the DCR immutable ID in the **Data Collection Rule Immutable ID** field. You can find the DCR Immutable ID on the **Overview** tab of the DCR in Microsoft Azure.

    Note: The DCR Immutable ID is in the format `dcr-` + 32 hex characters. For example, `dcr-0123456789abcdef0123456789abcdef` is a valid DCR Immutable ID.

    c. Enter your DCR Stream Name in the **Stream Name** field. You can find the DCR Stream Name in the DCR JSON view.

    Note: The DCR Stream Name is in the format `Custom-DCR Stream Name`. For example, `Custom-MyTable` is a valid DCR Stream Name.



6. If you need to configure a custom batch size, expand **Advanced**.
    - Enter a **Batch Size** for the maximum number of records per post. The default **Batch Size** is 500.

    Note: Each request is limited to 30 MB.

©2026 Tanium Inc. All Rights Reserved

Result

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: Data collection rules (DCRs) in Azure Monitor
- Microsoft Azure documentation: Assign Azure roles using the Azure portal

Configure filters

(Optional) In the **Configure Output** > **Filters** section, you can specify filters to modify the data that you are getting from your connection source before it is sent to the destination.

For more information about the types of filters you can configure, see Reference: Filtering options on page 257.

Format data for Microsoft Azure Monitor

You must send your file in JSON format, as listed in Reference: Format types on page 262.

Important: The Microsoft Azure Logs Ingestion API cannot support source columns with more than one space.

- ✗ `Computer Serial Number`
- ✓ `ComputerSerial Number`
- ✓ `Computer SerialNumber`
- ✓ `ComputerSerialNumber`

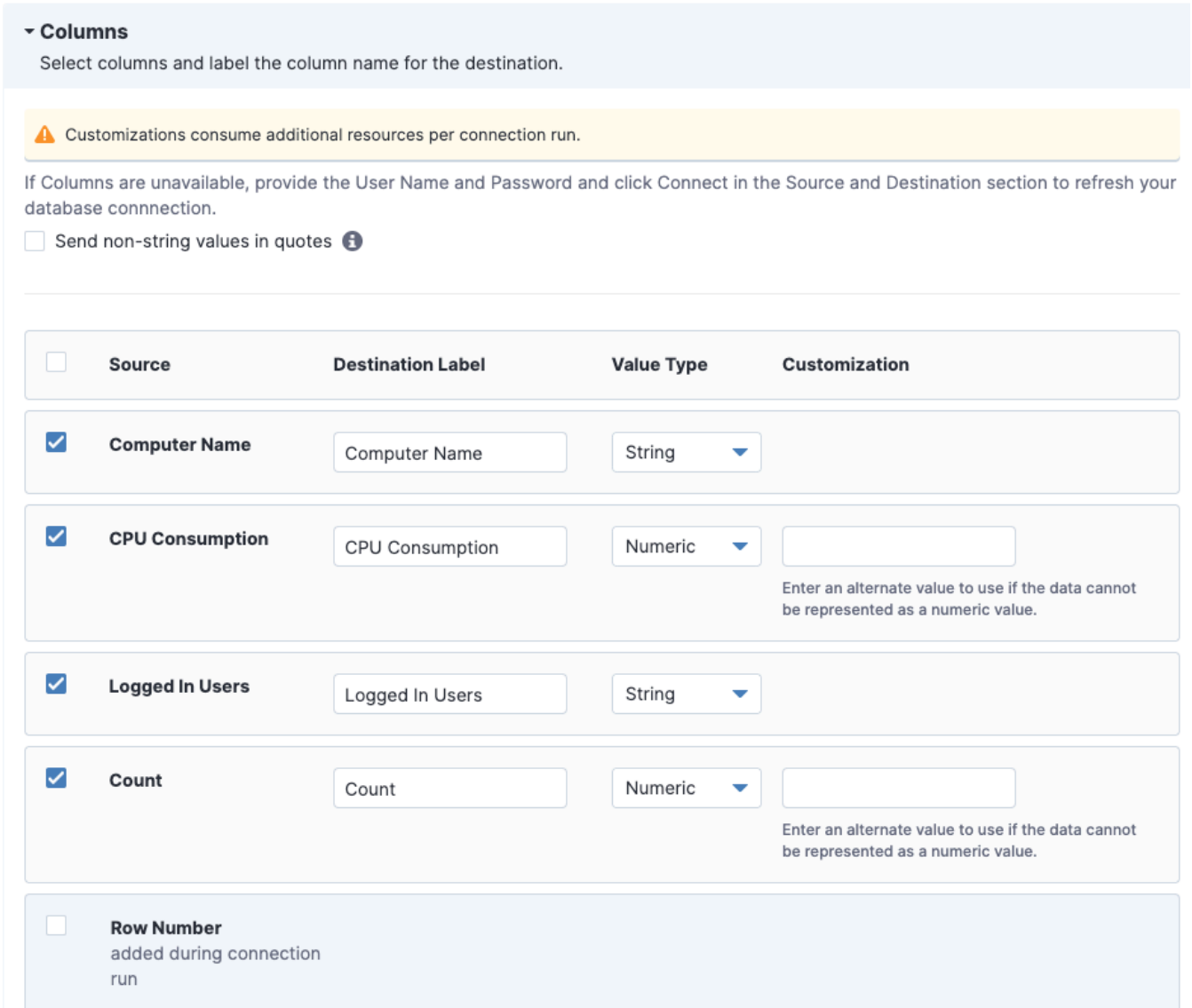
©2026 Tanium Inc. All Rights Reserved

Important: Select **Generate Document** and clear **Wrap data with source** to properly structure the JSON file for Microsoft Azure. Connection runs fail if you do not properly structure the JSON file.

Note: Azure Monitor table column names are limited to a maximum of 45 characters.

In the **Configure Output** > **Columns** section, you can change the **Destination Label** of each column and **Value Type** to force the column to be a String, Numeric, or Date/Time value.

Figure 21. Columns section with Destination Label and Value Type fields



If you choose **Numeric** for the value, you can specify a default value that is used if the data cannot be coerced into a numeric value. You can specify any negative or positive number.

©2026 Tanium Inc. All Rights Reserved

If you choose **Date/Time** for the value, specify the format that you want to use for the column. For more information about how to use a variable, see Time stamp variables on page 297.

For more information about column customizations, see Reference: Column customizations on page 248.

Note: After a connection run successfully completes, it may take several minutes or more for Azure Monitor to populate the destination table with the data.

Note: To find the data in Microsoft Azure, open Azure Portal, go to **Azure Portal** > **Workspace** > **Logs**, and query your table name.

Schedule the connection

Connections can run at a highly configurable time interval, such as multiple times per hour, day, week, or month.

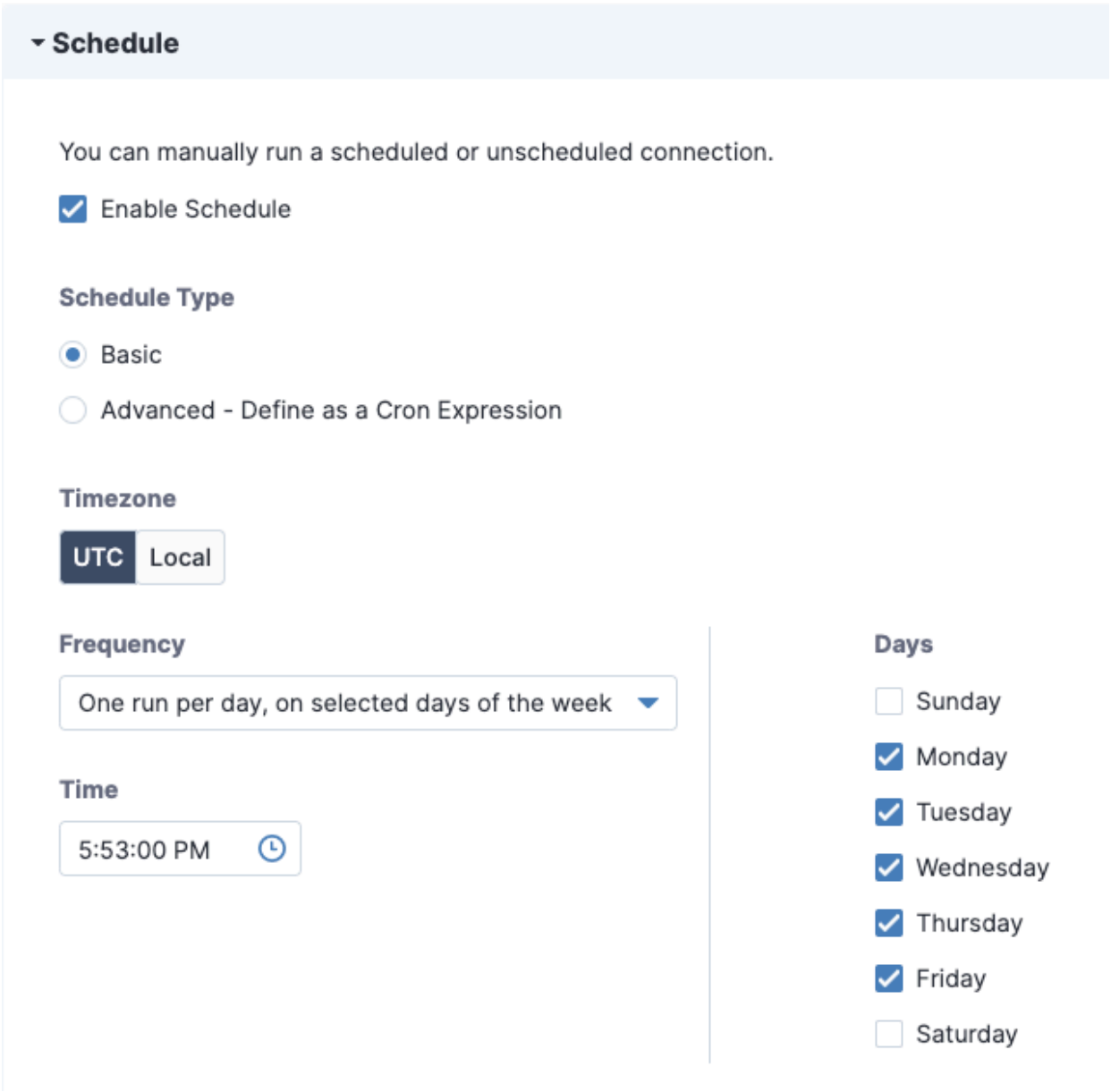
Important: Connections scheduled to run during an upgrade of Connect, or any Tanium solution configured as a connection source, might be interrupted or fail. Schedule your connections to run at a different time than your Tanium upgrades.

Note: If you do not enable the schedule, the connection only runs when you manually run it, unless you configure an **Event** source. Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Schedule** section to update the schedule:

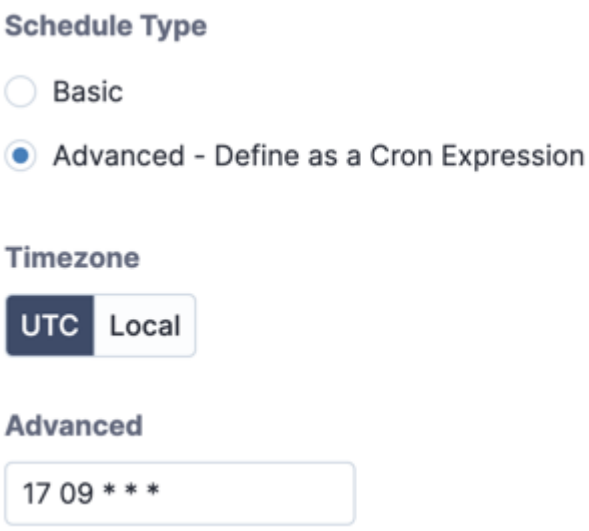
- Select **Enable schedule**.
- In the **Schedule Type**, select **Basic** to build a schedule with the provided controls.

©2026 Tanium Inc. All Rights Reserved



- To view or edit the cron expression directly, select **Advanced - Define as a Cron Expression**, and use the **Advanced** field to edit the cron expression.

©2026 Tanium Inc. All Rights Reserved



Note: If a user that owns a scheduled connection is deleted, future scheduled instances of that connection do not run. For more information, see Issue: Scheduled connection owned by a deleted user no longer runs on page 243.

For more information about cron syntax, see Reference: Cron syntax for Connect on page 253.

Enable listening for an event

Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Enablement** section to send data when a configured event is detected:

- Select **Listen for this Event**.

Save and verify connection

1. After you enter the details for the connection, click **Save**.

   Tip: To save the connection and immediately run the connection, click **Run and Save**.

   If needed, resolve any errors or missing information. After the connection creates successfully, the connection details appear.

©2026 Tanium Inc. All Rights Reserved

2. To view details when the connection runs, click the **Logs** tab.
3. To view an individual run log, expand the row table. For more information about how to resolve errors, see Troubleshooting on page 234.

©2026 Tanium Inc. All Rights Reserved

Configuring Microsoft Log Analytics destinations

Important: The Microsoft Log Analytics destination described in this chapter is deprecated and will be removed in a future release. Microsoft support for the HTTP Data Collector API discontinues in September 2026. Tanium support for Microsoft Azure continues through the **Azure Monitor** destination. To avoid disruptions, migrate your existing connections for **Microsoft Log Analytics** destinations to **Azure Monitor** destinations. For more information, see Configuring Microsoft Azure Monitor destinations on page 166.

You can send data from Connect to Microsoft Azure Monitor and query the data using Azure Log Analytics. You can choose to send all the data to Azure in a single batch or in multiple segments.

Note: Configure a network allow list rule for your Azure integration FQDN in the format `workspace-id.azure-domain`. The workspace ID is a 32 character hexadecimal string provided by Microsoft. The default Azure domain is `ods.opinsights.azure.com`, but you can configure your connection with a custom domain. After you configure your connection, you can view the connection details and copy the **Workspace ID** and **Azure Domain** field values. For more information about how to view details for a connection, see View connection status on page 62.

Microsoft Azure requirements

- Azure Log Analytics Workspace ID
- Azure Log Analytics Primary key
- table in the log data schema, used to store your Tanium data

Specify general connection information

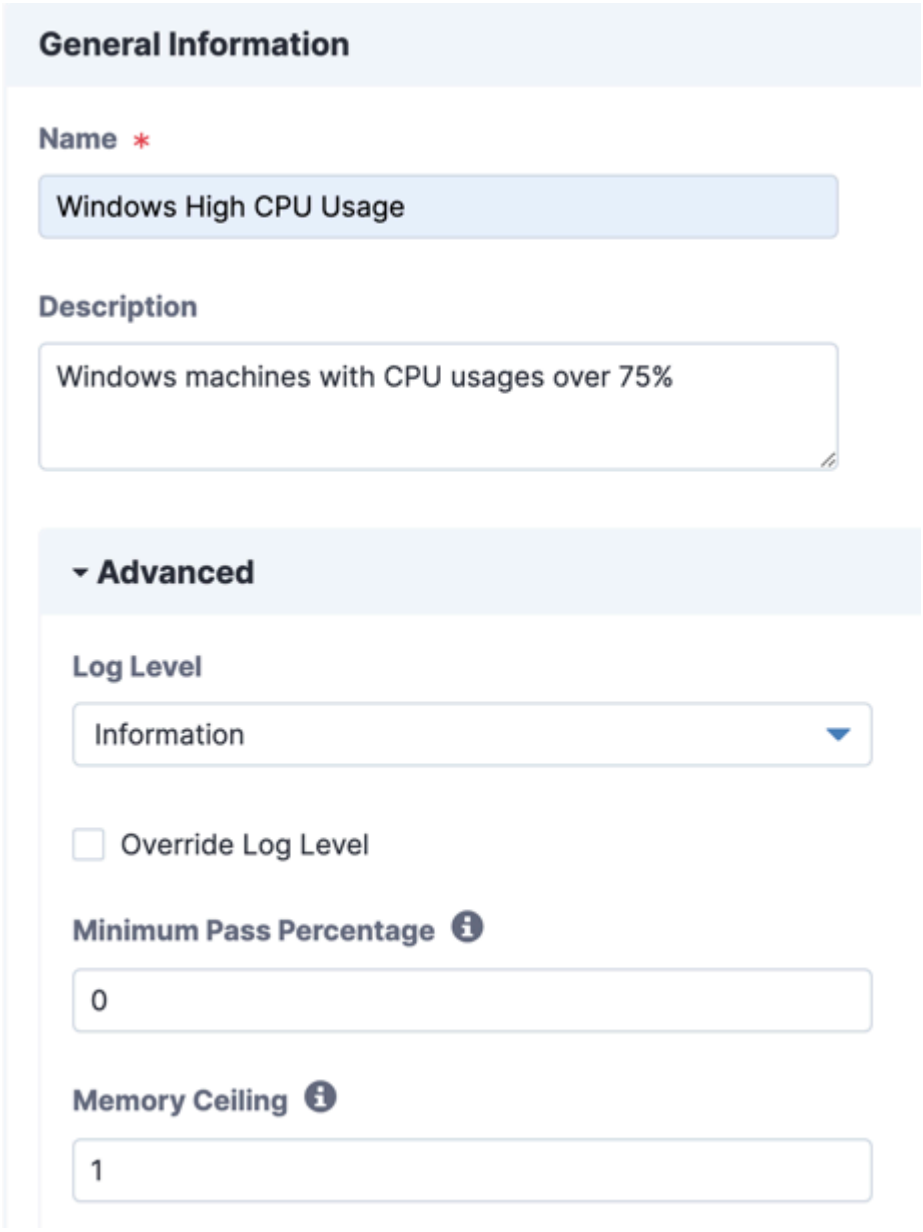
1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click **Create Connection**.

©2026 Tanium Inc. All Rights Reserved

2. Enter a name and description for the connection.
3. (Optional) In the **General Information** section, expand **Advanced** to configure the following settings:

   Log Level

   By default, **Log Level** is set to **Information**. To reduce the amount of logging, you can set **Log Level** to **Warning**, **Error**, or **Fatal**.



   Override Log Level

   If you are debugging the connection, select **Override Log Level** to set a **Temporary Log Level** (such as **Trace** or **Debug**) on this connection for a selected **Number of Runs** (up to **24**). A scheduled or manual connection run, once started, counts towards the number of

©2026 Tanium Inc. All Rights Reserved

runs, regardless of the connection status. After the number of runs elapses, the logging for this connection returns to the **Log Level** you selected to prevent finer-grained logging from consuming additional resources for an indefinite number of runs.

Minimum Pass Percentage
: Minimum percentage of the expected rows that must be processed for the connection to succeed.

Memory Ceiling (GB)
: Maximum memory for the node process to run the connection. This defaults to 1 GB per connection, and cannot exceed the global maximum sum of memory for all running connections (by default, 8 GB). Increase this setting if a connection frequently exhibits out of memory errors while running.

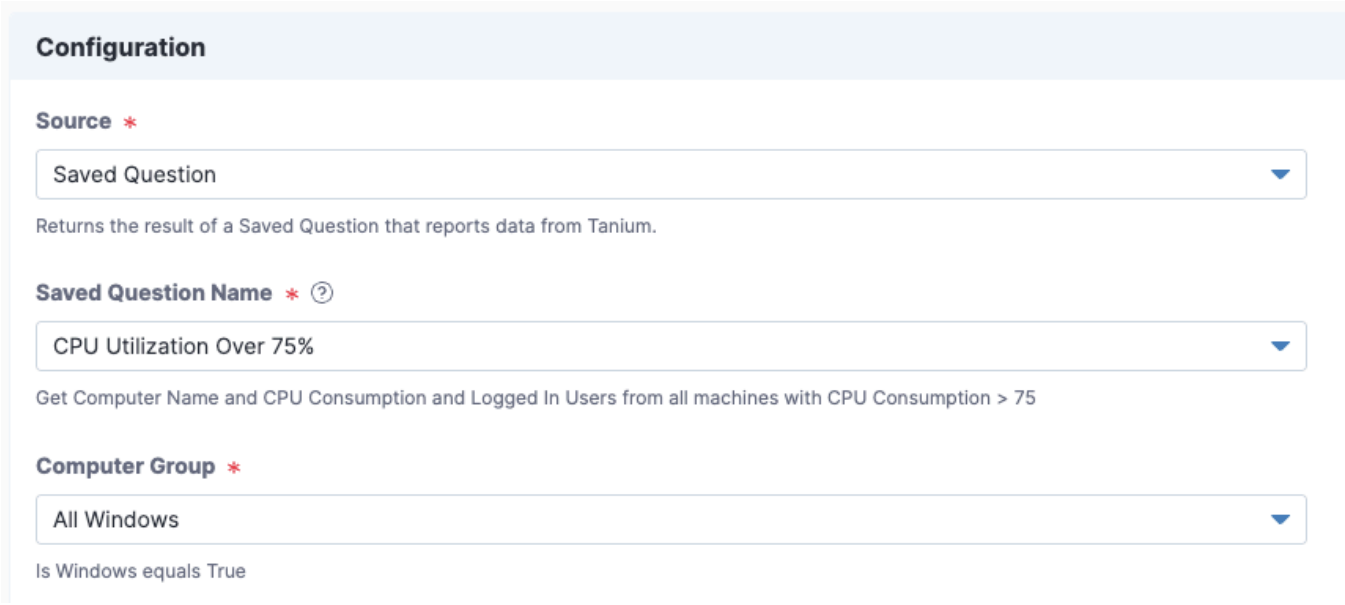
> **Note:** If the sum of simultaneously scheduled connection **Memory Ceiling** values exceed the global **Memory Ceiling**, connections run until the global **Memory Ceiling** is reached, then any remaining connections enter a waiting queue if you select the **Queue Connections** configuration setting, or fail if you clear the **Queue Connections** configuration setting.

Configure the connection source

The connection source determines what data you are sending to the destination. This data is usually information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

Figure 22. Connection source settings

©2026 Tanium Inc. All Rights Reserved



Note:

If a Tanium solution or source shows Critical, the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

Note: After you create a connection, you cannot update the connection source type, only the source configuration. If you want to change the source type, create a new connection.

For more information about available connection sources, see Connection sources on page 14.

Configure the Microsoft Log Analytics destination

About this task

Specify the Azure Log Analytics Workspace ID, Primary key, and table name for the Azure instance to which you want to send data.

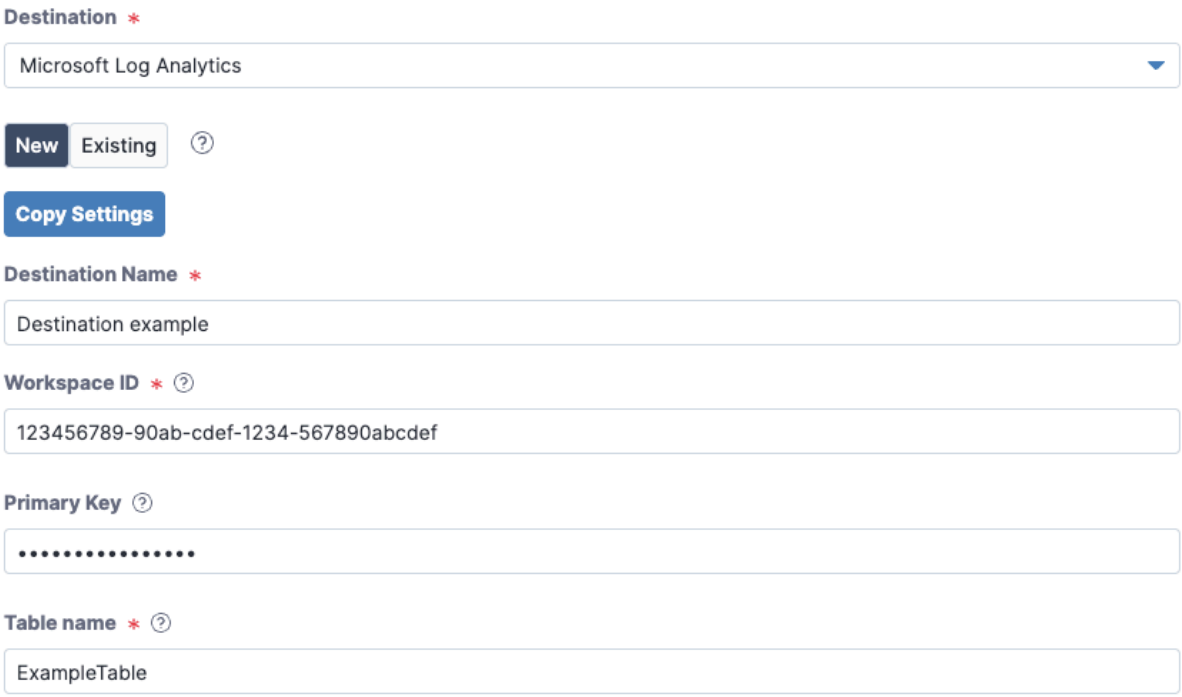
©2026 Tanium Inc. All Rights Reserved

Note: After you create a connection, you cannot update the connection destination type, only the destination configuration. If you want to change the destination, create a new connection.

Note: Individual field values in a row are limited to 32 KB. Values exceeding that limit are truncated to 32 KB.

1. Select Microsoft Log Analytics for the destination and then provide a name for the destination.
    - Create a new destination: Specify a unique name to save the configuration information as a new destination. Select **New** and then enter a **Destination Name**
    - Copy an existing destination: Select **New**, and then click **Copy Settings**. Select a destination, click **Apply**, and update the **Destination Name**.
    - Reuse an existing destination: Select **Existing**, and then select a **Destination Name**.

      Note: Configure a unique destination per connection. If you edit the settings for a shared destination for one connection, any other connections that use the shared destination are affected, and connection runs might fail.

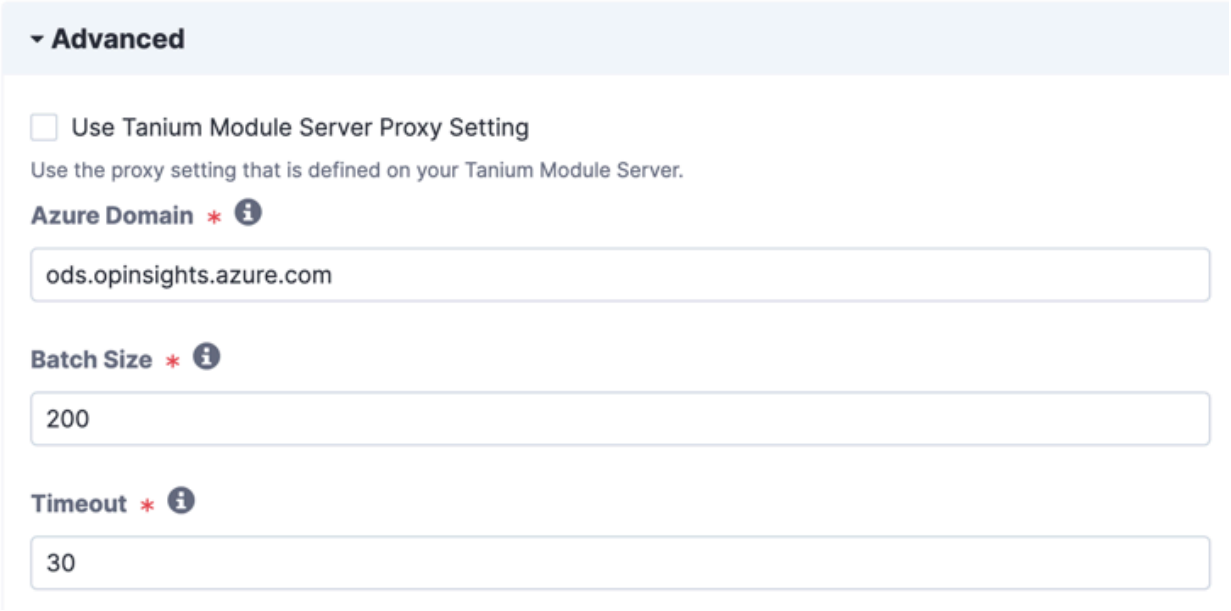


©2026 Tanium Inc. All Rights Reserved

2. Enter your Azure Log Analytics Workspace ID in the **Workspace ID** field.
3. Enter your Azure Log Analytics Primary key in the **Primary Key** field.
4. Enter the log data schema **Table name** to which you want to export your data.

   > **Note:** If you enter a table name that does not exist, the table is created in the log data schema with `_CL` appended to the table name.

5. If you need to configure a Tanium Module Server proxy, custom Azure domain, batch size, or timeout, expand **Advanced**.



   - If you have a proxy configured for your Tanium Module Server, select **Use Tanium Module Server Proxy Setting**. For more information about proxy server settings, see Tanium Console User Guide: Configuring proxy server settings.
   - Enter a custom **Azure Domain**, either `ods.opinsights.azure.com` for the default Azure domain, or `ods.opinsights.azure.us` for the Azure Government domain.
   - Enter a **Batch Size** for the maximum number of records per post. Enter `0` to send all records in a single post.

     > **Note:** Each request is limited to 30 MB. Do not set **Batch Size** to `0` if you send more than 30 MB of data per connection run.

   - Enter a connection **Timeout** in seconds.

©2026 Tanium Inc. All Rights Reserved

Configure filters

(Optional) In the **Configure Output** > **Filters** section, you can specify filters to modify the data that you are getting from your connection source before it is sent to the destination.

For more information about the types of filters you can configure, see Reference: Filtering options on page 257.

Format data for Microsoft Log Analytics

You must send your file in JSON format, as listed in Reference: Format types on page 262.

Important: Select **Generate Document** and clear **Wrap data with source** to properly structure the JSON file for Microsoft Azure. Connection runs fail if you do not properly structure the JSON file.

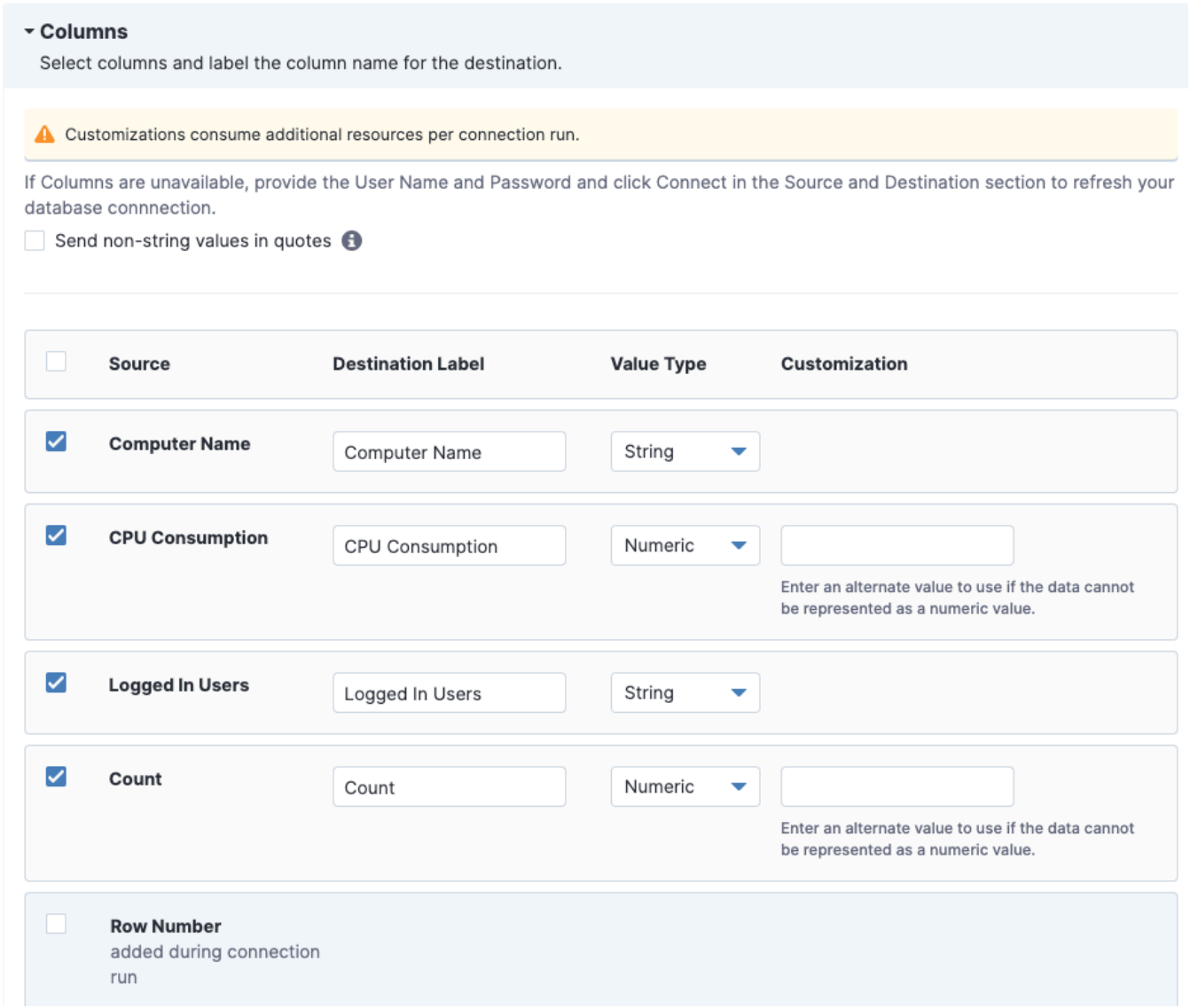
Note: Log Analytics table column names are limited to a maximum of 45 characters.

Note: If the data format supports row delimiter characters, update the characters to ensure that individual rows are sent in a format that the destination can parse. You can define one or more of `\n` (new line), `\r` (carriage return), and `\t` (tab).

In the **Configure Output** > **Columns** section, you can change the **Destination Label** of each column and **Value Type** to force the column to be a String, Numeric, or Date/Time value.

Figure 23. Columns section with Destination Label and Value Type fields

©2026 Tanium Inc. All Rights Reserved



If you choose **Numeric** for the value, you can specify a default value that is used if the data cannot be coerced into a numeric value. You can specify any negative or positive number.

If you choose **Date/Time** for the value, specify the format that you want to use for the column. For more information about how to use a variable, see Time stamp variables on page 297.

For more information about column customizations, see Reference: Column customizations on page 248.

Note: After a connection run successfully completes, it may take several minutes or more for Azure Log Analytics to populate the destination table with the data.

©2026 Tanium Inc. All Rights Reserved

Schedule the connection

Connections can run at a highly configurable time interval, such as multiple times per hour, day, week, or month.

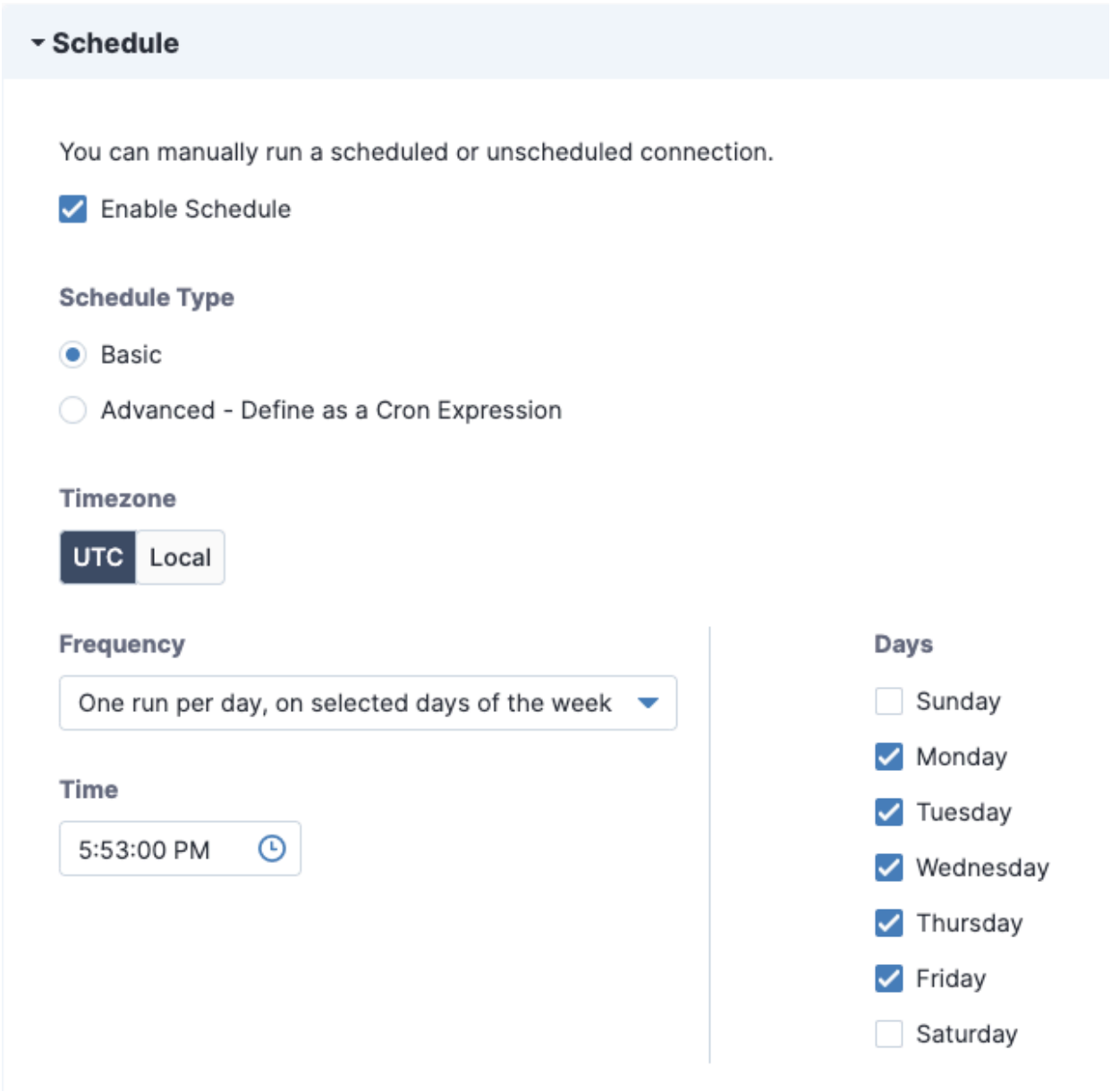
Important: Connections scheduled to run during an upgrade of Connect, or any Tanium solution configured as a connection source, might be interrupted or fail. Schedule your connections to run at a different time than your Tanium upgrades.

Note: If you do not enable the schedule, the connection only runs when you manually run it, unless you configure an **Event** source. Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Schedule** section to update the schedule:

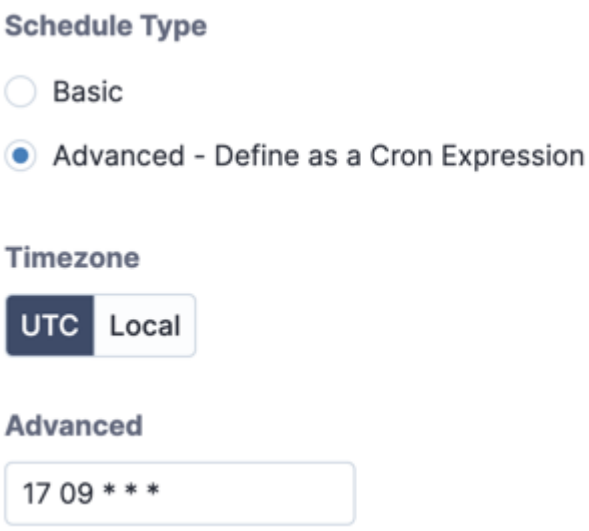
- Select **Enable schedule**.
- In the **Schedule Type**, select **Basic** to build a schedule with the provided controls.

©2026 Tanium Inc. All Rights Reserved



- To view or edit the cron expression directly, select **Advanced - Define as a Cron Expression**, and use the **Advanced** field to edit the cron expression.

©2026 Tanium Inc. All Rights Reserved



Note: If a user that owns a scheduled connection is deleted, future scheduled instances of that connection do not run. For more information, see Issue: Scheduled connection owned by a deleted user no longer runs on page 243.

For more information about cron syntax, see Reference: Cron syntax for Connect on page 253.

Enable listening for an event

Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Enablement** section to send data when a configured event is detected:

- Select **Listen for this Event**.

Save and verify connection

1. After you enter the details for the connection, click **Save**.

   Tip: To save the connection and immediately run the connection, click **Run and Save**.

   If needed, resolve any errors or missing information. After the connection creates successfully, the connection details appear.

©2026 Tanium Inc. All Rights Reserved

2. To view details when the connection runs, click the **Logs** tab.
3. To view an individual run log, expand the row table. For more information about how to resolve errors, see Troubleshooting on page 234.

©2026 Tanium Inc. All Rights Reserved

Configuring SMB file share destinations

You can send information from a connection source to a Server Message Block (SMB) file share.

Prerequisites

- Connect 4.13.4 or later.
- For Tanium Module Server on Tanium Appliance, 1.6.0 or later.
- For Tanium Module Server on Windows, any supported version.

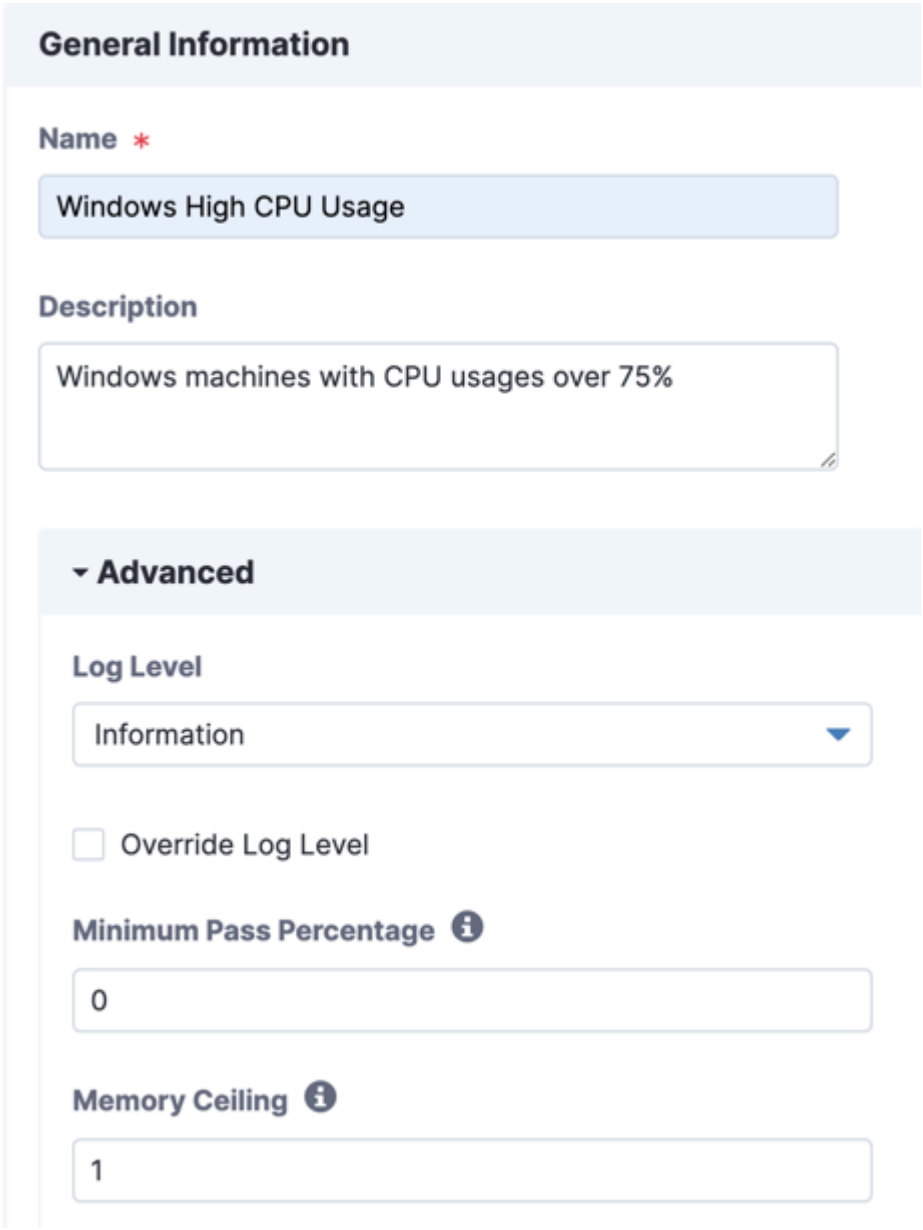
Specify general connection information

1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click **Create Connection**.
2. Enter a name and description for the connection.
3. (Optional) In the **General Information** section, expand **Advanced** to configure the following settings:

   Log Level

   By default, **Log Level** is set to **Information**. To reduce the amount of logging, you can set **Log Level** to **Warning**, **Error**, or **Fatal**.

©2026 Tanium Inc. All Rights Reserved



Override Log Level

If you are debugging the connection, select **Override Log Level** to set a **Temporary Log Level** (such as **Trace** or **Debug**) on this connection for a selected **Number of Runs** (up to **24**). A scheduled or manual connection run, once started, counts towards the number of runs, regardless of the connection status. After the number of runs elapses, the logging for this connection returns to the **Log Level** you selected to prevent finer-grained logging from consuming additional resources for an indefinite number of runs.

Minimum Pass Percentage

Minimum percentage of the expected rows that must be processed for the connection to succeed.

©2026 Tanium Inc. All Rights Reserved

Memory Ceiling (GB)

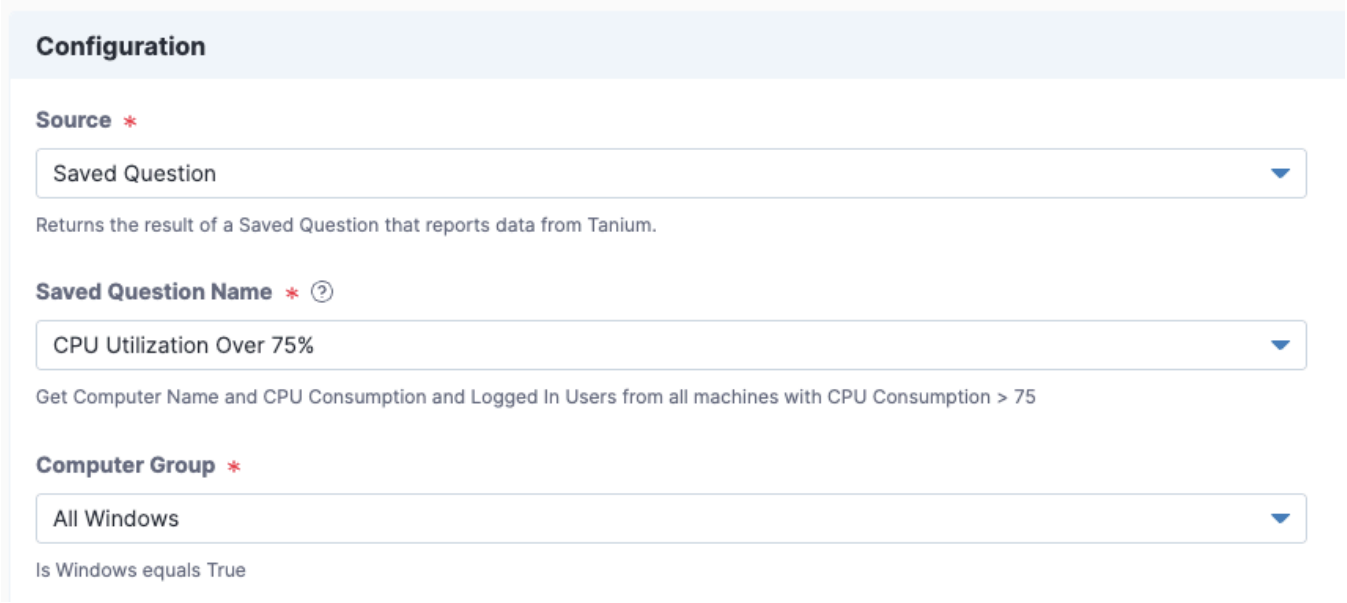
Maximum memory for the node process to run the connection. This defaults to 1 GB per connection, and cannot exceed the global maximum sum of memory for all running connections (by default, 8 GB). Increase this setting if a connection frequently exhibits out of memory errors while running.

> **Note:** If the sum of simultaneously scheduled connection **Memory Ceiling** values exceed the global **Memory Ceiling**, connections run until the global **Memory Ceiling** is reached, then any remaining connections enter a waiting queue if you select the **Queue Connections** configuration setting, or fail if you clear the **Queue Connections** configuration setting.

Configure the connection source

The connection source determines what data you are sending to the destination. This data is usually information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

Figure 24. Connection source settings



©2026 Tanium Inc. All Rights Reserved

Note:

If a Tanium solution or source shows Critical, the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

Note: After you create a connection, you cannot update the connection source type, only the source configuration. If you want to change the source type, create a new connection.

For more information about available connection sources, see Connection sources on page 14.

Configure the SMB file share destination

About this task

Specify details about the file share that you want Connect to send the data.

Best Practice: SMB protocol does not provide server authentication. To minimize risk, use a dedicated service account with a strong password and the minimum permissions required to write to the file share. A least-privileged service account limits the risk to your environment if credentials are compromised.

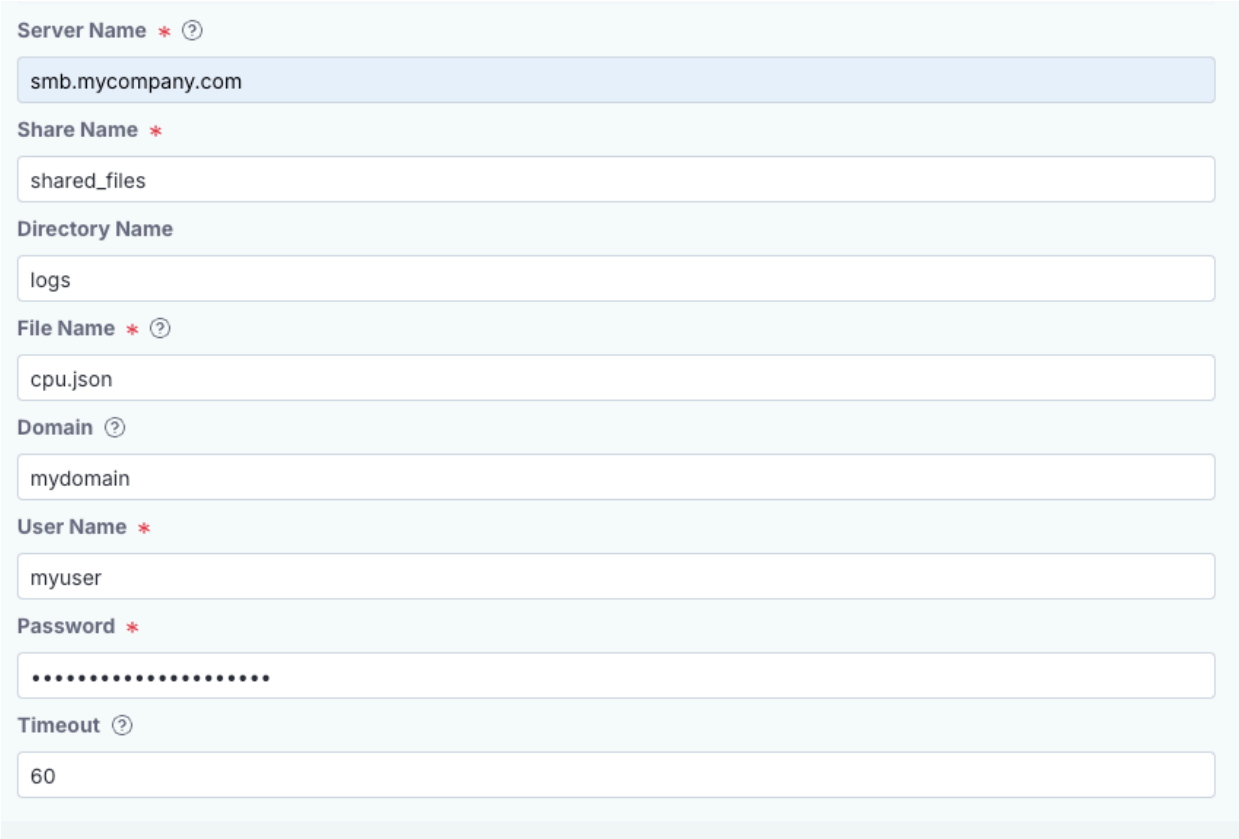
Note: After you create a connection, you cannot update the connection destination type, only the destination configuration. If you want to change the destination, create a new connection.

1. In the **Configuration** section, select **SMB File Share** for the destination, and then provide a name the destination.
    - Create a new destination: Specify a unique name to save the configuration information as a new destination. Select **New** and then enter a **Destination Name**
    - Copy an existing destination: Select **New**, and then click **Copy Settings**. Select a destination, click **Apply**, and update the **Destination Name**.

©2026 Tanium Inc. All Rights Reserved

- Reuse an existing destination: Select **Existing**, and then select a **Destination Name**.

> **Note:** Configure a unique destination per connection. If you edit the settings for a shared destination for one connection, any other connections that use the shared destination are affected, and connection runs might fail.



2. Specify the server name.

> **Important:** The server must support NTLM authentication.

3. Specify the share name, or use a variable as listed in Reference: Variables on page 295.
4. (Optional) Specify the directory name, or use a variable as listed in Reference: Variables on page 295.

> **Note:** The directory must exist on the SMB file share server. If the directory does not exist, connection runs to this destination fail.

5. Specify the file name, or use a variable as listed in Reference: Variables on page 295.
6. (Optional) Specify the domain or workgroup of the user.

©2026 Tanium Inc. All Rights Reserved

7. Specify the user name and password to access the file share.

   Best Practice: SMB protocol does not provide server authentication. To minimize risk, use a dedicated service account with a strong password and the minimum permissions required to write to the file share. A least-privileged service account limits the risk to your environment if credentials are compromised.

8. (Optional) Enter an SMB connection **Timeout** in seconds to increase the time available to complete a file transfer before the SMB connection times out.

Configure filters

(Optional) In the **Configure Output** > **Filters** section, you can specify filters to modify the data that you are getting from your connection source before it is sent to the destination.

For more information about the types of filters you can configure, see Reference: Filtering options on page 257.

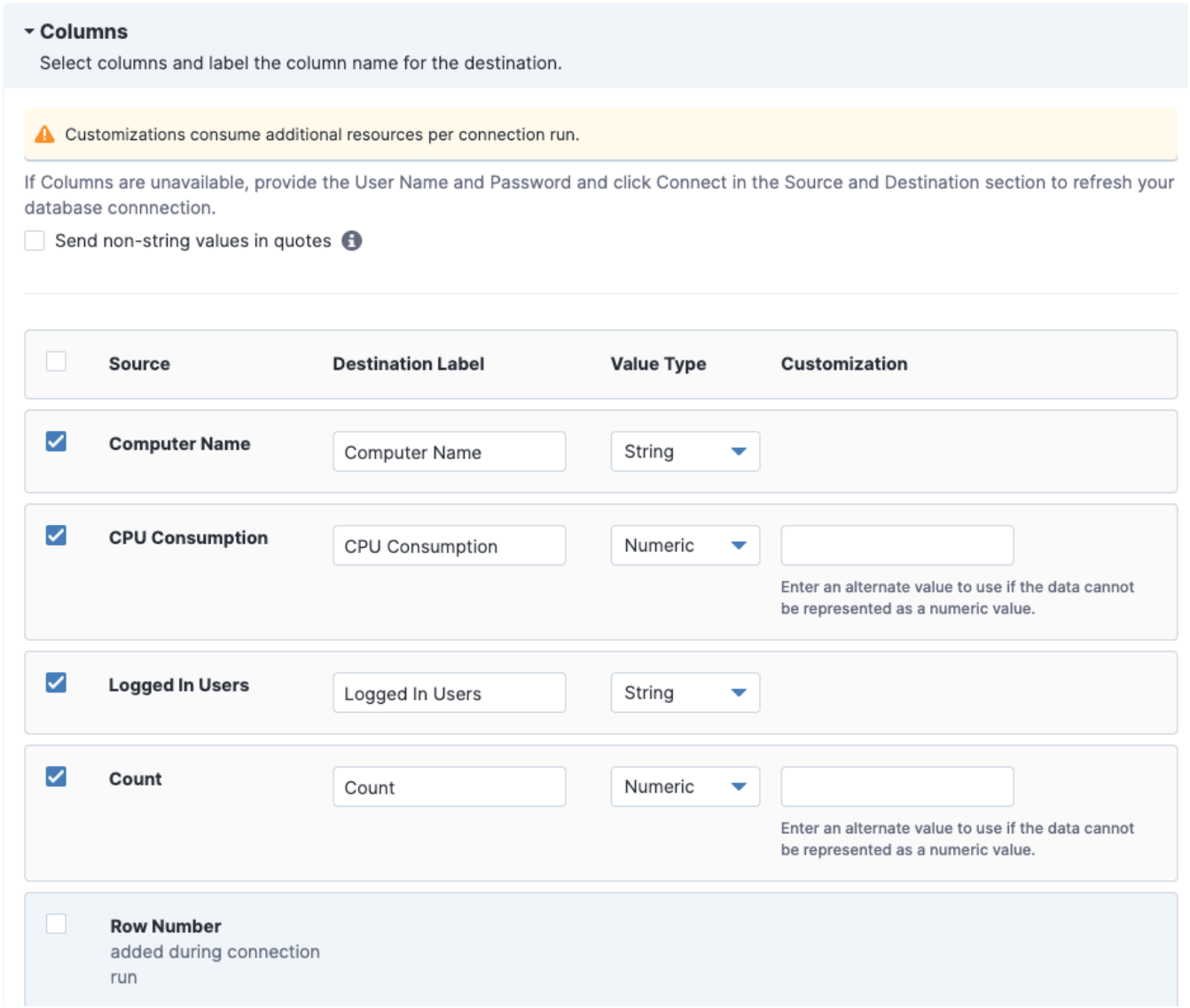
Format data for SMB file share

You can choose to save your file in any of the available formats, as listed in Reference: Format types on page 262. Each format has slightly different configuration options, but all allow you to choose which column data to save.

In the **Configure Output** > **Columns** section, you can change the **Destination Label** of each column and **Value Type** to force the column to be a String, Numeric, or Date/Time value.

Figure 25. Columns section with Destination Label and Value Type fields

©2026 Tanium Inc. All Rights Reserved



If you choose **Numeric** for the value, you can specify a default value that is used if the data cannot be coerced into a numeric value. You can specify any negative or positive number.

If you choose **Date/Time** for the value, specify the format that you want to use for the column. For more information about how to use a variable, see Time stamp variables on page 297.

For more information about column customizations, see Reference: Column customizations on page 248.

Schedule the connection

Connections can run at a highly configurable time interval, such as multiple times per hour, day, week, or month.

©2026 Tanium Inc. All Rights Reserved

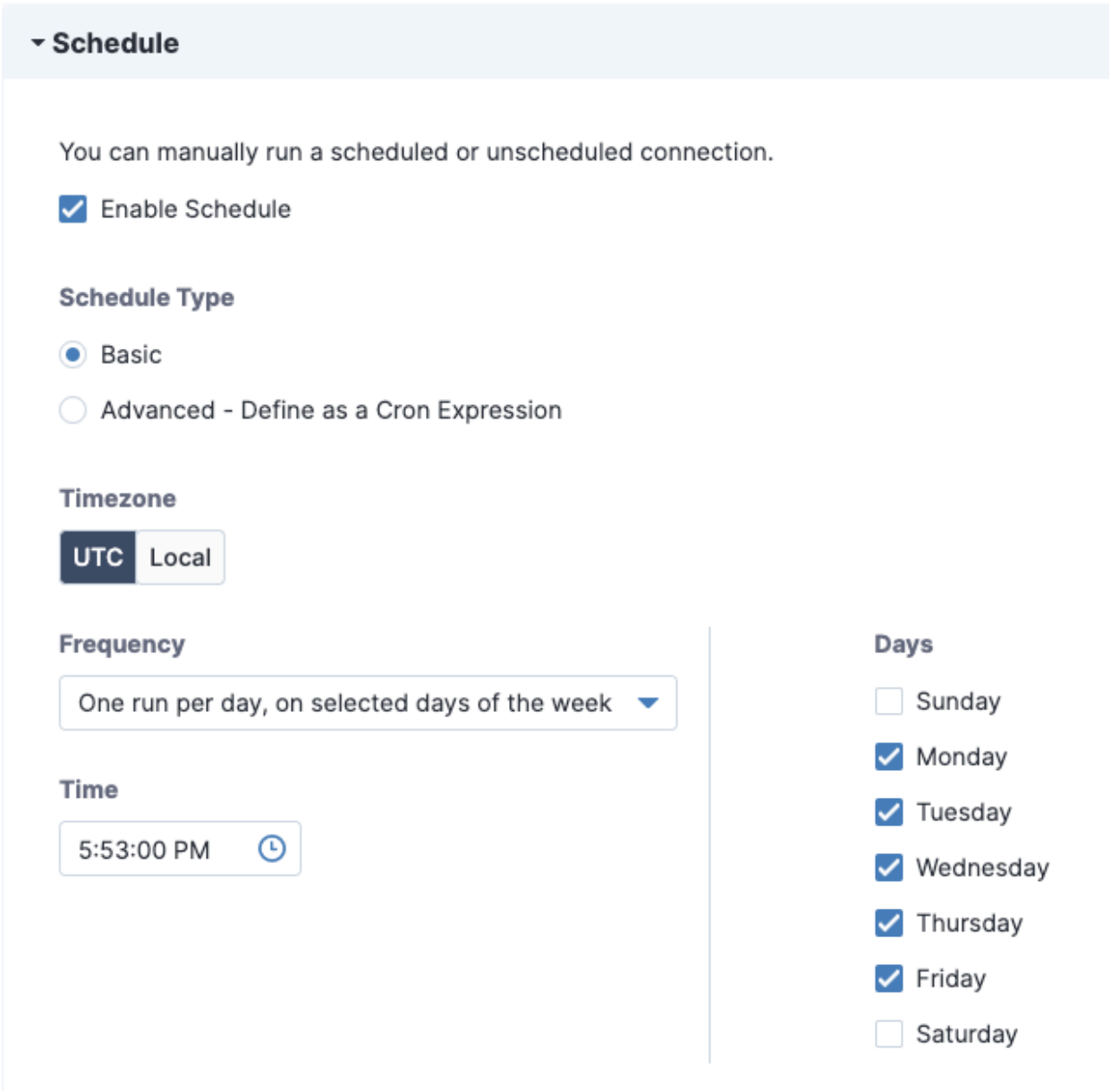
Important: Connections scheduled to run during an upgrade of Connect, or any Tanium solution configured as a connection source, might be interrupted or fail. Schedule your connections to run at a different time than your Tanium upgrades.

Note: If you do not enable the schedule, the connection only runs when you manually run it, unless you configure an **Event** source. Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Schedule** section to update the schedule:

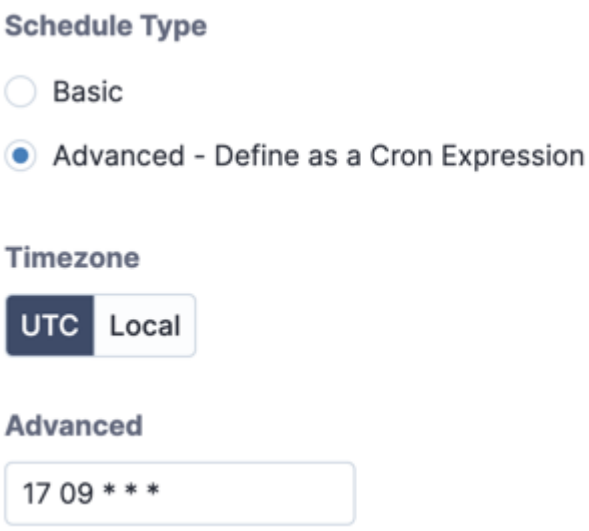
- Select **Enable schedule**.
- In the **Schedule Type**, select **Basic** to build a schedule with the provided controls.

©2026 Tanium Inc. All Rights Reserved



- To view or edit the cron expression directly, select **Advanced - Define as a Cron Expression**, and use the **Advanced** field to edit the cron expression.

©2026 Tanium Inc. All Rights Reserved



Note: If a user that owns a scheduled connection is deleted, future scheduled instances of that connection do not run. For more information, see Issue: Scheduled connection owned by a deleted user no longer runs on page 243.

For more information about cron syntax, see Reference: Cron syntax for Connect on page 253.

Enable listening for an event

Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Enablement** section to send data when a configured event is detected:

- Select **Listen for this Event**.

Save and verify connection

1. After you enter the details for the connection, click **Save**.

   Tip: To save the connection and immediately run the connection, click **Run and Save**.

   If needed, resolve any errors or missing information. After the connection creates successfully, the connection details appear.

©2026 Tanium Inc. All Rights Reserved

2. To view details when the connection runs, click the **Logs** tab.
3. To view an individual run log, expand the row table. For more information about how to resolve errors, see Troubleshooting on page 234.

©2026 Tanium Inc. All Rights Reserved

Configuring Socket (SIEM) destinations

Connect can send information to security information and event management (SIEM) products and services including Google Chronicle, IBM QRadar, LogRhythm, McAfee SIEM, Micro Focus ArcSight, and Splunk.

You can also configure a socket to receive data by configuring a Tanium **Socket Receiver** destination. The configuration options for the destination are the same as SIEM destinations.

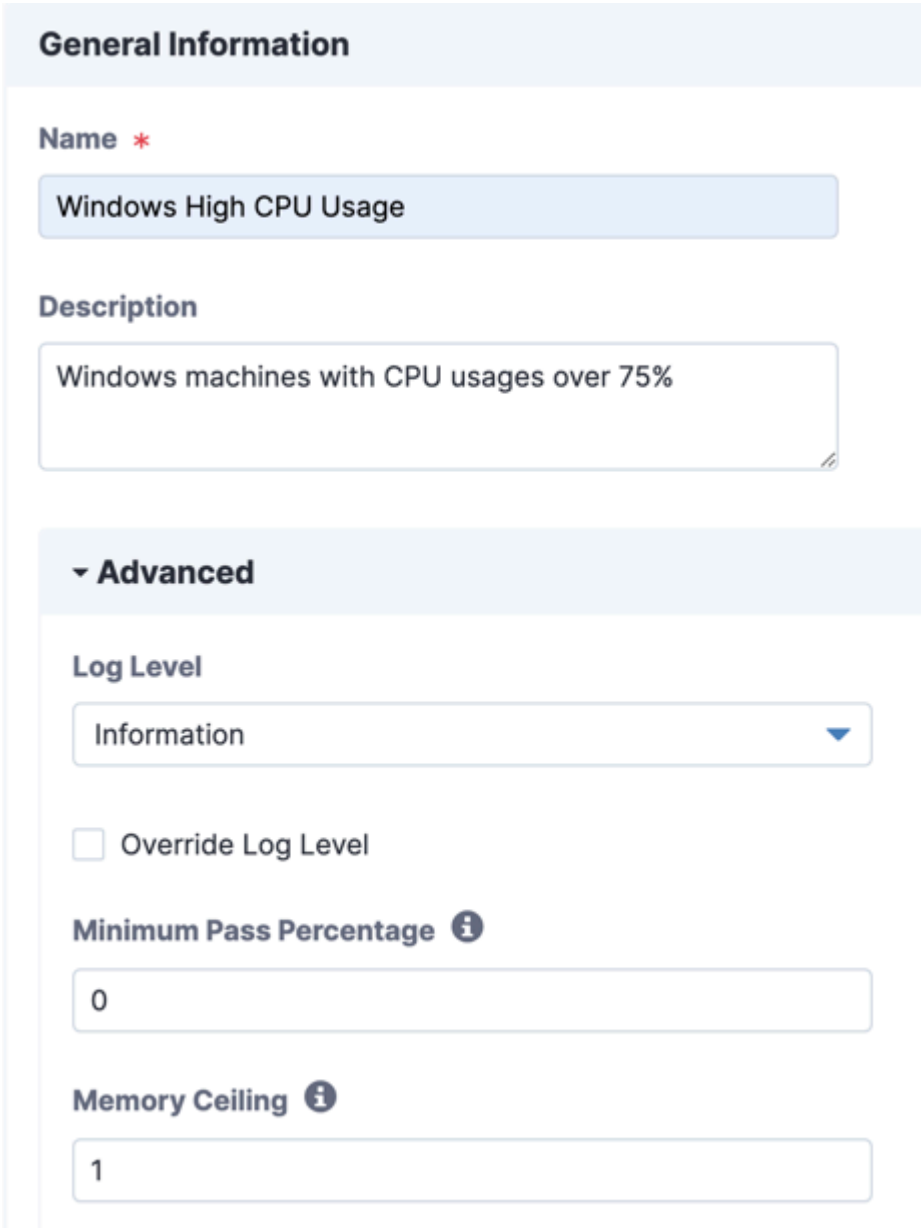
Specify general connection information

1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click **Create Connection**.
2. Enter a name and description for the connection.
3. (Optional) In the **General Information** section, expand **Advanced** to configure the following settings:

   Log Level

   By default, **Log Level** is set to **Information**. To reduce the amount of logging, you can set **Log Level** to **Warning**, **Error**, or **Fatal**.

©2026 Tanium Inc. All Rights Reserved



Override Log Level

If you are debugging the connection, select **Override Log Level** to set a **Temporary Log Level** (such as **Trace** or **Debug**) on this connection for a selected **Number of Runs** (up to **24**). A scheduled or manual connection run, once started, counts towards the number of runs, regardless of the connection status. After the number of runs elapses, the logging for this connection returns to the **Log Level** you selected to prevent finer-grained logging from consuming additional resources for an indefinite number of runs.

Minimum Pass Percentage

Minimum percentage of the expected rows that must be processed for the connection to succeed.

©2026 Tanium Inc. All Rights Reserved

Memory Ceiling (GB)

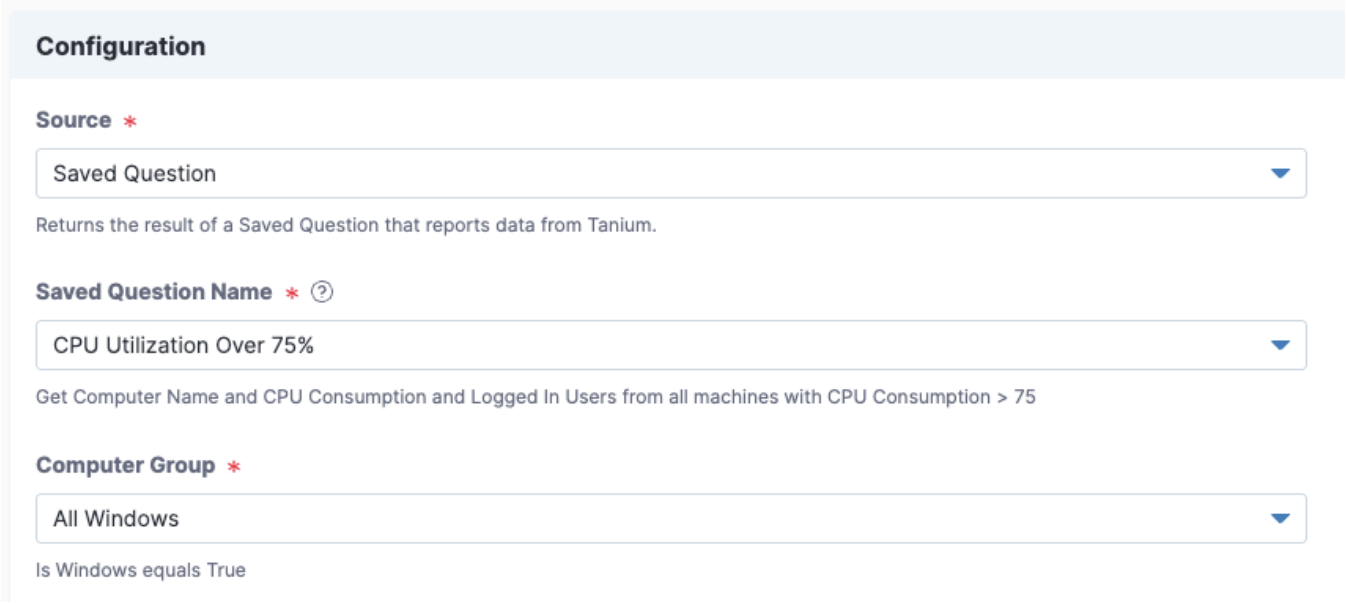
Maximum memory for the node process to run the connection. This defaults to 1 GB per connection, and cannot exceed the global maximum sum of memory for all running connections (by default, 8 GB). Increase this setting if a connection frequently exhibits out of memory errors while running.

> **Note:** If the sum of simultaneously scheduled connection **Memory Ceiling** values exceed the global **Memory Ceiling**, connections run until the global **Memory Ceiling** is reached, then any remaining connections enter a waiting queue if you select the **Queue Connections** configuration setting, or fail if you clear the **Queue Connections** configuration setting.

Configure the connection source

The connection source determines what data you are sending to the destination. This data is usually information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

Figure 26. Connection source settings



©2026 Tanium Inc. All Rights Reserved

Note:

If a Tanium solution or source shows Critical, the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

Note: After you create a connection, you cannot update the connection source type, only the source configuration. If you want to change the source type, create a new connection.

For more information about available connection sources, see Connection sources on page 14.

Configure the SIEM destination

About this task

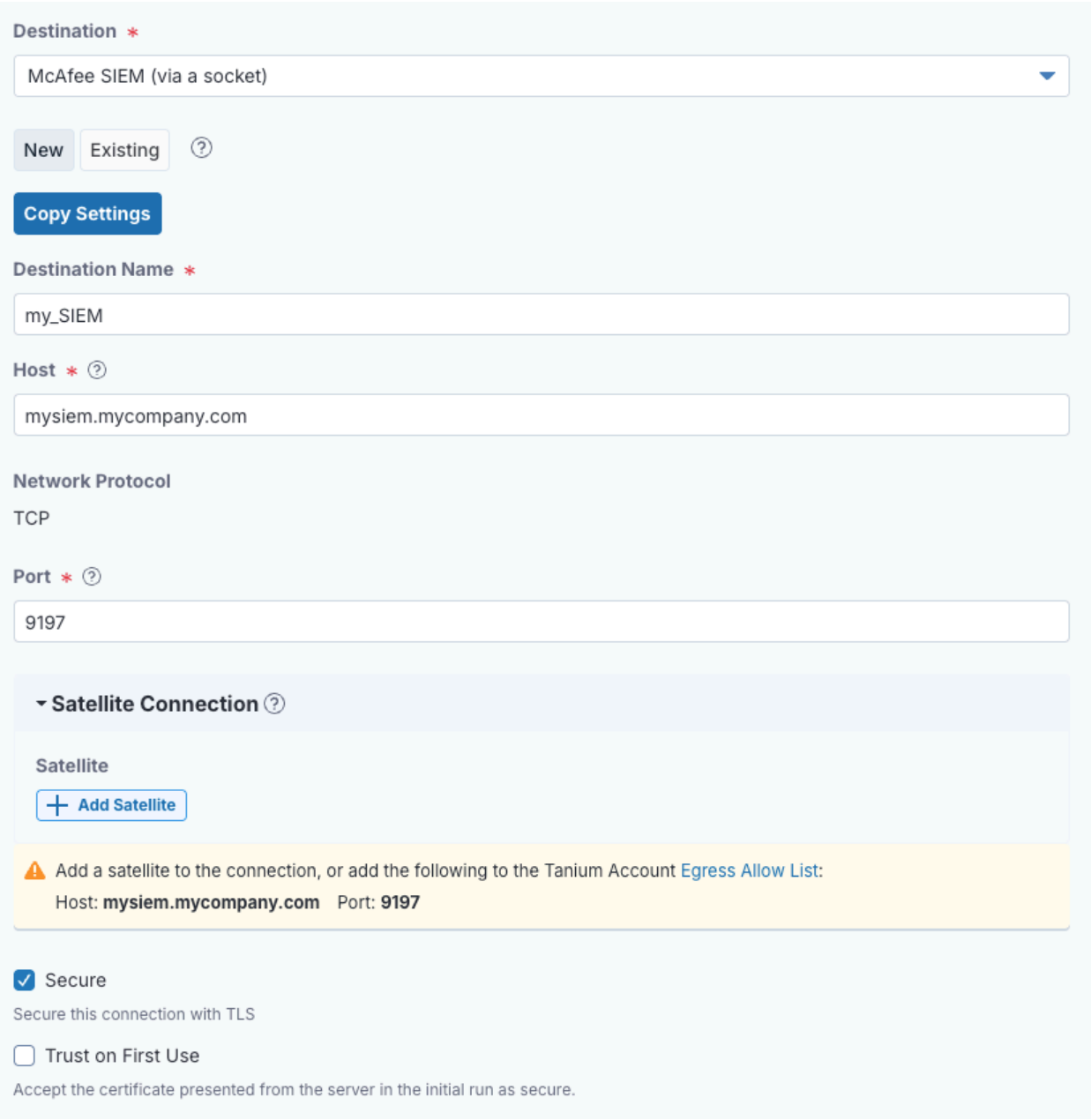
Specify details about the server to which you want to send the SIEM data.

Note: After you create a connection, you cannot update the connection destination type, only the destination configuration. If you want to change the destination, create a new connection.

1. For the **Destination**, select the type of SIEM that you are configuring.
2. Specify a name for the destination.
    - Create a new destination: Specify a unique name to save the configuration information as a new destination. Select **New** and then enter a **Destination Name**
    - Copy an existing destination: Select **New**, and then click **Copy Settings**. Select a destination, click **Apply**, and update the **Destination Name**.
    - Reuse an existing destination: Select **Existing**, and then select a **Destination Name**.

©2026 Tanium Inc. All Rights Reserved

> **Note:** Configure a unique destination per connection. If you edit the settings for a shared destination for one connection, any other connections that use the shared destination are affected, and connection runs might fail.



3. Specify how to connect with the server (TCP/UDP), and where you want the data to go, such as the SIEM host and port.
4. If your connection uses TCP, select **Secure** to enable TLS encryption. You can also select **Trust on First Use** to accept the certificate presented from the server and trust only that certificate for future connection runs.

©2026 Tanium Inc. All Rights Reserved

> **Note:** These fields are not available for UDP connections.

Configure filters

(Optional) In the **Configure Output** > **Filters** section, you can specify filters to modify the data that you are getting from your connection source before it is sent to the destination.

For more information about the types of filters you can configure, see Reference: Filtering options on page 257.

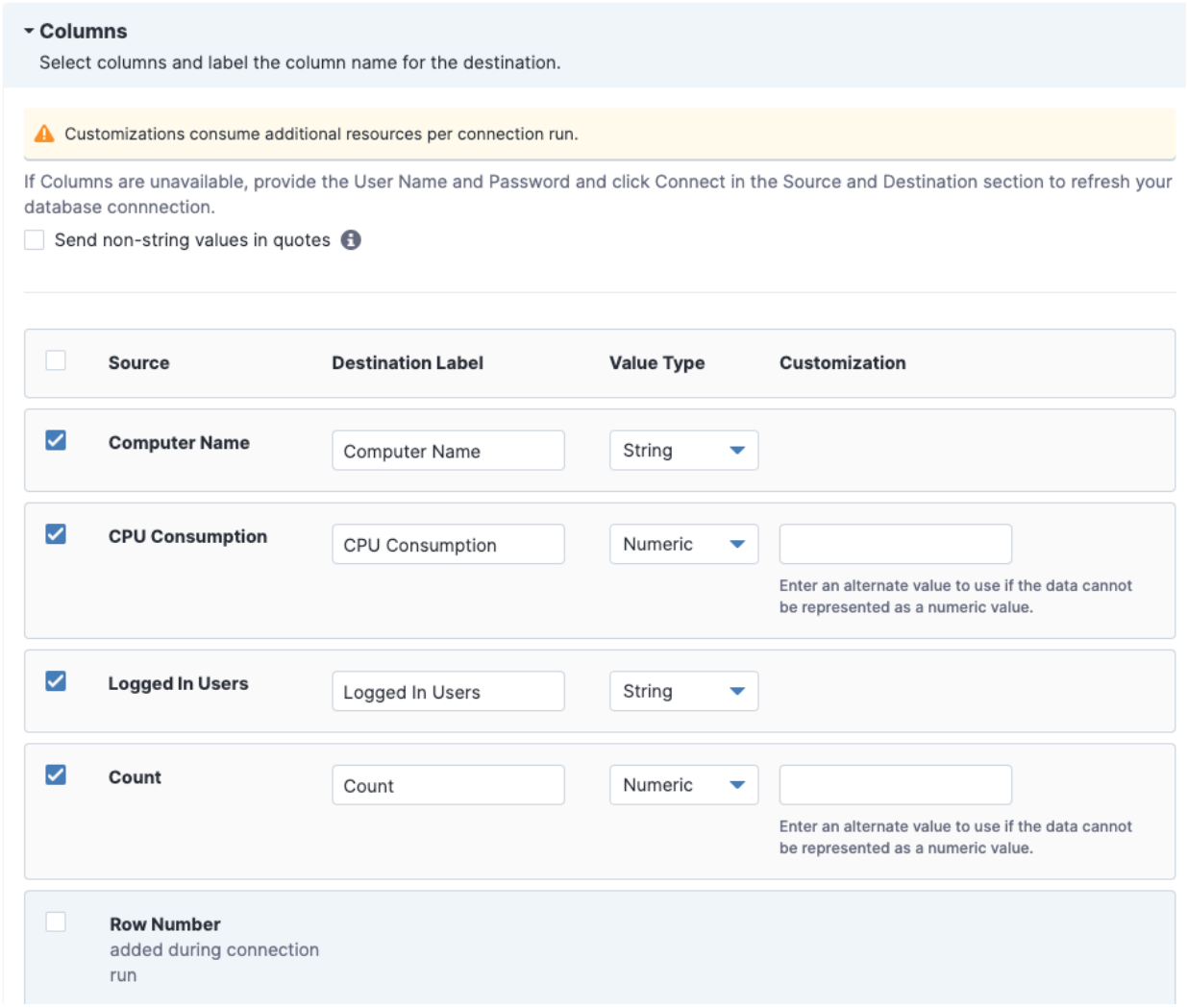
Format data

1. When you select a SIEM destination, the data format that is normally expected by that SIEM is automatically selected. For example, if you select Splunk, the Syslog RFC 5424 format is selected by default. However, you can customize the format as required. For more information about the data formats, see Reference: Format types on page 262.

   > **Note:** For the best results, select the JSON data format if the SIEM does not expect a specific data format.

2. Choose the columns that you want to send to the SIEM destination.

©2026 Tanium Inc. All Rights Reserved

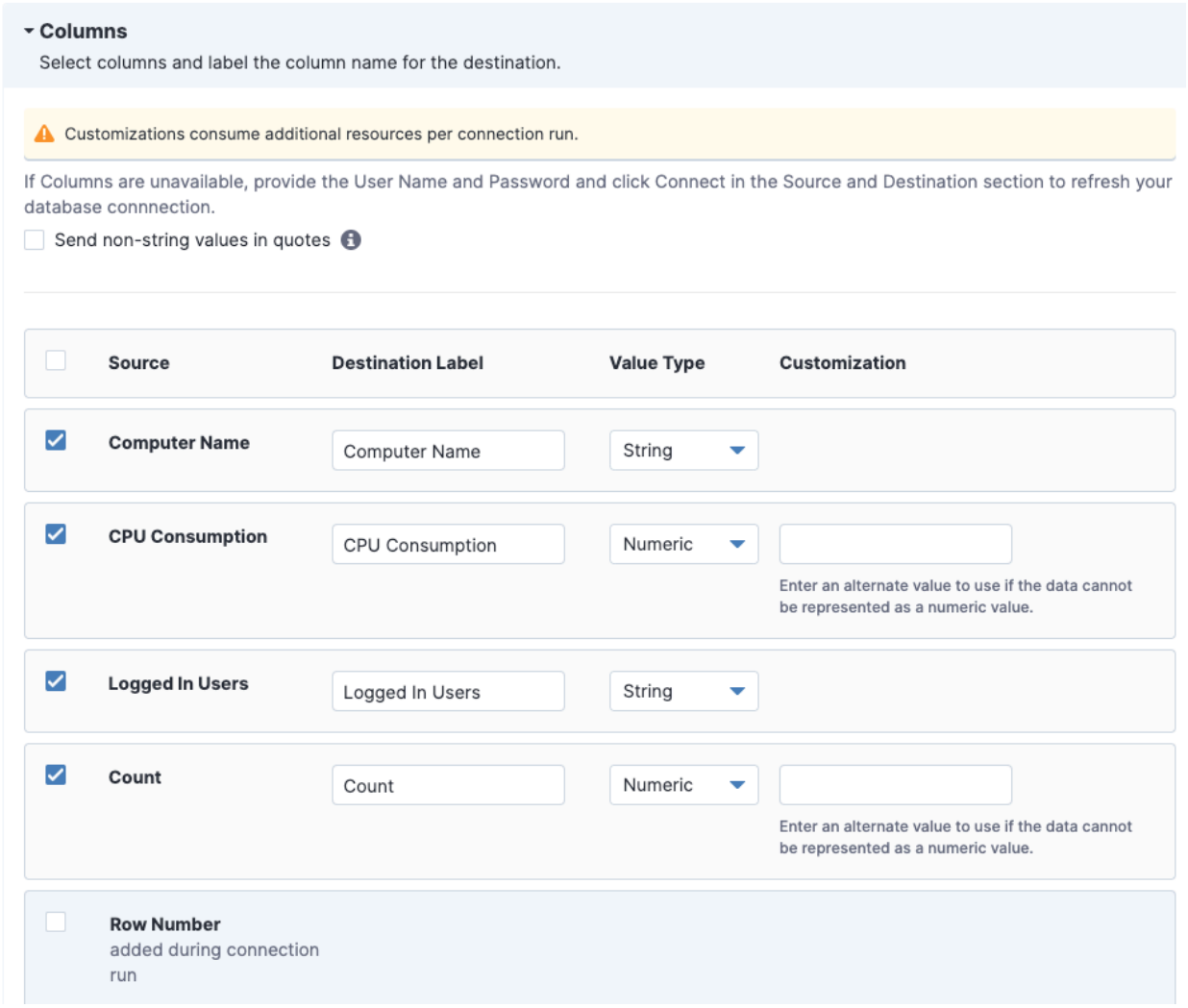


Note: If the data format supports row delimiter characters, update the characters to ensure that individual rows are sent in a format that the destination can parse. You can define one or more of `\n` (new line), `\r` (carriage return), and `\t` (tab).

3. Change the **Destination Label** and **Value Type** for each column.
   In the **Configure Output** > **Columns** section, you can change the **Destination Label** of each column and **Value Type** to force the column to be a String, Numeric, or Date/Time value.

   Figure 27. Columns section with Destination Label and Value Type fields

©2026 Tanium Inc. All Rights Reserved



If you choose **Numeric** for the value, you can specify a default value that is used if the data cannot be coerced into a numeric value. You can specify any negative or positive number.

If you choose **Date/Time** for the value, specify the format that you want to use for the column. For more information about how to use a variable, see Time stamp variables on page 297.

For more information about column customizations, see Reference: Column customizations on page 248.

Schedule the connection

Connections can run at a highly configurable time interval, such as multiple times per hour, day, week, or month.

©2026 Tanium Inc. All Rights Reserved

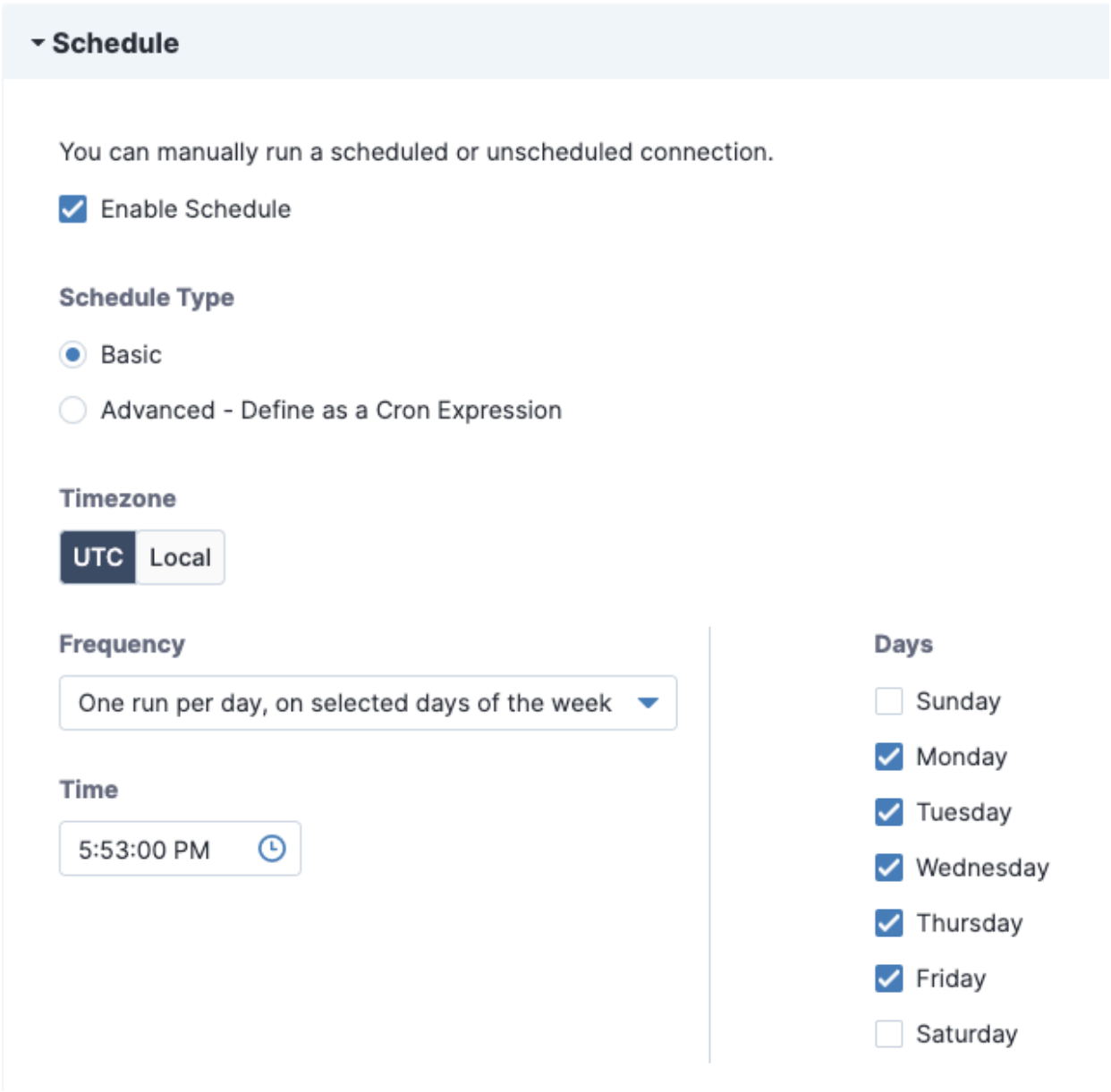
Important: Connections scheduled to run during an upgrade of Connect, or any Tanium solution configured as a connection source, might be interrupted or fail. Schedule your connections to run at a different time than your Tanium upgrades.

Note: If you do not enable the schedule, the connection only runs when you manually run it, unless you configure an **Event** source. Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Schedule** section to update the schedule:

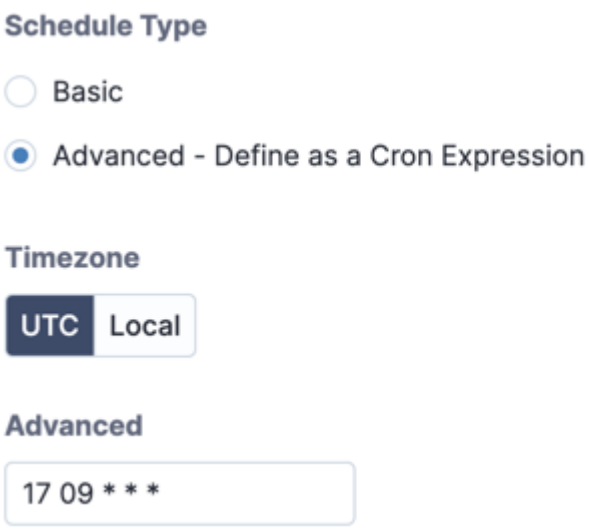
- Select **Enable schedule**.
- In the **Schedule Type**, select **Basic** to build a schedule with the provided controls.

©2026 Tanium Inc. All Rights Reserved



- To view or edit the cron expression directly, select **Advanced - Define as a Cron Expression**, and use the **Advanced** field to edit the cron expression.

©2026 Tanium Inc. All Rights Reserved



Note: If a user that owns a scheduled connection is deleted, future scheduled instances of that connection do not run. For more information, see Issue: Scheduled connection owned by a deleted user no longer runs on page 243.

For more information about cron syntax, see Reference: Cron syntax for Connect on page 253.

Enable listening for an event

Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Enablement** section to send data when a configured event is detected:

- Select **Listen for this Event**.

Save and verify connection

1. After you enter the details for the connection, click **Save**.

   Tip: To save the connection and immediately run the connection, click **Run and Save**.

   If needed, resolve any errors or missing information. After the connection creates successfully, the connection details appear.

©2026 Tanium Inc. All Rights Reserved

2. To view details when the connection runs, click the **Logs** tab.
3. To view an individual run log, expand the row table. For more information about how to resolve errors, see Troubleshooting on page 234.

©2026 Tanium Inc. All Rights Reserved

Configuring SQL Server destinations

You can use SQL Server destinations to store historical results for analysis and integration with third-party systems. You can forward the results from saved questions and other data sources to a database table.

System requirements

- Microsoft SQL Server 2008 or later, Microsoft SQL Server 2008 Express or later
- Database application server must be accessible from the Tanium Module Server
- User credentials with db_ddladmin and db_datawriter role membership to an account on the Microsoft SQL Server that can insert data, create tables (optional), and run stored procedures (optional)

Set up the database

About this task

Decide whether to use an existing database or create a new database.

1. Get the name of the database that you want to use for Connect. When you set up the destination, you can have Connect create a new table for your data or use an existing table.
2. The user account that Connect uses for the database must have log in permissions to that database and the appropriate permissions to tables and stored procedures (optional) within that database.
   Both SQL Server Authentication and Windows Authentication are supported. Set up the following privileges:
   - For each user, create a User Mapping for the database.
   - For each database, grant the CREATE TABLE permission.
   - For each schema, grant the ALTER and INSERT permissions.
   - (Optional) For stored procedures, grant at least the EXECUTE permission.

©2026 Tanium Inc. All Rights Reserved

3. (Optional) Create stored procedures. You can create procedures that run before the first database table row is inserted or after the last row is inserted. Before you create the connection, these procedures and any associated parameters must exist in your database. The SQL user account must also have permission to run these procedures.

Sample SQL Script for creating stored procedures

```
GO
/****** Object: Table [dbo].[connection_log]  Script Date: 4/25/2017 8:02:32 AM ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[connection_log](
  [connectionRunId] [bigint] NOT NULL,
  [connectionId] [bigint] NOT NULL,
  [connectionName] [nvarchar](200) NOT NULL,
  [source] [nvarchar](200) NOT NULL,
  [databaseTable] [nvarchar](100) NULL,
  [startTime] [datetime] NOT NULL,
  [endTime] [datetime] NULL,
  [runStatus] [nvarchar](20) NOT NULL,
  [expectedRowCount] [bigint] NOT NULL,
  [sourceRowCount] [bigint] NOT NULL,
  [destinationRowCount] [bigint] NOT NULL,
PRIMARY KEY CLUSTERED
(
  [connectionRunId] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS =
ON,
        ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO
/****** Object: StoredProcedure [dbo].[sp_onConnectionFinish]  Script Date: 4/25/2017 8:02:32
AM ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE proc [dbo].[sp_onConnectionFinish]
  @connectionRunId bigint,
  @runStatus nvarchar(20),
  @sourceRowCount bigint,
  @destinationRowCount bigint,
  @finishTime datetime
as
BEGIN
  update connection_log set runStatus = @runStatus, sourceRowCount = @sourceRowCount,
        destinationRowCount = @destinationRowCount, endTime = @finishTime
  where connectionRunId = @connectionRunId
END
GO
/****** Object: StoredProcedure [dbo].[sp_onConnectionStart]  Script Date: 4/25/2017 8:02:32
AM ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE PROCEDURE [dbo].[sp_onConnectionStart]
```

©2026 Tanium Inc. All Rights Reserved

```
  @connectionName nvarchar(200),
  @connectionId bigint,
  @connectionRunId bigint,
  @source nvarchar(200),
  @databaseTable nvarchar(100),
  @startTime datetime,
  @expectedRowCount bigint
AS
BEGIN
  if exists (select * from connection_log where ConnectionRunId = @connectionRunId) BEGIN
    delete connection_log where ConnectionRunId = @connectionRunId
  END
  insert into connection_log (connectionRunId, connectionId, connectionName, source,
databaseTable,
        startTime, endTime, runStatus, expectedRowCount, sourceRowCount, destinationRowCount)
  values (@connectionRunId, @connectionId, @connectionName, @source, @databaseTable,
@startTime, null,
        'Running', isnull(@expectedRowCount, 0), 0, 0)
END
GO
```

You can use the following parameters for pre-run stored procedures:

- Connection Name: `@connectionName`
- Connection ID: `@connectionId`
- Connection Run ID: `@connectionRunId`
- Source Name: `@source`
- Database Table: `@databaseTable`
- Start Time: `@startTime`
- Expected Row Count: `@expectedRowCount`

You can use the following parameters for post-run stored procedures:

- Connection Name: `@connectionName`
- Connection ID: `@connectionId`
- Connection Run ID: `@connectionRunId`
- Source Name: `@source`
- Database Table: `@databaseTable`

©2026 Tanium Inc. All Rights Reserved

- Start Time: `@startTime`
- Expected Row Count: `@expectedRowCount`
- Run Status: `@runStatus`
- Source Row Count: `@sourceRowCount`
- Destination Row Count: `@destinationRowCount`
- Finish Time: `@endTime`

Note: The `@runStatus` parameter always returns `Finished` because the post-run stored procedure runs only after a successful connection run. The `@endTime` parameter is the time the stored procedure is executed, and is UTC formatted as ISO8601. The `@databaseTable` parameter is in the format of `database schema.database table` (for example, `dbo.connection_log`). The `@expectedRowCount` parameter could return `NULL` for sources other than saved questions.

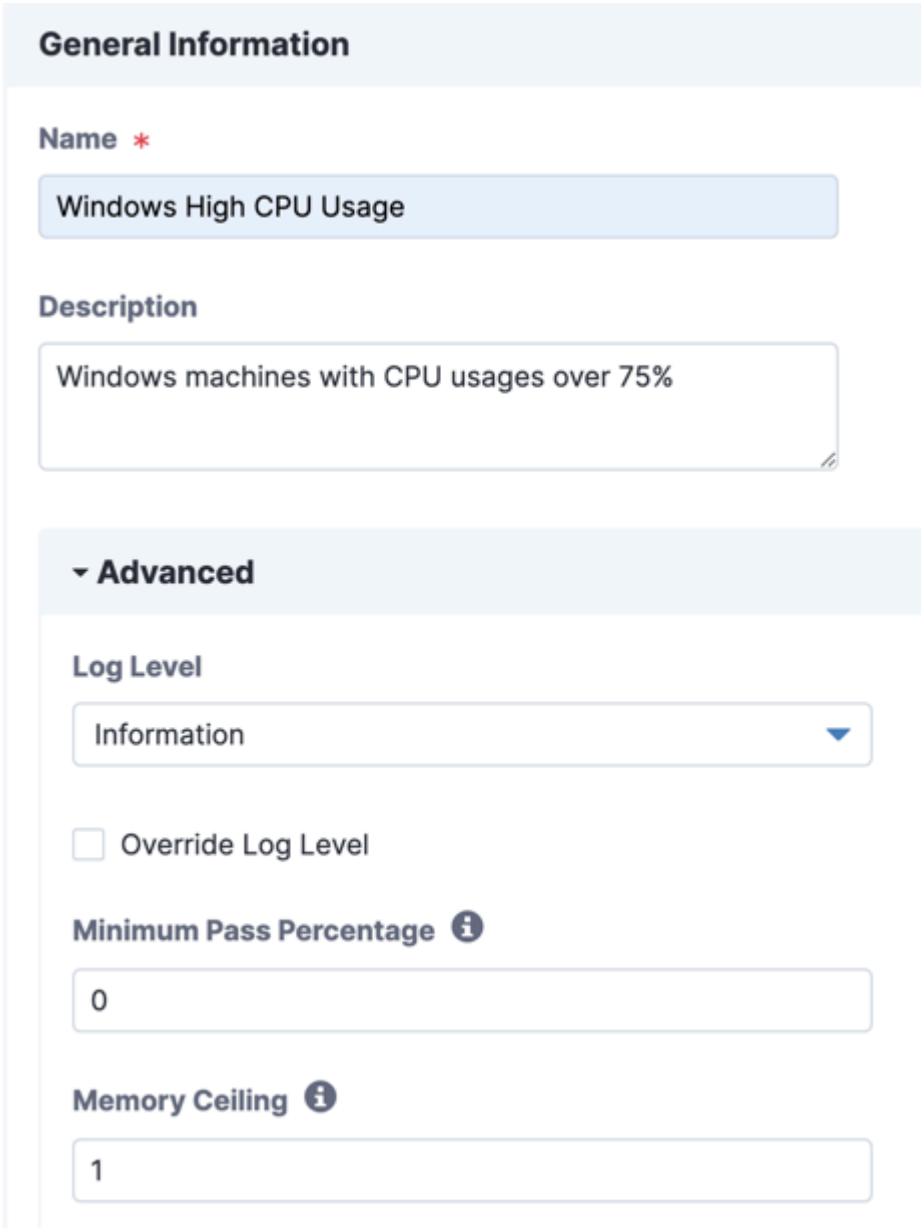
Specify general connection information

1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click **Create Connection**.
2. Enter a name and description for the connection.
3. (Optional) In the **General Information** section, expand **Advanced** to configure the following settings:

   Log Level

   By default, **Log Level** is set to **Information**. To reduce the amount of logging, you can set **Log Level** to **Warning**, **Error**, or **Fatal**.

©2026 Tanium Inc. All Rights Reserved



Override Log Level

If you are debugging the connection, select **Override Log Level** to set a **Temporary Log Level** (such as **Trace** or **Debug**) on this connection for a selected **Number of Runs** (up to **24**). A scheduled or manual connection run, once started, counts towards the number of runs, regardless of the connection status. After the number of runs elapses, the logging for this connection returns to the **Log Level** you selected to prevent finer-grained logging from consuming additional resources for an indefinite number of runs.

Minimum Pass Percentage

Minimum percentage of the expected rows that must be processed for the connection to succeed.

©2026 Tanium Inc. All Rights Reserved

Memory Ceiling (GB)

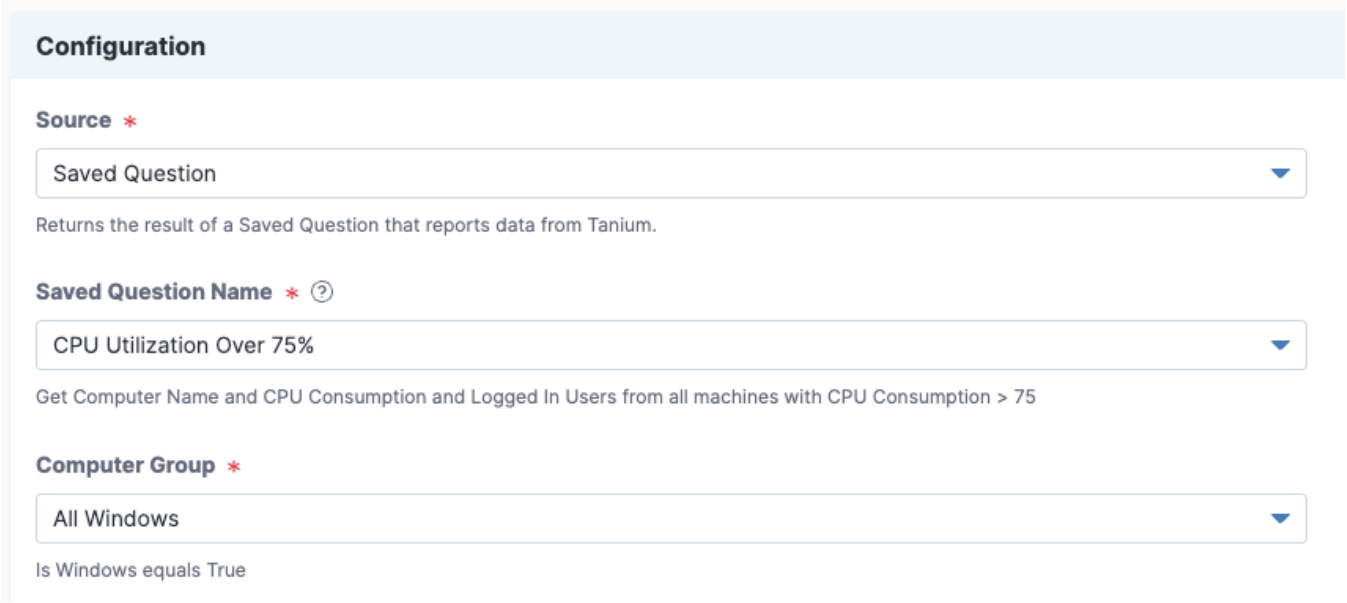
Maximum memory for the node process to run the connection. This defaults to 1 GB per connection, and cannot exceed the global maximum sum of memory for all running connections (by default, 8 GB). Increase this setting if a connection frequently exhibits out of memory errors while running.

> **Note:** If the sum of simultaneously scheduled connection **Memory Ceiling** values exceed the global **Memory Ceiling**, connections run until the global **Memory Ceiling** is reached, then any remaining connections enter a waiting queue if you select the **Queue Connections** configuration setting, or fail if you clear the **Queue Connections** configuration setting.

Configure the connection source

The connection source determines what data you are sending to the destination. This data is usually information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

Figure 28. Connection source settings



©2026 Tanium Inc. All Rights Reserved

Note:

If a Tanium solution or source shows Critical, the installed solution does not meet the minimum required version for proper compatibility and functionality. Upgrade the solution to the minimum required version or later.

Note: After you create a connection, you cannot update the connection source type, only the source configuration. If you want to change the source type, create a new connection.

For more information about available connection sources, see Connection sources on page 14.

Configure SQL Server destination

About this task

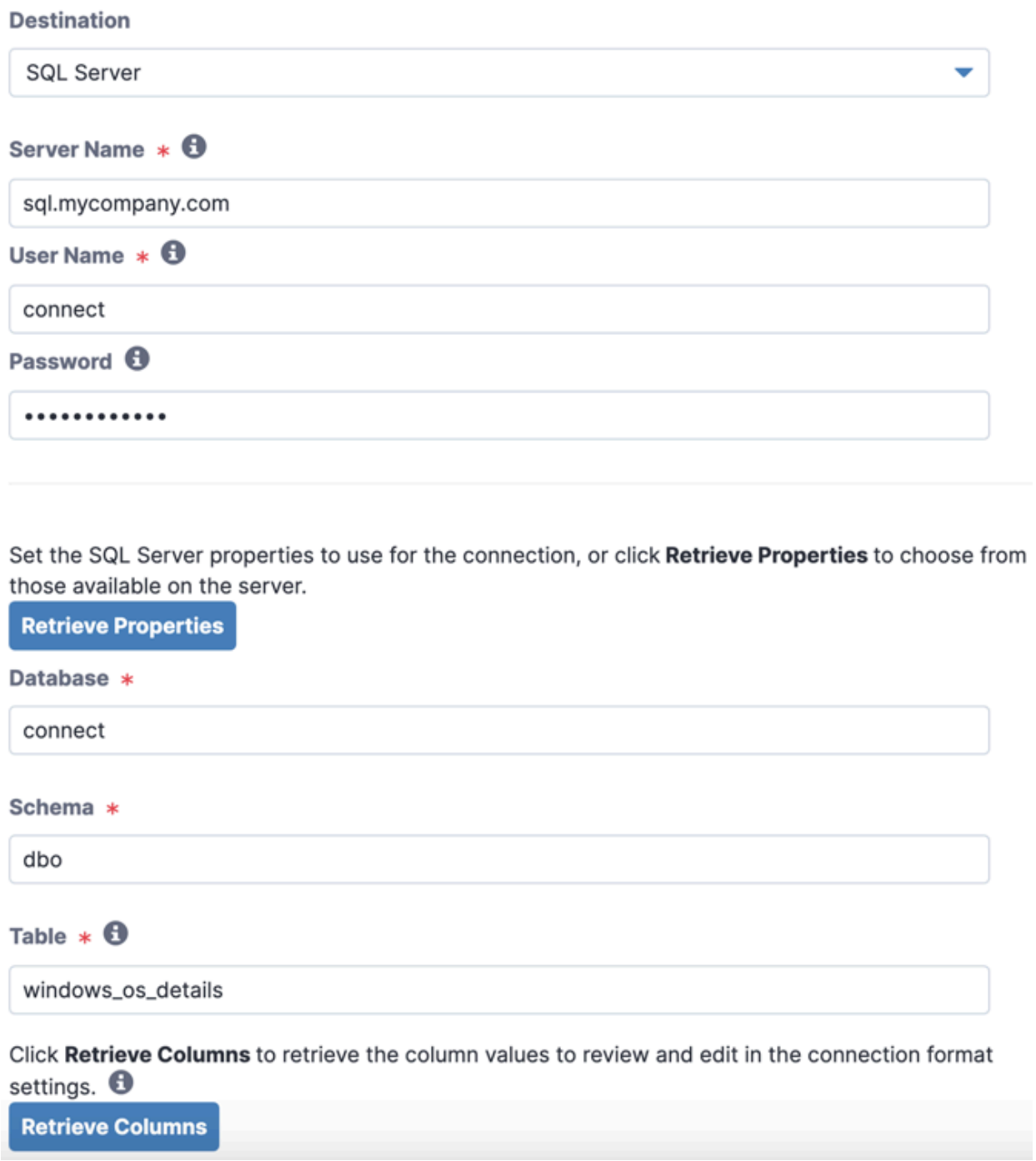
Specify information about how to connect to your database application server, test the database application server connection, and configure which data is added to the database tables and rows.

Note: After you create a connection, you cannot update the connection destination type, only the destination configuration. If you want to change the destination, create a new connection.

Note: Each time that a connection to a SQL Server destination runs, if the configured destination table does not exist, then the connection attempts to create the table using the configured database user account. The user account must be a member of the db_ddladmin database role to create the table.

1. In the **Configuration** section, select **SQL Server** for the destination.
2. Enter the **Server Name**.
3. Enter the **User Name** and **Password**.

©2026 Tanium Inc. All Rights Reserved



Enter a hostname (such as `sqlserver.domain.com`) or IPv4 address (such as `192.0.2.10`) in the **Server Name** field.

If you want to add a named instance, append a backslash followed by the instance name in the format `hostname\instance_name` (such as `sqlserver.domain.com\instance`) or `ip_address\instance_name` (such as `192.0.2.10\instance`).

If you want to add a custom port, append a comma followed by the port number in the

©2026 Tanium Inc. All Rights Reserved

format `hostname, port_number` (`sqlserver.domain.com, 1434`) or `ip_address, port_number` (such as `192.0.2.10, 1434`).

> **Note:** You cannot enter both a named instance and custom port number. If you specify a named instance, the database server must be running the SQL Server Browser service and must have port 1434/UDP opened. For information about port configuration, see Microsoft SQL documentation: How to check if SQL Server is listening on a dynamic port or static port.

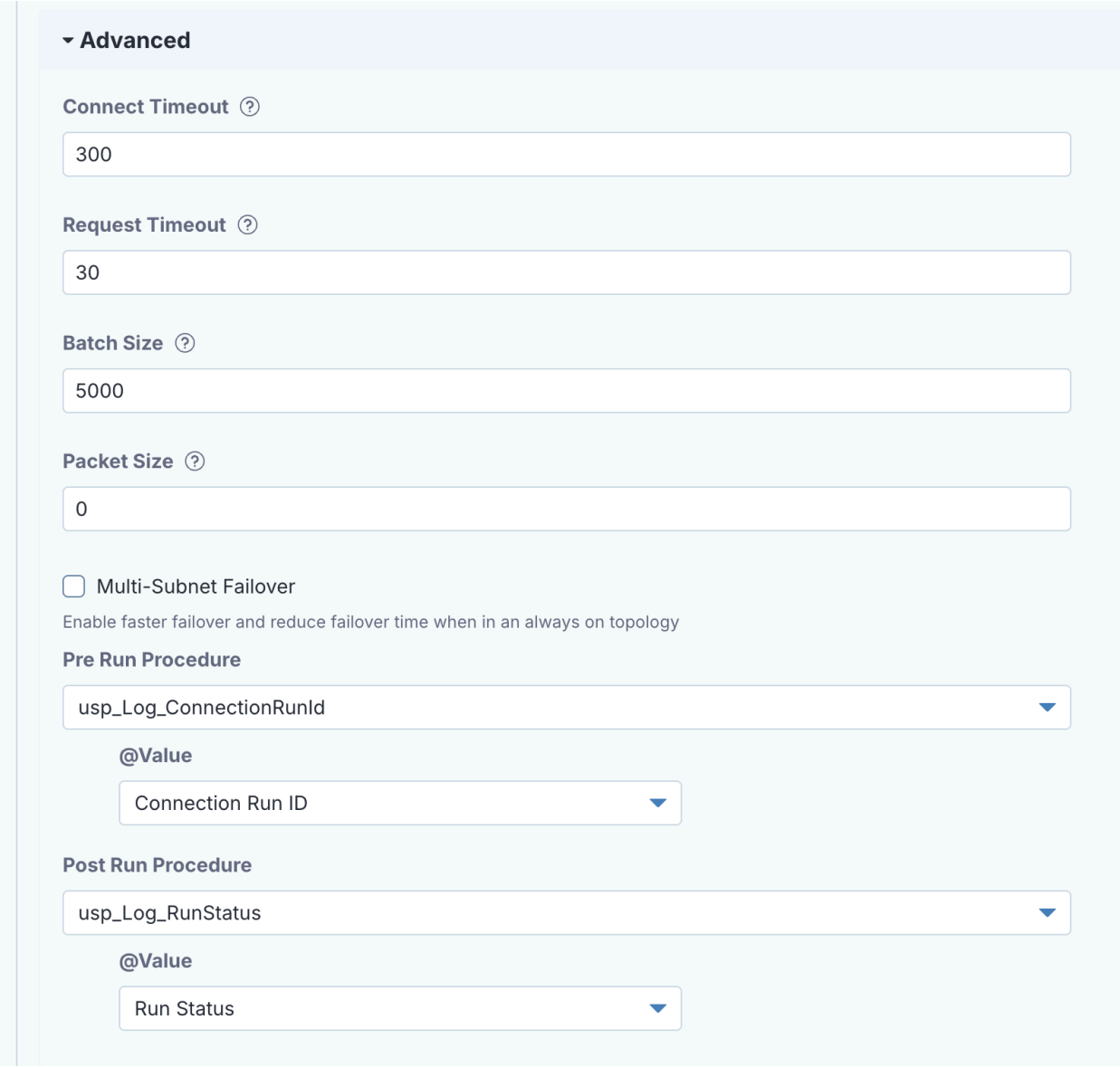
If you are using Windows Authentication, specify the **User Name** in the following format: `domain_name\login_name` (such as `domain_general\example_user`).

4. Specify the database application server properties or click **Retrieve Properties** to choose from those available on the server. If the connection to the database application server is successful, the fields for the database name, schema, and table appear.

   > **Note:** The option to **Retrieve Properties** is disabled if there are no servers configured.

5. (Optional) To retrieve stored procedures without using **Retrieve Properties**, enter a value in the **Database** and **Schema** fields and then click **Retrieve Stored Procedures**.
   Connect retrieves the stored procedures and their parameters for the specified database and schema, and populates the **Advanced** section for the destination settings with the stored procedure fields.

©2026 Tanium Inc. All Rights Reserved



Note: Use **Retrieve Stored Procedures** instead of **Retrieve Properties** when your SQL Server instance has a large number of properties and **Retrieve Properties** times out.

6. (Optional) Click **Retrieve Columns** to populate the column values in the **Columns** section.

   Note: You must be a member of the db_ddladmin database role to retrieve columns from the server.

7. (Optional) If you want to use encryption, select **Encrypt** and **Validate server's TLS certificate** to validate that the certificate is signed by a well-known, public certificate authority. If you want to use a self-signed certificate (not recommended) for testing purposes, deselect **Validate server's TLS certificate**.

©2026 Tanium Inc. All Rights Reserved

Important: Deselecting **Validate server's TLS certificate** is not recommended, because that allows any certificates to be accepted, including certificates that are not valid or malicious.

8. (Optional) In the destination settings, expand **Advanced** to configure advanced settings.

Note: Stored procedure fields and parameters are available only if your database already has stored procedures configured.

Tip: For connections that use a satellite to connect to on-premises destinations that are not accessible from the external internet, note that the **Retrieve Properties** and **Retrieve Columns** buttons use the configured **Connect Timeout** advanced setting value. Because on-premises destinations might require more time to establish a connection, increase **Connect Timeout** to `60` seconds or more.

Advanced settings for SQL Server destinations

Advanced setting	Description
Connect Timeout	The maximum number of seconds to establish a network connection between the connection source and the SQL Server destination. A connection run fails if a network connection is not established within this timeout period.
Request Timeout	The maximum number of seconds to complete a batch request from the connection source to the SQL Server destination, after establishing a network connection. Each batch request contains a batch of rows from the connection source. A connection run fails if a batch request does not complete within this timeout period. A single connection run might send more than one batch request to the SQL Server depending on the **Batch Size** and the number of rows available.
Batch Size	The maximum number of rows sent per batch from the connection source to the SQL Server destination. If the total number of rows exceeds the defined **Batch Size** for a single connection run, the connection run sends multiple batch requests, waiting for one batch request to complete before sending the next batch request. This has no effect if one row or fewer is available to send in a connection run.
Packet Size	The Tabular Data Stream protocol (TDS protocol) packet size, used for communication between the connection source and the SQL Server destination. If set to `0`, TDS protocol packet size is defined by the SQL Server setting (generally 4096 bytes).

©2026 Tanium Inc. All Rights Reserved

Advanced setting	Description
Multi-Subnet Failover	For Always On cluster deployments only, better resolve the active server DNS name and improve performance in failover situations.

Configure filters

(Optional) In the **Configure Output** > **Filters** section, you can specify filters to modify the data that you are getting from your connection source before it is sent to the destination.

For more information about the types of filters you can configure, see Reference: Filtering options on page 257.

Map database table columns

(Optional) You can view and change the mapping of the data from your source to the columns in your database table.

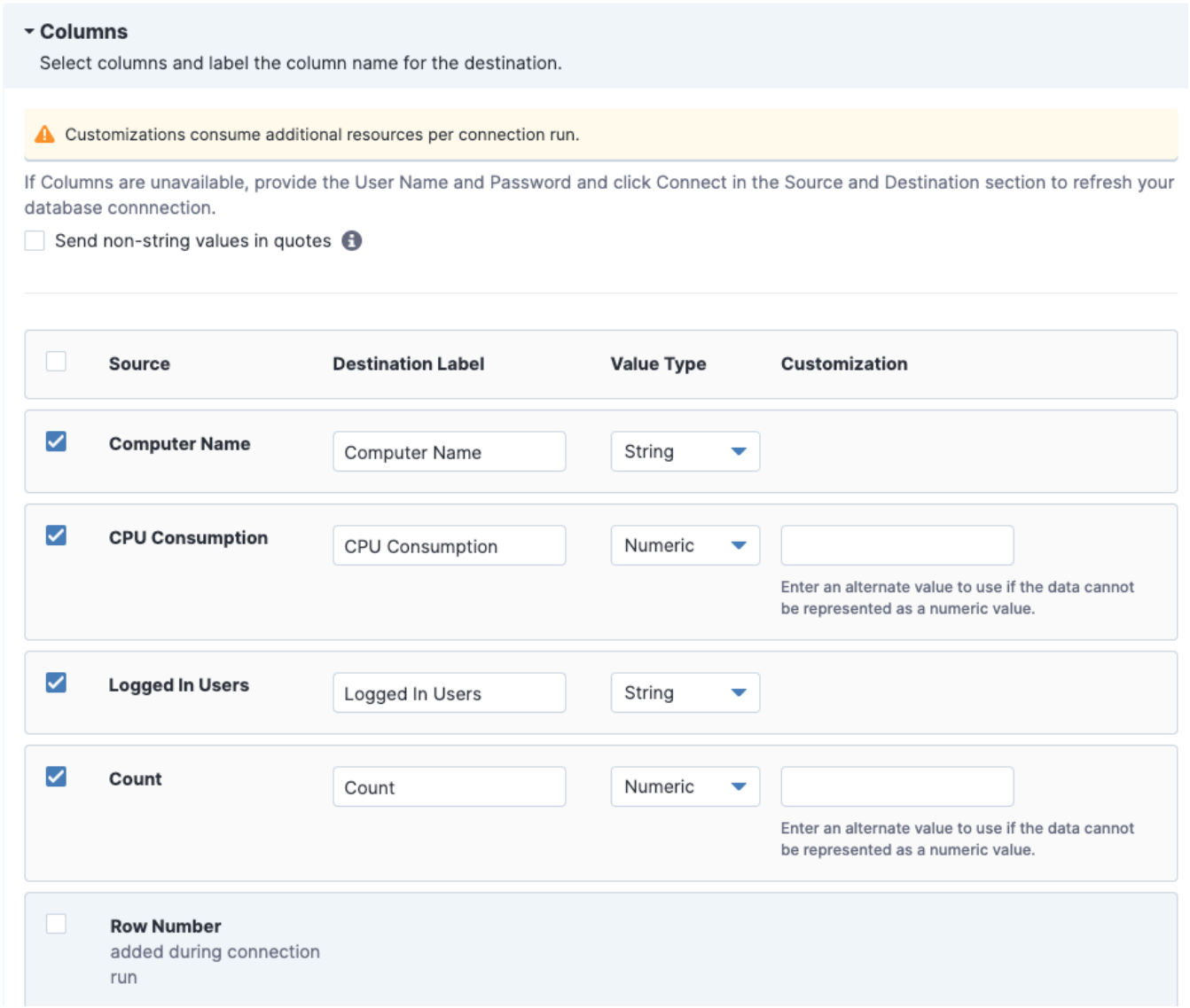
If the source is a saved question, the following columns are also available for writing to the SQL Server destination:

- Band Number: The source row number. When flattened, this number is in each row that is associated with a row number that is received from Tanium.
- Row Number: The destination row number. This value is a counter for the rows that are output per connection run. The value is unique for each connection run.

In the **Configure Output** > **Columns** section, you can change the **Destination Label** of each column and **Value Type** to force the column to be a String, Numeric, or Date/Time value.

Figure 29. Columns section with Destination Label and Value Type fields

©2026 Tanium Inc. All Rights Reserved



If you choose **Numeric** for the value, you can specify a default value that is used if the data cannot be coerced into a numeric value. You can specify any negative or positive number.

If you choose **Date/Time** for the value, specify the format that you want to use for the column. For more information about how to use a variable, see Time stamp variables on page 297.

For more information about column customizations, see Reference: Column customizations on page 248.

©2026 Tanium Inc. All Rights Reserved

Note: You can export data in the **MM/DD/YYYY**, **ISO 8601 with time zone**, and **ISO 8601 UTC (Zulu)** date/time formats to database columns of type date, datetime2, datetimeoffset, nvarchar, or time. If you specify a destination column that does not exist in the destination database, it is created as type nvarchar.

Important: When you edit a connection with the SQL Server destination, the columns that are in the database are not shown by default. You can edit the text fields for the columns, but you must provide the **User Name** and **Password** and click **Retrieve Columns** in the **Configuration** section to view the columns from the database.

Your connection is listed on the Connect **Overview** page and data is sent to the Microsoft SQL Server at the interval you specified. You might want to check your database table to verify that the data is being exported correctly.

Schedule the connection

Connections can run at a highly configurable time interval, such as multiple times per hour, day, week, or month.

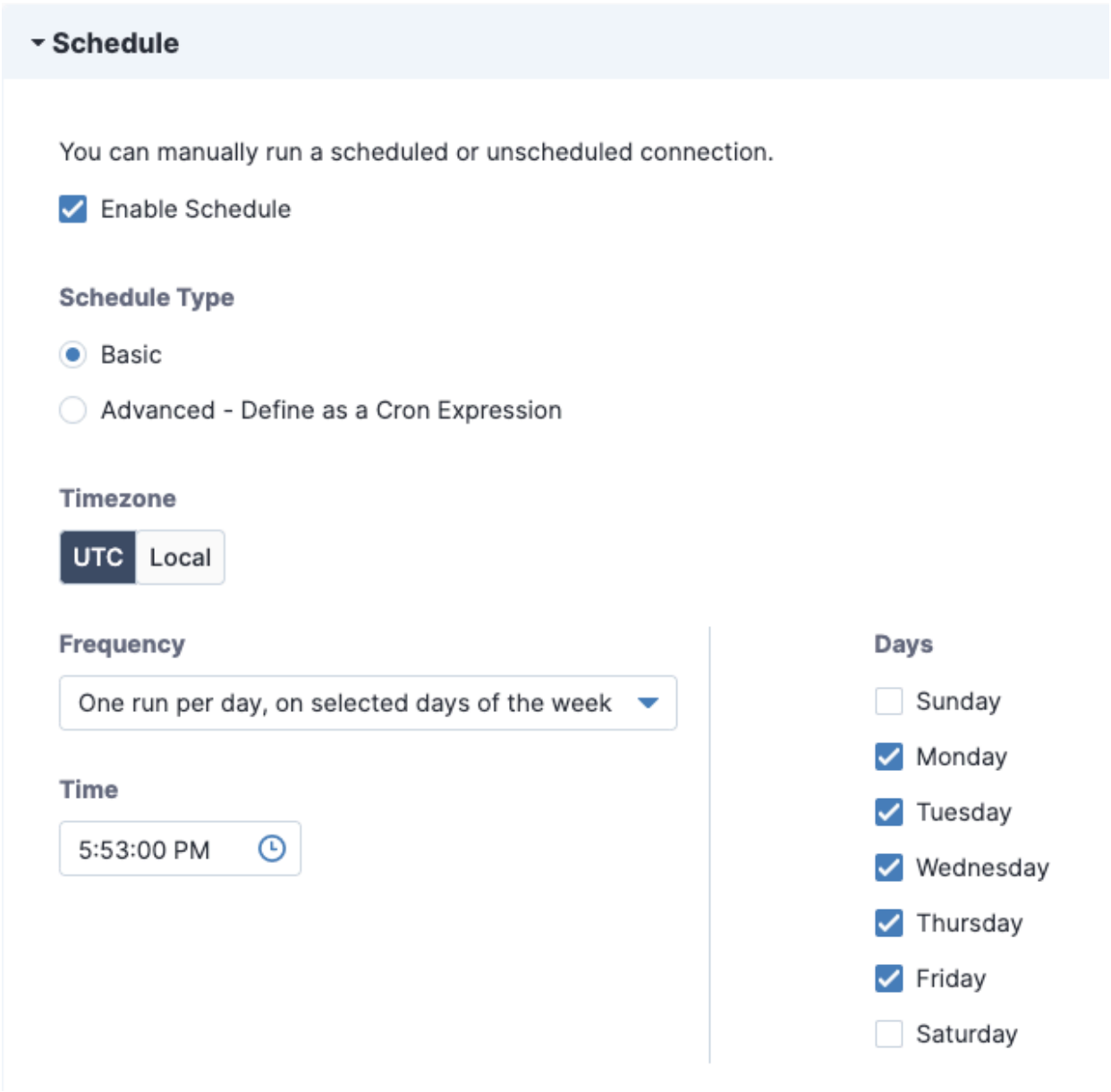
Important: Connections scheduled to run during an upgrade of Connect, or any Tanium solution configured as a connection source, might be interrupted or fail. Schedule your connections to run at a different time than your Tanium upgrades.

Note: If you do not enable the schedule, the connection only runs when you manually run it, unless you configure an **Event** source. Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Schedule** section to update the schedule:

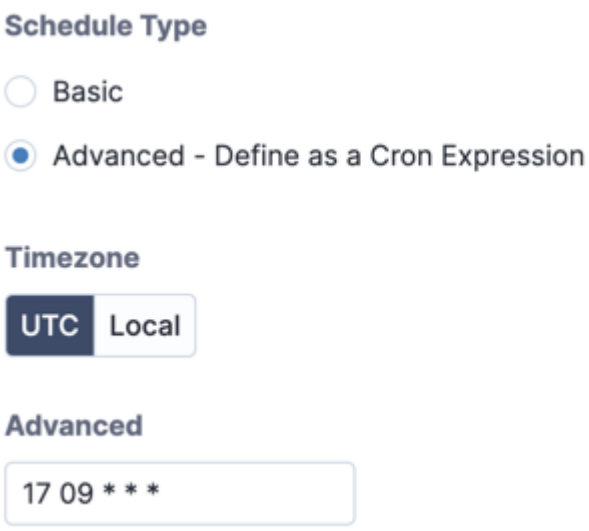
- Select **Enable schedule**.
- In the **Schedule Type**, select **Basic** to build a schedule with the provided controls.

©2026 Tanium Inc. All Rights Reserved



- To view or edit the cron expression directly, select **Advanced - Define as a Cron Expression**, and use the **Advanced** field to edit the cron expression.

©2026 Tanium Inc. All Rights Reserved



Note: If a user that owns a scheduled connection is deleted, future scheduled instances of that connection do not run. For more information, see Issue: Scheduled connection owned by a deleted user no longer runs on page 243.

For more information about cron syntax, see Reference: Cron syntax for Connect on page 253.

Enable listening for an event

Connections with **Event** sources only run when a configured event is detected, and cannot be scheduled or manually run.

Use the **Enablement** section to send data when a configured event is detected:

- Select **Listen for this Event**.

Save and verify connection

1. After you enter the details for the connection, click **Save**.

   Tip: To save the connection and immediately run the connection, click **Run and Save**.

   If needed, resolve any errors or missing information. After the connection creates successfully, the connection details appear.

©2026 Tanium Inc. All Rights Reserved

2. To view details when the connection runs, click the **Logs** tab.
3. To view an individual run log, expand the row table. For more information about how to resolve errors, see Troubleshooting on page 234.

©2026 Tanium Inc. All Rights Reserved

Maintaining Connect

Perform monthly maintenance tasks to ensure that Connect successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Connect is not performing as expected, you might need to troubleshoot issues or change settings. For more information about related procedures, see Troubleshooting on page 234.

Review and remediate connection issues

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

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

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

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

2. Review connection throughput metrics to check for issues. For more information, see Tanium Connect User Guide: View connection metrics.
3. Troubleshoot connection issues if necessary. For more information, see Tanium Connect User Guide: Troubleshooting.
4. Edit connections if necessary to resolve failures. For more information, see Tanium Connect User Guide: Edit connections.
5. Delete or disable connections that are no longer required if you have the authority to perform those actions:

©2026 Tanium Inc. All Rights Reserved

a. From the Main menu, go to **Modules** > **Connect** > **Connections**.
b. Select the connections that require an action and select **Actions** > **Disable** or **Actions** > **Delete**.

Review and remediate connection schedules

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

Review and update connection owners

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

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

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

©2026 Tanium Inc. All Rights Reserved

- If an alternative persona runs the connection, verify the persona permissions. For more information, see Tanium Console User Guide: View effective role permissions for a persona.

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

Review and remediate destination issues

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

©2026 Tanium Inc. All Rights Reserved

Troubleshooting

Troubleshoot Connect by using log files and the solutions to common issues. If you cannot resolve the issues, collect support 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.

To download logs:

1. From the **Connect Overview** page, click Help ?.
2. From the **Troubleshooting** tab, select the solutions for which to gather troubleshooting packages and click **Create Package**.
3. When the package is ready, click **Download Package**. A ZIP file of Connect information, and database information if selected, downloads to the local download directory.

   Tip: Some browsers might block multiple downloads by default. Make sure to configure your browser to permit multiple downloads from Tanium Console.
4. Contact Tanium Support to determine the best option to send the ZIP files. For information, see Contact Tanium Support on page 247.

Upgrading to Connect 5.18 or later

©2026 Tanium Inc. All Rights Reserved

Note: If you have a Connect version earlier than 5.13.391 installed, upgrade to Connect 5.13.391 first. Verify that your environment properly updated. Sign in to Tanium Console as a Platform Administrator, then navigate to the Connect Overview page. A banner appears if any problems occurred during the upgrade to Connect 5.13.391. No banner appears if the upgrade completed without any problems. Then upgrade to the current Connect version.

Connect 5.18 increases the minimum required version for several feature-specific solution dependencies. When you upgrade to Connect 5.18 or later, also upgrade all feature-specific solution dependencies to the new minimum required version. For more information about minimum versions, see Solution dependencies on page 26.

If you upgrade to Connect 5.18, and have feature-specific solution dependencies that do not meet the minimum version, connections that use the solution as a source prior to upgrade attempt to run, but log a warning and might return partial data or fail.

Configure per-connection log level

About this task

When you troubleshoot a connection or want to limit unnecessary logging, you can configure a log level that applies only to that connection without affecting the global log settings.

1. On the Connect **Overview** page, go to the **Connections** section. You have the following options:
   - Click **Create Connection**.
   - Click an existing connection. Then click **Edit**.
2. In the **General Information** section, expand **Advanced** to configure the following settings:

   Log Level

   By default, **Log Level** is set to **Information**. To reduce the amount of logging, you can set **Log Level** to **Warning**, **Error**, or **Fatal**.

   Override Log Level

   If you are debugging the connection, select **Override Log Level** to set a **Temporary Log Level** (such as **Trace** or **Debug**) on this connection for a selected **Number of Runs** (up to **24**). A scheduled or manual connection run, once started, counts towards the number of runs, regardless of the connection status. After the number of runs elapses, the logging for this connection returns to the **Log Level** you selected to prevent finer-grained

©2026 Tanium Inc. All Rights Reserved

logging from consuming additional resources for an indefinite number of runs.

To use the **Override Log Level** option to collect a trace log, see Collect a trace log for a connection on page 236.

Collect a trace log for a connection

About this task

Use the **Override Log Level** option to collect a trace log for a single connection. You can review the trace log to debug the connection or upload the log to a support case.

1. On the Connect **Overview** page, go to the **Connections** section. Click a connection, and then click **Edit**.
2. In the **General Information** section, expand **Advanced**.
3. Select **Override Log Level** to temporarily capture detailed log output for a set number of connection runs.
4. Set **Temporary Log Level** to **Trace**.
5. Set **Number of Runs** to `5`.
6. Click **Save and Run**.
7. After the connection runs complete, click Download to the right of the connection log.
8. Review the trace log or upload the log to a support case.

Result

For more information about the **Override Log Level** option, see Configure per-connection log level on page 235.

Configure general log settings

Adjust log expiration

To adjust the number of days before log files are removed, click Settings on the Connect **Overview** page and navigate to the **Configuration** tab. Edit the number of days in the **Connection Run Log**

©2026 Tanium Inc. All Rights Reserved

Expiration field and click **Save**.

Adjust log level

To adjust the log level, choose a log level from the **Connect Service Log Level** menu and click **Save**.

View logs

Service logs

In a TanOS environment, the Connect service records logs in the /opt/Tanium/TaniumModuleServer/services/connect-files/server.log file. In a Windows environment, the Connect service records logs in the \Program Files\Tanium\Tanium Module Server\services\connect-files\logs\server.log file. This file is in JSON format by default, but you can use the Bunyan CLI tool to view the logs. For example, from the \Program Files\Tanium\Tanium Module Server\services\connect-files\ directory in a Windows environment, run the following command:

```
..\connect-service\node ..\connect-service\node_modules\bunyan\bin\bunyan logs\server.log
```

Search this log for the following message to tell when the Connect service starts:

```
Tanium Connect Starting
```

Connection run logs

Connections generate a log file for each run of the connection. In a TanOS environment, the run logs are in the /opt/Tanium/TaniumModuleServer/services/connect-files/logs/connections/ directory. In a Windows environment, the run logs are in the \Program Files\Tanium\Tanium Module Server\services\connect-files\logs\connections\ directory.

Connect configuration state

Connect stores information about connections and user settings in a database managed by the Tanium RDB Service.

©2026 Tanium Inc. All Rights Reserved

Important: Do not directly access this database unless advised by Tanium Support. If you want to view this information, download a support package that includes database information. For more information, see Collect logs on page 234.

Test connections

About this task

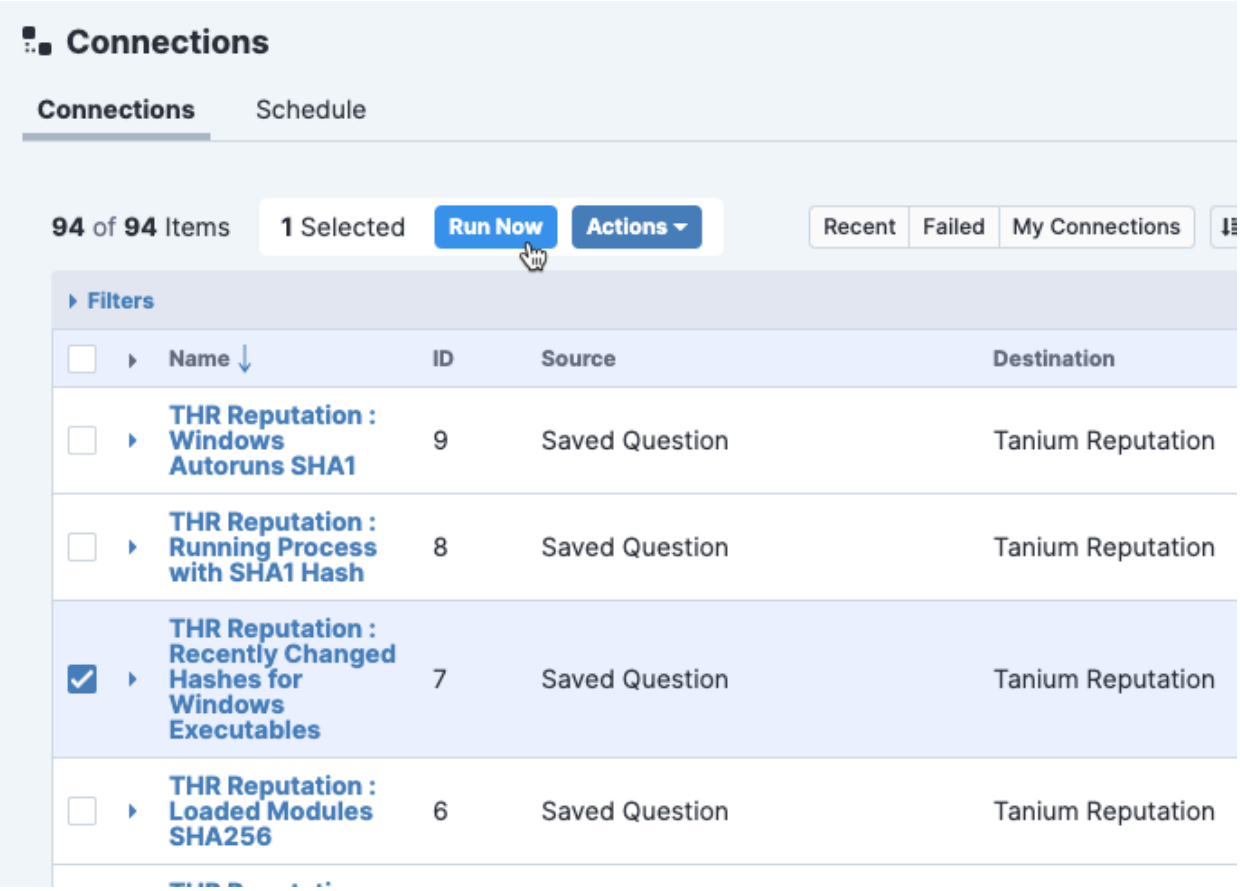
You might have trouble running a connection for one of the following reasons:

- The API token that Connect uses to run the connection was manually deleted or rotated
- The user who owns the connection no longer has access to the connection
- The persona used to run or schedule the connection is no longer associated with a user

You can sign in as the user that owns the connection and view the Connect **Overview** page, then run the connection outside of the scheduled intervals.

1. Sign in as the user that owns the connection. From the Main menu, go to **Modules** > **Connect** > **Overview**.
   Wait several minutes before moving on to the next step.
2. Send a test connection.

©2026 Tanium Inc. All Rights Reserved



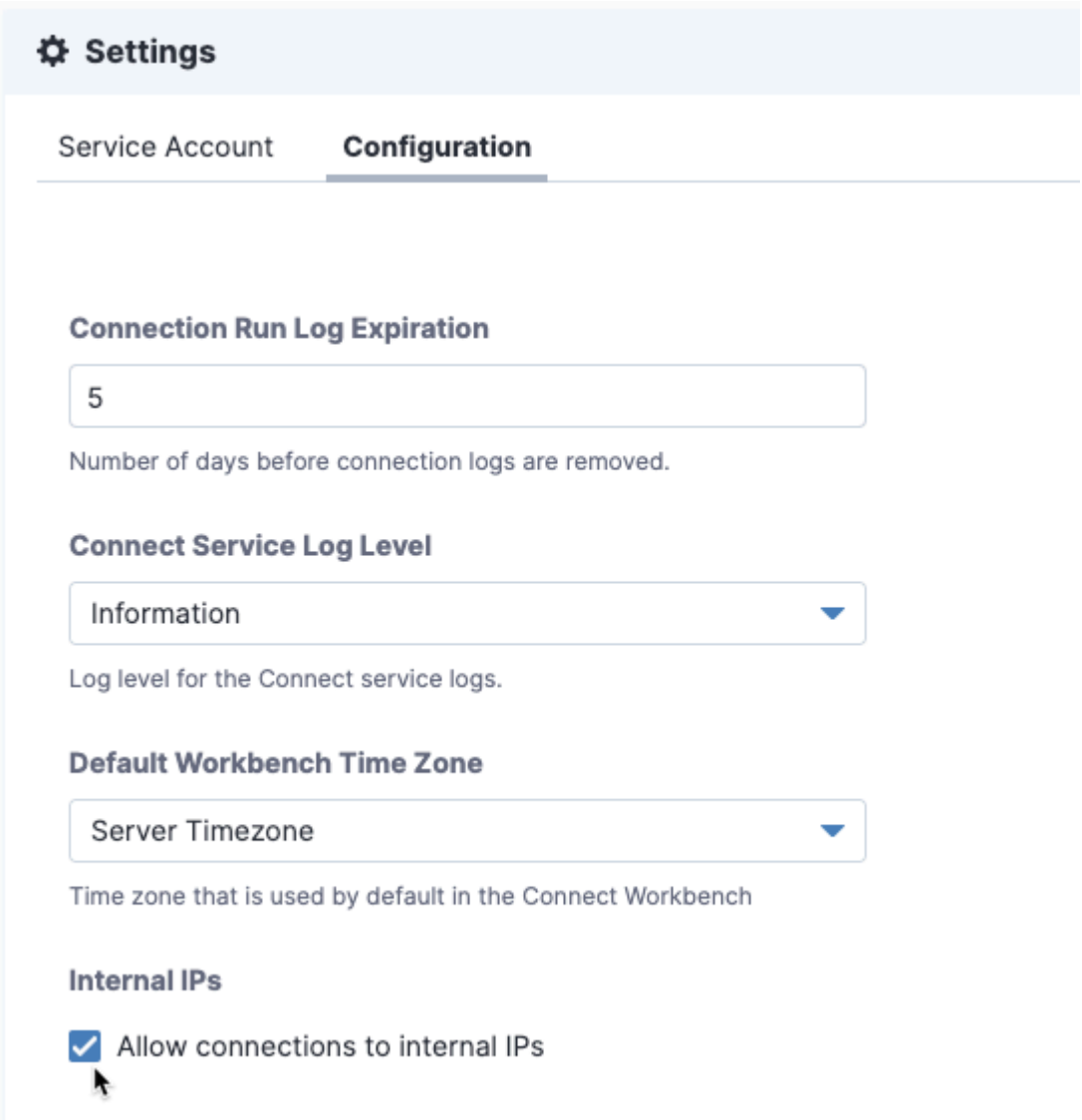
From the Connect **Overview** page, go to the **Connections** section. Select the checkbox next to the connection, click **Run Now**, and confirm to run the connection.

3. Click the connection and open the **Logs** tab to view information about each run for that connection. Expand an individual row to view the log.

   Tip: If you need more log data, open the **Details** tab, update the **Log Level** value, and click **Save**. Run the connection again to view the log with the updated log level.

4. If the IP address for a connection is on an internal network, only a Tanium administrator can run the connection by default.

©2026 Tanium Inc. All Rights Reserved



Click Settings on the Connect **Overview** page. On the **Configuration** tab, select **Internal IPs** to allow anyone to run connections to IPs on an internal network.

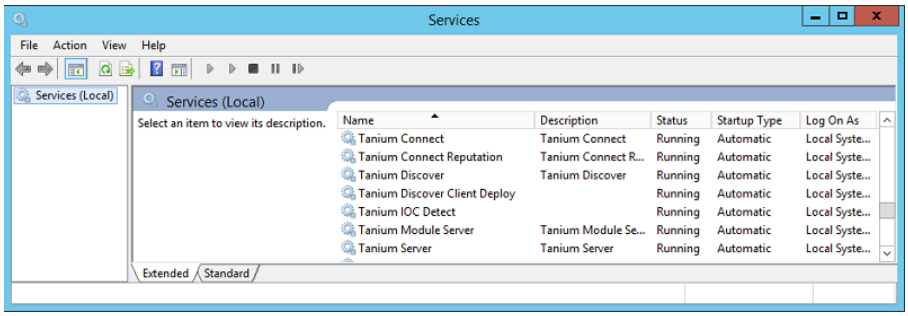
Troubleshoot issues

Note: If a connection fails to send any data in a 60-minute period, Connect automatically terminates the connection.

Issue: Cannot connect to Connect service

1. Verify that the Connect service is running on your Module Server.

©2026 Tanium Inc. All Rights Reserved



To view the running services, click **Start** > **Run**. Type `services.msc` and click **OK**. Verify that Connect is in the list and that the service is running.

2. Check the service logs for any errors or messages about insufficient rights for the user. In a TanOS environment, the Connect service records logs in the /opt/Tanium/TaniumModuleServer/services/connect-files/server.log file. In a Windows environment, the Connect service records logs in the \Program Files\Tanium\Tanium Module Server\services\connect-files\logs\server.log file.

Issue: Connection fails

There are multiple reasons that might cause connections to fail. When a connection fails, review the log of the connection to determine the reason why the connection failed:

1. From the Main menu, go to **Modules** > **Connect** > **Connections**.
2. In the row of the connection that failed, click the date in the **Last Run Status** column.
3. Expand the log for a failed run to review any errors.

   Alternatively, click Download and review the log in your preferred editor.

CONNECTION REACHED MEMORY CEILING

Connect has a global memory ceiling of 8GB for all connections in addition to an individual limit that you can configure for each connection.

Symptom

When a connection reaches its individual memory ceiling, an error similar to the following appears in the log:

```
Connection Failed. The node process which was running this connection returned an exit code/
```

©2026 Tanium Inc. All Rights Reserved

```
status which indicates the process ran out of memory.
```

Resolution

Potential resolutions include the following:

- Add filters to the connection to reduce the amount of data sent in the connection. For more information, see Reference: Filtering options on page 257.
- Increase the memory ceiling of the connection.
    1. From the Main menu, go to **Modules** > **Connect** > **Connections**.
    2. Click the name of the connection to view details for the connection, and then click **Edit**.
    3. In the **General Information** section, expand the **Advanced** sub-section.
    4. Edit the **Memory Ceiling** as necessary and then click **Save**.

Issue: <no value> in Tanium Data Service (TDS) output

1. Verify that the sensor for the saved question is registered with TDS. For more information, see Tanium Interact User Guide: View sensor registration details.
2. If the sensor is not registered, register it for collection. For more information, see Tanium Interact User Guide: Register or unregister sensors for collection.

Issue: Connection does not export all intended data

Connections use the role permissions of the owner to access content. If the connection owner has insufficient permission for content that a connection requires, such as inability to view a computer group, the connection might not fully export the data that you intend to export.

To resolve, update the owner's permissions to allow access to intended content. For more information and descriptions of content sets and permissions, see Tanium Console User Guide: RBAC overview.

Issue: Columns are missing from the Microsoft Azure Monitor table

©2026 Tanium Inc. All Rights Reserved

Symptom

After a connection run completes successfully, one or more columns are missing from the custom table in Microsoft Azure Monitor. Connect does not report an error.

Cause

The `streamDeclarations.columns` array in your data collection rule (DCR) does not include all columns that Connect is sending. Microsoft Azure silently drops any column that is not declared in `streamDeclarations.columns` before the transformation runs. No error is logged on either the Connect or Microsoft Azure side.

Resolution

Add the missing columns to both `streamDeclarations.columns` in the DCR and the Microsoft Azure Monitor table schema. The columns in `streamDeclarations.columns` must match your Connect connection output configuration exactly. For more information, see Configure the Microsoft Azure Monitor destination on page 170.

Missing column symptoms and resolutions for Microsoft Azure Monitor destinations

Symptom	Cause	Resolution
Some columns are missing from the Azure Monitor table	`streamDeclarations.columns` does not list those columns	Add the missing columns to `streamDeclarations.columns` and to the table schema
Only TimeGenerated and Type appear in the table, with no custom data	`streamDeclarations.columns` has no custom columns defined	Add all Connect output columns to `streamDeclarations.columns` and the table schema

Issue: Scheduled connection owned by a deleted user no longer runs

Scheduled connections require an existing Tanium user account owner to run scheduled instances. If the scheduled connection owner is deleted, future scheduled instances of that connection do not run.

To resolve, export and import the scheduled connection to create a new scheduled connection. For more information, see Export connections and Import connections.

©2026 Tanium Inc. All Rights Reserved

Issue: Tanium Audit Source connection fails with MaxNumberOfAuditEntriesPerCacheExceeded error

Connections configured with the **Tanium Audit Source** connection source might fail if you configure **Days of History Retrieved** as `0` or a very large value, and a large period of time elapses between connection runs. Update the **Days of History Retrieved** value to a small integer, such as `1` or `2`. For more information, see Reference: Tanium Audit Source data on page 301.

> **Note:** If you want to send a large number of audit entries per connection run, you can also increase the **max_soap_audit_entries_per_cache** advanced setting. Contact Tanium Support on page 247 for guidance before you edit advanced settings. For more information, see Tanium Console User Guide: Manage advanced settings.

Issue: Emails to Microsoft 365 destinations fail to send

Emails sent to Microsoft 365 destinations are subject to the following limitations:

- The Email (O365) destination requires an email server profile. If you delete an email server profile configuration that is referenced by a scheduled connection, future scheduled instances of that connection fail. Recreate the email server profile configuration, then reference the new email server profile in the scheduled connection.
- The Microsoft Graph API limits email requests to four concurrent requests. If you have multiple connections using the same email server profile configuration, emails over the four concurrent requests are queued for sending after prior requests resolve. Schedule connections using the same email server profile configuration to run at different times and minimize the number of requests sent simultaneously.
- If you assign the **Mail.Read** permission to your Microsoft Entra ID (formerly Azure Active Directory) application, you can send emails with attachments up to a total of 3 MB, or emails with a body up to 3 MB. If your connections send more data than that per run, do one of the following:
    - Schedule your connection to run more frequently, to try and reduce the size of each email.
    - Refine the connection source configuration to reduce the amount of data sent per

©2026 Tanium Inc. All Rights Reserved

connection run.

- Assign the **Mail.ReadWrite** permission to the Microsoft Entra ID application. This enables sending emails with attachments up to a total of 150 MB, subject to any other limits that you configure in your Azure environment.

Issue: Imported connections to Microsoft 365 destinations do not run

Exporting a connection that uses a Microsoft 365 destination from one environment and importing it in another does not also import the required email server profile configuration. To export a connection that uses a Microsoft 365 destination:

1. Export the connection from the originating environment, then import the connection in the target environment. For more information, see Export connections on page 71 and Import connections on page 72.

2. Create the email server profile in the target environment. For more information, see Configure email server profile settings for Microsoft 365 on page 44.

3. Edit the connection and select the **Email Server Profile**. For more information, see Configure the email results destination on page 125.

Issue: Created connection does not allow editing of source or destination type

After you create a connection, you cannot update the connection source type or destination type, only the source configuration or destination configuration. If you want to change the source type or destination type, create a new connection.

Issue: Cannot authenticate connection to Splunk instance using HTTP destination

Connections to Splunk instances that use the HTTP destination cannot authenticate against the Splunk instance unless `Splunk` and a space precede the token string. Configure an HTTP header named `Authorization`. Then configure an HTTP header value in the format `Splunk <token-string>`.

1. From the **Create Connection** page, enter a **Name** and select a **Source**. Then select **HTTP** as the **Destination**.

2. Select **Header Authentication** from **Use Authentication**.

©2026 Tanium Inc. All Rights Reserved

3. Enter `Authorization` in the **Auth Header Name** field.
4. Enter the Splunk token string in the **Secret** field, using the format `Splunk <token-string>`.
5. Enter other information required for the connection.
6. Click **Save**.

Uninstall Connect

The basic Connect module uninstallation is designed so that the data you have collected is restored if you later decide to reinstall Connect. In some cases, you might want to start "clean" and not restore the data. To do this, you must manually remove some files.

Important: Consult with Contact Tanium Support on page 247 before you uninstall or reinstall Connect.

Uninstall Connect so data is restored on reinstall

1. Sign in to Tanium Console as a user with the Administrator role.
2. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.
3. Under **Connect**, click **Uninstall**.
4. Review the summary and click **Uninstall**.
5. When prompted to confirm, enter your password.

If you later import the Connect solution, the previous data is restored.

Uninstall Connect so you start fresh when you reinstall

1. Uninstall Connect so data is restored on reinstall on page 246.
2. Manually delete the connect-files directory. You have the following options:

©2026 Tanium Inc. All Rights Reserved

- In a Windows environment, manually delete the \Program Files\Tanium\Tanium Module Server\services\connect-files\ directory.
- In a Linux environment, manually delete the /opt/Tanium/TaniumModuleServer/services/connect-files/ directory.

Deleting the connect-files directory removes all existing Connect data. All logs, output, the Connect database, and any other Connect data is deleted. If you later import the Connect solution, the previous data is not restored.

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: Column customizations

Use column customizations to modify how data from your connection source is sent to the destination. You can do the following:

- Use a regular expression to replace matching strings in the data
- Send custom columns
- Send a subset of the columns
- Change the column name sent to the destination
- Update the column value data type
- Reorder the columns for supported formats (CSV, Delimiter Separated Values, LEEF, or Syslog RFC 5424)

Column customizations require a source and a destination, and apply only to the configured connection. You can modify one or more columns for the connection, and send the remaining data without changes.



Note: Column customizations consume additional resources for each connection run.



Best Practice: For the best results, if you use any sensors with a **TDS Registered Sensor** label as a column customization, rather than updating an existing connection, create a new connection with these custom columns, then disable and delete your existing connection.

Replace data that matches a regular expression

About this task

Before data is sent to a destination, you can search the data for string values that match a regular

©2026 Tanium Inc. All Rights Reserved

expression escape statement, and replace matching strings with a data substitution value.

1. From the Main menu, go to **Modules** > **Connect** > **Overview**, go to the **Connections** section, and click **Create Connection**.
2. From the **Create Connection** page, in the **Configuration** section, select a **Source** and **Destination**.
3. Select **Configure Output** > **Format**.
4. Select a **Format** that is compatible with this source and destination.
5. In the **Value Escape Regex** field, enter a regular expression escape statement.
6. In the **Value Escape Replace** field, enter a data substitution value. Each string that matches the **Value Escape Regex** statement is replaced with this **Value Escape Replace** string.
7. Click **Save**.

Example

Regular expression syntax and behavior

The **Value Escape Regex** and **Value Escape Replace** fields work together to reformat sensitive or inconsistent data before it reaches the destination.

- **Value Escape Regex** uses JavaScript regular expression syntax. Matching is case-sensitive. The statement replaces every match in a value, not just the first match. Connect applies the pattern to each column value individually and does not modify numeric or empty values.
- **Value Escape Replace** contains the text that replaces each match. Leave the field empty to delete the matched text. Reference capture groups from the pattern with `$1`, `$2`, and so on, or use `$&` to reference the entire match. To include a literal dollar sign in the replacement text, use `$$`.
- If the regular expression is not a valid statement, or if the pattern causes excessive processing such as nested repetition like `(a+)+`, the connection run fails with an error.

Regular expression examples

Goal	Value Escape Regex	Value Escape Replace	Input value	Output value
Escape commas before sending CSV data	`,`	`\,`	`Smith, John`	`Smith\, John`
Replace line breaks with a single space	`\r?\n`	A space character	A multiple line value	A single line value

©2026 Tanium Inc. All Rights Reserved

Goal	Value Escape Regex	Value Escape Replace	Input value	Output value
Mask digits in a value	`[0-9]`	`*`	`Card 4111`	`Card ****`
Redact a Social Security number format	`\d{3}-\d{2}-\d{4}`	`***-**-****`	`123-45-6789`	`***-**-****`
Remove double quotes from a value	`"`	Leave the field empty	`"C:\temp"`	`C:\temp`
Reorder a date using capture groups	`(\d{2})/(\d{2})/(\d{4})`	`$3-$1-$2`	`01/03/2000`	`2000-01-03`

Send custom columns to the destination

About this task

You can send the following custom column values:

- **Connection Variable**, which sends the **Connection Name**, **Connection Run ID**, or **Source Name**
- **Timestamp** of when the data is sent
- **User Specified Value** as a numeric, string, or unmodified value

You can add multiple custom columns for each connection.

1. From the Main menu, go to **Modules** > **Connect** > **Overview**. Go to the **Connections** section and click **Create Connection**.
2. From the **Create Connection** page, in the **Configuration** section, select a **Source** and **Destination**.
3. Select **Configure Output** > **Columns**.
4. Click **+ Add Column**.
5. Enter a **Source Column Name**.
6. Select a **Custom Column Type**. You have the following options:
    - If you select **Connection Variable**, select a **Value Type** and **Destination Value**.
    - If you select **Timestamp**, select the Date/Time **Value Type** and a **Date/Time Format**:

©2026 Tanium Inc. All Rights Reserved

Example outputs for date/time formats

Date/Time format	Output format	Example
MM/DD/YYYY	`MM/DD/YYYY`	`01/03/2000` - January 3, 2000
ISO 8601 with time zone (formerly **RFC-3339 Timestamp**)	`YYYY-MM-DDThh:mm:ss+hh:mm`, with the time zone offset set to either the local time zone, or Coordinated Universal Time (UTC) if the column input or Tanium Server time zone is UTC	`2000-01-03T04:05:06-05:00` - January 3, 2000 at 04:05:06 in Eastern Standard Time (UTC-05:00)
ISO 8601 UTC (Zulu)	`YYYY-MM-DDThh:mm:ssZ`, with the timestamp set to UTC	`2000-01-03T04:05:06Z` - January 3, 2000 at 04:05:06 in UTC

- If you select **User Specified Value**, select a **Value Type** and enter a **Destination Value**.

7. Click **Save**.

Customize the source columns sent to the destination

1. From the Main menu, go to **Modules** > **Connect** > **Overview**, scroll to the **Connections** section, and click **Create Connection**.
2. From the **Create Connection** page, in the **Configuration** section, select a **Source** and **Destination**.
3. Select **Configure Output** > **Columns**.
4. Select which source columns to send to the destination. Select a **Source** checkbox to send the column values, or clear a **Source** checkbox to not send the column values.
5. Update a column name. Enter a **Destination Label**, or select one from the dropdown list if you selected the CEF output format.
6. Update the data type of a column. Select a **Value Type** from the dropdown list, or select **Unmodified** if you do not want to change the data type. Note the following:
    - If you choose **Numeric** for the value, you can specify a default value that is used if the data cannot be coerced into a numeric value. You can specify any negative or positive

©2026 Tanium Inc. All Rights Reserved

number.

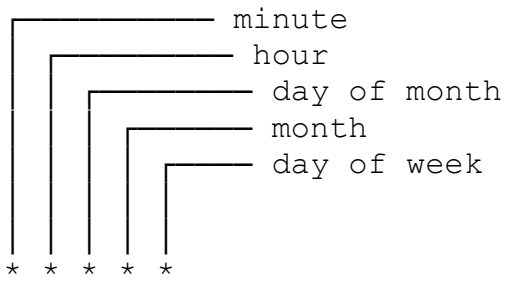
- If you choose **Date/Time** for the value, specify the format that you want to use for the column.

7. Reorder how the data values are sent to the destination if you select the CSV, Delimiter Separated Values, LEEF, or Syslog RFC 5424 output format. Click **Reorder Columns**. Drag the columns into the desired order, then click **Confirm**.
8. Click **Save**.

©2026 Tanium Inc. All Rights Reserved

Reference: Cron syntax for Connect

A quick reference to cron syntax follows. You can use Crontab to build a cron expression.



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: Deprecated connection migration

Connection sources and destinations might be deprecated in favor of other connection sources or destinations that offer improved functionality, or for other reasons. If your connections use deprecated functionality, update your Connect configuration to create connections that use the suggested replacement.

Migrating Tanium Trends connections to Tanium Reporting connections

About this task

The Trends solution is deprecated beginning May 20, 2025. Migrate Trends boards to the Tanium Reporting solution. For more information, see Tanium Trends User Guide: Migrating Trends boards to Reporting.

For each connection that is configured with the **Tanium Trends** source , configure a replacement connection that uses either the **Tanium Reporting (Reports and Dashboards)** source or the **Tanium Reporting (Source Data)** source:

1. Migrate the Trends board to Reporting. Verify that the Trends board migrated successfully, and record the name of the migrated Reporting dashboard or report. For more information, see Tanium Trends User Guide: Migrating Trends boards to Reporting.
2. From the Main menu, go to **Modules** > **Connect** > **Connections**.
3. Click **Create Connection**.
4. Enter a connection **Name** that describes that this connection uses a migrated Trends board, such as prepending `(MIGRATION-TEST)` to the name.
5. Optionally, update the connection **Description** with the name of the deprecated connection that uses a **Tanium Trends** source for reference.
6. You have the following options:

©2026 Tanium Inc. All Rights Reserved

- If the Trends board is migrated to a Reporting dashboard, select **Tanium Reporting (Reports and Dashboards)** from **Source**, and then select the migrated **Dashboard**.
- If the Trends board is migrated to a Reporting report, select **Tanium Reporting (Source Data)** from **Source**, and then select the migrated **Report**.

7. Select a **Destination**. Configure the destination to point to a test server as needed.
8. Click **Save**.
9. Click **Run** to test the connection and verify that it properly sends information to the intended destination. Update the configuration as needed.
10. From the Main menu, go to **Modules** > **Connect** > **Connections**.
11. Select the deprecated connection that uses a **Tanium Trends** source. Click **Edit**.
12. Update the connection **Name** to signify that it uses a deprecated source, such as prepending `(DEPRECATED)` to the name.
13. Optionally, update the **Description** with the replacement connection name for reference.
14. If this connection has a configured schedule, clear **Enable Schedule**.
15. Click **Save**.
16. Update the new connection configuration to rename the connection to a permanent name and remove information such as `(MIGRATION-TEST)`, to send data to an intended destination, and to update the schedule as needed.

Result

Repeat this procedure for each connection that is configured with the Tanium Trends source. Monitor the new connections to confirm that the configuration is expected, and that Reporting data is sent to the intended destination on the intended schedule. Only after you confirm that all of your migrations work as expected, delete the deprecated connections:

1. From the Main menu, go to **Modules** > **Connect** > **Connections**.
2. Enter the string value that you used to identify deprecated connections, such as `(DEPRECATED)`, in the **Filter items** field. The table updates to show only these connections.
3. Review the list to confirm that each connection has been replaced with a new connection

©2026 Tanium Inc. All Rights Reserved

that uses either the **Tanium Reporting (Reports and Dashboards)** source or the **Tanium Reporting (Source Data)** source.

4. If you want to create a backup, select all connections, and then click **Actions** > **Export**.

5. Select all connections, and then click **Actions** > **Delete**. Confirm the deletion.

©2026 Tanium Inc. All Rights Reserved

Reference: Filtering options

Use filters to modify the data that you are getting from your connection source before it is sent to the destination. If you do not define a filter, all data from the source is sent to the destination.

You can filter data by regular expressions, new items, or numeric operators.

Filters are linked to specific connections. You can create a filter when you create a connection, or you can edit the existing connection to add or update a filter. You can define multiple filters per connection. If you define multiple filters, a piece of data must meet the conditions in all of the filters to get passed on to the destination.

For example, when you use the **CPU utilization over 75%** saved question, you can specify a numeric filter that has a condition for CPU consumption greater than 80%, and a regular expression filter for computer name that starts with `srv*`. Both these filter conditions must be met for the data in a row to be passed to the destination.

New Items

With the New Items filter, only new data is sent to the destination. When you configure this filter, you set a *learning period* value and the number of days to learn. During this period, no data is sent to the destination while a set of baseline data is established. A hash of the data is stored in a database that tracks the baseline.

If the number of days is set to zero, the learning period is skipped and data begins to send immediately. Because the baseline starts empty, the first connection run sends all rows currently returned by the source. Subsequent runs send only new or changed rows.



Note: Connect uses a non-cryptographic FNV hash function in a Bloom filter to filter data. In rare instances, the Bloom filter might improperly identify new data and not send it to the destination. However, the Bloom filter always properly identifies existing data, which is not sent to the destination.

All the values in each row of data are considered when the data is evaluated for updates. For

©2026 Tanium Inc. All Rights Reserved

example, your connection source might be a saved question that has four columns: computer name, running processes, MD5 hash of running process, and logged in user. A change to any of the values in those columns causes the row to be flagged as new. All the data in the row is sent to the connection destination.

Selecting a subset of columns to index adjusts which columns are evaluated when determining if a new result should be added to the output of the next connection run.

Note:

The following columns are always excluded from hashing and are never used to evaluate uniqueness, even if you select them as index columns:

- `Connection Run ID`
- `Count`
- `Age`
- `Computer ID`
- `RowId`
- `Band Number`
- `Row Number`

To track data per endpoint, use `Computer Name` or `Computer Serial Number` instead of `Computer ID`.

Only successful connections update the baseline data. If a connection fails, the baseline data remains the same as before the failed connection attempt started, to prevent the loss of new data.

To clear the baseline data or restart the learning period, see Clear New Items cache on page 76.

Continue Learning options

©2026 Tanium Inc. All Rights Reserved

After the learning period, only new or changed data is sent through to the destination. The default behavior is for the baseline data to continue to be updated with new data after the learning period.

However, you can also deselect the **Continue Learning** setting. When this setting is disabled, the baseline data from the original learning period is maintained going forward and is not updated.

The **Persist Data** setting, when enabled, keeps the filter on disk in between connection runs. This default behavior works for most configurations. You might want to disable this setting if you are trying to replicate the behavior of the removed Unique Values from Columns filter.



Important: The **Persist Data** setting must be enabled for the learning period configuration to work.

You can also specify how often the filter, along with the learned baseline data, is periodically reset in the **Scheduled Filter Reset Days** setting. When **Learning Period** is greater than `0`, a scheduled reset does not cause all data to be resent. When **Learning Period** is set to `0` days, the first connection run after a reset sends all rows currently returned by the source.

Using the New Items filter with time-windowed sources

For sources that return time-windowed data (such as Interact events or Guide alerts), events that fall outside the query window are no longer available in subsequent runs. To avoid missing events during slow collection periods, configure the lookback window of the source query to be longer than the connection run interval.



Note: When time windows overlap, some rows appear in consecutive runs. The New Items filter deduplicates these rows automatically. Any row already seen in a prior run is not forwarded to the destination a second time.

To begin sending events on the first run without delay, set **Learning Period** to `0` days.

Regular Expression

With the Regular Expression match option search, you choose a column in your results to evaluate against your regular expression. If any matches occur, the whole row that contains the matched

©2026 Tanium Inc. All Rights Reserved

column is returned as a result.

Tip: Connect uses regular expression syntax that is compatible with JavaScript, and evaluated as case-insensitive.



Note: Do not use regular expressions that are vulnerable to catastrophic backtracking.

Connect validates regular expression filters for vulnerability to catastrophic backtracking. Any connections that fail this validation do not run successfully; this helps prevent both excess resource use and frozen or failed connection runs. If you upgrade to Connect 5.18 or later, you also cannot save new or existing connections that fail this validation.

Valid regular expression example

Suppose that you want to filter for only 100 Mbps Connections with the Link Speed sensor. The saved question is `Get computer name and Tanium IP Address and Link Speed`. Create a filter on the Link Speed column with the regular expression: `(?!10000)(?!1000)(100)`. This particular example excludes 1000 and 10000, because by default these values are returned when searching for 100.

Invalid regular expression example

Suppose that you want to filter for endpoints that have a local reported IPv4 address they are using to communicate with the Tanium Server. The saved question is `Get computer name and Tanium Client IP Address`.

If you create a filter on the Tanium Client IP Address column with the regular expression `^(?:[0-9]{1,3}\.){3}[0-9]{1,3}$`, then try to save the connection, the connection fails to save. This regular expression has excessive backtracking to evaluate the IPv4 address octets, and does not pass validation.

If you update the connection filter with the regular expression `^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$`, then try to save the connection, the connection saves. This regular expression evaluates each IPv4 octet without backtracking, and passes validation.

©2026 Tanium Inc. All Rights Reserved

Numeric Operator

Filter on a specific numeric column in your data set. You specify the column name, an operation (greater than or less than) and a target value. The data set is evaluated, and only the rows that meet the condition specified are sent to the destination.

©2026 Tanium Inc. All Rights Reserved

Reference: Format types

When you create or edit a connection, you can select the format of the data to send.

You can include identifying information with data sent to destinations, such as a SIEM, depending on the data format available for a source.

To include the system-generated source name, you can use a logging data format or JSON:

- CEF data format - the default **Source** field value
- LEEF data format - the default **Source** field value
- JSON data format - select **Wrap Data with Text**
- Syslog RFC 5424 data format - the default **SD-ID** field value

To include the system-generated saved question name, you can use the Syslog RFC 5424 data format with saved question-related sources:

- Syslog RFC 5424 data format with **Saved Question** source - select **Send Question Source**
- Syslog RFC 5424 data format with **Tanium Data Service** (TDS) source - select **Send Question Source**

To include custom information, you can use column customizations, or specific fields for the CEF and Syslog RFC 5424 data formats:

- CEF data format - the **Signature ID** field value, or a column customization
- Syslog RFC 5424 data format - the **MSG ID** field value, or a column customization
- other data formats - a column customization

For more information about column customizations, see Reference: Column customizations on page 248.

©2026 Tanium Inc. All Rights Reserved

Note: You cannot include identifying information with data from the **Tanium Endpoint Configuration** or **Tanium Trends** sources.

CEF

Common Event Format (CEF) is the default format for HP ArcSight. When you define CEF format for your destination, you can include advanced settings such as the device vendor, product and version, product name, version, source, and the end of entry separator character. For the separator, you can use escape characters such as: `\t` (tab), `\n` (new line), and `\r` (carriage return). Select the columns that you want to pass through to the destination. Some fields also support variable substitution, as listed in Reference: Variables on page 295.

Note: You cannot select this format if you select an event data source.

This format generates CEF version 0.1 output.

```
May 29 19:34:20 example_host CEF:0|Tanium|Tanium Application Server|1|0|Tanium
Audit Source|0|objectid=732 auditname=New-Session-Created creationtime=Wed May
29 2024 19:33:53 GMT+0000 (Coordinated Universal Time) modificationtime=Wed May
29 2024 19:33:53 GMT+0000 (Coordinated Universal Time) lastmodifiedby=
modifieruserid=0 details=User:-admin@example.com;-Session-ID:-65406781;
-Authentication-Type:-User;-Originated-from-SOAPPluginScheduler
auditrowid=58245268 type=0 typename=CreateObject objectname=
objecttypename=authentication audittype=authentication_audit
```

You can use the **Source** field to include the system-generated source name with each entry, or the **Signature ID** field or column customizations to include custom information with each entry.

CEF usage of the Signature ID and Source fields

Field	Default value	Output value	Notes
Signature ID	n/a	the defined value	The CEF header includes the user-defined value.
Source	`{Source}`	`source_name`	The CEF header includes the system-generated source name.

Default destinations: HP ArcSight

CSV

©2026 Tanium Inc. All Rights Reserved

Comma-separated values. Select whether you want to include column headers in the output. Select the columns that you want to pass through to the destination.

You can use column customizations to include custom information with each entry.

Select **Include headers** to include headers in the first row.

```
"audit_row_id","creation_time","details","last_modified_by","mod_user",
"mod_persona","modification_time","modifier_user_id","object_id","type",
"audit_type","object_type_name","type_name","object_name","audit_name"
"58245351","Wed May 29 2024 19:35:07 GMT+0000 (Coordinated Universal Time)",
"User: admin@example.com; Session ID: 65406864; Authentication Type: User;
Originated from SOAPPluginScheduler","","","","Wed May 29 2024 19:35:07 GMT+0000
(Coordinated Universal Time)","0","432","0","authentication_audit",
"authentication","CreateObject","","New Session Created"
```

Clear **Include headers** to exclude headers from the output.

```
"58245351","Wed May 29 2024 19:35:07 GMT+0000 (Coordinated Universal Time)",
"User: admin@example.com; Session ID: 65406864; Authentication Type: User;
Originated from SOAPPluginScheduler","","","","Wed May 29 2024 19:35:07 GMT+0000
(Coordinated Universal Time)","0","432","0","authentication_audit",
"authentication","CreateObject","","New Session Created"
```

Select **Detect Dynamic Data Exchange (DDE)** to prepend `'` to each cell value that starts with `=`, `+`, `-`, or `@`.

```
"58245351","Wed May 29 2024 19:35:07 GMT+0000 (Coordinated Universal Time)",
"User: '+@example.com; Session ID: 65406864; Authentication Type: User;
Originated from SOAPPluginScheduler","","","","Wed May 29 2024 19:35:07 GMT+0000
(Coordinated Universal Time)","0","432","0","authentication_audit",
"authentication","CreateObject","","New Session Created"
```

Clear **Detect Dynamic Data Exchange (DDE)** to send cell values that start with `=`, `+`, `-`, or `@` without a prepended `'`.

```
"58245351","Wed May 29 2024 19:35:07 GMT+0000 (Coordinated Universal Time)",
"User: '@example_user; Session ID: 65406864; Authentication Type: User;
Originated from SOAPPluginScheduler","","","","Wed May 29 2024 19:35:07 GMT+0000
(Coordinated Universal Time)","0","432","0","authentication_audit",
"authentication","CreateObject","","New Session Created"
```

Default destinations: AWS S3, File

Delimiter separated values

To create a delimiter separated values format, enter the characters that you want to use for column and row delimiters. In addition to single characters, you can use escape characters such as: `\t` (tab), `\n` (new line), and `\r` (carriage return). Select the columns that you want to pass through to the

©2026 Tanium Inc. All Rights Reserved

destination.

You can use column customizations to include custom information with each entry.

Select **Include headers** to include headers in the first row.

```
audit_row_id|creation_time|details|last_modified_by|mod_user|mod_persona|
modification_time|modifier_user_id|object_id|type|audit_type|object_type_name|
type_name|object_name|audit_name
58245451|Wed May 29 2024 19:38:11 GMT+0000 (Coordinated Universal Time)|UserID:
4128; Session ID: 65406964; IP Address: 192.0.2.10||undefined|undefined|Wed May
29 2024 19:38:11 GMT+0000 (Coordinated Universal Time)|0|442|0|
authentication_audit|authentication|CreateObject||New System User Session
Created
```

Clear **Include headers** to exclude headers from the output.

```
58245451|Wed May 29 2024 19:38:11 GMT+0000 (Coordinated Universal Time)|UserID:
4128; Session ID: 65406964; IP Address: 192.0.2.10||undefined|undefined|Wed May
29 2024 19:38:11 GMT+0000 (Coordinated Universal Time)|0|442|0|
authentication_audit|authentication|CreateObject||
New System User Session Created
```

Elasticsearch

The Elasticsearch format is the only valid format when Elasticsearch is selected as the destination. If a saved question is selected as a source, you can expand **Advanced** in the **Format** section and select **Group columns by sensor** to return the results as an array of objects instead of an array of simple value types. You cannot customize the columns with this option. Select the columns that you want to pass through to the destination. For more information, see Configuring Elasticsearch destinations on page 107.

You can use column customizations to include custom information with each entry.

This format generates Elasticsearch-compatible output.

```
{"index":{}}
{"object_id":2179,"audit_name":"New Session Created","creation_time":
"2024-05-29T19:41:14.000Z","modification_time":"2024-05-29T19:41:14.000Z",
"last_modified_by":"","modifier_user_id":0,"details":"User: admin@example.com;
Session ID: 65407076; Authentication Type: User; Originated from
SOAPPluginScheduler","audit_row_id":58245564,"type":0,"type_name":
     "CreateObject","object_name":"","object_type_name":"authentication",
     "audit_type":"authentication_audit","@timestamp":"2024-05-29T19:42:36.75+00:00"}
```

Default destinations: Elasticsearch

©2026 Tanium Inc. All Rights Reserved

HTML

Select whether you want to include column headers in the output. Select the columns that you want to pass through to the destination.

You can use column customizations to include custom information with each entry.

This format generates an HTML document containing a table.

```
<body>
<table class="Tgrid"><tr><th>audit_row_id</th><th>creation_time</th><th>details</th>
<th>last_modified_by</th><th>mod_user</th><th>mod_persona</th><th>modification_time</th>
<th>modifier_user_id</th><th>object_id</th><th>type</th><th>audit_type</th>
<th>object_type_name</th><th>type_name</th><th>object_name</th><th>audit_name</th></tr>
<tr><td>58245676</td><td>"2024-05-29T19:43:14.000Z"</td><td>User: admin@example.com;
Session ID: 65407188; Authentication Type: User; Originated from SOAPPluginScheduler</td>
<td></td><td></td><td></td><td>"2024-05-29T19:43:14.000Z"</td><td>0</td><td>70</td>
<td>0</td><td>authentication_audit</td><td>authentication</td><td>CreateObject</td>
<td></td><td>New Session Created</td></tr></table>
</body>
```

Default destinations: Email

JSON

JavaScript Object Notation (JSON) is a lightweight data-interchange format. If a saved question is selected as a source, select **Group columns by sensor** to return the results as an array of objects instead of an array of simple value types. You cannot customize the columns with this option. You can specify the row delimiter that goes between the individual entries. In addition to single characters, you can use escape characters such as: `\t` (tab), `\n` (new line), and `\r` (carriage return). Select the columns that you want to pass through to the destination.

By default, the JSON format includes each entry as a JSON object inside braces (`{}`), without commas separating objects.

```
{"object_id":1,"audit_row_id":"38769","details":"User: admin; Session ID:
38467; Authentication Type: User; Originated from SOAPPluginScheduler",
"creation_time":"2021-08-31T14:02:38","modification_time":
"2021-08-31T14:02:38","last_modified_by":"","modifier_user_id":0,
"mod_user":null,"mod_persona":null,"type":0,"object_name":"",
"object_type_name":"authentication_audit","type_name":"CreateObject",
"audit_type":"authentication_audit"}{"object_id":1,"audit_row_id":
"38770","details":"User: admin; Session ID: 38468; Authentication Type:
User; Originated from SOAPPluginScheduler","creation_time":
"2021-08-31T14:02:48","modification_time":"2021-08-31T14:02:48",
"last_modified_by":"","modifier_user_id":0,"mod_user":null,
"mod_persona":null,"type":0,"object_name":"","object_type_name":
"authentication_audit","type_name":"CreateObject","audit_type":
```

©2026 Tanium Inc. All Rights Reserved

```
"authentication_audit"}
```


Select **Generate Document** for a JSON array inside brackets ([]). The array contains each entry as a JSON object inside braces, with commas separating objects.


```
[{"object_id":1,"audit_row_id":"38769","details":"User: admin; Session ID:
38467; Authentication Type: User; Originated from SOAPPluginScheduler",
"creation_time":"2021-08-31T14:02:38","modification_time":
"2021-08-31T14:02:38","last_modified_by":"","modifier_user_id":0,
"mod_user":null,"mod_persona":null,"type":0,"object_name":"",
"object_type_name":"authentication_audit","type_name":"CreateObject",
"audit_type":"authentication_audit"},{"object_id":1,"audit_row_id":"38770",
"details":"User: admin; Session ID: 38468; Authentication Type: User;
Originated from SOAPPluginScheduler","creation_time":"2021-08-31T14:02:48",
"modification_time":"2021-08-31T14:02:48","last_modified_by":"",
"modifier_user_id":0,"mod_user":null,"mod_persona":null,"type":0,
"object_name":"","object_type_name":"authentication_audit","type_name":
"CreateObject","audit_type":"authentication_audit"}]
```


Select **Wrap Data with Source** for a JSON object inside braces. The object name is the source. The object value is a JSON array inside brackets. The array contains each entry as a JSON object inside braces, with commas separating objects.


```
{ "Tanium Audit Source": [{"object_id":1,"audit_row_id":"38769","details":
"User: admin; Session ID: 38467; Authentication Type: User;
Originated from SOAPPluginScheduler","creation_time":"2021-08-31T14:02:38",
"modification_time":"2021-08-31T14:02:38","last_modified_by":"",
"modifier_user_id":0,"mod_user":null,"mod_persona":null,"type":0,
"object_name":"","object_type_name":"authentication_audit","type_name":
"CreateObject","audit_type":"authentication_audit"},{"object_id":1,
"audit_row_id":"38770","details":"User: admin; Session ID: 38468;
Authentication Type: User; Originated from SOAPPluginScheduler",
"creation_time":"2021-08-31T14:02:48","modification_time":
"2021-08-31T14:02:48","last_modified_by":"","modifier_user_id":0,
"mod_user":null,"mod_persona":null,"type":0,"object_name":"",
"object_type_name":"authentication_audit","type_name":"CreateObject",
"audit_type":"authentication_audit"}] }
```


Note: If your destination expects a valid JSON array, select **Generate Document**. If your document expects a valid JSON object, select **Wrap Data with Source**.

You can use the **Wrap Data with Text** field to include the system-generated source name with the file, or column customizations to include custom information with each entry.

©2026 Tanium Inc. All Rights Reserved

JSON usage of the Wrap Data with Text field

Field	Default value	Output value	Notes
Wrap Data with Text	cleared	the source name	The system-generated source name value is the name in the JSON element, followed by an array of JSON elements, one entry per element. The source name value is not included with each entry.

Default destinations: HTTP

LEEF

Log Event Extended Format (LEEF) is the default format for: IBM QRadar, LogRhythm, and McAfee SIEM. When you define LEEF format for your destination, you can include Advanced Settings such as the LEEF version, product name, version, source, and the end of entry separator character. In addition to single characters, you can use escape characters such as: `\t` (tab), `\n` (new line), and `\r` (carriage return) for the separator. Some fields also support variable substitution, as listed in Reference: Variables on page 295.



Note: You cannot select this format if you select an event data source.

Select **1.0** from **LEEF Version** for LEEF version 2.0 format.

```
May 29 19:45:15 example_host LEEF:1.0|Tanium|Tanium Application Server|1|
TaniumAuditSource|objectid=256 auditname=New-Session-Created creationtime=Wed
May 29 2024 19:44:24 GMT+0000 (Coordinated Universal Time)
modificationtime=Wed May 29 2024 19:44:24 GMT+0000 (Coordinated Universal Time)
lastmodifiedby=        modifieruserid=0 details=User:-admin@example.com;
-Session-ID:-65407219;-Authentication-Type:-User;
-Originated-from-SOAPPluginScheduler auditrowid=58245707 type=0
typename=CreateObject objectname= objecttypename=authentication
audittype=authentication_audit
```

Select **2.0** from **LEEF Version** for LEEF version 2.0 format.

```
May 29 19:45:15 example_host LEEF:1.0|Tanium|Tanium Application Server|1|
TaniumAuditSource| |objectid=256 auditname=New-Session-Created creationtime=Wed
May 29 2024 19:44:24 GMT+0000 (Coordinated Universal Time) modificationtime=Wed
May 29 2024 19:44:24 GMT+0000 (Coordinated Universal Time) lastmodifiedby=
modifieruserid=0 details=User:-admin@example.com;-Session-ID:-65407219;
-Authentication-Type:-User;-Originated-from-SOAPPluginScheduler
auditrowid=58245707        type=0 typename=CreateObject objectname=
objecttypename=authentication audittype=authentication_audit
```

©2026 Tanium Inc. All Rights Reserved

You can use the **Source** field to include the system-generated source name with each entry, or column customizations to include custom information with each entry.

LEEF usage of the Source field

Field	Default value	Output value	Notes
Source	`{Source}`	`sourcename`	The LEEF header includes the system-generated source name. Spaces are removed from the source name value.

Default destinations: IBM QRadar, LogRhythm, and McAfee SIEM

SQL server

When you are exporting data to SQL server, you can map the columns from the source to the columns in the database table. For more information, see Configuring SQL Server destinations on page 214.

You can use column customizations to include custom information with each entry.

Syslog RFC 5424

An IETF standard for message logging defined in RFC 5424. This output format also supports the earlier BSD message logging format defined in RFC 3164. You can define the syslog message components, including the facility code, severity, message identifier, and separator. For the separator, you can use escape characters such as: `\t` (tab), `\n` (new line), and `\r` (carriage return). If the source is a saved question, you can also select whether you want to send the question source to the output or not. The default for new connections is to send the question source. Select the columns that you want to pass through to the destination. Some fields also support variable substitution, as listed in Reference: Variables on page 295.



Note: You cannot select this format if you select an event data source.

Clear **BSD Syslog** to output IETF (RFC 5424) syslog message format.

```
636 <134>1 2024-05-29T19:46:02.430+00:00 example_host Tanium 32208 -
[Tanium-Audit-Source@017472 object_id="429" audit_name="New Session Created"
creation_time="Wed May 29 2024 19:44:38 GMT+0000 (Coordinated Universal Time)"
```

©2026 Tanium Inc. All Rights Reserved

```
modification_time="Wed May 29 2024 19:44:38 GMT+0000 (Coordinated Universal
Time)" last_modified_by="" modifier_user_id="0" details="User:
admin@example.com; Session ID: 65407232; Authentication Type: User; Originated
from SOAPPluginScheduler" audit_row_id="58245720" type="0"
type_name="CreateObject" object_name="" object_type_name="authentication"
audit_type="authentication_audit"]
```

Select **BSD Syslog** to output BSD (RFC 3164) syslog message format.

```
<134>1 2024-05-30T18:22:06.716+00:00 example_host Tanium 28014 -
[Tanium-Audit-Source@017472 object_id="772" audit_name="New Session Created"
creation_time="Thu May 30 2024 18:21:03 GMT+0000 (Coordinated Universal Time)"
modification_time="Thu May 30 2024 18:21:03 GMT+0000 (Coordinated Universal
Time)" last_modified_by="" modifier_user_id="0" details="User:
admin@example.com; Session ID: 65463018; Authentication Type: User; Originated
from SOAPPluginScheduler" audit_row_id="58301886" type="0"
type_name="CreateObject" object_name="" object_type_name="authentication"
audit_type="authentication_audit"]
```

You can use the **Source** field to include the system-generated source name with each entry, or the **Signature ID** field or column customizations to include custom information with each entry.

RFC 5424 field usage

Field	Default value	Output value	Notes
MSG ID	n/a	the defined value	The defined value precedes the structured-data brackets. Dashes replace spaces in the defined value.
SD-ID	`{Source}@017472`	`source-name@017472`	The structured-data includes the system-generated source name and port number as the first value. Dashes replace spaces in the source name value.
Send Question Source	cleared	`Question="saved-question-name"`	The structured-data includes the system-generated saved question name as the last value. Dashes replace spaces in the saved question name value.

Default destinations: Socket Receiver, Splunk

©2026 Tanium Inc. All Rights Reserved

Reference: Gateway examples for Connect

Tanium Gateway provides a GraphQL API integration point for Tanium solutions, including Connect. Connect queries and mutations require Connect to retrieve information about connections and connection runs, and to start or stop connection runs.

For additional Gateway example syntax, see Tanium Gateway User Guide: Reference: Filter syntax and Tanium Gateway User Guide: Reference: Gateway examples.

Connect REST API replacement

The Connect GraphQL APIs are at stability index `1.2 - Experimental (Release Candidate)`. For the best results, if a GraphQL API provides functionality, use that instead of the corresponding legacy Connect REST API. Connect REST APIs not listed in the table do not have comparable functionality in Tanium Gateway, or are otherwise not used in favor of other Connect REST APIs.

Gateway GraphQL API replacements for Connect v1 REST API endpoints

Connect v1 REST API endpoint	Gateway GraphQL API replacement	Notes
`DELETE v1/connections/:id`	n/a	Delete a connection by ID
`GET v1/connectionruns` (legacy)	`query.connectRuns`	Get connection runs
`GET v1/connections` (legacy)	`query.connectConnections`	Get connections
`GET v1/connections/:id` (legacy)	`query.connectConnection`	Get a connection by ID
`GET v1/connections/:id/runs/:connectionrunid` (legacy)	`query.connectRun`	Get a connection run by ID
`GET v1/connections/:id/runs/:connectionrunid/download`	n/a	Get the log data for a connection run
`POST v1/connections/:id/runs` (legacy)	`mutation.connectConnectionStart`	Start a connection run
`POST v1/connections/:id/stop` (legacy)	`mutation.connectConnectionStop`	Stop an in-progress connection run
`POST v1/import`	n/a	Create or modify a connection

©2026 Tanium Inc. All Rights Reserved

Get a connection by ID

(query.connectConnection)

The following query retrieves a connection that matches the ID.

```
query exampleGetSingleConnection($id: ID!) {
  connectConnection(ref: {id: $id}) {
    id
    currentRun {
      id
      connectionID
      status
      createdTime
      updatedTime
    }
    description
    displayName
    isScheduled
    lastRunStatus
    lastRunTime
    pastRuns {
      edges {
        node {
          id
          connectionID
          status
          createdTime
          updatedTime
        }
      }
    }
  }
}
```

Include an ID variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "id": "123"
}
```

Example response:

```
{
  "data": {
    "connectConnection": {
      "id": "123",
      "currentRun": null,
      "description": "Example connection description",
      "displayName": "Example connection name",
      "isScheduled": true,
      "lastRunStatus": "Finished",
      "lastRunTime": "2026-05-08T17:00:15.737Z",
      "pastRuns": {
        "edges": [
          {
            "node": {
```

©2026 Tanium Inc. All Rights Reserved

```
              "id": "234",
              "connectionID": "23",
              "status": "Finished",
              "createdTime": "2026-05-08T17:00:15.737Z",
              "updatedTime": "2026-05-08T17:00:21.276Z"
            }
          },
          {
            "node": {
              "id": "345",
              "connectionID": "23",
              "status": "Finished",
              "createdTime": "2026-05-08T15:45:00.575Z",
              "updatedTime": "2026-05-08T15:45:03.567Z"
            }
          }
        ]
      }
    }
  }
}
```

Get a connection run by ID

(query.connectRun)

The following query retrieves a connection run that matches the ID.

```
query exampleGetSingleConnectionRun($id: ID!) {
  connectRun(ref: {id: $id}) {
    id
    connectionID
    status
    createdTime
    updatedTime
  }
}
```

Include an ID variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "id": "123"
}
```

Example response:

```
{
  "data": {
    "connectRun": {
      "id": "123",
      "connectionID": "234",
      "status": "Finished",
      "createdTime": "2023-08-15T07:01:21.824Z",
      "updatedTime": "2023-08-15T07:01:30.912Z"
    }
  }
}
```

©2026 Tanium Inc. All Rights Reserved

Get connection runs

(query.connectRuns)

The following query retrieves the first 2 connection runs.

```
query exampleGetConnectionRuns($first: Int) {
  connectRuns(first: $first) {
    edges {
      node {
        id
        connectionID
        status
        createdTime
        updatedTime
      }
    }
    pageInfo {
      hasPreviousPage
      hasNextPage
      startCursor
      endCursor
    }
    totalRecords
  }
}
```

Include a pagination variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "first": 2
}
```

Example response:

```
{
  "data": {
    "connectRuns": {
      "edges": [
        {
          "node": {
            "id": "1",
            "connectionID": "123",
            "status": "Finished",
            "createdTime": "2023-08-15T07:01:21.824Z",
            "updatedTime": "2023-08-15T07:01:30.912Z"
          }
        },
        {
          "node": {
            "id": "2",
            "connectionID": "234",
            "status": "Finished",
            "createdTime": "2023-08-15T07:01:19.678Z",
            "updatedTime": "2023-08-15T07:01:23.757Z"
          }
        }
```

©2026 Tanium Inc. All Rights Reserved

```
      ],
      "pageInfo": {
        "hasPreviousPage": false,
        "hasNextPage": true,
        "startCursor": "MA==",
        "endCursor": "MQ=="
      },
      "totalRecords": 504
    }
  }
}
```

Get connections

(query.connectConnections)

The following query retrieves the first 2 connections.

```
query exampleGetConnections($first: Int) {
  connectConnections(first: $first) {
    edges {
      node {
        id
        currentRun {
          id
          connectionID
          status
          createdTime
          updatedTime
        }
        description
        displayName
        isScheduled
        lastRunStatus
        lastRunTime
        pastRuns {
          edges {
            node {
              id
              connectionID
              status
              createdTime
              updatedTime
            }
          }
        }
      }
    }
    pageInfo {
      hasNextPage
      hasPreviousPage
      startCursor
      endCursor
    }
    totalRecords
  }
}
```

©2026 Tanium Inc. All Rights Reserved

Include a pagination variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "first": 2
}
```

Example response:


```
{
  "data": {
    "connectConnections": {
      "edges": [
        {
          "node": {
            "id": "23",
            "currentRun": null,
            "description": "Example connection description",
            "displayName": "Example connection name",
            "isScheduled": true,
            "lastRunStatus": "Finished",
            "lastRunTime": "2026-05-08T15:36:00.010Z",
            "pastRuns": {
              "edges": [
                {
                  "node": {
                    "id": "234",
                    "connectionID": "23",
                    "status": "Finished",
                    "createdTime": "2026-05-08T15:36:00.010Z",
                    "updatedTime": "2026-05-08T15:46:09.098Z"
                  }
                },
                {
                  "node": {
                    "id": "345",
                    "connectionID": "23",
                    "status": "Finished",
                    "createdTime": "2026-05-08T12:36:00.012Z",
                    "updatedTime": "2026-05-08T12:46:06.430Z"
                  }
                }
              ]
            }
          }
        },
        {
          "node": {
            "id": "13",
            "currentRun": null,
            "description": "Example connection description 2",
            "displayName": "Example connection name 2",
            "isScheduled": false,
            "lastRunStatus": "Finished",
            "lastRunTime": "2026-02-12T21:27:46.686Z",
            "pastRuns": {
              "edges": []
            }
          }
        }
      ],
      "pageInfo": {
```

```
        "hasNextPage": true,
        "hasPreviousPage": false,
        "startCursor": "MA==",
        "endCursor": "MQ=="
      },
      "totalRecords": 23
    }
  }
}
```

Get multiple Connect connections by ID

(query.connectConnections)

About this task

The following query requires Connect 5.45 or later and retrieves the connections that match either ID `1234` or `5678`.

```
query exampleGetMultipleConnectionsByIDs($first_id: ID!, $second_id: ID!) {
  connectConnections(filter: {ids: [$first_id, $second_id]}) {
    totalRecords
    edges {
      node {
        id
        displayName
        isScheduled
        lastRunTime
        lastRunStatus
      }
    }
  }
}
```

Include the ID variables in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "first_id": "1234",
  "second_id": "5678"
}
```

Example response:

```
{
  "data": {
    "connectConnections": {
      "totalRecords": 2,
      "edges": [
        {
          "node": {
            "id": "1234",
            "displayName": "Example connection 1",
            "isScheduled": false,
            "lastRunTime": "2026-02-12T21:27:46.686Z",
            "lastRunStatus": "Finished"
```

©2026 Tanium Inc. All Rights Reserved

```
          }
        },
        {
          "node": {
            "id": "5678",
            "displayName": "Example connection 2",
            "isScheduled": false,
            "lastRunTime": null,
            "lastRunStatus": null
          }
        }
      ]
    }
  }
}
```

Get multiple Connect connections by description

(query.connectConnections)

About this task

The following query requires Connect 5.45 or later and retrieves connections that contain `Example` in the description.

```
query exampleGetConnectionsByDescription($target_description: String) {
  connectConnections(filter: {description: $target_description}) {
    totalRecords
    edges {
      node {
        id
        displayName
        description
        isScheduled
        lastRunStatus
        lastRunTime
      }
    }
  }
}
```

Include the description variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "target_description": "Example"
}
```

Example response:

```
{
  "data": {
    "connectConnections": {
      "totalRecords": 3,
      "edges": [
        {
```

©2026 Tanium Inc. All Rights Reserved

```
          "node": {
            "id": "1234",
            "displayName": "Example connection 1",
            "description": "An example description",
            "isScheduled": true,
            "lastRunStatus": "Finished",
            "lastRunTime": "2026-05-08T15:36:00.010Z"
          }
        },
        {
          "node": {
            "id": "567",
            "displayName": "Example connection 2",
            "description": "Example description",
            "isScheduled": false,
            "lastRunStatus": null,
            "lastRunTime": null
          }
        },
        {
          "node": {
            "id": "8901",
            "displayName": "Example connection 3",
            "description": "A description that contains example",
            "isScheduled": false,
            "lastRunStatus": null,
            "lastRunTime": null
          }
        }
      ]
    }
  }
}
```


Get Connect connection by ID and displayName

(query.connectConnections)

About this task

The following query requires Connect 5.45 or later and retrieves the connection that matches ID `1234` and contains `Example Connection` in the displayName field.

```
query exampleGetConnectionByIDAndDisplayName($target_id: ID!, $target_display_name: String) {
  connectConnections(filter: { ids: [$target_id], displayName: $target_display_name }) {
    totalRecords
    edges {
      node {
        id
        displayName
      }
    }
  }
}
```

Include the ID and display name variables in the **QUERY VARIABLES** panel or in your variables

©2026 Tanium Inc. All Rights Reserved

dictionary:

```
{
  "target_id": "1234",
  "target_display_name": "Example Connection"
}
```

Example response:

```
{
  "data": {
    "connectConnections": {
      "totalRecords": 1,
      "edges": [
        {
          "node": {
            "id": "1234",
            "displayName": "Example Connection"
          }
        }
      ]
    }
  }
}
```

Get SQL Server stored procedures

(query.connectSQLServerStoredProcedures)

About this task

The following query requires Connect 5.52 or later and retrieves the stored procedures defined in one or more schemas within a SQL Server database. For each procedure, the query returns the procedure name, whether the configured user has `EXECUTE` permission, and the declared parameters with their SQL Server data types.

```
query exampleGetSQLServerStoredProcedures(
  $server: String!
  $username: String!
  $password: String!
  $database: String!
  $schemaNames: [String!]!
) {
  connectSQLServerStoredProcedures(
    input: {
      connectionConfiguration: {
        server: $server
        username: $username
        password: $password
        encrypt: false
        validateServerCertificate: false
        connectTimeoutMillis: 5000
        requestTimeoutMillis: 30000
        cancelTimeoutMillis: 5000
```

©2026 Tanium Inc. All Rights Reserved

```
        packetSizeBytes: 4096
        multiSubnetFailover: false
      }
      database: $database
      schemaNames: $schemaNames
    }
  ) {
    schemaName
    procedures {
      name
      hasExecute
      parameters {
        name
        dataType
      }
    }
  }
}
```

Include variables in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "server": "sql.example.com",
  "username": "reportuser",
  "password": "examplepassword",
  "database": "Sales",
  "schemaNames": [
    "dbo",
    "reporting"
  ]
}
```

Example response:

```
{
  "data": {
    "connectSQLServerStoredProcedures": [
      {
        "schemaName": "dbo",
        "procedures": [
          {
            "name": "sp_onConnectionStart",
            "hasExecute": true,
            "parameters": [
              {
                "name": "@connectionName",
                "dataType": "nvarchar"
              },
              {
                "name": "@connectionId",
                "dataType": "bigint"
              },
              {
                "name": "@connectionRunId",
                "dataType": "bigint"
              },
              {
                "name": "@source",
                "dataType": "nvarchar"
              },
              {
```

©2026 Tanium Inc. All Rights Reserved

```
                "name": "@databaseTable",
                "dataType": "nvarchar"
              },
              {
                "name": "@startTime",
                "dataType": "datetime"
              },
              {
                "name": "@expectedRowCount",
                "dataType": "bigint"
              }
            ]
          },
          {
            "name": "sp_onConnectionFinish",
            "hasExecute": true,
            "parameters": [
              {
                "name": "@connectionRunId",
                "dataType": "bigint"
              },
              {
                "name": "@runStatus",
                "dataType": "nvarchar"
              },
              {
                "name": "@sourceRowCount",
                "dataType": "bigint"
              },
              {
                "name": "@destinationRowCount",
                "dataType": "bigint"
              },
              {
                "name": "@finishTime",
                "dataType": "datetime"
              }
            ]
          }
        ]
      },
      {
        "schemaName": "reporting",
        "procedures": []
      }
    ]
  }
}
```

Get SQL Server stored procedures through a satellite

(query.connectSQLServerStoredProcedures)

About this task

The following query requires Connect 5.52 or later and retrieves the stored procedures defined in one or more schemas within a SQL Server database through a satellite. For each procedure, the query

returns the procedure name, whether the configured user has `EXECUTE` permission, and the declared parameters with their SQL Server data types.

```
query exampleGetSQLServerStoredProceduresThroughSatellite(
  $server: String!,
  $username: String!,
  $password: String!,
  $database: String!,
  $satelliteID: ID!,
  $schemaNames: [String!]!
) {
  connectSQLServerStoredProcedures(
    input: {
      connectionConfiguration: {
        server: $server,
        username: $username,
        password: $password,
        satelliteID: $satelliteID,
        encrypt: false,
        validateServerCertificate: false,
        connectTimeoutMillis: 5000,
        requestTimeoutMillis: 30000,
        cancelTimeoutMillis: 5000,
        packetSizeBytes: 4096,
        multiSubnetFailover: false
      },
      database: $database,
      schemaNames: $schemaNames
    }
  ) {
    schemaName
    procedures {
      name
      hasExecute
      parameters {
        name
        dataType
      }
    }
  }
}
```

Include variables in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "server": "sql.example.com",
  "username": "reportuser",
  "password": "examplepassword",
  "database": "Sales",
  "satelliteID": "e66081b7-5900-46bb-97eb-fcbf16d2c24f",
  "schemaNames": [
    "dbo"
  ]
}
```

©2026 Tanium Inc. All Rights Reserved

Start connection run

(mutation.connectConnectionStart)

The following mutation starts a connection run from a connection that matches the connection ID.

```
mutation exampleStartConnection($connectionID: ID!) {
  connectConnectionStart(input: {connectionID: $connectionID}) {
    run {
      id
      connectionID
      status
      createdTime
      updatedTime
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include an ID variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "connectionID": "123"
}
```

Example response:

```
{
  "data": {
    "connectConnectionStart": {
      "run": {
        "id": "12345",
        "connectionID": "123",
        "status": "Starting",
        "createdTime": "2023-08-15T18:16:54.509Z",
        "updatedTime": "2023-08-15T18:16:54.512Z"
      },
      "error": null
    }
  }
}
```

Stop the active run for a Connect connection

(mutation.connectConnectionStop)

The following mutation stops the active run, if any, for the specified Connect connection. If the connection has no in-progress run, this mutation succeeds with `runID` set to `null`. No run is started.

©2026 Tanium Inc. All Rights Reserved

```
mutation exampleStopConnection($connectionID: ID!) {
  connectConnectionStop(input: {connectionID: $connectionID}) {
    runID
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include an ID variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "connectionID": "234"
}
```

Example response:

```
{
  "data": {
    "connectConnectionStop": {
      "runID": "123",
      "error": null
    }
  }
}
```

Stop a specific connection run

(mutation.connectConnectionRunStop)

The following mutation stops a connection run that is currently in progress. The connection run is identified by ID. This request returns an error if the connection run is not in progress.

```
mutation exampleStopConnectionRun($runID: ID!) {
  connectConnectionRunStop(input: {runID: $runID}) {
    run {
      id
      connectionID
      status
      createdTime
      updatedTime
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include an ID variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
```

©2026 Tanium Inc. All Rights Reserved

```
  "runID": "123"
}
```

Example response:

```
{
  "data": {
    "connectConnectionRunStop": {
      "run": {
        "id": "123",
        "connectionID": "234",
        "status": "Running",
        "createdTime": "2023-08-15T18:36:29.739Z",
        "updatedTime": "2023-08-15T18:36:32.235Z"
      },
      "error": null
    }
  }
}
```

Start multiple connection runs

(mutation.connectConnectionsBulkStart)

The following mutation starts a run for each connection ID in `connectionIDs`. Each connection is processed independently, and each failure is recorded in `errors` with the connection ID, its position in the request list, and a structured error. `connectionIDs` is limited to 100 IDs per request by default.

```
mutation exampleBulkStartConnections($connectionIDs: [ID!]!) {
  connectConnectionsBulkStart(input: {connectionIDs: $connectionIDs}) {
    runs {
      id
      connectionID
      status
      createdTime
      updatedTime
    }
    successCount
    failureCount
    errors {
      connectionID
      inputIndex
      error {
        code
        message
        retryable
      }
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

©2026 Tanium Inc. All Rights Reserved

Include an ID list variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "connectionIDs": ["123", "456"]
}
```

Example response with one success and one failure:

```
{
  "data": {
    "connectConnectionsBulkStart": {
      "runs": [
        {
          "id": "12345",
          "connectionID": "123",
          "status": "Starting",
          "createdTime": "2026-07-17T18:16:54.509Z",
          "updatedTime": "2026-07-17T18:16:54.512Z"
        }
      ],
      "successCount": 1,
      "failureCount": 1,
      "errors": [
        {
          "connectionID": "456",
          "inputIndex": 1,
          "error": {
            "code": "validation_exists",
            "message": "Connection 456 does not exist or is not visible to the caller.",
            "retryable": null
          }
        }
      ],
      "error": null
    }
  }
}
```

Stop multiple in-progress connection runs

(mutation.connectConnectionsBulkStop)

The following mutation stops the active run, if any, for each connection ID in `connectionIDs`. Connections with no run in progress are counted as successes. `connectionIDs` is limited to 100 IDs per request by default.

```
mutation exampleBulkStopConnections($connectionIDs: [ID!]!) {
  connectConnectionsBulkStop(input: {connectionIDs: $connectionIDs}) {
    stoppedRunIDs
    successCount
    failureCount
    errors {
      connectionID
      inputIndex
      error {
```

©2026 Tanium Inc. All Rights Reserved

```
        code
        message
        retryable
      }
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include an ID list variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "connectionIDs": ["123", "456"]
}
```

Example response:

```
{
  "data": {
    "connectConnectionsBulkStop": {
      "stoppedRunIDs": ["78901"],
      "successCount": 2,
      "failureCount": 0,
      "errors": [],
      "error": null
    }
  }
}
```

Enable multiple connections

(mutation.connectConnectionsBulkEnable)

The following mutation enables each connection ID in `connectionIDs` for scheduled runs.

Connections are processed independently. `connectionIDs` is limited to 100 IDs per request by default.

```
mutation exampleBulkEnableConnections($connectionIDs: [ID!]!) {
  connectConnectionsBulkEnable(input: {connectionIDs: $connectionIDs}) {
    connections {
      id
      displayName
    }
    successCount
    failureCount
    errors {
      connectionID
      inputIndex
      error {
        code
        message
        retryable
      }
```

©2026 Tanium Inc. All Rights Reserved

```
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include an ID list variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "connectionIDs": ["123", "456"]
}
```

Example response:

```
{
  "data": {
    "connectConnectionsBulkEnable": {
      "connections": [
        { "id": "123", "displayName": "Trends — Endpoint Inventory" },
        { "id": "456", "displayName": "Comply Findings Export" }
      ],
      "successCount": 2,
      "failureCount": 0,
      "errors": [],
      "error": null
    }
  }
}
```

Disable multiple connections

(mutation.connectConnectionsBulkDisable)

The following mutation disables each connection ID in `connectionIDs` from scheduled runs. Connections are processed independently. `connectionIDs` is limited to 100 IDs per request by default.

```
mutation exampleBulkDisableConnections($connectionIDs: [ID!]!) {
  connectConnectionsBulkDisable(input: {connectionIDs: $connectionIDs}) {
    connections {
      id
      displayName
    }
    successCount
    failureCount
    errors {
      connectionID
      inputIndex
      error {
        code
        message
        retryable
      }
    }
```

©2026 Tanium Inc. All Rights Reserved

```
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include an ID list variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "connectionIDs": ["123", "456"]
}
```

Example response:

```
{
  "data": {
    "connectConnectionsBulkDisable": {
      "connections": [
        { "id": "123", "displayName": "Trends — Endpoint Inventory" },
        { "id": "456", "displayName": "Comply Findings Export" }
      ],
      "successCount": 2,
      "failureCount": 0,
      "errors": [],
      "error": null
    }
  }
}
```

Delete multiple connections

(mutation.connectConnectionsBulkDelete)

The following mutation deletes each connection ID in `connectionIDs`. Connections are processed independently. Set `deleteComponents` to `false` to preserve the source, destination, filter, and format components for reuse by other connections. `connectionIDs` is limited to 100 IDs per request by default.

```
mutation exampleBulkDeleteConnections($connectionIDs: [ID!]!, $deleteComponents: Boolean) {
  connectConnectionsBulkDelete(input: {connectionIDs: $connectionIDs, deleteComponents:
$deleteComponents}) {
    deletedIDs
    successCount
    failureCount
    errors {
      connectionID
      inputIndex
      error {
        code
        message
        retryable
      }
```

©2026 Tanium Inc. All Rights Reserved

```
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the ID list and `deleteComponents` variables in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "connectionIDs": ["123", "456"],
  "deleteComponents": true
}
```

Example response:

```
{
  "data": {
    "connectConnectionsBulkDelete": {
      "deletedIDs": ["123", "456"],
      "successCount": 2,
      "failureCount": 0,
      "errors": [],
      "error": null
    }
  }
}
```

Transfer ownership of multiple connections

(mutation.connectConnectionsBulkTransferOwnership)

The following mutation transfers ownership of each connection ID in `connectionIDs` to the calling user. This mutation cannot transfer ownership to a third party; the calling user always takes ownership. The persona of each connection is reset to the active persona of the calling user. Connections are processed independently. `connectionIDs` is limited to 100 IDs per request by default.

```
mutation exampleBulkTransferOwnershipConnections($connectionIDs: [ID!]!) {
  connectConnectionsBulkTransferOwnership(input: {connectionIDs: $connectionIDs}) {
    connections {
      id
      displayName
    }
    successCount
    failureCount
    errors {
      connectionID
      inputIndex
      error {
        code
        message
```

©2026 Tanium Inc. All Rights Reserved

```
        retryable
      }
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include an ID list variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "connectionIDs": ["123", "456"]
}
```

Example response:

```
{
  "data": {
    "connectConnectionsBulkTransferOwnership": {
      "connections": [
        { "id": "123", "displayName": "Trends — Endpoint Inventory" },
        { "id": "456", "displayName": "Comply Findings Export" }
      ],
      "successCount": 2,
      "failureCount": 0,
      "errors": [],
      "error": null
    }
  }
}
```

Change the persona of multiple connections

(mutation.connectConnectionsBulkChangePersona)

The following mutation changes the persona that each connection ID in `connectionIDs` runs as. The calling user must own every connection in the request. Set `targetPersonaID` to `0` to use the default persona of the owner at run time, or specify a persona ID available to the calling user. Connections are processed independently. `connectionIDs` is limited to 100 IDs per request by default.

```
mutation exampleBulkChangePersonaConnections($connectionIDs: [ID!]!, $targetPersonaID: ID!) {
  connectConnectionsBulkChangePersona(input: {connectionIDs: $connectionIDs, targetPersonaID:
$targetPersonaID}) {
    connections {
      id
      displayName
    }
    successCount
    failureCount
    errors {
      connectionID
```

©2026 Tanium Inc. All Rights Reserved

```
      inputIndex
      error {
        code
        message
        retryable
      }
    }
    error {
      message
      retryable
      timedOut
    }
  }
}
```

Include the ID list and `targetPersonaID` variables in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "connectionIDs": ["123", "456"],
  "targetPersonaID": "0"
}
```

Example response:

```
{
  "data": {
    "connectConnectionsBulkChangePersona": {
      "connections": [
        { "id": "123", "displayName": "Trends — Endpoint Inventory" },
        { "id": "456", "displayName": "Comply Findings Export" }
      ],
      "successCount": 2,
      "failureCount": 0,
      "errors": [],
      "error": null
    }
  }
}
```

©2026 Tanium Inc. All Rights Reserved

Reference: Microsoft Security Copilot integration with Tanium skills

Important: The Microsoft Security Copilot integration is available in Tanium Integrations Gallery. For more information, see Tanium Integrations Gallery User Guide: Managing the Microsoft Security Copilot integration.

©2026 Tanium Inc. All Rights Reserved

Reference: Variables

You can use variables when you create a connection. For some connection destinations and formats, you can use variables for configured fields that can be replaced with new values when the connection run starts.

Connection variables

Use connection variables with supported fields to customize the information that Connect sends to a destination. Enclose a connection variable in curly bracket characters: `{` and `}`. For example:

- `{fileextension}` is replaced in the output field as `json`.
- `{computer group}` is replaced in the output field as `Example computer group`.



Note: Variables enclosed in curly brackets that do not match a connection variable, and that are not supported by the source, are interpreted as timestamp variables. Characters that match timestamp variables are replaced in the output, and other characters are passed through to the destination. For example, if you enter `{sourcecomputergroup}` as a variable, because it does not match either the `{source}` or the `{computergroup}` variable, characters that match timestamp variables are replaced in the output, such as `45ourc4co38put4rgroup`.

Connection variables

Variable	Supported fields
`connection id` `connectionid` Numeric ID of the connection; unique only to a specific Module Server	• AWS S3 source • **S3 Bucket Name and Optional Path** • **AWS S3 File Name** • Elasticsearch source
`connection name` `connectionname` User-configured name of the connection	
`connection run id` `connectionrunid` Numeric ID of the connection run; unique only to a specific Module Server	

©2026 Tanium Inc. All Rights Reserved

Variable	Supported fields
`source` [1] Human-readable name of the connection source	• **URL** • Email (O365, SMTP) source • **Subject** • **Attachment File Name** • File source • **File Name** • SMB source • **File Name** • **Share Name** • **Directory Name** • CEF format • **Source** • LEEF format • **Source** • Syslog RFC 5424 format • **SD-ID**
`computer group` [2] `computergroup` [2] Name of the computer group from the Tanium Server	
`file extension` [3] `fileextension` [3] File extension of the chosen format	

[1] The `source` variable is interpreted as the data source name (for example, Client Status) for most data sources. For saved question and Tanium Data Service (TDS) data sources, the `source` variable is interpreted as the saved question name. If you configure the Syslog RFC 5424 format, you can select **Send Question Source** to add `Question={Source}` to the output.

©2026 Tanium Inc. All Rights Reserved

Variable	Supported fields

[2] The `computer group` and `computergroup` variables are available for only the saved question data source. No other data sources offer computer group filtering.

[3] The `file extension` and `fileextension` variables are available only if you configure a CSV, HTML, or JSON format.

Time stamp variables

Use time stamp variables with the **File Name Time Stamp Format**, **File Name**, AWS S3 **S3 Bucket Name and Optional Path**, and Elasticsearch **URL** fields to customize the time stamp that Connect appends. Enclose one or more time stamp variables in curly bracket characters: `{` and `}`. For example:

- `{%m/%d/%y}` is replaced in the output field as `010124`.
- `{%A-%m/%d/%y-%l:%M:%S %p}` is replaced in the output field as `Monday-010124-102030PM`.

Note: Time stamp variables are case sensitive.

Note: Any characters in the format string that are not associated with a timestamp variable are passed through to the destination. If you add special characters, such as a slash (`/`), hyphen (`-`), or colon (`:`), file name, file path, or URL fields might not render as expected, or fail to render.

Common time stamp variable combinations

Variable combination [1]	Description	Example
`%m/%d/%y`	United States [2] : mm/dd/yy	01/15/00
`%Y-%m-%d`	ISO 8601 [3] : yyyy-mm-dd	2000-01-15
`%d-%m-%Y`	dd-mm-yyyy	15-01-2000

©2026 Tanium Inc. All Rights Reserved

Variable combination [1]	Description	Example
`%A, %B %e, %Y`	DAY, MONTH dd, yyyy	Saturday, January 15, 2000
`%b %e %a`	mmm dd Day	Jan 15 Sat
`%H:%M`	hh:mm	15:45
`%I:%M %p`	hh:mm p	3:45 PM

[1] Time stamp variable combinations with special characters might not work properly if used for a file name, file path, or URL. Special characters might change how a file is saved, prevent a file from saving properly, create a non-standard URL format, or change how a URL is parsed.

[2] `MM-DD-YYYY` is supported as a legacy variable. For the best results, use `%m/%d/%y` for improved support.

[3] `YYYY-MM-DD` is supported as a legacy variable. For the best results, use `%Y-%m-%d` for improved support.

Date-related time stamp variables

Variable	Description	Example
`%v`	VMS: dd-mmm-yyyy	01-Jan-2025
`%C`	Century number as two-digit integer	20 (20th century)
`%y`	Year as two-digit integer without century	25 (the year 2025)
`%Y`	Year as four-digit integer with century	2025
`%m`	Month from 01 to 12	01 (January)
`%b`	Month abbreviation	Jan
`%B`	Month	January
`%W`	Week of the current year two-digit number, assuming Monday first	45 (45th week of the year)
`%U`	Week of the current year two-digit number, assuming Sunday first	21 (21st week of the year)
`%a`	Weekday abbreviation	Mon

©2026 Tanium Inc. All Rights Reserved

Variable	Description	Example
`%A`	Weekday	Monday
`%d`	Day from 01 to 31	05
`%e`	Day from 1 to 31	15
`%w`	Day from 0 to 6, with Sunday being 0	3 (Wednesday)
`%j`	Day from 001 to 366	045
`%u`	Day from 1 to 7, with Monday being 1	4 (Wednesday)

Time-related time stamp variables

Variable	Description	Example
`%H`	Hour from 00 to 23	01
`%I`	Hour from 01 to 12	01
`%k`	Hour from 0 to 23	1
`%l`	Hour from 0 to 12	1
`%M`	Minute	23
`%S`	Second	45
`%s`	Unix timestamp (seconds after January 1, 1970)	1704999658
`%L`	Millisecond from 000 to 999	123
`%s%L`	Unix timestamp (milliseconds after January 1, 1970)	1704999658390
`%p`	AM/PM	AM
`%P`	am/pm	am
`%r` `%l:%M:%S %p`	12-hour time (seconds) [1]	012345 PM 01:23:45 PM

©2026 Tanium Inc. All Rights Reserved

Variable	Description	Example
`%R` `%H:%M`	24-hour time (minutes) [1]	1530 15:30
`%T` `%H:%M:%S`	24-hour time (seconds) [1]	153045 15:30:45
`%z`	Time zone hour offset from Greenwich Mean Time	+0000
`%Z`	Time zone name abbreviation	GMT

[1] This variable might not work properly if used for a file name, file path, or URL. Special characters might change how a file is saved, prevent a file from saving properly, create a non-standard URL format, or change how a URL is parsed.

©2026 Tanium Inc. All Rights Reserved

Reference: Tanium Audit Source data

You can use Tanium Connect to retrieve Tanium Server audit logs through the **Tanium Audit Source**. Most audit logs contain entries when objects on the Tanium Server are created, modified, or deleted. The data that is available in the audit logs depends on the version of the Tanium Core Platform, and the type of audit.

You can configure **Days of History Retrieved** per connection run. If you set this to:

- `0`, the first connection run exports no prior days of audit log information. For each connection run after the first, the connection exports audit log information that was generated after the previous connection run.
- `1` or greater, the first connection run exports up to that many days of audit log information, prior to the connection run timestamp. For each connection run after the first, the connection exports up to that many prior days of audit log information that was generated after the previous connection run.

If set to `0`, this export may contain a small number of audit log results if you select multiple audit types and some audit log results are generated after the connection run starts.

Note: If a connection run using the **Tanium Audit Source** fails with a `MaxNumberOfAuditEntriesPerCacheExceeded` error, see Issue: Tanium Audit Source connection fails with MaxNumberOfAuditEntriesPerCacheExceeded error on page 244.

Important: The following tables show the data returned by Tanium Core Platform 7.5.6.1067 and later.

Supported audit types

Connect supports the following audit types through the **Tanium Audit Source**:

©2026 Tanium Inc. All Rights Reserved

Audit types supported by Connect

Audit type	`object_type_name` log value [1]	Audit information
Allowed URL	`white_listed_url`	Includes entries when allowed URLs are created, modified, or deleted. **Allowed URL log entry example** {"object_id":1234, "audit_name":"https://example.url.com", "creation_time":"2023-01-01T22:45:02Z", "modification_time":"2023-01-01T22:45:02Z", "last_modified_by":"user@example.com", "modifier_user_id":1234, "mod_user":{"id":1234,"name":"user", "domain":"example","display_name":""}, "details":"","audit_row_id":1234, "type":2,"type_name":"DeleteObject", "object_name":"https://example.url.com", "object_type_name":"white_listed_url"}
API token	`api_token`	Includes entries when API tokens are created, modified, or deleted. **API token log entry example** {"object_id":12345, "audit_name":"RevokedToken ID 12345", "creation_time":"2023-01-01T11:10:37.000Z", "modification_time":"2023-01-01T11:10:37.000Z", "last_modified_by":"user@example.com", "modifier_user_id":123, "mod_user":{"id":123,"name":"user@example.com", "domain":"","display_name":""}, "mod_persona":{"id":1234, "name":"user_example_persona"}, "details":"Revoked for user 123 with persona 1234", "audit_row_id":12345,"type":2, "type_name":"DeleteObject","object_name":"", "object_type_name":"api_token"}
Authentication	`authentication`	Successful and failed sign-on attempts. **Authentication log entry example** {"object_id":123, "audit_name":"New Session Created", "creation_time":"2023-01-01T23:44:59.000Z", "modification_time":"2023-01-01T23:44:59.000Z", "last_modified_by":"","modifier_user_id":0, "details":"User: user@example.com; Session ID: 12345678; Authentication Type: User; Originated from SOAPPluginScheduler", "audit_row_id":12345678,"type":0, "type_name":"CreateObject","object_name":"", "object_type_name":"authentication"}
Content set	`content_set_privilege`	Includes entries when content sets are created, modified, or deleted.

©2026 Tanium Inc. All Rights Reserved

Audit type	`object_type_name` log value [1]	Audit information

		Content set privilege log entry example
		<pre>{"object_id":1234,
		"audit_name":"connect owner write",
		"creation_time":"2023-01-01T15:56:31Z",
		"modification_time":"2023-01-01T15:56:31Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":123,
		"mod_user":{"id":123,"name":"user@example.com",
		"domain":"","display_name":""},
		"details":"","audit_row_id":123,"type":2,
		"type_name":"DeleteObject",
		"object_name":"screen sharing provisioning read",
		"object_type_name":"content_set_privilege"}</pre>

Content set role	`content_set_role`	Includes entries when roles are created, modified, or deleted.
		Content set role log entry example
		<pre>{"object_id":1234,"audit_name":"example role read",
		"creation_time":"2023-01-01T20:41:36Z",
		"modification_time":"2023-01-01T20:41:36Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":123,
		"mod_user":{"id":123,"name":"user@example.com",
		"domain":"","display_name":""},
		"details":"Replaced content set role privileges
		[ ] with [12345]",
		"audit_row_id":1234,"type":0,
		"type_name":"CreateObject",
		"object_name":"example role read",
		"object_type_name":"content_set_role"}</pre>

Content set role membership	`content_set_role_membership`	Includes entries when a user is assigned to a role or removed from a role.
		Content set role membership log entry example
		<pre>{"object_id":1234,
		"audit_name":"ContentSetRoleMembership ID 1234",
		"creation_time":"2023-01-01T15:26:41Z",
		"modification_time":"2023-01-01T15:26:41Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":2345,
		"mod_user":{"id":2345,"name":"user@example.com",
		"domain":"","display_name":""},
		"details":"Assigned role 1234 to user 123",
		"audit_row_id":3456,"type":0,
		"type_name":"CreateObject","object_name":"",
		"object_type_name":"content_set_role_membership"}</pre>

Content set role privilege	`content_set_role_privilege`	Includes entries when privileges are created, modified, or deleted.
		Content set role privilege log entry example
		<pre>{"object_id":12345,"audit_name":"",
		"creation_time":"2023-01-01T19:46:48Z",</pre>

©2026 Tanium Inc. All Rights Reserved

Audit type	`object_type_name` log value [1]	Audit information

		<pre>"modification_time":"2023-01-01T19:46:48Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":1234,
		"mod_user":{"id":1234,"name":"user@example.com",
		"domain":"","display_name":""},
		"details":"","audit_row_id":12345,"type":2,
		"type_name":"DeleteObject","object_name":"",
		"object_type_name":"content_set_role_privilege"}</pre>

Content set user group role membership	`content_set_user_group_role_membership`	Includes entries when a role is assigned to or removed from a user group.
		Content set user group role membership log entry example
		<pre>{"object_id":123,
		"audit_name":"ContentSetUserGroupRoleMembership ID 433",
		"creation_time":"2023-03-29T15:26:41Z",
		"modification_time":"2023-03-29T15:26:41Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":1234,
		"mod_user":{"id":1234,"name":"user@example.com",
		"domain":"","display_name":""},
		"details":"Assigned role 1234 to user group 123",
		"audit_row_id":123,"type":0,
		"type_name":"CreateObject","object_name":"",
		"object_type_name":
		"content_set_user_group_role_membership"}</pre>

Dashboard	`dashboard`	Includes entries when dashboards are created, modified, or deleted.
		Dashboard log entry example
		<pre>{"object_id":123,"audit_name":"",
		"creation_time":"2023-01-01T11:13:06Z",
		"modification_time":"2023-01-01T11:13:06Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":123,
		"mod_user":{"id":123,"name":"user@example.com",
		"domain":"","display_name":""},
		"details":"","audit_row_id":123,"type":1,
		"type_name":"UpdateObject",
		"object_name":"example dashboard",
		"object_type_name":"dashboard"}</pre>

Dashboard group	`dashboard_group`	Includes entries when dashboard groups are created, modified, or deleted.
		Dashboard group log entry example
		<pre>{"object_id": 123,"audit_name": "",
		"creation_time": "2023-01-01T13:56:27Z",
		"modification_time": "2023-01-01T13:56:27Z",
		"last_modified_by": "user@example.com",
		"modifier_user_id": 123,
		"mod_user": {"id": 123,
		"name": "user@example.com",
		"domain": "","display_name": ""} ,</pre>

©2026 Tanium Inc. All Rights Reserved

Audit type	`object_type_name` log value [1]	Audit information

		<pre>"details": "","audit_row_id": 123,"type": 1,
		"type_name": "UpdateObject",
		"object_name": "example category group",
		"object_type_name": "dashboard_group"}</pre>

Downloader authorized certificate	`downloader_auth_cert`	Includes entries when certificate authentication remote sources for downloads authentication are created, modified, or deleted.
		Downloader authorized certificate log entry example
		<pre>{"object_id":123,
		"audit_name":"Updated downloader_auth_cert",
		"creation_time":"2023-01-01T00:56:16Z",
		"modification_time":"2023-01-01T00:56:16Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":123,
		"mod_user":{"id":123,"name":"user@example.com",
		"domain":"","display_name":""},
		"details":"Updated downloader_auth_cert (ID:123)",
		"audit_row_id":123,"type":1,
		"type_name":"UpdateObject",
		"object_name":"https://example.url.com",
		"object_type_name":"downloader_auth_cert"}</pre>

Downloader authorized user	`downloader_auth_user`	Includes entries when credential authentication remote sources for downloads authentication are created, modified, or deleted.
		Downloader authorized user log entry example
		<pre>{"object_id":123,
		"audit_name":"Deleted downloader_auth_user",
		"creation_time":"2022-01-01T16:21:38Z",
		"modification_time":"2022-01-01T16:21:38Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":123,
		"mod_user":{"id":123,"name":"user@example.com",
		"domain":"","display_name":""},
		"details":"Deleted downloader_auth_user (ID:123)",
		"audit_row_id":123,"type":2,
		"type_name":"DeleteObject","object_name":"example",
		"object_type_name":"downloader_auth_user"}</pre>

Downloader trusted certificate	`downloader_trusted_cert`	Includes entries when trusted certificates for downloads authentication are created, modified, or deleted.
		Downloader trusted certificate log entry example
		<pre>{"object_id":123,
		"audit_name":"Created downloader_trusted_cert",
		"creation_time":"2023-01-01T16:56:56Z",
		"modification_time":"2023-01-01T16:56:56Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":123,
		"mod_user":{"id":123,"name":"user@example.com",</pre>

©2026 Tanium Inc. All Rights Reserved

Audit type	`object_type_name` log value [1]	Audit information

		<pre>"domain":"","display_name":""},
		"details":"Created downloader_trusted_cert (ID:1234)",
		"audit_row_id":1234,"type":0,
		"type_name":"CreateObject","object_name":"",
		"object_type_name":"downloader_trusted_cert"}</pre>

Group	`group`	Includes entries when groups are created, modified, or deleted. Includes entries for filter groups and management rights groups.
		Group log entry example
		<pre>{"object_id":6411330,
		"audit_name":"example computer group",
		"creation_time":"2023-01-01T17:13:46Z",
		"modification_time":"2023-01-01T17:13:46Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":1234,
		"mod_user":{"id":1234,"name":"user",
		"domain":"example","display_name":""},
		"details":"","audit_row_id":12345,"type":0,
		"type_name":"CreateObject",
		"object_name":"example computer group",
		"object_type_name":"group"}</pre>

HTTPS Certificate	`https_certificate`	Includes entries for new Tanium Server certificate signing requests and when certificates are uploaded.
		HTTPS certificate log entry example
		<pre>{"object_id": 0,
		"audit_name": "test.example.local",
		"creation_time": "2025-07-23T14:16:14Z",
		"modification_time": "2025-07-23T14:16:14Z",
		"last_modified_by": "example",
		"modifier_user_id": 1,
		"mod_user": {"id": 1, "name": "example",
		"domain": "", "display_name": ""},
		"details": "Add Certificate Signing Request
		for server: test.example.local",
		"audit_row_id": 1, "type": 0,
		"type_name": "CreateObject",
		"object_name": "",
		"object_type_name": "https_certificate"}</pre>

Intentional subnet	`intentional_subnet`	Includes entries when intentional subnets are created, modified, or deleted.
		Intentional subnet log entry example
		<pre>{"object_id":123,
		"audit_name":"Created intentional_subnet",
		"creation_time":"2023-01-01T19:18:28.000Z",
		"modification_time":"2023-01-01T19:18:28.000Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":123 ,
		"mod_user":{"id":123,"name":"user@example.com",</pre>

©2026 Tanium Inc. All Rights Reserved

Audit type	`object_type_name` log value [1]	Audit information

		<pre>"domain":"","display_name":""},
		"details":"Created intentional_subnet (ID:123)",
		"audit_row_id":123,"type":0,
		"type_name":"CreateObject",
		"object_name":"www.example.com",
		"object_type_name":"intentional_subnet"}</pre>

Isolated subnet	`isolated_subnet`	Includes entries when isolated subnets are created, modified, or deleted.
		Isolated subnet log entry example
		<pre>{"object_id":123,
		"audit_name":"Created isolated_subnet",
		"creation_time":"2023-01-01T19:18:07.000Z",
		"modification_time":"2023-01-01T19:18:07.000Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":123,
		"mod_user":{"id":123,"name":"user@example.com",
		"domain":"","display_name":""},
		"details":"Created isolated_subnet (ID:0)",
		"audit_row_id":1,"type":0,
		"type_name":"CreateObject","object_name":"",
		"object_type_name":"isolated_subnet"}</pre>

Local setting	`local_setting`	Includes entries when local settings are created, modified, or deleted.
		Local setting log entry example
		<pre>{"object_id":123,
		"audit_name":"example_setting",
		"creation_time":"2023-01-01T19:14:20.000Z",
		"modification_time":"2023-01-01T19:14:20.000Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":123,
		"mod_user":{"id":123,"name":"user@example.com",
		"domain":"","display_name":""},
		"details":"Server: example server",
		"audit_row_id":1,"type":0,
		"type_name":"CreateObject","object_name":"",
		"object_type_name":"local_setting"}</pre>

Package spec	`package_spec`	Includes entries when packages are created, modified, or deleted.
		Package log entry example
		<pre>{"object_id":123456,
		"audit_name":"Example package",
		"creation_time":"2023-01-01T22:39:10.000Z",
		"modification_time":"2023-01-01T22:39:10.000Z",
		"last_modified_by":"","modifier_user_id":0,
		"details":"","audit_row_id":123456,"type":2,
		"type_name":"DeleteObject",
		"object_name":"Example package",
		"object_type_name":"package_spec"}</pre>

©2026 Tanium Inc. All Rights Reserved

Audit type	`object_type_name` log value [1]	Audit information
Persona	`persona`	Includes entries when personas are created, modified, or deleted. **Persona log entry example** `{"object_id":1234, "audit_name":"example persona", "creation_time":"2023-01-01T17:26:56Z", "modification_time":"2023-01-01T17:26:56Z" , "last_modified_by":"user@example.com", "modifier_user_id":1234, "mod_user":{"id":1234,"name":"user@example.com", "domain":"","display_name":"example persona"}, "details":"Insert persona", "audit_row_id":1234,"type":0, "type_name":"CreateObject", "object_name":"example persona", "object_type_name":"persona"}`
PKI key configuration	`pki_key_ configuration`	Includes entries when root key configurations are created, modified, or deleted. **PKI key configuration log entry example** `{"object_id":123,"audit_name":"", "creation_time":"2023-01-01T14:39:19.000Z", "modification_time":"2023-01-01T14:39:19.000Z", "last_modified_by":"user@example.com", "modifier_user_id":123, "mod_user":{"id":123,"name":"user@example.com", "domain":"","display_name":""}, "details":"","audit_row_id":1, "type":0,"type_name":"CreateObject", "object_name":"", "object_type_name":"pki_key_configuration"}`
PKI root key	`pki_root_key`	Includes entries when root keys are created, modified, or deleted. **PKI root key log entry example** `{"object_id":123, "audit_name":"example_host Root 1", "creation_time":"2023-01-01T14:39:19.000Z", "modification_time":"2023-01-01T14:39:19.000Z", "last_modified_by":"user@example.com", "modifier_user_id":123, "mod_user":{"id":123,"name":"user@example.com", "domain":"","display_name":""}, "details":"Created key with fingerprint 8b0cd398201a1749a6e812342357783d 90689058707d71c768083c1e336accf 7b5ce90b7b0abcd8175b963bb621fa32 956785009cb610c4345f3ef713dfca983", "audit_row_id":1,"type":0, "type_name":"CreateObject","object_name":"", "object_type_name":"pki_root_key"}`

©2026 Tanium Inc. All Rights Reserved

Audit type	object_type_name log value [1]	Audit information
PKI server registration request	pki_server_registration_requests	Includes entries when server registration requests are created, modified, or deleted. **PKI server registration request log entry example** {"object_id":123,"audit_name":"", "creation_time":"2023-01-01T14:39:19.000Z", "modification_time":"2023-01-01T14:39:19.000Z", "last_modified_by":"user@example.com", "modifier_user_id":123, "mod_user":{"id":123,"name":"user@example.com", "domain":"","display_name":""}, "details":"","audit_row_id":1,"type":0, "type_name":"CreateObject","object_name":"", "object_type_name":"pki_server_registration_requests"}
Platform setting	system_setting	Includes entries when platform settings are created, modified, or deleted. **Platform setting log entry example** {"object_id":5, "audit_name":"max_strings_total_mb", "creation_time":"2023-01-01T22:34:32Z", "modification_time":"2023-01-01T22:34:32Z", "last_modified_by":"","modifier_user_id":0, "details":"Last updated by 'root' through the command line.","audit_row_id":1234, "type":1,"type_name":"UpdateObject", "object_name":"max_strings_total_mb", "object_type_name":"system_setting"}
Plugin schedule	plugin_schedule	Includes entries when plugin schedules are created, modified, or deleted. **Plugin schedule log entry example** {"object_id":12345, "audit_name":"Connect Scheduled Connections For 1234:user@example.com", "creation_time":"2023-01-01T06:06:07.000Z", "modification_time":"2023-01-01T06:06:07.000Z", "last_modified_by":"user@example.com", "modifier_user_id":1234, "mod_user":{"id":1234,"name":"user@example.com", "domain":"","display_name":""}, "details":"","audit_row_id":12345,"type":0, "type_name":"CreateObject", "object_name":"Connect Scheduled Connections For 1234:user@example.com", "object_type_name":"plugin_schedule"}
Saved action	saved_action	Includes entries when saved actions are created, modified, or deleted. **Saved action log entry example** {"object_id":123456, "audit_name":"Example saved action",

©2026 Tanium Inc. All Rights Reserved

Audit type	`object_type_name` log value [1]	Audit information

		<pre>"creation_time":"2023-01-01T23:05:53.000Z",
		"modification_time":"2023-01-01T23:05:53.000Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":1234,
		"mod_user":{"id":1234,"name":"user",
		"domain":"example","display_name":""},
		"details":"","audit_row_id":123456,
		"type":2,"type_name":"DeleteObject",
		"object_name":"Example saved action",
		"object_type_name":"saved_action"}</pre>

Saved question	`saved_question`	Includes entries when saved questions are created, modified, or deleted.
		Saved question log entry example
		<pre>{"object_id":12345,
		"audit_name":"Example saved question",
		"creation_time":"2023-01-01T21:06:04.000Z",
		"modification_time":"2023-01-01T21:06:04.000Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":1234,
		"mod_user":{"id":123,"name":"user",
		"domain":"example","display_name":""},
		"details":"","audit_row_id":123456,
		"type":0,"type_name":"CreateObject",
		"object_name":"Example saved question",
		"object_type_name":"saved_question"}</pre>

Sensor	`sensor`	Includes entries when sensors are created, modified, or deleted.
		Sensor log entry example
		<pre>{"object_id":1234,
		"audit_name":"example sensor",
		"creation_time":"2023-01-01T17:07:27Z",
		"modification_time":"2023-01-01T17:07:27Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":123,
		"mod_user":{"id":123,"name":"user@example.com",
		"domain":"","display_name":""},
		"details":"","audit_row_id":12345,"type":1,
		"type_name":"UpdateObject",
		"object_name":"example sensor",
		"object_type_name":"sensor"}</pre>

Separated subnet	`separated_subnet`	Includes entries when separated subnets are created, modified, or deleted.
		Separated subnet log entry example
		<pre>{"object_id":123,
		"audit_name":"Created separated_subnet ",
		"creation_time":"2023-01-01T19:17:54.000Z",
		"modification_time":"2023-01-01T19:17:54.000Z",
		"last_modified_by":"user@example.com",
		"modifier_user_id":123,
		"mod_user":{"id":123,"name":"user@example.com",</pre>

©2026 Tanium Inc. All Rights Reserved

Audit type	`object_type_name` log value [1]	Audit information

		`"domain":"","display_name":""},`
		`"details":"Created separated_subnet  (ID:0)",`
		`"audit_row_id":123,"type":0,`
		`"type_name":"CreateObject","object_name":"",`
		`"object_type_name":"separated_subnet"}`

Server throttle	`server_throttle`	Includes entries when server throttles are created, modified, or deleted.
		Server throttle log entry example
		`{"object_id": 1, "audit_name": "",`
		`"creation_time": "2025-05-10T08:14:26Z",`
		`"modification_time": "2025-05-10T08:14:26Z",`
		`"last_modified_by": "user@example.com",`
		`"modifier_user_id": 1017,`
		`"mod_user": {"id": 1017,`
		`"name": "user@example.com",`
		`"domain": "", "display_name": ""},`
		`"details": "", "audit_row_id": 136,`
		`"type": 1, "type_name": "UpdateObject",`
		`"object_name": "",`
		`"object_type_name": "server_throttle"}`

Server trust	`server_trust`	Includes entries when server trusts are enabled or revoked between Tanium Servers in an active-active cluster.
		Server trust log entry example
		`{"object_id": 2,`
		`"audit_name": "8344008916864534899",`
		`"creation_time": "2025-07-22T04:55:37Z",`
		`"modification_time": "2025-07-22T04:55:37Z",`
		`"last_modified_by": "john.doe",`
		`"modifier_user_id": 1,`
		`"mod_user": {"id": 1, "name": "john.doe",`
		`"domain": "", "display_name": ""},`
		`"details": "Trust server",`
		`"audit_row_id": 2, "type": 0,`
		`"type_name": "CreateObject",`
		`"object_name": "",`
		`"object_type_name": "server_trust"}`

Site throttle	`site_throttle`	Includes entries when site throttles are created, modified, or deleted.
		Site throttle log entry example
		`{"object_id": 299, "audit_name": "example",`
		`"creation_time": "2025-04-25T04:47:32Z",`
		`"modification_time": "2025-04-25T04:47:32Z",`
		`"last_modified_by": "user@example.com",`
		`"modifier_user_id": 1555,`
		`"mod_user": {"id": 1555,`
		`"name": "user@example.com",`
		`"domain": "", "display_name": ""},`
		`"details": "", "audit_row_id": 241,`
		`"type": 2, "type_name": "DeleteObject",`

©2026 Tanium Inc. All Rights Reserved

Audit type	object_type_name log value [1]	Audit information
		`"object_name": "", "object_type_name": "site_throttle"}`
Users	`user`	Includes entries when users are created, modified, or deleted. **User log entry example** `{"object_id":1234, "audit_name":"user@example.com", "creation_time":"2023-01-01T14:46:43Z", "modification_time":"2023-01-01T14:46:43Z", "last_modified_by":"","modifier_user_id":1234, "details":"Auto-provisioned user", "audit_row_id":1234,"type":0, "type_name":"CreateObject", "object_name":"user@example.com", "object_type_name":"user"}`
User group	`user_group`	Includes entries when user groups are created, modified, or deleted. **User group log entry example** `{"object_id":265, "audit_name":"ContentSetUserGroupRoleMembership ID 1234", "creation_time":"2023-01-01T15:26:41Z", "modification_time":"2023-01-01T15:26:41Z", "last_modified_by":"user@example.com", "modifier_user_id":123, "mod_user":{"id":123,"name":"user@example.com", "domain":"","display_name":""}, "details":"Assigned role 1234 to user group 123", "audit_row_id":1234,"type":1, "type_name":"UpdateObject", "object_name":"example user group", "object_type_name":"user_group"}`
Zone server assignment	`zone_server_assignment`	Includes entries when zone server assignments are created, modified, or deleted. **Zone server assignment log entry example** `{"object_id":123,"audit_name":"", "creation_time":"2023-01-01T11:13:06Z", "modification_time":"2023-01-01T11:13:06Z", "last_modified_by":"user@example.com", "modifier_user_id":123, "mod_user":{"id":123,"name":"user@example.com", "domain":"","display_name":""}, "details":"","audit_row_id":123,"type":1, "type_name":"UpdateObject", "object_name":"example zone server assignment", "object_type_name":"zone_server_assignment"}`

©2026 Tanium Inc. All Rights Reserved

Audit type	object_type_name log value [1]	Audit information

[1] The `object_type_name` values might have `_audit` appended.

General audit table columns

General audit table columns in Connect

Column	Description
`audit_row_id`	The row ID from the database table.
`audit_name`	The type of audit entry. Use this field to identify the audit type of the entry when you retrieve more than one audit type.
`audit_type`	The audit type category.
`creation_time`	The UTC timestamp of when the object was created.
`details`	Contains a description of the action.
`last_modified_by`	The name of the user who last modified the object.
`mod_persona`	Details for the persona who last modified the object. This field is null if no persona was used.
`mod_user`	Details for the user who last modified the object.
`modification_time`	The UTC timestamp of the last time that the object was modified.
`modifier_user_id`	The unique ID of the user who last modified the object. If the ID is 0, this is a system-generated event.
`object_id`	The ID of the object.
`object_name`	The name of the object that was modified. This field is empty for authentication audits.
`object_type_name`	The audit entry category. Use this field when you export audit entries of multiple categories to identify the audit type for individual entries.
`type`	The type of action that generated the audit entry. Values include:

©2026 Tanium Inc. All Rights Reserved

Column	Description
	• `0` - Create • `1` - Update • `2` - Delete • `5` - Failed delete
`type_name`	The type of action that initiated the audit entry, in string form. Values include: • `CreateObject` • `DeleteObject` • `FailedCreateObject` • `FailedDeleteObject` • `UpdateObject`

Authentication audit table columns

The authentication audit table is different from the other audit log tables because it tracks sign-on attempts, not configuration changes.

Authentication audit columns in Connect

Column	Description
`audit_row_id`	The row ID from the database table.
`audit_name`	The type of audit entry. Use this field to identify the audit type of the entry when you retrieve more than one audit type.
`creation_time`	The UTC timestamp of the sign-on attempt.
`details`	Contains a description of the sign-on attempt. A successful sign-on shows the user, session ID, and IP address. A failed sign-on contains a reason for the failed attempt. Examples: • `Failed Authentication Invalid session supplied. Session ID doesn't exist.` • `User: Administrator; Session ID: 2151; IP Address: 192.168.61.180`

©2026 Tanium Inc. All Rights Reserved

Column	Description
	• `User: Administrator; Session ID: 69; Authentication Type: User; Originated from SOAPPluginScheduler` • `Incorrect User User does not exist: fake_user; IP Address: 192.168.61.180`
`last_modified_by`	Not used.
`mod_persona`	Not used.
`mod_user`	Details for the user who initiated the sign-on attempt.
`modification_time`	The UTC timestamp of the sign-on attempt.
`modifier_user_id`	The unique ID of the user who initiated the sign-on attempt. If the ID is 0, this is a system-generated event; see the details column for more information.
`object_id`	The ID of the user who initiated the sign-on attempt. If the ID is 0, the user does not exist; see the details column for more information.
`object_name`	Not used for authentication audits.
`object_type_name`	The type of audit entry. Use this field when you export audit entries of multiple types to identify the audit type for individual entries.
`type`	The ID of the type of sign-on event that generated the entry. Values include: • `0` - New session created • `1` - Unused • `2` - User signed out • `3` - Failed authentication
`type_name`	The type of the sign-on event that generated the entry. Values include: • `CreateObject` - New session created • `DeleteObject` - User Logged out • `FailedCreateObject` - Failed authentication

©2026 Tanium Inc. All Rights Reserved