

Tanium™ Console User Guide

Autonomous IT. Unstoppable Business.

2026H1 Semiannual Release

Version 3.35

October 14, 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 services provided 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 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 at support@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 their respective owners.

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

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

© 2026 Tanium Inc. All Rights Reserved

© 2026 Tanium Inc. All rights reserved.

Table of contents

Part 1: Tanium Console and Interact overview **42**

Tanium Console 42

Tanium Interact 43

Tanium Data Service 43

Tanium Core Platform 43

Tanium solutions 44

Endpoints 44

Questions 44

Actions 45

Content 45

RBAC 45

Tanium Autonomous IT Platform in Console and Interact 46

Supported languages 46

Part 2: Getting started with Console and Interact **47**

Set up Console and Interact 47

Initial content 48

Action groups and computer groups 48

Content-only solutions 48

Default Content and Core Content 49

Default Computer Groups 49

Sign in to Console 49

Sign in through the Tanium Server 50

Authentication types 50

Sign in 50

Sign in through a SAML IdP portal 52

Initial Console page and content imports 52

Sign out of Console 53

© 2026 Tanium Inc. All Rights Reserved

Session validity and timeouts ... 53
Console components and navigation ... 54
Header ... 55
Logo ... 55
Quick Search bar ... 55
Environment details ... 56
Guardian notifications ... 57
Guide notifications ... 57
Help ... 57
User and persona options ... 57
Warning indicator ... 57
Breadcrumbs ... 58
Display pane ... 58
Solution menu ... 58
Main menu ... 59
Keyboard navigation ... 61
Data grid viewing options ... 61
Tanium Home page ... 62
Manage the display of Home page sections ... 65
View environment status ... 65
Online Endpoints ... 65
Total Endpoints ... 66
Operating Platform ... 66
Unmanaged Network Interfaces ... 66
Explore endpoint data ... 66
Ask a Question ... 66
Search Endpoints ... 67
Build Question ... 67
Work with Quick Links ... 67
Access Tanium module workbenches ... 68

© 2026 Tanium Inc. All Rights Reserved

Work with Reporting dashboards ... 68
Dashboard section ... 69
Dashboard List section ... 70
Work with favorite Interact categories, dashboards, and saved questions ... 71
Use Interact ... 72
Part 3: Tanium Console and Interact requirements ... 73
Web browsers ... 73
Core platform dependencies ... 73
Console solution dependencies ... 73
Interact and TDS solution dependencies ... 74
Tanium recommended installation ... 74
Import specific solutions ... 74
Required dependencies ... 74
Feature-specific dependencies ... 75
Core Platform resources ... 75
Endpoints ... 75
Supported operating systems ... 75
Disk space requirements ... 75
Processor requirements ... 76
Host and network security ... 76
Security exclusions ... 76
Ports ... 76
Internet URLs ... 76
User role requirements ... 76
Tanium Core Platform configuration permissions ... 77
Tanium Interact and TDS permissions ... 80
Interact permissions ... 81
Tanium Data Service (TDS) permissions ... 85
Action management permissions ... 89
Content management permissions ... 97

© 2026 Tanium Inc. All Rights Reserved

RBAC management permissions ... 102
Troubleshooting permissions ... 106
Part 4: Managing Tanium solutions ... **108**
Tanium solutions overview ... 108
Solutions page contents and widgets ... 108
Content grid filters ... 109
Solutions page buttons ... 110
Tanium releases ... 111
Semiannual releases ... 112
Release lifecycle ... 112
Skipping releases ... 112
Tanium Client and endpoint tools support ... 112
Maintenance release updates ... 112
Skipping releases ... 113
Installing an update that is not the latest ... 113
Tanium manifest ... 113
Installing a new deployment ... 114
Fresh installation of TanOS and Appliance ... 114
Fresh installation of Tanium Core Platform servers for Windows ... 114
Fresh installation of Tanium solutions and content ... 114
Fresh installation of Tanium Client and endpoint tools ... 114
Updating an existing deployment ... 114
TanOS updates (Appliance only) ... 115
Tanium Core Platform servers updates ... 115
Tanium solutions and content updates ... 115
Tanium Client and endpoint toolset updates ... 116
Release status ... 116
Installation not started ... 116
Installation in progress ... 117
Installation completed ... 118

© 2026 Tanium Inc. All Rights Reserved

Modules ... 118
Modules overview ... 118
View and manage modules ... 119
Shared services ... 119
Shared services overview ... 119
View and manage shared services ... 120
Content-only solutions ... 120
Overview of content-only solutions ... 120
Default imports ... 120
View and manage content-only solutions ... 120
Imports and updates in active-active deployments ... 121
Tools deployment and restricted targeting ... 121
Dependencies and default settings ... 122
Import all modules and services ... 123
Default settings and content imports ... 124
Before you begin ... 124
Import all solutions ... 125
Import or update specific solutions ... 125
Solution versions ... 125
Labs content ... 126
Tanium Emerging Issues Content ... 126
Before you begin ... 126
Import, re-import, or update solutions ... 126
Install a Tanium release update ... 128
Solution dependencies in a release ... 128
Before you begin ... 128
Install the update ... 129
Troubleshoot release update issues ... 131
Error messages for updates ... 131
Resolve update errors ... 131

© 2026 Tanium Inc. All Rights Reserved

Export and import specific solution versions through URLs ... 132
Before you begin ... 132
Export a solution as a URL ... 132
Import a solution from a URL ... 133
Export content files ... 133
Import content files ... 134
Resolve import conflicts ... 135
Best practices for resolving import conflicts ... 136
Tip 1: Read release notes ... 137
Tip 2: Verify restore points ... 137
Tip 3: Update the lab deployment first ... 137
Tip 4: Limit customizations to Tanium content ... 138
Tip 5: Recreate content that uses parameterized sensors or packages ... 138
Tip 6: Avoid bulk overwrites to Tanium content ... 138
Uninstall solutions ... 138
Tanium Server synchronization ... 141
Manage certificates for Tanium Server synchronization ... 141
Resolve Tanium Server synchronization errors ... 142
Verify browser URL entry ... 142
Verify Tanium Server port ... 143
Verify certificate trust ... 143
Enable CORS support ... 143
Disable synchronization for module operations ... 143
Manage service accounts for solutions ... 144
Manage Tanium service accounts ... 144
Service account passwords ... 144
Manual or automatic service account configuration ... 144
Update Tanium service account settings ... 144
Manage Windows service accounts (not applicable to the Tanium Appliance) ... 145
Tanium solution service accounts ... 145

© 2026 Tanium Inc. All Rights Reserved

LocalSystem service account ... 145
Tanium Core Platform service accounts ... 145
Update Windows service accounts ... 145
Part 5: Customizing Console and Interact ... 147
Configure a pre-login banner ... 147
Before you begin ... 147
Banner with only text and basic formatting ... 148
Banner with images, links, or complex text formatting ... 148
Create the pre-login banner file for an Appliance deployment ... 148
Create the pre-login banner file for a Windows deployment ... 150
Enable the pre-login banner ... 150
Select the Console color ... 151
Configure Console header text ... 152
Select the task confirmation prompt ... 153
Add a help URL ... 153
Customize the Console logo ... 154
Configure Console user preferences ... 155
Consider question results complete at ... 156
Suspend console automatically if no activity detected for ... 156
Theme ... 156
Language ... 157
Hide error results from questions ... 157
Open Search Bar Results in New Tab ... 157
Show Environment Details ... 157
Customize solution overview pages ... 157
Configuring the Tanium Core Platform ... 159
Settings for Tanium Core Platform servers ... 159
Settings for Tanium Clients ... 160
Configuring the Tanium Core Platform ... 161
Settings for Tanium Core Platform servers ... 161

© 2026 Tanium Inc. All Rights Reserved

Settings for Tanium Clients ... 162
Customizing the Tanium environment through platform settings ... 163
Manage platform settings ... 163
Manage advanced settings ... 164
Types of Tanium Core Platform settings ... 164
Hidden settings ... 165
Override settings on individual servers and Clients ... 165
View advanced settings ... 165
Edit advanced settings ... 165
Create advanced settings ... 166
Allowing Tanium Client downloads from Internet URLs ... 168
View allowed URLs ... 168
Add allowed URLs ... 169
Edit allowed URLs ... 169
Delete allowed URLs ... 170
Export or import allowed URLs ... 170
Export allowed URLs ... 170
Import allowed URLs ... 171
Copy allowed URL details ... 172
Enabling authentication between platform servers and remote systems ... 173
Manage remote systems ... 177
View remote systems ... 177
Add remote systems ... 177
Before you begin ... 177
Add a remote system ... 178
Edit remote systems ... 179
Delete remote systems ... 179
Manage trusted certificates ... 179
View trusted certificates ... 179
Add trusted certificates ... 180

© 2026 Tanium Inc. All Rights Reserved

Edit trusted certificates ... 180
Delete trusted certificates ... 180
Configuring Internet access through proxy servers ... 181
Overview of proxy servers ... 181
Types of proxy servers ... 182
Configure proxy server settings ... 182
Throttling bandwidth and connections to Tanium Clients ... 187
Bandwidth throttling overview ... 187
Before you begin ... 187
Evaluate default throttle settings ... 188
Default throttles for bandwidth ... 188
Default throttles for concurrent connections ... 188
Evaluate network bandwidth requirements ... 188
Bandwidth trends ... 188
Global throttles ... 189
Site throttles ... 189
Zone Server throttles ... 190
Tanium Connect exports ... 190
Overlapping IP address ranges ... 190
Configure global throttles ... 190
Configure site throttles ... 191
Base throttles on local or NAT IP addresses ... 192
Add sites ... 192
Add site throttles ... 192
Verify throttle delays ... 194
Monitor bandwidth and connection usage ... 195
Optimizing Tanium Client peering through subnets ... 196
Overview of Client subnets ... 196
Client peering ... 196
Topology of Client subnets ... 196

© 2026 Tanium Inc. All Rights Reserved

Configure separated subnets ... 197
Configure separated subnets that are the same for Tanium Servers and Zone Servers ... 198
Add subnets ... 198
Edit subnets ... 198
Configure separated subnets that are specific to Zone Servers ... 198
Windows infrastructure ... 199
Tanium Appliance infrastructure ... 199
Configure isolated subnets ... 199
Configure isolated subnets that are the same for Tanium Servers and Zone Servers ... 200
Add subnets ... 200
Edit subnets ... 201
Configure isolated subnets that are specific to Zone Servers ... 201
Isolate all Clients connected to any Zone Server ... 201
Isolate all Clients connected to a particular Zone Server ... 201
Isolate Clients on specific subnets with Windows infrastructure ... 202
Isolate Clients on specific subnets with Tanium Appliance infrastructure ... 202
Configure intentional subnets ... 202
Overview of intentional subnets ... 202
Before you begin ... 203
Define intentional subnets using Sites ... 205
Add subnets ... 205
Edit subnets ... 205
Define intentional subnets using the PeerNeighborhood Client setting ... 205
Verify intentional subnets ... 205
Managing the Tanium license ... 206
License expiration ... 206
View license details ... 206
Replace the license ... 207
View the count of managed endpoints ... 207
Troubleshoot license issues ... 208

© 2026 Tanium Inc. All Rights Reserved

Securing Tanium connections and operations through digital keys **209**
Tanium keys overview 209
TLS communication 209
Communication with external systems 210
Root keys 211
Subordinate keys 211
Subordinate key types 211
Rotation intervals for subordinate keys 213
Key rotation 214
HSM integration 215
View root key information 216
Encrypt the root keys database 217
Set the encryption password 217
Change the encryption password 217
Generate root keys 218
Revoke root keys 218
Download infrastructure configuration files (keys) 218
Securing Console and API access through certificates **220**
Overview of SSL/TLS certificates 220
Before you begin 220
View details for the current certificates or CSR 221
Generate and download a CSR 222
Upload certificates 223
Synchronizing active-active Tanium Servers **224**
Overview of Tanium Server trust 224
Enable trust between Tanium Servers 224
Before you begin 224
Approve trust 225
Revoke trust between Tanium Servers 225
View Tanium Server trust history 225

© 2026 Tanium Inc. All Rights Reserved

Enabling communication between Zone Servers and Hubs ... **226**
Overview of trust and mappings among Zone Servers and Hubs ... 226
Establish trust and configure mappings ... 227
Before you begin ... 227
Approve trust for Zone Server Hubs ... 227
Map Zone Servers to a Zone Server Hub ... 228
Revoke trust and delete mappings ... 229
Revoke a Zone Server Hub ... 229
Revoke a Zone Server ... 230
Delete a Zone Server Hub-to-Zone Server mapping ... 230
Part 6: Exploring and accessing endpoints in Console and Interact ... **231**
What is a question? ... 231
What is a sensor? ... 232
Example: Single row of results ... 233
Example: Multiple rows of results ... 233
Example: Multiple rows and columns of results ... 234
Counting and non-counting questions ... 235
Results aggregation ... 235
Results readability and network traffic ... 237
Merge questions ... 237
Recent results ... 237
[too many results] message ... 237
Convert counting questions to non-counting questions ... 237
Questions with multiple sensors ... 238
Questions with parameterized sensors ... 238
Questions with target filters ... 240
Issue a free-form question ... 241
Overview of free-form questions ... 241
Valid syntax matching ... 242
Enhanced search ... 243

© 2026 Tanium Inc. All Rights Reserved

Issue a question ... 244
Issue a question through the Question Builder ... 245
Search endpoints ... 249
Jump to endpoints ... 250
Jump Gate overview ... 250
Jump to an endpoint ... 251
Question expiration ... 252
Question history ... 253
Reissue a question ... 253
Export question history ... 253
Copy question history details ... 254
Saved questions ... 254
Part 7: Analyzing question results in Console and Interact ... 255
Question results overview ... 255
Results aggregation ... 256
Results for saved questions and dashboards ... 256
Selecting rows ... 256
Enable or disable live updates ... 257
Display results for online and offline endpoints ... 258
Filter question results ... 259
Filter by text ... 260
Filter by computer group ... 260
Filter by advanced conditions ... 261
Overview of advanced filters ... 261
Configure advanced filters ... 262
Copy question results to the clipboard ... 262
Export question results ... 262
Merge questions ... 264
Drill down into results ... 267
View details for a single endpoint ... 270

© 2026 Tanium Inc. All Rights Reserved

Optimizing and automating workflows through the Autonomous IT Platform ... **273**
Overview of Tanium Autonomous IT Platform ... 273
Guided initial configuration ... 273
Proactive guidance ... 273
Adaptive actions and playbooks ... 273
Action oversight ... 274
Autonomous IT Platform across Tanium solutions ... 274
Automate ... 274
Benchmark ... 274
Comply ... 275
Console ... 275
Deploy ... 275
Enforce ... 275
Guide ... 275
Interact ... 276
Patch ... 276
Threat Response ... 276
Ring-based deployment ... 276
Advantages of adaptive actions ... 277
Testing and restriction of action impacts ... 277
Mitigation of action-related disruptions ... 277
Protection for sensitive endpoints ... 277
Deployment types ... 277
Deployment plans ... 278
Endpoint targeting ... 278
Ring-defined targets ... 279
Online and offline endpoints ... 281
Action targeting criteria ... 283
Example: Custom deployment plan ... 283
Example: Dynamic deployment plan ... 286

© 2026 Tanium Inc. All Rights Reserved

Computer group assignments ... 289
First ring ... 292
Last ring ... 292
Ring progression criteria ... 292
Progression criteria evaluation ... 292
Progression criteria descriptions ... 293
Progression criteria status ... 294
Deployment timing factors and maintenance windows ... 295
Example: platform action timing ... 296
Example: Deploy (software) deployment timing ... 296
Deferred endpoints ... 298
Actions overview ... 299
What is an action? ... 299
Example: Action deployment use case ... 299
RBAC for actions ... 299
Action status and logs ... 300
Action packages ... 300
Action groups ... 300
Action locks ... 301
Scheduled actions ... 301
Action approval ... 301
Adaptive actions and simple actions ... 302
Policy actions ... 302
Action best practices ... 303
Optimize questions for action targeting ... 303
Example: optimizing the "Get" clause ... 303
Example: optimizing the "from" clause ... 305
Best practices for action questions ... 306
Optimize action groups and computer groups for targeting ... 306
Conserving resources through action distribution ... 307

© 2026 Tanium Inc. All Rights Reserved

Action deployment overview ... 307
Administrative setup for actions ... 307
Review and edit global settings for actions ... 308
Review and customize action content ... 309
Configure RBAC for action users ... 310
Configure downloads authentication ... 313
Configure and deploy actions ... 313
Monitor actions ... 316
View action status and settings ... 316
Troubleshoot actions ... 318
Actions overview ... 320
What is an action? ... 320
Example: Action deployment use case ... 320
RBAC for actions ... 320
Action status and logs ... 321
Action packages ... 321
Action groups ... 321
Action locks ... 322
Scheduled actions ... 322
Action approval ... 322
Adaptive actions and simple actions ... 323
Policy actions ... 323
Action best practices ... 324
Optimize questions for action targeting ... 324
Example: optimizing the "Get" clause ... 324
Example: optimizing the "from" clause ... 326
Best practices for action questions ... 327
Optimize action groups and computer groups for targeting ... 327
Conserving resources through action distribution ... 328
Action deployment overview ... 328

© 2026 Tanium Inc. All Rights Reserved

Administrative setup for actions ... 328
Review and edit global settings for actions ... 329
Review and customize action content ... 330
Configure RBAC for action users ... 331
Configure downloads authentication ... 334
Configure and deploy actions ... 334
Monitor actions ... 337
View action status and settings ... 337
Troubleshoot actions ... 339
Managing scheduled actions and action history ... 341
Scheduled actions overview ... 341
Predefined scheduled actions ... 341
Scheduled actions with parameterized packages ... 341
Manage scheduled actions ... 342
Update action packages ... 347
Export actions ... 347
Import actions ... 348
Manage actions that are completed or in progress ... 349
View status for simple actions ... 352
Action states ... 353
Investigate action-related issues through logs ... 355
Track action IDs ... 355
View action IDs on Tanium Console ... 356
Navigate Tanium Client logs by action IDs ... 357
Managing ring deployments ... 359
Role permissions for managing deployments ... 359
Analyze multiple deployments ... 359
Deployment details on the Ring Deployment Status page ... 360
Use display options on the Ring Deployment Status page ... 361
Analyze and manage a single deployment ... 362

© 2026 Tanium Inc. All Rights Reserved

Before you begin ... 362
Access the deployment as the creator ... 362
Determine the deployment ID ... 362
Analyze, investigate, or manage a single deployment ... 363
Summary ... 364
Deployment Plan Status ... 366
Attempt (platform actions only) ... 367
Endpoint count ... 367
Message banner ... 367
Ring Details ... 368
Endpoint Execution Status ... 368
Progression Criteria ... 369
Includes Deferred Endpoints ... 370
Ring Progression Failures ... 370
Endpoint Details ... 370
Endpoint Status ... 370
Filter the grid ... 371
Sort the grid ... 372
View additional information ... 372
Ring Deployment Attempts ... 372
Evaluation Results ... 373
Filter the grid ... 373
View additional information ... 373
Explore deployment status and targeting ... 373
Explore multiple endpoints ... 373
Explore and manage a single endpoint ... 374
Stop, pause, or resume deployments ... 375
Reissue deployments ... 376
Manually progress deployments through rings ... 377
Retry a deployment in one ring ... 378

© 2026 Tanium Inc. All Rights Reserved

Skip the wait intervals during deployment ... 378
Troubleshoot deployments ... 379
Action status on endpoints ... 380
Deployment status ... 381
Ring status ... 382
Managing deployment plans for ring deployments ... 384
Deployment plan types ... 384
Custom deployment plans ... 384
Dynamic deployment plans ... 384
View deployment plans ... 385
Create a deployment plan ... 385
Before you begin ... 385
Add a deployment plan ... 386
Configure the deployment plan overview ... 386
Configure rings, progression criteria, and deferred endpoints ... 387
Preview and save the deployment plan ... 389
Clone a deployment plan ... 389
Edit a deployment plan ... 390
Delete a deployment plan ... 390
Deploying actions and playbooks in Console and Interact ... 391
Select an action or playbook initiation method ... 391
Initiate a new action ... 392
Initiate an existing action ... 392
Initiate an existing playbook ... 393
Deploy a predefined action ... 393
Configure action settings ... 395
Review action status ... 399
Targeting actions through action groups ... 400
View action groups ... 400
Create an action group ... 401

© 2026 Tanium Inc. All Rights Reserved

Edit an action group ... 402
Edit action group assignments for scheduled actions ... 402
Export and import action groups ... 402
Export action groups ... 402
Import action groups ... 403
Copy action group configuration details ... 404
Delete an action group ... 405
Best practices for action groups ... 405
Reconfigure action groups that target No Computers ... 405
Define a specific use for each action group ... 406
Limit access to edit action groups ... 406
Minimize action group complexity ... 406
Locking down actions on endpoints ... 407
Solution-specific impacts and overrides for action locks ... 407
Turn on action locks ... 408
Test action locks ... 408
Turn off action locks ... 409
Override action locks ... 410
Managing action approval ... 411
Action approval overview ... 411
RBAC for action approval ... 411
Approval impact on action timing ... 411
Create an action approver role ... 411
Create a bypass action approval role ... 412
Assign the action approval and bypass roles ... 412
Enable or disable action approval ... 412
Review and manage pending actions ... 412
Approve pending actions ... 413
Solution content overview ... 415
What is content? ... 415

© 2026 Tanium Inc. All Rights Reserved

Custom content development 415
Managing content 416
Content sets 416
Content-only solutions 416
Content ownership 417
Content exports and imports 417
Solution content overview 418
What is content? 418
Custom content development 418
Managing content 419
Content sets 419
Content-only solutions 419
Content ownership 420
Content exports and imports 420
Managing sensors for collecting endpoint data 421
Sensors overview 421
Sensor scripts 421
Parameterized sensors 422
Virtual sensors 422
Virtual sensor creation and registration 422
Virtual sensor limitations 422
Solution-generated sensor attributes 423
Example: Sensor with Comply-generated attributes 423
Limitations for sensors with solution-generated attributes 423
Sensor results caching and refreshing 423
Sensor data types 424
View sensor details 425
Clone a sensor 426
Create a sensor 427
Edit a sensor 429

© 2026 Tanium Inc. All Rights Reserved

Limitations and best practices for editing sensors ... 429
Edit the sensor configuration ... 430
Move sensors between content sets ... 430
Export or import sensors ... 430
Export sensors ... 430
Import sensors ... 431
Copy sensor configuration details ... 432
Delete sensors ... 433
Manage sensor quarantines ... 433
Overview of sensor quarantines ... 433
View quarantined sensors ... 434
Remove sensors from quarantine ... 435
Enable or disable enforcement of quarantined sensors ... 435
Export quarantined sensor details ... 436
Copy quarantined sensor details ... 437
Manage sensor results collection ... 437
Assessing question impacts on endpoints through sensor runtime indicators ... 438
Sensor runtime thresholds overview ... 438
Sensor runtime calculations ... 438
Sensor runtime icons and defaults ... 438
Sensor runtime caveats and exceptions ... 439
Configure sensor thresholds ... 440
Verify sensor thresholds ... 440
Managing packages for platform actions ... 442
Packages overview ... 442
Manage client applications through packages ... 442
Package files ... 443
Scheduled action with parameterized package ... 443
Running a package command within a process group ... 443
Package verification ... 444

© 2026 Tanium Inc. All Rights Reserved

Verification Exit Codes ... 444
Verification Query ... 444
View package details ... 445
Re-download package files ... 445
Clone a package ... 447
Create a package ... 447
Edit a package ... 450
Move packages between content sets ... 450
Export or import packages ... 451
Export packages ... 451
Import packages ... 452
Copy package configuration details ... 453
Deploy actions from the Packages page ... 453
Delete packages ... 453
Managing saved questions in Console and Interact ... 455
Saved questions overview ... 455
Scheduled saved questions ... 455
Predefined and custom saved questions ... 456
Best practices for saved questions ... 456
Configuring the refresh frequency of sensor results ... 456
Use Reporting to view the results of questions with registered sensors ... 456
Do not edit Tanium-defined questions ... 456
Viewing the results of saved questions in Interact or Reporting ... 457
Interact dashboards and categories ... 457
RBAC for saved questions, dashboards, and categories ... 458
Content set permissions and dependencies ... 458
Visibility options ... 458
User-specific settings and results for saved questions ... 459
View saved question details ... 459
View saved question settings ... 460

© 2026 Tanium Inc. All Rights Reserved

Filter by categories and dashboards ... 460
Filter by text strings ... 461
Filter by favorites ... 462
Filter by question attributes ... 462
Clone a saved question ... 463
Create a saved question ... 463
Edit a saved question ... 465
Move saved questions between content sets ... 466
Issue a saved question ... 466
Issue a dashboard of saved questions ... 467
Manage categories and dashboards ... 469
View and filter categories or dashboards ... 469
Create a category ... 469
Create a dashboard ... 470
Assign dashboards to a category ... 470
Assign saved questions to a dashboard ... 470
Edit category or dashboard settings ... 471
Export categories, dashboards, or questions ... 471
Delete a category or dashboard configuration ... 472
Export or import saved questions ... 472
Export saved questions ... 472
Import saved questions ... 473
Copy saved question configuration details ... 474
Delete saved questions ... 475
Managing filter groups for filtering questions and results ... 476
Filter groups overview ... 476
Filter group permissions ... 476
View filter group details ... 477
Configure a filter group ... 477
Export or import filter groups ... 478

© 2026 Tanium Inc. All Rights Reserved

Export filter groups ... 478
Import filter groups ... 479
Copy filter group configuration details ... 480
Delete filter groups ... 481
Authenticating content files ... 482
Overview of content imports and exports ... 482
Supported file formats ... 482
Digital signatures and keys ... 482
Import and export permissions ... 483
Import and export procedures ... 483
Create content authentication keys ... 483
Windows: Create content authentication keys ... 484
Linux: Create content authentication keys ... 484
Sign content files ... 485
Windows: Sign content files ... 486
Linux: Sign content files ... 486
Verify content file signatures ... 487
Windows: Verify file signatures ... 487
Linux: Verify file signatures ... 488
Copy the public key to the key store ... 488
Windows: Copy the public key to the key store ... 488
Linux: Copy the public key to the key store ... 489
Example: Package files ... 490
Example: Multi-column sensors ... 492
Sensor script for multi-column sensors ... 492
Configure settings for multi-column sensors ... 493
Example: Parameterized sensors ... 495
Overview of parameterized sensors ... 495
Sample question with parameterized sensor ... 495
Script for a parameterized sensor ... 497

© 2026 Tanium Inc. All Rights Reserved

Parameter names ... 497
UTF-8 encoding and decoding ... 498
Configure parameter inputs for a sensor ... 502
Parameter types ... 503
Parameter options ... 504
Validation expressions ... 507
Example: Parameterized packages ... 508
Overview of parameterized packages ... 508
Package script and command-line parameters ... 510
Parameter positions ... 510
UTF-8 encoding and decoding ... 512
Configure parameter inputs for a package ... 516
Parameter types ... 517
Parameter options ... 518
Validation expressions ... 521
Example: Sensor-sourced packages ... 522
Overview of sensor-sourced packages ... 522
Script for a sensor-sourced package ... 523
Configure settings for a sensor-sourced package ... 523
Command setting ... 523
Package Name setting (optional) ... 524
Example: Saved questions with associated packages ... 525
RBAC overview ... 527
Roles and permissions ... 527
Content sets ... 528
Users ... 529
User groups ... 529
Personas ... 529
Computer groups ... 530
RBAC configuration overview ... 530

© 2026 Tanium Inc. All Rights Reserved

1. Configure custom roles 531
2. Define computer management groups 532
3. Define alternative personas 533
4. Configure user groups 534
5. Configure users 534
6. Sign in to Tanium Console to access the default persona 535
7. Switch to an alternative persona 536
Complete RBAC workflow 538
Plan your RBAC implementation 539
Naming convention 540
Computer groups 540
Membership criteria 540
Resource usage for actions and questions 540
Content sets 542
Roles 542
Users and user groups 542
LDAP support 542
User group permissions 543
User permissions 543
SAML authentication 543
RBAC overview **544**
Roles and permissions 544
Content sets 545
Users 546
User groups 546
Personas 546
Computer groups 547
RBAC configuration overview 547
1. Configure custom roles 548
2. Define computer management groups 549

© 2026 Tanium Inc. All Rights Reserved

3. Define alternative personas ... 550
4. Configure user groups ... 551
5. Configure users ... 551
6. Sign in to Tanium Console to access the default persona ... 552
7. Switch to an alternative persona ... 553
Complete RBAC workflow ... 555
Plan your RBAC implementation ... 556
Naming convention ... 557
Computer groups ... 557
Membership criteria ... 557
Resource usage for actions and questions ... 557
Content sets ... 559
Roles ... 559
Users and user groups ... 559
LDAP support ... 559
User group permissions ... 560
User permissions ... 560
SAML authentication ... 560
Managing access to content through content sets ... 561
Content sets overview ... 561
Role permissions for content sets ... 561
View content set details ... 564
Create a content set ... 564
Move content between content sets ... 565
Before you begin ... 565
Move content to a different content set ... 566
Export or import content sets ... 566
Export content sets ... 566
Import content sets ... 567
Delete a content set ... 568

© 2026 Tanium Inc. All Rights Reserved

Managing access permissions through roles **569**
Roles overview 569
Custom and system roles 569
Custom roles 569
System roles 569
Role components 570
Allow and deny roles 572
Provided role permissions 576
Dependencies between read-write permissions 577
Task-based dependencies among permissions 577
Interaction between deny and provided permissions 578
Provided permissions on content sets 580
Inherited roles 580
Roles for personas 581
Reserved roles 581
Administrator reserved role 582
Content Set Administrator reserved role 582
Content Administrator reserved role 583
Deny All reserved role 584
Tasks that require reserved roles 585
View role details 585
Configure a custom role 586
Manage user and user group assignments for a role 587
Manage persona assignments for a role 587
Manage role permissions 588
View effective role permissions 588
Configure role permissions 591
Assign or unassign permissions for a single role 591
Assign permissions and content sets to multiple roles 592
Unassign permissions and content sets from multiple roles 594

© 2026 Tanium Inc. All Rights Reserved

Administration permissions ... 594
Solution permissions ... 598
Platform content permissions ... 600
Manage content set permissions for a role ... 605
Manage content set permissions for multiple roles ... 605
Manage content set permissions for a single role ... 605
Export and import roles ... 607
Export roles ... 607
Import roles ... 608
Copy role configuration details ... 608
Delete a role ... 609
Controlling endpoint management rights through computer groups ... 610
Computer groups overview ... 610
Computer group types ... 610
Computer management groups ... 611
Computer filter groups ... 611
Computer management and filter groups ... 612
Computer groups in questions ... 612
Computer group membership ... 614
Dynamic membership ... 614
Manually defined membership ... 615
Default computer groups ... 615
View computer group details ... 616
Configure a computer group ... 617
Considerations for creating computer groups ... 617
Considerations for editing computer groups ... 617
Create, clone, or edit a computer group ... 618
Assign computer groups ... 618
Manage computer group membership through custom tags ... 619
Review custom tags ... 619

© 2026 Tanium Inc. All Rights Reserved

Add custom tags ... 620
Remove custom tags ... 620
Export or import computer groups ... 621
Export computer groups ... 621
Import computer groups ... 622
Copy computer group configuration details ... 622
Delete computer groups ... 623
Managing users ... 625
Users overview ... 625
Local and imported user accounts ... 625
User assignments in Tanium RBAC ... 625
User authentication ... 626
Default user ... 627
View user details ... 627
Create a user ... 629
LDAP integrations ... 629
SAML integrations ... 629
RBAC assignments ... 629
Create a local or AD user ... 630
Configure user display name and properties ... 631
Manage role assignments for a user ... 631
View effective role permissions for a user ... 631
Configure role assignments for a user ... 635
Manage user group assignments for a user ... 635
Manage persona assignments for a user ... 635
Manage computer group assignments for a user ... 636
Delete content or transfer ownership ... 637
Delete or transfer the content of an active user ... 638
Delete or transfer the content of a non-active user ... 638
Export user details ... 639

© 2026 Tanium Inc. All Rights Reserved

Copy user configuration details 640
Delete, un-delete, or lock out a user 640
Considerations when deleting users 640
Locked-out users 641
Delete a user 641
Un-delete a user 641
Disable or enable local user access 642
Local users on a Tanium Appliance 642
Local users on a Windows server 642
Managing user groups 643
User groups overview 643
Local and imported user groups 643
User group assignments in Tanium RBAC 643
View user group details 644
Configure a user group 645
Manage role assignments for a user group 646
View effective role permissions for a user group 646
Configure role assignments for a user group 650
Manage user assignments for a user group 650
Manage persona assignments for a user group 650
Manage computer group assignments for a user group 651
Set the default user group 652
Export user group details 653
Copy user group configuration details 653
Delete a user group 654
Managing role and computer group permissions through personas 655
Personas overview 655
Persona types 655
Default persona 655
Alternative persona 655

© 2026 Tanium Inc. All Rights Reserved

Persona assignments in Tanium RBAC ... 656
View persona details ... 656
Configure a persona ... 657
Manage role assignments for a persona ... 658
View effective role permissions for a persona ... 658
Configure role assignments for a persona ... 662
Manage user and user group assignments for a persona ... 662
Manage computer group assignments for a persona ... 662
Transfer content that a persona owns ... 663
Select a persona for your Console session ... 663
Export persona details ... 664
Copy persona configuration details ... 665
Delete a persona ... 665
Importing and authenticating users through LDAP ... 666
LDAP overview ... 666
LDAP synchronization ... 666
RBAC configuration for new users and user groups ... 666
LDAP logs and troubleshooting ... 667
Example: LDAP synchronization and authentication ... 667
User and user group filtering ... 669
Best practices for LDAP integrations ... 671
Create users and user groups on the LDAP server ... 672
Manage Tanium access through the LDAP server ... 672
Control LDAP server access ... 672
Maintain a local administrator account ... 672
Deleting users ... 672
Configure LDAP server connections ... 673
Before you begin ... 673
Configure an LDAP server connection ... 674
Clone an LDAP server ... 681

© 2026 Tanium Inc. All Rights Reserved

Manually synchronize with an LDAP server ... 681
Import LDAP server connection configurations ... 682
Pause or resume an LDAP server ... 683
Delete an LDAP server ... 683
Enabling SSO through SAML ... 684
SAML overview ... 684
IdP-initiated SSO ... 684
SP-initiated SSO ... 685
Before you begin ... 686
Generate a request-signing certificate ... 687
Generate a request-signing certificate in a Tanium Appliance deployment ... 687
Generate a request-signing certificate in a Windows deployment ... 687
Configure SAML on the Tanium Server ... 689
Configure SAML on the IdP ... 693
Before you begin ... 693
Configure Tanium Server settings on the IdP ... 694
Disable or enable SAML SSO ... 694
Disable SSO through Console ... 694
Enable SSO through Console ... 694
Disable SP-initiated SSO without Console access ... 694
Appliance: Disable SSO ... 695
Windows: Disable SSO ... 695
Enabling long-lived Tanium sessions through API tokens ... 696
API tokens overview ... 696
Token permissions ... 696
Best practices for tokens ... 696
View API token details ... 697
Create an API token ... 698
Rotate an API token ... 698
Enable API token authentication behind a reverse proxy ... 699

© 2026 Tanium Inc. All Rights Reserved

Configure token expiration settings 699
Revoke API tokens 700
Part 12: Troubleshooting Console and Interact 701
Basic troubleshooting tips 701
Troubleshoot Console issues 702
Troubleshoot Console access 702
Console is unavailable 703
Console authentication errors 703
Troubleshoot session termination issues 705
Troubleshoot license issues 705
Work with the Console error log 705
Troubleshoot core platform server issues 705
Troubleshoot platform server disk space consumption 706
Troubleshoot platform server trust issues 706
Troubleshoot certificate and key issues 706
Troubleshoot API token access issues 708
Configure server logging levels 708
Troubleshoot proxy server issues 708
Troubleshoot Interact issues 708
Troubleshoot question runtimes 708
Troubleshoot question results issues 709
Troubleshoot action deployment issues 711
Troubleshoot TDS issues 711
Manage the package file repository 711
View package file repository usage 712
Clean the package file repository (Windows infrastructure only) 712
Relocate the package file repository (Windows infrastructure only) 713
Troubleshoot RBAC issues 713
Troubleshoot permission issues 713
Troubleshoot service account lockouts 714

© 2026 Tanium Inc. All Rights Reserved

Troubleshoot solution issues ... 715
Verify and update solution versions ... 715
Troubleshoot installation, update, or uninstallation issues ... 715
Troubleshoot plugin issues ... 716
Troubleshoot solution-specific issues ... 716
Troubleshoot Tanium Client issues ... 717
View the status of Tanium Client registration and communication ... 718
Export Tanium Client status details ... 721
Copy Tanium Client status details ... 722
Deploy actions to remediate Client registration or connectivity issues ... 722
View the Tanium Server info page ... 723
Contact Tanium Support ... 724
Reference: Example questions in Console and Interact ... 725
Example questions ... 725
How can I get a list of running services on endpoints? ... 725
How can I get a list of running processes on endpoints? ... 725
How can I see Windows Registry keys and values? ... 726
How can I get a list of open ports? ... 726
How can I get user authentication information? ... 726
How can I get sign-in information for service accounts? ... 727
How can I get certificate information? ... 728
How can I detect all running Oracle instances within a Linux environment? ... 728
How can I get asset information? ... 729
Example dashboard questions ... 729
Security > Data Leakage ... 729
Security > Proactive Network Security ... 729
Security > Wireless Network Security ... 730
Security > Workstation USB Write Protection ... 730
Reference: Advanced question syntax in Console and Interact ... 731
Use question filters ... 731

© 2026 Tanium Inc. All Rights Reserved

Filters in get clause ... 731
Filters in from clause ... 731
Exclude [no results] ... 732
Filter operators ... 733
Use reserved words or characters ... 735
Reserved words or characters in question text ... 735
Reserved words in sensor names ... 736
Use regular expression filters ... 739
Processing limits for regular expressions ... 739
Example: Match a starting character ... 739
Example: Match any digit ... 739
Example: Negation ... 740
Use computer group filters ... 741
Use sensor column filters ... 742
Use $substring() filters ... 743
Use the "in" operator for filtering ... 743
Use nested filters ... 744
Target random endpoints ... 745
Use advanced sensor options ... 746
Case Sensitivity ... 747
Matching ... 748
Treat Data As ... 748
Maximum Data Age ... 749
Use advanced question options ... 749
Reference: User-specific saved questions ... 750
Overview of user-specific saved questions ... 750
Example: Saved question shared among multiple users ... 750
Role permissions ... 751
Visibility ... 751
User settings ... 752

© 2026 Tanium Inc. All Rights Reserved

User settings for a new saved question ... 752
User settings for an existing saved question ... 753
Saved question configuration copies ... 755
Recent results and computer group assignments ... 755
Recent results and computer group assignments ... 756
Reference: Manage sensor string growth ... 758
Sensor string cleaning ... 758
Maximum string age ... 758
Maximum strings per sensor ... 758
Check sensor string growth ... 759
Check string growth through Health Check ... 759
Check string growth through Console ... 759
Set the maximum string age ... 760
Reference: Language support ... 761
Language selection for solution workbenches ... 761
Browser default for language ... 761
Language selection for users and personas ... 761
Language selection for solution workbenches ... 761
Translation inclusions and exclusions ... 761
Select the language and date format ... 762
Language selection for Tanium documentation ... 762
Translation inclusions, exclusions, and feedback ... 762
Select the documentation language ... 763
Solutions that support multiple languages ... 764
Supported languages ... 764
Reference: Tanium Core Platform settings ... 765

© 2026 Tanium Inc. All Rights Reserved

Part 1: Tanium Console and Interact overview

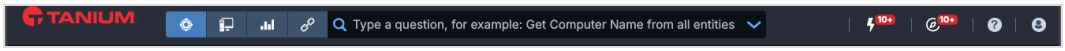
Tanium Console

Tanium Console is the graphical user interface (GUI) that you use to manage the Tanium™ Core Platform and to access Tanium modules (such as Tanium Interact on page 43) and Tanium shared services (such as Tanium Data Service on page 43). Console is a web application that is installed with the Tanium™ Server and does not require separate licensing. You use Console to perform the following key tasks:

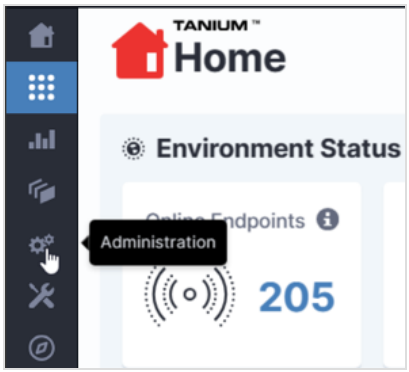
- Import and use Tanium solutions on page 44, which include modules, shared services, and content-only solutions.
- Manage Content on page 45, including sensors, packages, saved questions, and filter groups.
- Deploy and manage Actions on page 45.
- Manage RBAC on page 45 configurations for users, personas, user groups, roles, computer groups, and content sets.
- Configure Tanium Core Platform on page 43 settings that affect the behavior of Console, other Tanium solutions, platform servers, and Tanium Clients.
- Use features of Tanium Autonomous IT Platform for automation and guidance. For more information, see Optimizing and automating workflows through the Autonomous IT Platform on page 273.

You must Sign in to Console on page 49 to perform the preceding tasks. After you sign in, Console components such as the Header on page 55 and Main menu on page 59 remain visible regardless of which solution workbench you subsequently open. Within the Main menu, Console also includes all pages in the **Administration** submenu, which you use to manage your Tanium environment. For more information, see Console components and navigation on page 54.

Console header



Console Main menu



You can customize Console to suit your specific environment. For more information, see Part 5: Customizing Console and Interact on page 147.

© 2026 Tanium Inc. All Rights Reserved

Tanium Interact

Tanium Interact is a module that you use to issue Questions on page 44 to managed endpoints and analyze their results (answers). You can then select results to deploy Actions on page 45 to the endpoints.

For example, if you issue the question `Get Computer Name and Uptime from all entities with Uptime > 60 days`, the Interact **Question Results** page lists all the endpoints that have been running for more than 60 days after they last rebooted. You can then select specific endpoints and deploy an action with the **Reboot Windows Machine** package to those endpoints.

You can also use question results to start a playbook in Tanium™ Automate or access comprehensive information about a single endpoint in Tanium™ Reporting.

For more information, see:

- Part 6: Exploring and accessing endpoints in Console and Interact on page 231
- Part 7: Analyzing question results in Console and Interact on page 255
- Tanium Automate User Guide
- Tanium Reporting User Guide: Working with a single endpoint

Tanium Data Service

Tanium Data Service (TDS) is a shared service that periodically collects and caches sensor results from endpoints. The cache enables Tanium Console, Tanium Interact, and other Tanium solutions to respond quickly to questions about endpoint status, configuration, or activity, even for endpoints that are currently offline. Many sensors are automatically registered with TDS for collection. You can also manually register additional sensors to support workflows and content (such as dashboards) that depend on the data.

For example, Interact users can issue a question to view cached data about the hardware specifications of offline endpoints. As another example, Tanium Reporting dashboards can quickly load both real-time data and historical cached data for charts that show trends related to common vulnerabilities and exposures (CVEs).

TDS does not have a dedicated workbench. You register sensors and customize TDS settings through the Interact workbench. For more information, see Tanium Interact User Guide: Managing Tanium Data Service (TDS).

Tanium Core Platform

The Tanium Core Platform is the infrastructure that provides backend services for all the features and data that you access through Tanium Console and other Tanium solutions. The platform also includes:

- Platform servers, which include Tanium Servers, Tanium Module Servers, Tanium Zone Servers, and Tanium Zone Server Hubs.
- Tanium solutions that are included by default in the Tanium license, such as Tanium Console and Tanium™ Client Management. The Tanium Core Plaform does not include solutions that require separate licenses, such as Tanium™ Patch.
- Tanium Clients.

© 2026 Tanium Inc. All Rights Reserved

If you are responsible for maintaining the health and operational efficiency of the Tanium Core Platform, you can use Console to configure settings that affect the behavior of various platform components. For example, you can configure bandwidth throttles for the data that platform servers send to Tanium Clients to ensure that data bottlenecks do not interfere with the operations of Tanium users. For more information, see Configuring the Tanium Core Platform on page 161.

For more information about the components and setup of the Tanium Core Platform, see:

- Tanium Appliance Deployment Guide
- Tanium Core Platform User Guide for Windows Deployments
- Tanium Client Management User Guide

Tanium solutions

Tanium solutions include modules (such as Tanium Deploy), shared services (such as Tanium Client Management), and content-only solutions (such as Default Content). Each module and shared service comprises a *workbench* and content. A workbench is the user interface that you use to perform module operations. Users use the workbenches and content to perform their Tanium workflows, such as managing, monitoring, and protecting the endpoints in your environment.

For example, the workbench of the Tanium Comply module includes an **Assessments** page for monitoring the status of assessments, which evaluate endpoints for security configuration exposures and software vulnerabilities. In terms of content, the module includes **Comply - Run Assessment** packages for running the assessments.

For more information, see Part 4: Managing Tanium solutions on page 108.

Endpoints

An *endpoint* is a computing device or node through which data can enter or exit the computer network to which the endpoint connects. Endpoints are devices such as desktops, laptops, servers, virtual machines, or containers. A *managed endpoint* is a device that Tanium users and Tanium solutions can query and manage through a Tanium Client. For example, the Client returns answers to questions that you issue through Interact. The Client runs on the endpoint and registers with the Tanium Server to receive configuration information, tools, and updates from Tanium solutions.

You assign a set of endpoints to a *computer group* to manage as a unit with respect to operations that Tanium users, modules, and shared services perform. For example, you can define a computer group that includes all endpoints that are in a data center, and assign the group only to users who issue questions and deploy actions to data center endpoints. For more information, see Controlling endpoint management rights through computer groups on page 610.

Questions

A Tanium *question* is a query that you issue through Tanium solutions to managed endpoints. Tanium Clients running on the endpoints process the question and return answers that you can view on the **Question Results** page. Questions enable you to explore endpoints in the course of various Tanium operations for managing, monitoring, and protecting your environment.

For example, you can issue the question `Get Computer Name and Last Logged In User from all machines with Last Logged In User contains <user name>` to determine which endpoints a particular user is accessing.

© 2026 Tanium Inc. All Rights Reserved

A *dynamic question* is one that you create from scratch and issue through the Interact features **Ask a Question** and **Question Builder**. For more information, see Issue a free-form question on page 241 and Issue a question through the Question Builder on page 245.

A *saved question* is a configuration object that enables you to reissue a question without recreating it. For more information, see Saved questions overview on page 455.

For more information, see Part 6: Exploring and accessing endpoints in Console and Interact on page 231.

Actions

A Tanium action is a configuration object that you deploy to endpoints to manage a change on those endpoints. In the action configuration, you specify the package that performs the change, endpoint targeting criteria such as an action group, and deployment conditions such as scheduling. You can schedule the action to run immediately or in the future and as a one-time deployment or at recurring intervals. An *adaptive action* deploys in progressive phases called rings that you define in a deployment plan. A *simple action* deploys to all targeted endpoints in one phase.

For more information, see Actions overview on page 320.

Content

In a Tanium deployment, *content* refers to configuration objects such as sensors, packages, saved questions, dashboards, filter groups, and scheduled actions. You use content in various operations for managing, monitoring, and protecting your environment. For example, you can use the **Running Applications** saved question to determine which applications are running on endpoints and use the **All Windows** filter group to show results only from Windows endpoints. You might then deploy an action that runs the **Kill Application** package to stop a specific application on those endpoints.

Tanium provides predefined content through solutions that you manually import or that the Tanium Server imports automatically. For example, Tanium Comply provides predefined reports for vulnerability findings. For more information, see Part 4: Managing Tanium solutions on page 108.

You can create custom content to extend Tanium solutions for particular environments or objectives. For example, if users start using a new application in your environment, a content developer can write a sensor script that maintains data about the application and write a package script that starts or stops the application.

For more information, see Solution content overview on page 418.

RBAC

Role-based access control (RBAC) enables you to configure granular permissions that control what individual Tanium users can see and do with Tanium solutions, and which endpoints those users can monitor and manage. For example, you can configure RBAC that allows all data center users to issue questions to data center servers but allows only administrators to deploy actions to those servers.

In the Tanium implementation of RBAC, permissions derive from roles and computer groups that are assigned to user accounts, personas, and user groups. Content such as sensors, packages, and saved questions are assigned to content sets, for which permissions control user access. For example, if your organization allows only data center administrators to reboot data center

© 2026 Tanium Inc. All Rights Reserved

servers, you can create a role that includes **Package read** permission on the **Core Content** content set, which contains the packages for rebooting endpoints. You would also create a computer group that includes the servers, and then assign the role and computer group to the administrators.

For more information, see RBAC overview on page 544.

Tanium Autonomous IT Platform in Console and Interact

Tanium Autonomous IT Platform comprises a set of interrelated features across multiple Tanium solutions. The Autonomous IT Platform proactively collects intelligence about conditions in Tanium environments, provides guidance based on those conditions, and enables automated workflows to address issues. For more information about the Autonomous IT Platform features that Console and Interact provide, see Optimizing and automating workflows through the Autonomous IT Platform on page 273.

Supported languages

You can select a language for user interface (UI) text in the Tanium Console and Tanium documentation. The selected language for Console also sets the date and time format. Your selection applies only to your view of Console and the documentation, and does not change the selections of other users.

For more information about language support, which types of text are translated, and the steps to select a language, see Reference: Language support on page 761.

© 2026 Tanium Inc. All Rights Reserved

Part 2: Getting started with Console and Interact

Set up Console and Interact

Perform the following tasks in Tanium Console during the initial setup of the Tanium Core Platform.

NOTE

To view these tasks in the context of setting up the entire platform, see the workflow for your Tanium infrastructure:

- Tanium Appliance Deployment Workflow
- Tanium Deployment Workflow for Windows infrastructure

1. Review the system, network, security, and user role requirements for Console, Interact, and Tanium Data Service (TDS). For more information, see Part 3: Tanium Console and Interact requirements on page 73.
2. Sign in to Console to start the import of initial content. For more information, see Sign in to Console on page 49 and Initial content on page 48.
3. (Optional) Configure Tanium Core Platform settings such as Tanium Client subnets and bandwidth throttles. For more information, see Configuring the Tanium Core Platform on page 161.
4. (Best practice) Reconfigure the predefined action groups for the deployment of endpoint tools that initial content provides. For more information, see Tanium Endpoint Configuration User Guide: View and manage content-only solutions.
5. Import the Tanium modules (including Interact), shared services, and content-only solutions that you will use. For more information, see Part 4: Managing Tanium solutions on page 108.
6. Set up role-based access control (RBAC) to determine what users can see and do with the Tanium Core Platform. This involves configuring users, user groups, user roles, personas, computer groups, and content set permissions. For more information, see RBAC overview on page 544.
7. (Optional) Create custom content (such as packages and saved questions) to complement the Tanium-defined content that you import through Tanium modules, shared services, and content-only solutions. For more information, see Solution content overview on page 418.
8. (Optional) Customize Console and Interact. For example, you can customize the border color and logo in the Console header, select a language for solution workbenches, and reorganize the Interact **Overview** page. For more information, see Part 5: Customizing Console and Interact on page 147.
9. (Optional) Register sensors with TDS for automatic collection of results. When you issue questions with those sensors, you can view cached results for endpoints that are offline. Certain sensors are registered by default. For more information, see Tanium Interact User Guide: Managing Tanium Data Service.

© 2026 Tanium Inc. All Rights Reserved

Initial content

The Tanium Server installation process automatically creates or imports predefined content that enables you to start performing many operations in Tanium Console and Interact without creating custom content or manually importing solutions. The following sections describe the initial content and how you use it.

Action groups and computer groups

The Tanium Server installation process automatically creates the following predefined action groups and their associated computer groups to enable action deployment and Tanium tools deployment:

Predefined action groups and computer groups in initial content

Action Group	Description and computer group assignment
Default - All Computers	This is the default action group selection when you deploy a custom action. It targets the **All Computers** computer group. Therefore, actions that are assigned the **Default - All Computers** action group deploy to all the endpoints managed using Tanium Client in your organization.
Default	This action group targets only the **No Computers** computer group. Therefore, actions that are assigned the **Default** action group do not deploy to endpoints. **Default** is the default action group for scheduled actions that you import with Tanium solutions, except the actions that Tanium™ Endpoint Configuration uses to deploy tools. **Default** is also the default action group for scheduled actions that you import from another Tanium Server.
Tanium Default Content Tanium Default Content - 7Zip Tanium Default Content - Optional Tanium Core Content	Tanium Endpoint Configuration creates these action groups for deploying tools that Tanium content-only solutions provide. Initially, the tools do not deploy to endpoints because the action groups target the **No Computers** computer group.  BEST PRACTICE As part of initial setup for Tanium Console and Interact, reconfigure the **Tanium Default Content** and **Tanium Core Content** action groups to target **All Computers** for tools deployment. Reconfiguring the **Tanium Default Content - 7Zip** and **Tanium Default Content - Optional** action groups is necessary only if you require the associated tools. For more information, see Tanium Endpoint Configuration User Guide: Configure action groups for content-only solutions.

Content-only solutions

Content-only solutions provide content such as sensors but do not have a workbench or service. After the Tanium Server is installed, it automatically imports the content-only solutions Default Content and Default Computer Groups when the first user signs in to Tanium Console. Console shows a pop-up window that shows the import progress.

If you perform the **Tanium Recommended Installation** (see Import all modules and services on page 123), the Tanium Server automatically imports several more content-only solutions, but you must manually import others.

When you import Interact, the Tanium Server automatically imports the content-only solution Core Content because it is a dependency for that module.

The following initial content-only solutions provide basic Interact functionality.

© 2026 Tanium Inc. All Rights Reserved

NOTE For more information about content-only solutions, see Content-only solutions on page 120.

DEFAULT CONTENT AND CORE CONTENT

The Tanium Default Content and Core Content solutions provide sensors and saved questions for collecting basic inventory and state information from endpoints. TDS periodically issues questions that contain many of these sensors (such as **Computer ID**) to all endpoints to update its cache of sensor results. For more information, see Tanium Interact User Guide: Managing sensor results collection through TDS.

The Default Content and Core Content solutions also provide the following tools:

- **Default Content**: Contains utilities necessary for all Tanium-provided sensors and packages in the **Base** and **Client Management** content sets.
- **Default Content - 7Zip**: Contains optional utilities for custom content that uses the 7zip file archiver.
- **Default Content - Optional**: Contains optional utilities for custom content that uses the following processes: TPowerShell, runasuser, run-allusers-wrappers, unzip-and-run, or copy-to-tanium-dir-predist.
- **Core Content**: Contains utilities that are required for all Tanium-provided sensors and packages in the **Core Content** content set.

Endpoint Configuration manages tool deployment for these content-only solutions. For more information, see Tanium Endpoint Configuration User Guide: View and manage content-only solutions.

DEFAULT COMPUTER GROUPS

This solution provides computer groups that you can use to target endpoints based on operating system (OS) or platform type (such as physical or virtual). For more information, see Default computer groups on page 615.

Sign in to Console

You access Tanium Console through a supported web browser. For more information, see Web browsers on page 73. The steps to access Tanium Console depend on where you sign in:

- Sign in through the Tanium Server on page 50
- Sign in through a SAML IdP portal on page 52

For information about the Console page that opens after you sign in and about the content that the Tanium Server imports for the first user session, see Initial Console page and content imports on page 52.

For information about the validity period for your Console session after you sign in, see Session validity and timeouts on page 53.

TIP If you cannot access Console, see Troubleshoot Console access on page 702.

© 2026 Tanium Inc. All Rights Reserved

Sign in through the Tanium Server

AUTHENTICATION TYPES

The type of authentication that is configured for your user account determines the sign-in prompt that you see:

- **SAML authentication**

  If the Tanium Server functions as a Security Assertion Markup Language (SAML) service provider (SP) and your account on the Server matches an account on the SAML Identity Provider (IdP), Console provides single sign-on (SSO) authentication. SSO enables a user to start new Console sessions repeatedly without re-authenticating, until the IdP session times out. For more information, see SP-initiated SSO on page 685.

  The IdP session timeout is configured on the IdP server. Consult your IdP administrator for more information.

- **LDAP or local authentication**

  If the Tanium Server authenticates your account through local authentication or Lightweight Directory Access Protocol (LDAP) authentication instead of SAML SSO, you sign in for each session with a user name and password. For more information, see User authentication on page 626 and Importing and authenticating users through LDAP on page 666.

SIGN IN

Perform the following steps to sign in through the Tanium Server.



If you are starting the first user session after Tanium Server installation, you can use the default user account to sign in. For more information, see Default user on page 627.

1. Open a web browser and go to the Tanium Server URL.

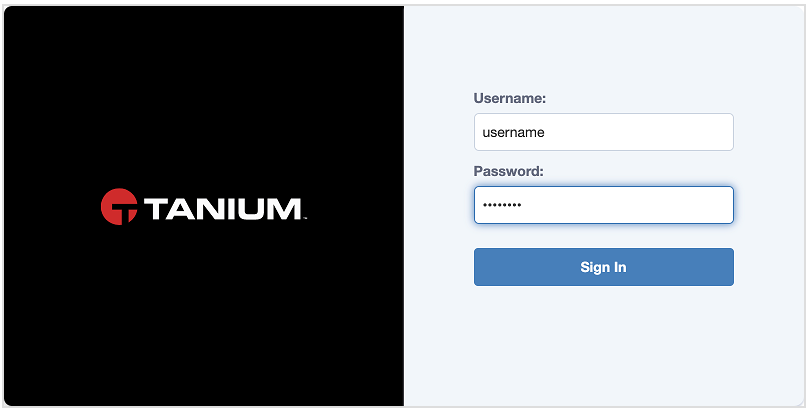
   The URL has the format: `https://<FQDN or IP address>[:<port>]`. If the Tanium Server uses the default port (443), you do not need to specify the port.

   If a pre-login banner is configured, read the banner text and click **I Agree**. For more information, see Configure a pre-login banner on page 147.

   If you are using LDAP or local authentication and SAML SSO is not configured for any user, the sign-in page shows only the **Username** and **Password** fields.

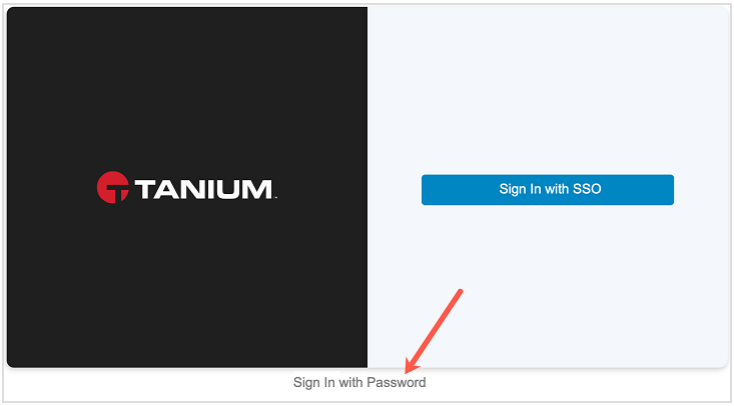
© 2026 Tanium Inc. All Rights Reserved

Sign in page for user credentials



If the Tanium Server is configured to authenticate some users through SAML SSO, the sign-in page shows a **Sign In with SSO** button and a **Sign In with Password** link below it.

Sign in page for SSO



2. (SSO authentication only) Sign in through SAML SSO:
   a. Click **Sign In with SSO**.
   b. If you never signed in to the IdP or your IdP session has timed out, sign in to the IdP with your username and password. If you previously signed in to the IdP and your IdP session is active, you do not need to enter credentials.
3. (LDAP or local authentication only) Enter your **Username** and **Password**. If the sign-in page does not display these fields, click **Sign In with Password** and then enter your credentials.

TIP

By default, the Tanium Server applies the permissions of your default persona when you sign in. If your account has multiple personas and you want to switch to an alternative persona, see Select a persona for your Console session on page 663.

© 2026 Tanium Inc. All Rights Reserved

Sign in through a SAML IdP portal

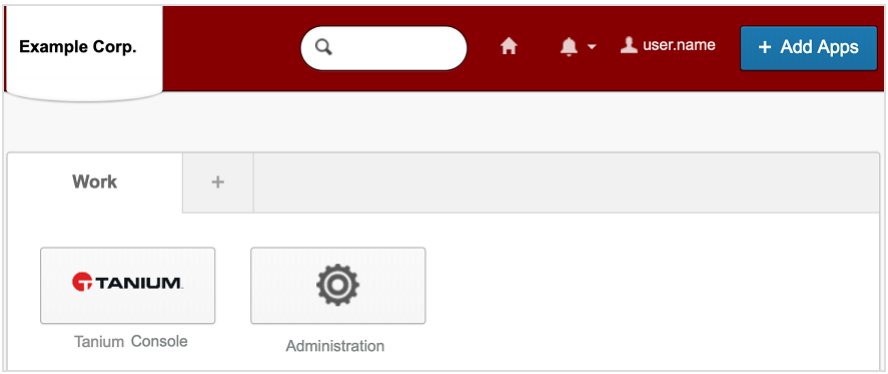
If the Tanium Server integrates with the IdP portal that your organization uses for accessing applications, the portal provides SSO access to Console. For more information, see IdP-initiated SSO on page 684.

NOTE

If you are starting the first user session after Tanium Server installation, you can use the default user account to sign in. For more information, see Default user on page 627.

1. Go to the IdP SSO portal.
2. If you never signed in to the IdP or your IdP session has timed out, sign in to the IdP using your user name and password. If you previously signed in to the IdP and your IdP session is active, you do not need to enter credentials.
   The IdP portal displays a tile for each application that you can access.

   IdP SSO portal



3. Click the **Tanium Console** tile.
   The IdP redirects you to the Tanium Server and Tanium Console opens in your browser. If a pre-login banner is configured, you must read the banner text and click **I Agree** before Console can open. For more information, see Configure a pre-login banner on page 147,

TIP

By default, the Tanium Server applies the permissions of your default persona when you sign in. If your account has multiple personas and you want to switch to an alternative persona, see Select a persona for your Console session on page 663.

Initial Console page and content imports

When you sign in to start the first user session after Tanium Server installation, Tanium Console opens a pop-up window that shows the progress of initial content imports. After the imports, Console opens the **Solutions** page, which you use to import Tanium solutions.

© 2026 Tanium Inc. All Rights Reserved

For user sessions after the first session, Console shows the Tanium **Home** page by default: `https://<Tanium Server>/#/home`.

If your browser URL field specified another Console page (such as `https://<Tanium Server>/#/actions/scheduled/`) when the browser timed out or you signed out, that page opens when you next sign in through the same browser.

For more information, see:

- Initial content on page 48
- Part 4: Managing Tanium solutions on page 108
- Tanium Home page on page 62

Sign out of Console

To end your Tanium Console user session, go to the Console header, hover over , and select **Sign Out**.

If you are accessing Console in multiple browser tabs, Console automatically ends your session on all the tabs when you sign out from any single tab. To access Console again, you must sign in to start a new session.

If the Tanium Server is configured to integrate with a SAML IdP, your IdP session can remain active even after you sign out of Console. As long as your IdP session remains active, you can access Console again without re-authenticating. For more information, see Session validity and timeouts on page 53.



Sign out of Console before closing the browser that you use to access it.

Session validity and timeouts

After you sign in to Tanium Console, the system that you use to access Console sends the Tanium Server a heartbeat message periodically (every 2.5 minutes by default) as long as you keep the browser open. The heartbeat ensures that your user session persists (remains valid) until one of the following events occur:

- **Missed heartbeat**: The Tanium Server does not receive a heartbeat after the configured interval (default is 5 minutes). Events such as a network connectivity issue might interrupt the heartbeat.

  The **session_expiration_seconds** platform setting controls how long the Tanium Server waits for a heartbeat before ending the session (default is 5 minutes). The heartbeat frequency is half the value of that setting. To edit the setting, see Edit advanced settings on page 165.

- **Sign out**: You manually sign out, as described in Sign out of Console on page 53.
- **Browser closure**: You close the browser that you used to sign in.
- **Inactivity timeout**: The inactivity timeout expires. The default is 10 minutes but you can change the timeout. For more information, see Suspend console automatically if no activity detected for on page 156.

© 2026 Tanium Inc. All Rights Reserved

NOTE

The browser that you use to access Console might display the **401 Unauthorized** error when a session expires.

If the Tanium Server is configured to integrate with a SAML IdP, your IdP session can remain active after any of these events. As long as your IdP session remains active, you can access Console again through SSO without re-authenticating. The IdP session timeout is configured on the IdP server. Consult your IdP administrator for more information.

Console components and navigation

Tanium Console provides the following components for accessing all solution workbenches and features, including the Console **Administration** pages. These components are always available, regardless of which page is currently open. The figure Tanium Console components and navigation on page 54 shows the location of each component.

1 Header on page 55

2 Breadcrumbs on page 58

3 Display pane on page 58

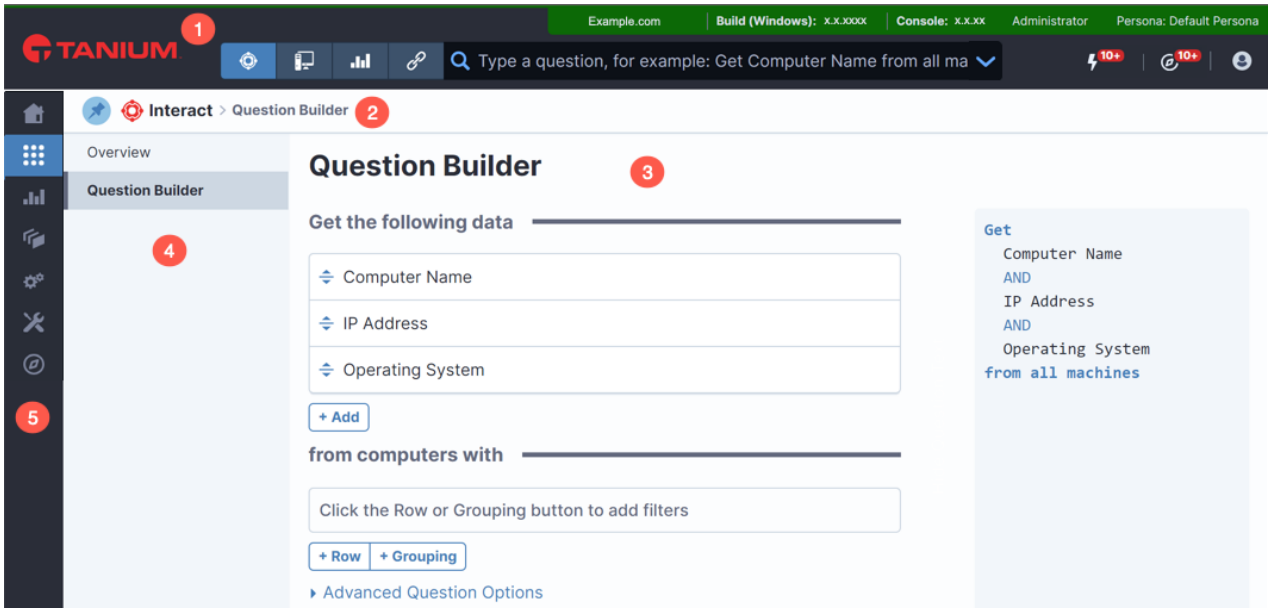
4 Solution menu on page 58

5 Main menu on page 59

TIP

You can use Keyboard navigation on page 61 instead of a mouse to access Console pages and select options.

Tanium Console components and navigation



© 2026 Tanium Inc. All Rights Reserved

Header

The Tanium Console header provides quick access to frequently used features and (optionally) shows basic information about the Tanium environment and current session. The header contains the following elements:

- Logo on page 55
- Quick Search bar on page 55
- Environment details on page 56
- Guardian notifications on page 57
- Guide notifications on page 57
- Help on page 57
- User and persona options on page 57
- Warning indicator on page 57

LOGO

In the Console header, click the logo to return to the Tanium Home page on page 62 from any other Console page. To change the logo image, see Customize the Console logo on page 154.



QUICK SEARCH BAR

In the Console header, click the icon for the feature that you want to access:

- **Issue questions**

  Issue a dynamic question to endpoints as you would in the Interact **Ask a Question** field. For more information, see Issue a free-form question on page 241.

- **Search or access endpoints**

  Use this field to immediately show basic information about a single endpoint without issuing a question. This field also provides the following features:

  - **Endpoint Details**: Clicking a **Computer Name** opens the Endpoint Details page in Tanium Reporting, where you can view comprehensive information about a single endpoint and perform management tasks on it, such as stopping processes. For more information, see Search endpoints on page 249.
  - **Jump Gate**: In the **Access Endpoint** column, click Create Jump to access a PowerShell session on a Windows endpoint or a Bash session on a macOS or Linux endpoint. For more information, see Jump to endpoints on page 250.

- **Reports and dashboards**

  To open a report or dashboard in the Tanium Reporting workbench, enter all or part of the report or dashboard name or description and then select the correct match in the dropdown list.

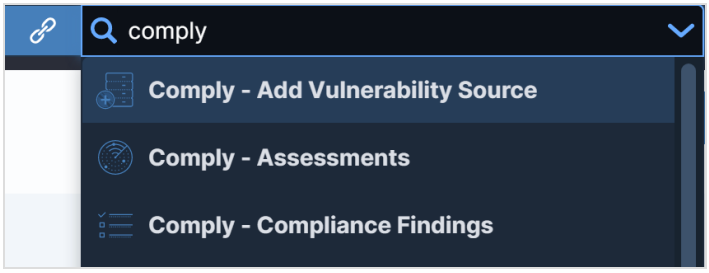
© 2026 Tanium Inc. All Rights Reserved

NOTE

Reporting dashboards differ from Interact dashboards. For more information, see Tanium Reporting User Guide: Dashboards and Interact dashboards and categories on page 457.

- **Quick links**

  To open any page or dialog in Tanium Console or a solution workbench, enter a text string to populate the dropdown list with matching *quick links* and then select one. For example, after you enter `comply`, you can select a quick link to open a Tanium™ Comply page.



  If you do not know the exact string to match with a quick link, try entering related keywords. For example, the keyword `BitLocker` might be associated with a BitLocker policy in Tanium™ Enforce.

NOTE

The quick links field appears only if all your licensed Tanium solutions support the feature. For more information, see Console solution dependencies on page 73.

You can select whether the results of the Quick Search bar open in a new browser tab (default) or in the current tab. For more information, see Open Search Bar Results in New Tab on page 157.

ENVIRONMENT DETAILS

The Console header contains the following environmental and session information.

- **Custom text**: Add custom text (**Example.com** in the preceding example) to help users identify the environment that they are using. For more information, see Configure Console header text on page 152.
- **Platform version**: Indicates the type of Tanium Core Platform infrastructure (Windows or Appliance) and platform version.
- **Console version**: Indicates the Console version.
- **User**: Indicates the user name of the account that you used to sign in to Console.
- **Persona**: Indicates the persona that you selected for the current session.



© 2026 Tanium Inc. All Rights Reserved

TIP

You can customize the background color of the header for all Console users. Individual users can remove the information from their own view of Console. For more information, see Select the Console color on page 151 and Configure Console user preferences on page 155.

GUARDIAN NOTIFICATIONS

In the Console header, click the Guardian icon to open a slide-out panel to view critical emerging issues from Tanium Guardian. A red number appears beside the icon if new (unread) Guardian notifications exist. If the number of notifications exceeds 10, the icon shows `10+`. Feed 1.6.84 or later and Console 3.6.69 or later are required to see Guardian notifications. For more information, see Tanium Guide User Guide.

GUIDE NOTIFICATIONS

In the Console header, click the Guide icon to open a slide-out panel that shows product announcements and other notifications from Tanium™ Guide. A red number appears beside the icon if new (unread) notifications exist. If the number of notifications exceeds 10, the icon shows `10+`. For more information, see Tanium Guide User Guide.

HELP

In the Console header, click the Help icon to open the Tanium documentation portal, where you can access the user guides. If you add the URL for a custom help system, the Help menu provides options for both Tanium documentation and custom help. For more information, see Add a help URL on page 153.

USER AND PERSONA OPTIONS

In the Console header, hover over the user icon to open a menu that contains the following information and options:

- **User**: The user name of the account that you used to sign in to Console.
- **Persona:** ***<current persona>***: The menu shows the current persona only if you signed in to Console with a user account that has alternative personas assigned. Click the item to select another persona as described under Select a persona for your Console session on page 663.
- **Preferences**: Click to the adjust the Tanium Console inactivity timeout, color scheme, and aspects of question results behavior for the account that you used to sign in. For more information, see Configure Console user preferences on page 155.
- **Local Error Log**: Click to view or copy details about the last 100 errors that were returned to Console in response to actions taken with the browser. For more information, see Work with the Console error log on page 705.
- **Sign Out**: Click to end your current Console sign-in session. For more information, see Sign out of Console on page 53.
- **Last Sign In**: The date and time when you last signed in to Console.

WARNING INDICATOR

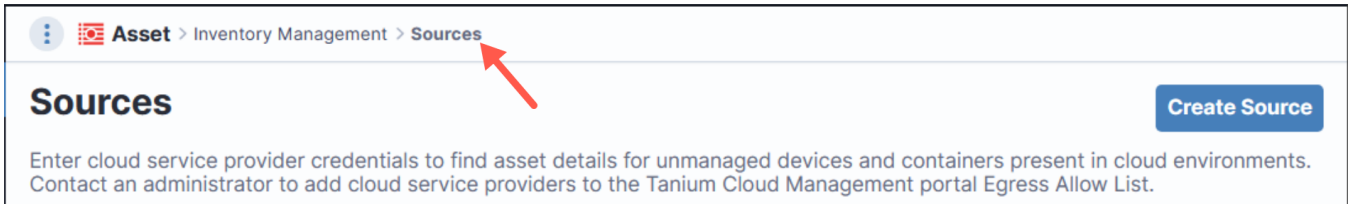
The Console header shows a Warning icon only if warning conditions exist. Console initially shows the warnings when you sign in. Click this icon to redisplay the warnings.

© 2026 Tanium Inc. All Rights Reserved

Breadcrumbs

Breadcrumbs in each page indicate your current location in Console. You can click the solution name in the breadcrumbs to open the solution **Overview** page. The following example shows the breadcrumbs for the **Sources** page in the Asset module. In this case, you can click **Asset** in the breadcrumbs to open the Asset **Overview** page.

Breadcrumbs in Console



Display pane

The Console display pane shows the main body of the current page. The display pane in the figure Tanium Console components and navigation on page 54 shows the Interact **Question Builder** page.

Solution menu

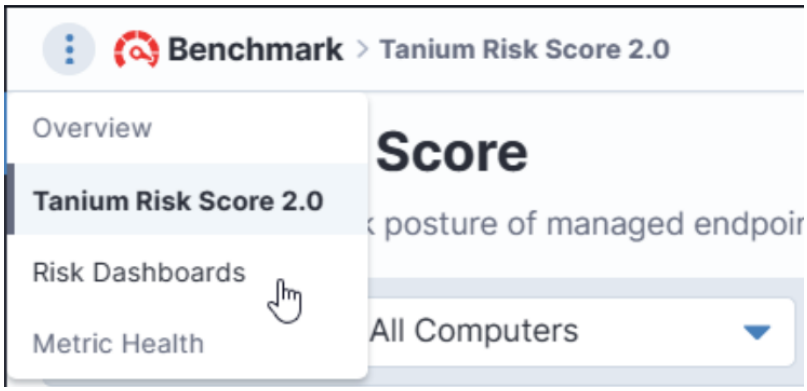
The workbench of every Tanium solution (module or shared service) provides a solution menu that you can use to navigate the workbench pages. Console **Administration** pages provide a similar menu. Console provides the following options to show the menu:

- **Expand menu**: Hover over the Options icon to expand the menu, as shown in the figure Example of a solution menu on page 58. The menu collapses when you move your cursor away from the menu.
- **Pin menu**: Click the Pinned icon to keep the menu expanded regardless of cursor movement. Click the icon again to revert to a collapsed menu.

TIP

You can also use the Modules on page 60 menu to navigate all module pages even if they are nested. You can use the **Shared Services** menu to access only the **Overview** pages of shared services.

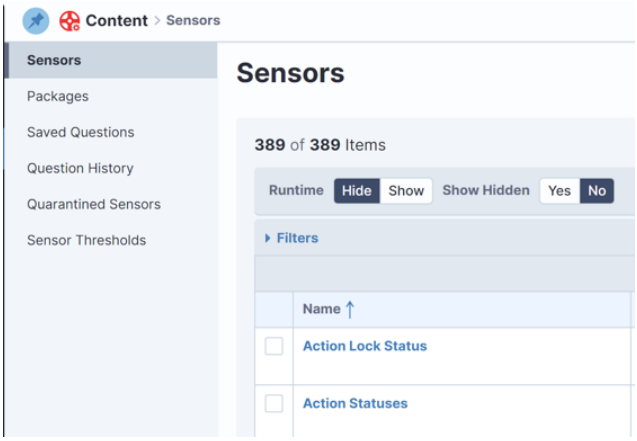
Example of a solution menu



© 2026 Tanium Inc. All Rights Reserved

In Console **Administration** pages, you can pin the submenu for each category of pages: **Actions**, **Content**, **Permissions**, or **Configuration**. The following example shows the **Content** submenu pinned.

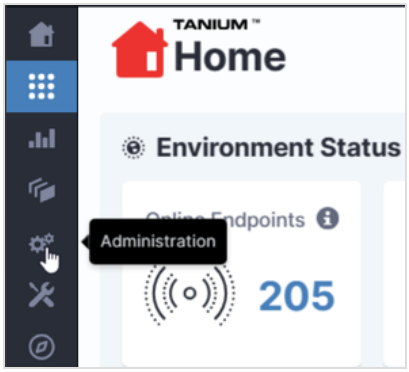
Example of a pinned submenu



Main menu

Use the Console Main menu to navigate among Tanium modules, shared services, and the pages that you use to administer the Tanium Core Platform. The Main menu shows only icons unless you hover over an icon to show its associated text label. The following example shows the hover text for the Console **Administration** menu.

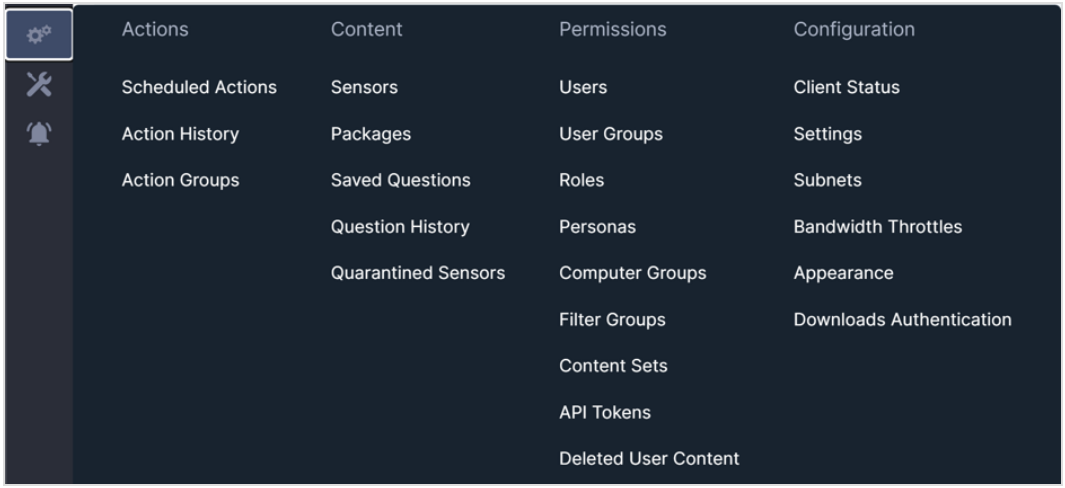
Main menu in Console



Click an icon to open its submenus.

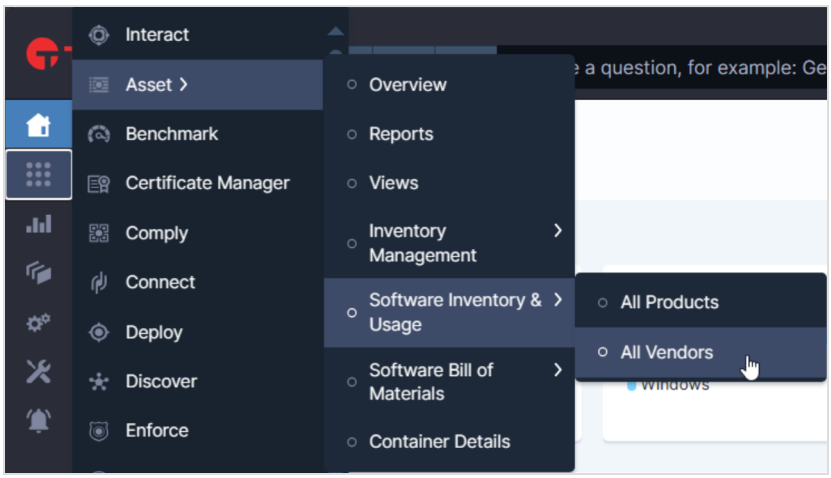
Expanded submenus in Console

© 2026 Tanium Inc. All Rights Reserved



The following table describes how you use each Main menu element to access solutions and pages.

Elements in the Console Main menu

Element	Description
Tanium Home	Click to return to the Tanium **Home** page from any other Console page.
Modules	Use this menu to navigate the pages of Tanium modules. The menu contains only the modules that are imported and that you have role permissions to access. Click a module name to open its **Overview** page. Hover over a module name to open submenus for navigating to other pages in the module: 
Data	Use this menu to navigate the Tanium™ Reporting pages for managing reports and dashboards. For more information, see Tanium Reporting User Guide.

© 2026 Tanium Inc. All Rights Reserved

Elements in the Console Main menu (continued)

Element	Description
Automate 	Use this menu to navigate the Tanium™ Automate workbench for using and managing playbooks. For more information, see Tanium Automate User Guide.
Administration 	Use this menu to navigate Console administration pages. The menu contains only the administration pages that you have role permissions to access.  NOTE If approval is required for actions that other users created and you have the **Approve Action** permission, a red number beside the menu indicates the number of actions that you can approve. For more information, see Managing action approval on page 411.
Shared Services 	Use this menu to access the workbenches of Tanium shared services. The menu contains only the shared services that you have role permissions to access.
Guide 	Click to access the Tanium Guide workbench for viewing notifications, emerging issues, product announcements, and release notes. For more information, see Tanium Guide User Guide.

Keyboard navigation

You can use the following keyboard keys to navigate Console and select options:

Keyboard navigation in Console

Keys	Navigation
Tab	Navigate to the next option on the page.
Shift + **Tab**	Navigate to the previous option on the page.
Enter	Activate a link or button. The Main menu contains a **Skip to Main Content** button that appears when you tab into the Main menu. Press the **Enter** key to skip all options in the Main menu and to navigate to the first option in the display pane.
Spacebar	• Expand or collapse a dropdown list menu or section. • Select checkboxes.

Data grid viewing options

Many Console page show grids of data. For example, the **Question Results** page shows a grid with the results of questions. The following options for customizing a grid display are common.

© 2026 Tanium Inc. All Rights Reserved

Common viewing options for Console grids

Viewing options	
Sorting 	To sort rows alphabetically or numerically based on the values in a specific column, click the column header. You can toggle between sorting in ascending ↑ or descending ↓ order. To perform a secondary sort based on another column, press the **Shift** key and click the other column header.
Refreshing 	Refresh the grid if you think its data might have changed after you opened the page.
Exporting 	Export data as a CSV file for viewing in another application.
Column visibility and order 	To change which columns the grid shows, click Customize Columns ||| in the grid toolbar and select (show) or clear (hide) the column checkboxes. You can also change the order of columns by dragging ⇕ them.
Filters 	Filter by one or more data attributes. For example, you can filter the **Questions Results** grid by a specific sensor value.
Filter by text 	Filter by an alphanumeric text string that matches one or more column values. For example, after you issue a question with the **Running Applications** sensor, you can filter the **Questions Results** grid to show only applications that have the string `Java` in their name.
Copy row information 	Select one or more rows and click Copy .
Copy cell information 	To copy the contents of a grid cell, perform one of the following steps: • Hover over the cell, click Options , and click Copy Cell Value . • Press the **Alt** key (Windows) or **Option** key (macOS) and click in the grid cell.

Tanium Home page

The Tanium **Home** page provides an overview of your environment and quick access to Tanium solutions. You can customize the **Home** page to suit your regular activities. For example, if your role is to manage OS patches on endpoints, you can add quick links to Tanium™ Patch pages, add patch-related dashboards for monitoring, and assign favorite status to patch-related reports and saved questions.

Tanium Home page

© 2026 Tanium Inc. All Rights Reserved

Tanium Home page

© 2026 Tanium Inc. All Rights Reserved

© 2026 Tanium Inc. All Rights Reserved

Your customizations to the **Home** page apply to all the personas that are assigned to your user account, but do not apply to other user accounts.

The role permissions that are assigned to your user account and personas apply as a filter to the page contents. For example, if you add a quick link to a module for which your user account has access permissions, the quick link is not visible if you switch to a persona that does not have those permissions. Similarly, the computer groups that are assigned to your user account and personas apply as a filter to the endpoints that you can explore and to the endpoint data that you can view on the **Home** page.

You can perform the following tasks on the **Home** page:

- Manage the display of Home page sections on page 65
- View environment status on page 65
- Explore endpoint data on page 66
- Work with Quick Links on page 67
- Access Tanium module workbenches on page 68
- Work with Reporting dashboards on page 68
- Work with favorite Interact categories, dashboards, and saved questions on page 71

Manage the display of Home page sections

The steps to show, hide, move, collapse , or expand sections on the Tanium **Home** page are the same as the steps in Customize solution overview pages on page 157.

View environment status

On the Tanium **Home** page, the **Environment Status** section shows charts with general metrics related to your enterprise inventory. The charts contain endpoint counts that you can click to issue questions that return details about the associated endpoints. Interact then shows the **Question Results** page in a new browser tab.

NOTE

The charts show data only from endpoints in computer groups for which you have management rights. As a result, different users might see different numbers in the same environment. Users with **Unrestricted Management Rights** will see data from all endpoints in the environment. To change management rights, see Assign computer groups on page 618.

ONLINE ENDPOINTS

On the Tanium **Home** page, the **Online Endpoints** chart shows the number of managed endpoints that have registered with the Tanium Server in the last 31 minutes. Click the number to issue the saved question: `Get Computer Name and IP Address and Operating System from all machines`. This question returns results from endpoints managed using Tanium Client that are online at the moment you click the number.

© 2026 Tanium Inc. All Rights Reserved

TOTAL ENDPOINTS

On the Tanium **Home** page, the **Total Endpoints** chart shows the total number of online and offline managed endpoints. The Tanium Server calculates the number based on multiple identifiers that TDS collects from each endpoint. Using multiple identifiers improves the accuracy of the count in environments where, for any particular endpoint, one identifier might change over time while other identifiers do not. The number includes offline endpoints only if they have registered with the Server within the retention period (default is 30 days).

Click the **Total Endpoints** number to issue the saved question: `Get Computer Name and IP Address and Operating System from all machines`. The Server collects the question results from the TDS cache for all endpoints that have registered within the retention period. To change the retention period, see Tanium Interact User Guide: Configure removal of expired results.

OPERATING PLATFORM

On the Tanium **Home** page, the **Operating Platform** chart shows the number of offline and online endpoints, grouped by OS platform. The **Other** count applies to endpoints that do not run the Windows, Linux, or macOS platform. Click the count for a platform to issue the following question:

`Get Computer Name and IP Address and Operating System from all machines with OS Platform equals <OS platform>`.

UNMANAGED NETWORK INTERFACES

On the Tanium **Home** page, the **Unmanaged Network Interfaces** chart shows the number of unmanaged network interfaces that Tanium™ Discover has found. Unmanaged interfaces are unique MAC addresses that are not currently Tanium managed. It is normal to see more interfaces than endpoints; an endpoint with multiple network interface controllers (NICs) shows as multiple interfaces. Click the number to open the **Interfaces** page in Discover. This chart appears only if Discover is installed and you have a user role with the **Discover Asset read** permission. For more information, see Tanium Discover User Guide: View interface data.

> **NOTE** After you install Discover, the **Unmanaged Network Interfaces** chart appears when Discover finds any unmanaged network interfaces. The amount of time to find unmanaged network interfaces depends on the complexity of your environment. For more information, see Tanium Discover User Guide.

Explore endpoint data

The Tanium **Home** page provides the following methods for exploring the endpoints in your environment and for accessing endpoint management features: **Ask a Question** field, **Search Endpoints** field, and **Build Question** button.

ASK A QUESTION

In the **Ask a Question** field on the Tanium **Home** page, you can enter a question in ordinary language and Interact then issues it as a syntactically valid query. The Interact **Question Results** page shows the endpoint responses in a grid. You can drill-down into the results with additional questions and perform other operations on the responding endpoints, such as deploying actions or playbooks. For more information, see Issue a free-form question on page 241.

© 2026 Tanium Inc. All Rights Reserved

TIP You can also access the question field on any Console page by clicking in the Console header.

SEARCH ENDPOINTS

Use the **Search Endpoints** field on the Tanium **Home** page to immediately show basic information about a single endpoint without issuing a question. This field also provides the following features:

- **Endpoint Details**: Clicking a **Computer Name** opens the Endpoint Details page in Tanium Reporting, where you can view comprehensive information about a single endpoint and perform management tasks on it, such as stopping processes. For more information, see Search endpoints on page 249.
- **Jump Gate**: In the **Access Endpoint** column, click Create Jump to access a PowerShell session on a Windows endpoint or a Bash session on a macOS or Linux endpoint. For more information, see Jump to endpoints on page 250.

TIP You can access the search endpoints field on any Console page by clicking the search icon in the Console header.

BUILD QUESTION

Click **Build Question** on the Tanium **Home** page to open the **Question Builder**, which provides a form to guide you through the process of constructing a question. The **Question Builder** is useful when you know the specific sensors that you want to include in a question but you need guidance for advanced sensor and question options. For more information, see Issue a question through the Question Builder on page 245.

Work with Quick Links

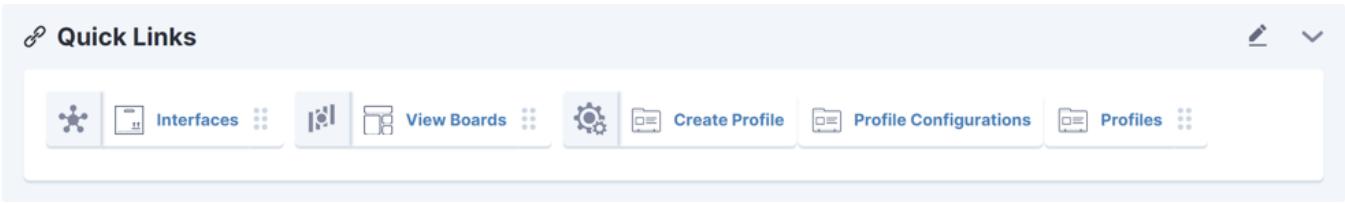
When you install Tanium solutions, the **Quick Links** section on the Tanium **Home** page automatically populates with links to pages that users typically access often in the workbenches of those solutions. You can customize the quick links for your own user account to make your most common workflows more efficient. For example, you can add a quick link for **Client Health** if you frequently open the **Client Health** page in the Tanium Client Management workbench.

By default, the **Quick Links** section is hidden. Perform the following steps to show the section and manually add or remove quick links:

© 2026 Tanium Inc. All Rights Reserved

1. Click **Customize Page**, select **Quick Links**, and click **Save**.
2. Click Edit in the **Quick Links** section.
3. Perform one of the following steps to find specific quick links:
    - In the **Filter by Quick Link** field, enter a text string that contains all or part of the quick link name if you know it. For example, enter `question` to list all the quick links that pertain to questions.
    - Select an option in the column of categories to list all the quick links for that category. For example, select **Actions** to list all the quick links that pertain to actions.
4. Select or clear checkboxes to add or remove the corresponding quick links, and then click **Save**.

Quick Links on the Tanium Home page



TIP

You can also access quick links by clicking in the Tanium Console header and entering a search string that contains all or part of the solution name or page title. For more information, see Quick Search bar on page 55.

Access Tanium module workbenches

On the Tanium **Home** page, the **Modules** section shows a tile and short description for each Tanium module that is imported and that you have permissions to access. You can open the **Overview** page of a module by clicking its tile.

Work with Reporting dashboards

On the Tanium **Home** page, the **Dashboard** and **Dashboard List** sections show Tanium Reporting dashboards, which provide visualizations (charts) of report data. You can choose which dashboards to include based on your most common workflows.

For example, if you are responsible for removing applications that end users do not use, you can add a dashboard that includes a chart showing the top 10 unused applications.

For the information and options that are specific to each section, see Dashboard section on page 69 and Dashboard List section on page 70. The following table describes the options that both sections provide.

NOTE

For more information about Reporting dashboards and reports, see Tanium Reporting User Guide: Overview.

© 2026 Tanium Inc. All Rights Reserved

NOTE

A Reporting dashboard differ from an Interact dashboard, which is a collection of related saved questions. For more information, see Interact dashboards and categories on page 457.

Tanium Home page: Options in the Dashboard and Dashboard List sections

Option	Description
Open dashboard	Click a dashboard name to view and manage that dashboard in the Reporting workbench. For more information, see Tanium Reporting User Guide: View dashboards.
View All Dashboards	Click this link to view the Reporting **Dashboards** page, which lists all the dashboards that you have permissions to access.
Open report	The data in each chart derives from a report. Click a chart name or a data point in a chart to open its associated report in a new browser tab. For more information, see Tanium Reporting User Guide: View reports.
Filter by computer group	You can filter the data in all charts or in a specific chart by computer group. For more information, see Tanium Reporting User Guide: Filter by Computer Group.
Set refresh interval 	Select an automatic refresh interval from the dropdown list or click to manually refresh the chart data. TDS collects and stores the data that reports provide for the charts. For more information, see Tanium Reporting User Guide: Data sources.

DASHBOARD SECTION

On the Tanium **Home** page, the **Dashboard** section shows a dashboard with full-sized charts. This section is useful when you want to see all the details for the charts of a single dashboard.

For information about the options that appear in both the **Dashboard** and **Dashboard List** sections, see Tanium Home page: Options in the Dashboard and Dashboard List sections on page 69. The following table shows the options that are specific to the **Dashboard** section.

NOTE

The **Dashboard** section is hidden by default. To show the section, click **Customize Page**, select **Dashboard**, and click **Save**.

Tanium Home page: Options in the Dashboard section

Option	Description
Select dashboard	To specify the dashboard that the section shows, click Edit and select the dashboard name.

© 2026 Tanium Inc. All Rights Reserved

Tanium Home page: Options in the Dashboard section (continued)

Option	Description
Filter by conditional formatting highlights or by favorites 	Click and select a filtering option: • **Default view**: The section shows all the charts in the dashboard. • **Conditional Formatting Highlights Only**: The section shows only the charts with data that matches the threshold for a certain condition. For example, a chart that shows risk scores might match the `Needs Improvement` threshold. For more information, see Tanium Reporting User Guide: Conditional Formatting. • **Favorites Only**: The section shows only the charts with favorite status. Assign or unassign favorite status to charts before selecting this option.

DASHBOARD LIST SECTION

On the Tanium **Home** page, the **Dashboard List** section shows dashboards with small (micro) charts. This section is useful when you want to view only a summary of the charts for multiple dashboards instead of viewing the full details for each chart.

For information about the options that appear in both the **Dashboard** and **Dashboard List** sections, see Tanium Home page: Options in the Dashboard and Dashboard List sections on page 69. The following table shows the options that are specific to the **Dashboard List** section.

Tanium Home page: Options in the Dashboard List section

Option	Description
Select dashboards	The section can show up to five dashboards: click Edit and select (show) or clear (hide) the checkboxes beside the dashboard names.
Filter Dashboards	Enter a text string containing all or part of the name of a dashboard or a dashboard chart to show only the dashboards that match the string.
Filter by conditional formatting highlights or favorites 	Click and select a filtering option: • **Default view**: The section shows all the charts in all the selected dashboards. • **Conditional Formatting Highlights Only**: The section shows only the dashboards that have charts with data that matches the threshold for a certain condition. Only the matching charts appear. For more information, see Tanium Reporting User Guide: Conditional Formatting. • **Favorites Only**: If a dashboard has favorite status, the section shows all its charts regardless of their favorite status. If a dashboard is not a favorite but some of its charts are, the section shows the dashboard with only those charts. If neither a dashboard nor any of its charts are favorites, the section does not show the dashboard. Assign or unassign favorite status to dashboards or charts before selecting this option.

© 2026 Tanium Inc. All Rights Reserved

Work with favorite Interact categories, dashboards, and saved questions

Interact organizes saved questions by dashboard and organizes dashboards by category. If you assign favorite status to specific categories, dashboards, and questions, the Tanium **Home** page shows them in the **Favorite Interact <*Content*>** sections. Assign favorite status based on how frequently you use specific content in your workflows.

For example, you might add favorite status to the saved question **Running Applications** if you are responsible for monitoring application usage across your environment. You can then issue that question with one click on the **Home** page instead of navigating to the Interact **Overview** page and searching its **Saved Questions** panel.

> NOTE
>
> Favorite status also determines which categories, dashboards, and questions appear on the Interact **Overview** page. For more information, see Filter by favorites on page 462.

You can perform the following tasks in the **Favorite Interact <*Content*>** sections:

- **Change favorite status**

  Toggle the Favorites icons to add or remove the favorite status of individual categories, dashboards, and questions. If the section does not show the content that you want to include in the favorites, you can add favorite status on the Interact **Overview** page instead. For more information, see Filter by favorites on page 462.

- **Issue questions or dashboards**

  Click the name of a question or dashboard to issue it. For more information, see Issue a saved question on page 466 and Issue a dashboard of saved questions on page 467.

The following table describes how to manage the contents of each section.

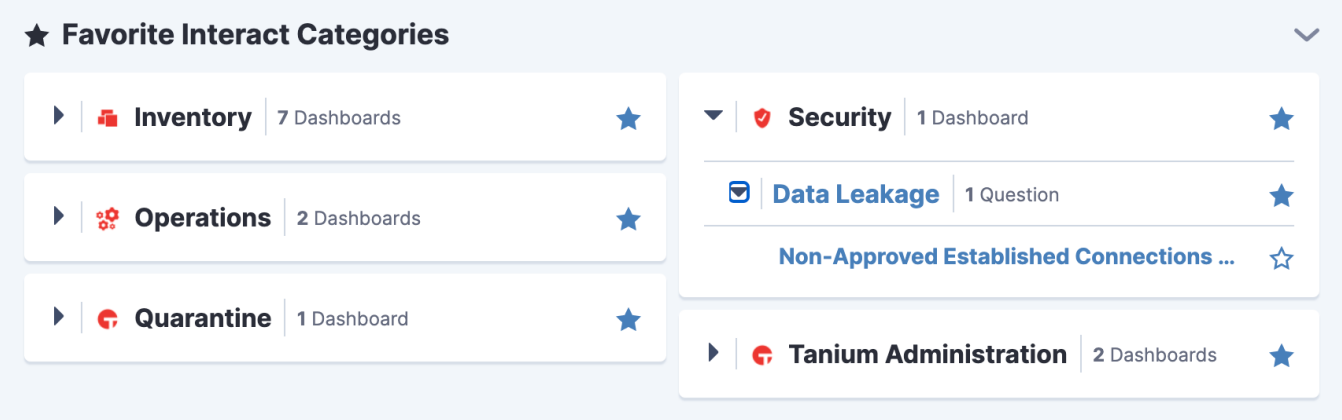
Tanium Home page: Interact favorites sections

Section	Description
Favorite Interact Categories	This section shows only favorite categories. Expand a category to list its dashboards and expand a dashboard to list its questions. The expanded lists shows both favorite and non-favorite dashboards and questions.
Favorite Interact Dashboards	This section shows only favorite dashboards but is hidden by default. To show the section, click **Customize Page**, select **Favorite Interact Dashboards**, and click **Save**. Expand a dashboard to list its favorite and non-favorite questions.
Favorite Interact Saved Questions	This section shows only favorite questions but is hidden by default. To show the section, click **Customize Page**, select **Favorite Interact Questions**, and click **Save**.

In the following example, you can click **Data Leakage** to issue all the questions in that dashboard or click **Non-Approved Established Connections** to issue that specific question. In this example, **Data Leakage** has favorite status and therefore you can Expand it to view all its questions. **Non-Approved Established Connections** does not have favorite status and therefore it does not appear in the **Favorite Interact Saved Questions** section.

© 2026 Tanium Inc. All Rights Reserved

Favorite Interact Categories



NOTE

Interact dashboards differ from Tanium Reporting dashboards. For more information, see Tanium Reporting User Guide: Dashboards.

For more information about Interact categories, dashboards, and saved questions, see Managing saved questions in Console and Interact on page 455.

Use Interact

The following are regular tasks that you perform after the initial setup of Tanium Console and Interact:

1. Issue dynamic or saved questions to view specific information about multiple endpoints in your network, or view comprehensive details about a single endpoint. For more information, see Part 6: Exploring and accessing endpoints in Console and Interact on page 231.
2. Manage saved questions. For example, you can create saved questions, assign them to dashboards, and assign the dashboards to categories. For more information, see Managing saved questions in Console and Interact on page 455.
3. Analyze and manage question results. For example, you can drill down into the question results with additional questions, filter the **Question Results** grid, and export its content. For more information, see Part 7: Analyzing question results in Console and Interact on page 255.
4. Deploy actions and playbooks. For example, you can deploy ad-hoc actions or schedule recurring actions based on question results, and configure an action approval workflow. For more information, see Deploying actions and playbooks in Console and Interact on page 391.

© 2026 Tanium Inc. All Rights Reserved

Part 3: Tanium Console and Interact requirements

The installation process for the Tanium Server automatically includes Tanium Console and you import other solutions such as Tanium Interact during initial provisioning. Therefore, review the infrastructure and security requirements for Console and Interact before deploying the Tanium Core Platform to ensure these solutions can function securely and effectively after deployment. During post-deployment provisioning, configure and assign roles to ensure that users can perform all their expected workflows.

Web browsers

Use a recent version of one of the following supported browsers to access Tanium Console:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Safari

Tanium Console is designed for a display resolution of at least 1280 pixels wide and at least 720 pixels high. Console might not appear as designed in browser windows that are smaller than these dimensions.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Tanium Console, Tanium Interact, and Tanium Data Service (TDS). For more information about how to get Console, Interact, and TDS, see Tanium Solutions & Bundles.
- Tanium™ Client: Any supported version of Tanium Client. For more information, see Tanium Client Management User Guide: Client version and host system requirements.
  If you use a Client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed Client versions.
- Tanium Core Platform servers. For more informaton, see Tanium Core Platform on page 43.

Console solution dependencies

Tanium Console supports all Tanium modules, shared services, and content-only solutions.

© 2026 Tanium Inc. All Rights Reserved

Interact and TDS solution dependencies

Other Tanium solutions are required for Interact and TDS to function (required dependencies) or for specific Interact and TDS 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.



Some Interact and TDS dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 74 and Feature-specific dependencies on page 75. Note that the links open the user guides for the latest version of each solution.

For the Tanium Core Platform and license requirements of Interact and TDS, see Core platform dependencies on page 73.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Interact and TDS, the Tanium Server automatically imports all your licensed solutions at the same time. For more information, see Import all modules and services on page 123.

Import specific solutions

If you select only Interact or TDS 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 Interact or TDS, the Server automatically updates those dependencies to the latest available versions.



You can import TDS without Interact, but you cannot import Interact without TDS.

Required dependencies

Interact and TDS both have the following required solution dependencies:

- Tanium™ Core Content
- Tanium™ Default Computer Groups
- Tanium™ Default Content



For more information about the preceding solutions, see Content-only solutions on page 48.

Interact also requires TDS and TDS has the following additional required solution dependencies:

- Tanium™ RDB Service

© 2026 Tanium Inc. All Rights Reserved

Feature-specific dependencies

If you select only Interact or TDS to import, you must manually import the following solutions:

- Tanium™ Jump Gate is required to jump to endpoints. For more information, see Jump to endpoints on page 250.
- Tanium™ Reporting is required to perform the following tasks:
  - Show Reporting dashboards on the Tanium **Home** page. For more information, see Work with Reporting dashboards on page 68.
  - Access the Endpoint Details page from the Interact workbench. For more information, see Search endpoints on page 249.

Core Platform resources

Tanium Console and Interact workbenches are installed on the Tanium Server. Tanium Data Service (TDS) installs and runs as a service on the Tanium Module Server. The resource specifications for the Tanium Server include the host computer resource and network requirements for Tanium Console, Interact, and TDS. For more information, see the guide for your deployment:

- Tanium Core Platform User Guide for Windows Deployments: Requirements
- Tanium Appliance User Guide: Requirements

Endpoints

Supported operating systems

Tanium Console, Interact, and TDS support the same operating systems (OSs) for endpoints that the Tanium Client supports:

- Windows
- MacOS
- Linux
- AIX
- Solaris

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

Disk space requirements

On endpoints managed using Tanium Client, Tanium Console, Interact, and TDS require at least 100 MB of disk space and another 100 MB of cache space for data files. The cache space includes the Tanium Client chunk cache and objects such as sensors and logs. For the disk space that endpoints require to run packages during action deployment, see Packages overview on page 442.

© 2026 Tanium Inc. All Rights Reserved

Processor requirements

On endpoints managed using Tanium Client, Tanium Console, Interact, and TDS require at least 10 MB of RAM and account for less than 0.5% of idle CPU usage.

Host and network security

Security exclusions

Security exclusions for the Tanium Core Platform apply to Tanium Console, Interact, and TDS. For more information, see:

- Tanium Clients: Tanium Client Management Guide: Reference: Endpoint security exclusions
- Tanium Core Platform servers: Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform Server security exclusions (Windows-based Tanium Core Platform deployments only)

Ports

Port requirements for the Tanium Core Platform apply to Tanium Console and Interact. For more information, see:

- Tanium Appliance User Guide: Network connectivity and firewall
- Tanium Core Platform User Guide for Windows Deployments: Ports and firewalls

For the port requirements of TDS, see Tanium Interact User Guide: Ports.

Internet URLs

Internet URL requirements for the Tanium Core Platform apply to Tanium Console, Interact, and TDS. For more information, see:

- Tanium Appliance User Guide: Internet access (direct or by proxy)
- Tanium Core Platform User Guide for Windows Deployments: Internet URLs

User role requirements

The following sections describe the permissions that enable users to perform Tanium Console and Interact workflows. The sections also list the Reserved roles on page 581 and predefined Interact roles that provide some of the permissions. Use these sections to decide which roles to assign to users and to determine if custom roles are necessary.

- Tanium Core Platform configuration permissions on page 77
- Tanium Interact and TDS permissions on page 80
- Action management permissions on page 89
- Content management permissions on page 97
- RBAC management permissions on page 102
- Troubleshooting permissions on page 106

To configure custom roles and review the descriptions of individual permissions, see Configure a custom role on page 586.

© 2026 Tanium Inc. All Rights Reserved

To assign roles, see:

- Manage user and user group assignments for a role on page 587
- Manage role assignments for a persona on page 658.

Tanium Core Platform configuration permissions

The following table summarizes the roles and administration permissions that are required to import or upgrade Tanium solutions and content, customize Tanium Console, and configure Tanium Core Platform on page 43 settings. For administration permissions that are related to troubleshooting, see Troubleshooting permissions on page 106.

User roles and permissions for configuring your Tanium environment

Tasks	Tanium Console Administration pages	Roles and permissions
Export, import, update, or uninstall Tanium solutions and content Automatic deployment of solution-specific tools	**Solutions**	**Export Content**: This permission is required to export the following content types in JSON format: • Actions • Allowed URLs • Computer management groups • Filter groups • Packages • Saved questions • Sensors Only the **Administrator** reserved role can export categories and dashboards. **Import Signed Content**: This permission is required to import digitally signed content files. **Global Settings**: Write permission is required to enable or disable the **Restricted Targeting** platform setting, which controls the default action group to which certain Tanium solutions deploy tools. For more information, see Tools deployment and restricted targeting on page 121. The **Administrator** reserved role can export, import, update, or uninstall all Tanium solutions and content.
Customize the Console appearance, help URL, and confirmation prompt	**Configuration > Appearance**	**Administrator** reserved role only

© 2026 Tanium Inc. All Rights Reserved

User roles and permissions for configuring your Tanium environment (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage allowed URLs	**Permissions > Allowed URLs**	**Allowed URLs**: • Write permission is required to create, modify, or delete the allowed URLs configurations. • Read permission is required to export the allowed URLs list in CSV format. **Export Content**: This permission is required to export allowed URLs configurations in JSON format. **Import Signed Content**: This permission is required to import allowed URL configurations. The **Administrator** reserved role has these permissions and can import allowed URLs configurations.
Manage proxy server settings	**Configuration > Proxy Settings**	**Administrator** reserved role only
Download infrastructure configuration files (TLS keys)	**Configuration > Infrastructure**	**Public Key**: Read permission is required for Tanium REST API users to download the Tanium public key (`tanium.pub`) or initialization file (`tanium-init.dat`). Only the **Administrator** reserved role can access the **Infrastructure** page to download those files through Tanium Console.
Configure Tanium Client subnets	**Configuration > Subnets**	**Isolated Subnets**: • Write permission is required to create, modify, or delete the isolated subnets configuration. • Read permission is required to view the isolated subnets configuration. **Separated Subnets**: • Write permission is required to create, modify, or delete the separated subnets configuration. • Read permission is required to view the separated subnets configuration. **Intentional Subnets**: • Write permission is required to create, modify, or delete the intentional subnets configuration. • Read permission is required to view the intentional subnets configuration. The **Administrator** reserved role has all these permissions.

© 2026 Tanium Inc. All Rights Reserved

User roles and permissions for configuring your Tanium environment (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage bandwidth throttling	**Configuration > Bandwidth Throttles**	**Global Bandwidth Throttles**: • Write permission is required to create, modify, or delete global bandwidth throttles. • Read permission is required to view the global bandwidth throttles configuration. **Subnet Bandwidth Throttles**: • Write permission is required to create, modify, or delete site (subnet-specific) bandwidth throttles. • Read permission is required to view the site bandwidth throttles configurations. **Metrics read** permission is required to view the **Monitor Usage** tab on the **Bandwidth Throttles** page. For the tab charts, **Global Bandwidth Throttles read** permission is required to view global bandwidth usage and **Subnet Bandwidth Throttles read** permission is required to view site bandwidth usage. The **Administrator** reserved role has all these permissions.
Manage Tanium licenses	**Configuration > Tanium License**	**Administrator** reserved role only
Manage Tanium keys	**Configuration > Key & Trust Management > Current Server** **Configuration > Key & Trust Management > Activity Log**	**Administrator** reserved role only
Manage certificates for Console and API access	**Configuration > SSL Certificates**	**Https Certificates**: Read permission is required to access the **SSL Certificate** page, which displays information about the current certificate and certificate signing request (CSR). Only the **Administrator** reserved role can generate CSRs and upload new certificates.

© 2026 Tanium Inc. All Rights Reserved

User roles and permissions for configuring your Tanium environment (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage trust approval and revocation among Tanium Core Platform servers	**Configuration > Key & Trust Management > Trusted Servers** **Configuration > Key & Trust Management > Activity Log** **Configuration > Zone Servers**	**Administrator** reserved role only
Configure server logging levels	**Configuration > Logging**	**Administrator** reserved role only
Configure platform settings	**Configuration > Settings**	**Global Settings**: • Read permission is required to view platform settings for Tanium Core Platform servers and Tanium Clients. • Write permission is required to create, modify, or delete platform settings. The **Administrator** reserved role has this permission.

Tanium Interact and TDS permissions

Interact users require both Interact and TDS permissions to perform Interact activities. The following sections list the permissions and the predefined roles that provide those permissions.

- Interact permissions on page 81
- Tanium Data Service (TDS) permissions on page 85



Interact users who deploy adaptive actions require additional permissions to assign deployment plans. For more information, see Manage deployment plans on page 91.

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

© 2026 Tanium Inc. All Rights Reserved

- RBAC overview on page 544 (provides an overview of roles, permissions, and content sets)
- Provided role permissions on page 576
- View effective role permissions on page 588
- Configure a custom role on page 586

INTERACT PERMISSIONS

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

- Interact solution permissions on page 81
- Interact administration and platform content permissions on page 82: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Tanium Interact User Guide: Set up Interact users.

The table Required permissions to perform Interact tasks on page 83 summarizes the permissions required to perform specific tasks in Interact.

Interact solution permissions

Permission	Interact Power User	Interact Basic User	Interact Read-Only User	Interact Show
Ask Dynamic Questions Issue questions through the Interact **Ask a Question** field and **Question Builder**.	✓ SPECIAL	✓ SPECIAL	✗	✗
Interact View the Interact workbench.	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW
Interact Execute Deploy actions in Interact.	✓ ACTION	✗	✗	✗
Interact Module View and manage Interact content.	✓ READ WRITE	✓ READ WRITE	✓ READ	✗

The permissions for the preceding roles provide solution permissions for other solutions. To view the provided permissions, see View effective role permissions on page 588.

© 2026 Tanium Inc. All Rights Reserved

Interact administration and platform content permissions

Permission	Permission Type	Interact Power User	Interact Basic User	Interact Read-Only User	Interact Show
Action Group	Administration	✓ READ	✓ READ	✗	✗
Action	Platform Content	✓ READ WRITE	✗	✗	✗
Dashboard[1]	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Dashboard Group[2]	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Filter Group	Platform Content	✓ READ	✓ READ	✓ READ	✗
Own Action	Platform Content	✓ READ	✗	✗	✗
Package	Platform Content	✓ READ	✗	✗	✗
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Sensor	Platform Content	✓ READ	✓ READ	✓ READ	✗

To view the content sets to which the platform content permissions apply, see View effective role permissions on page 588.

[1] The **Dashboard read** and **write** permissions apply to Interact dashboards, not Reporting dashboards.

[2] The **Dashboard Group read** and **write** permissions apply to Interact categories, not Reporting dashboards.

The following table summarizes the permissions required to perform specific tasks in Interact. Interact includes the Interact **Overview** page and **Question Builder** page. The **Administrator** reserved role has all the listed permissions. The table also indicates whether other reserved roles have permissions for the features.

© 2026 Tanium Inc. All Rights Reserved

Required permissions to perform Interact tasks

Tasks	Roles and permissions
Install or uninstall Interact	**Administrator** reserved role only
All tasks in Interact	**Interact show** (module) permission is required for all Interact features, so be sure to assign a role with that permission to all Interact users.
View Interact content	**Interact Module read** (module) permission is required to view content in the Interact content set.
Manage Interact content	**Interact Module write** (module) permission is required to add, edit, or delete content in the Interact content set.
Issue questions through the **Ask a Question** field and **Question Builder**	**Ask Dynamic Questions** (module) permission is required to issue questions through the **Ask a Question** field and **Question Builder**. You can assign the permission to any custom role. **Sensor read** content set permissions determine which sensors are available for you to select for questions. **Filter Group read** content set permissions determine which computer filter groups are available for you to view and select for questions and question results. Depending on whether Tanium™ Reporting, Tanium™ Asset, or both are installed, you require additional permissions to see endpoint details through the **Search Endpoints** field or the **Question Results** page. For more information, see View details for a single endpoint on page 270. The **Administrator** and **Content Administrator** reserved roles have all these permissions.
Save a question	**Saved Question write** permission is required to assign a saved question to content sets for which you have permission. **Saved Question write** is also required to create, edit, or delete saved questions. The **Sensor read** content set permissions determine the available sensors. **Filter Group read** content set permissions determine the available filter groups. In addition to **Saved Question write** permission, users require **Package write** and **Action write** permissions (on the content sets of the associated packages) to add associated packages to a new saved question configuration. In addition to these three permissions, users require owner permissions for the question if they want to modify or delete the associated packages. The **Administrator** and **Content Administrator** reserved roles have all these permissions.
Use Interact Saved Questions	**Saved Question read** content set permissions determine the saved questions that you can see in Tanium Console, such as on the Interact **Overview** page, **Question Builder** page, and **Question Results** grid drill-down. **Sensor read** permission is required for the sensors specified in a saved question that you want to issue. **Filter Group read** content set permission is required for the filter groups specified in the saved question. **Ask Dynamic Questions** permission is required to use the drill down feature in the saved question results grid.

© 2026 Tanium Inc. All Rights Reserved

Required permissions to perform Interact tasks (continued)

Tasks	Roles and permissions
Use Interact Categories	**Dashboard Group read** content set permissions determine the categories that you can see in Console, such as on the Interact **Overview** page. **Dashboard Group write** permission is required to create, modify, or delete category configurations. **Dashboard read** content set permissions determine which Interact dashboards are available in categories. The **Administrator** and **Content Administrator** reserved roles can export and import categories.
Use Interact Dashboards	**Dashboard read** content set permissions determine the Interact dashboards that you can see in Console, such as on the Interact **Overview** page. **Dashboard write** permission is required to create, modify, or delete Interact dashboard configurations. **Saved Question read** content set permissions determine which saved questions are available in dashboards. These **Dashboard read** and **write** permissions apply to Interact dashboards, not Reporting dashboards. The **Administrator** or **Content Administrator** reserved role can export and import Interact dashboards.
Deploy an action	**Action write** permission on any content set is required to see the **Deploy Action** button on the **Question Results** page. To deploy an action, and subsequently perform management tasks for it (such as editing), the permission must be assigned to the content set of the package that you select for the action. **Package read** content set permissions determine which packages are available for you to select for actions. **Sensor read** and **Saved Question read** permissions on the **Reserved** content set are required to complete the deploy action workflow. During the workflow, these permissions allow special saved questions that the Tanium Server uses to track and report action status. **Interact Execute action** (module) permission implies all the permissions that enable users to deploy actions in Interact. The **Administrator** reserved role and **Interact Power User** role have all these permissions. NOTE Users who deploy adaptive actions require additional permissions to assign deployment plans, as described in Manage deployment plans on page 91. Users who perform management tasks (such as pausing or stopping) for adaptive action deployments require the permissions described in Manage ring deployments on page 92.

© 2026 Tanium Inc. All Rights Reserved

Required permissions to perform Interact tasks (continued)

Tasks	Roles and permissions
Use the Interact **Overview** page	To see the following sections of the Interact **Overview** page, users require the specified permissions: • **Overview**: **Dashboard Group read**, **Dashboard read**, and **Saved Question read** permissions control the summary counts. • **Favorite Categories**: **Dashboard Group read** permission • **Favorite Dashboards**: **Dashboard read** permission • **Favorite Saved Questions**: **Saved Question read** permission The **Dashboard** permissions apply to Interact dashboards, not Reporting dashboards. The **Administrator** reserved role has all these permissions.

TANIUM DATA SERVICE (TDS) PERMISSIONS

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

- TDS solution permissions on page 85
- TDS administration and platform content permissions on page 88: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Tanium Interact User Guide: Set up TDS users.



Do not assign the **Tanium Data Service Account**, **Tanium Data Service Account - All Content Sets**, or **Data Collection Service Account** roles to users. These roles are for internal purposes only.

TDS solution permissions

Permission	Data Collection Administrator	Data Collection Operator
Data Collection Administrator Unrestricted access to configure data collection	✓ ADMINISTER	✗
Data Collection OPERATOR: Access to configure data collection settings	✗	✓ OPERATOR

© 2026 Tanium Inc. All Rights Reserved

TDS solution permissions (continued)

Permission	Data Collection Administrator	Data Collection Operator
Data Collection API Identify Endpoint The following permissions are for internal purposes only and apply to the TDS content set: READ: Read the results of the internal Endpoint ID sensor WRITE: Allocate Endpoint ID values to endpoints DELETE: Purge the sensor results of specific endpoints from TDS based on Endpoint ID values	READ WRITE DELETE	READ DELETE
Data Collection Bundle Config View and edit configuration data for the next support bundle (internal purposes only)	READ WRITE	
Data Collection EID Namespace Read and write endpoint ID namespaces (internal purposes only)		
Data Collection Group EIDs READ: View the list of EIDs that are members of a computer group (internal purposes only)		
Data Collection Identify Endpoint The following permissions are for internal purposes only: READ: View which sensors TDS uses for determinining the endpoint ID (EID) WRITE: Allocate the sensors that TDS uses to determinine the EID	READ WRITE	
Data Collection Job Read and cancel pipeline jobs (internal purposes only)		
Data Collection Metrics View the **Data Service Sensor Metrics** and **Data Service Database Metrics** charts in the Interact **Info** page	READ	READ

© 2026 Tanium Inc. All Rights Reserved

TDS solution permissions (continued)

Permission	Data Collection Administrator	Data Collection Operator
Data Collection Operator Settings View and edit TDS settings (internal purposes only)	✓ READ WRITE	✓ READ WRITE
Data Collection Pipeline Read pipeline data (internal purposes only)	✗	✗
Data Collection Pipeline Write Write pipeline data (internal purposes only)	✗	✗
Data Collection Purge Purge data for specific sensors (internal purposes only)	✓ SENSOR	✓ SENSOR
Data Collection RDB Connect to the Tanium™ RDB service (internal purposes only)	✗	✗
Data Collection Registration READ: View the Interact **Settings > Registration and Collection** page to see which sensors are registered for results collection WRITE: Register or unregister sensors for results collection, pause (disable) or resume (enable) collection, and purge results	✓ READ WRITE	✓ READ WRITE
Data Collection Sensor Write virtual sensor data (internal purposes only)	✗	✗
Data Collection Service Account View and update the current service account (internal purposes only)	✓ READ WRITE	✗
Data Collection Settings View and edit TDS settings (internal purposes only)	✓ READ WRITE	✗

© 2026 Tanium Inc. All Rights Reserved

TDS solution permissions (continued)

Permission	Data Collection Administrator	Data Collection Operator
Data Collection Status View the **Data Service Status** chart in the Interact **Info** page	✓ READ	✓ READ
Data Collection Virtual Sensor Definition View and edit virtual sensors (internal purposes only)	✗	✗
Data Service Access the TDS workbench	✓ SHOW	✓ SHOW
Result Exclusion Read and write exclusions (internal purposes only)	✓ READ WRITE	✓ READ
Result Expansion Read and write expansions (internal purposes only)	✓ READ WRITE	✓ READ
Result Views Allows Tanium solution services to access sensor results beyond those granted through content set assignments (internal purposes only)	✗	✗

The permissions for the preceding roles provide solution permissions for other solutions. To view the provided permissions, see View effective role permissions on page 588.

The predefined TDS roles provide the following administration and platform content permissions:

TDS administration and platform content permissions

Permission	Permission Type	Data Collection Administrator	Data Collection Operator
User	Administration	✓ READ	✗
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE
Sensor	Platform Content	✓ READ	✓ READ

To view the content sets to which the platform content permissions apply, see View effective role permissions on page 588.

© 2026 Tanium Inc. All Rights Reserved

Action management permissions

The following table summarizes the roles and permissions that are required to manage actions. When you configure roles, apply the permissions to the content sets that include the packages associated with the actions. The listed permissions are platform content permissions except where otherwise noted.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing actions

Tasks	Tanium Console Administration pages	Roles and permissions
Deploy actions	**Question Results** **Saved Question Results** **Action Deployment**	The following permissions are required to deploy actions, including action locks, from the **Questions Results** and **Saved Question Results** pages: • Interact solution permissions: ◦ **Ask Dynamic Questions special** permission is required to deploy actions based on dynamic questions. This permission is not required to deploy actions based on saved questions. ◦ **Interact show** ◦ **Interact Module read** • Platform content permissions: ◦ **Action write** permission on the content sets of packages enables you to deploy actions that use those packages. ◦ **Package read** permission on the content sets of packages enables you to select those packages for actions. ◦ **Sensor read** and **Saved Question read** permissions are required on the **Reserved** content set. The Tanium Server uses special saved questions to track and report action status within the deploy action workflow. Therefore, these permissions are required to complete the action deployment workflow. ◦ **Deployment Plan read** permission on the content sets of deployment plans enables you to assign plans to adaptive (ring-based) actions. Additional permissions are required to view certain plan settings and edit plans. For more information, see Manage deployment plans on page 91. The **Administrator** reserved role, **Content Administrator** reserved role, and **Interact Power User** role have all these permissions. TIP **Interact Execute action** permission provides all the permissions that are required to deploy simple (non-ring-based) actions.  NOTE Users who deploy adaptive actions require additional permissions to assign deployment plans, as described in Manage deployment plans on page 91. Users who perform management tasks (such as pausing or stopping) for adaptive action deployments require the permissions described in Manage ring deployments on page 92.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing actions (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage deployment plans	**Actions > Deployment Plans**	**Deployment Plan read** permission is required to perform the following tasks on the **Deployment Plans** page. These tasks are enabled only for deployment plans that are in a content set to which you apply the permission. • View the list of plans on the **Deployment Plans** page. • Assign plans to deployments. • Open plan configurations in view mode. The following additional permissions determine which plan settings are visible: ◦ **Progression Criteria Set read** permission is required to view progression criteria values in a plan configuration. You must assign the permission to the content sets of the deployment plans that use the criteria. ◦ **Ring Set read** permission is required to view the ring set in a plan configuration. You must assign the permission to the content sets of the deployment plans that use the ring sets. ◦ **Filter Group read** permission is required to view the filter groups that are selected for assigned endpoints or deferred endpoints in the ring set of a plan configuration. You must apply the permission to the content sets that contain the filter groups. **Deployment Plan write** permission is required to perform the following tasks on the **Deployment Plans** page. These tasks are enabled only for deployment plans that are in a content set to which you apply the permission. • Create and clone plans. These tasks also require: ◦ **Progression Criteria Set write** permission, which you must assign to the content sets of the deployment plans that use the criteria ◦ **Ring Set write** permission, which you must assign to the content sets of the deployment plans that use the ring sets ◦ **Filter Group read** permission on the content sets that contain the filter groups that you select for assigned endpoints or deferred endpoints in ring sets • Edit plan settings. Additional permissions are required to edit specific settings in a plan: ◦ **Progression Criteria write** permission is required to edit progression criteria. You must assign the permission to the content sets of the deployment plans that use the criteria. ◦ **Ring Set write** permission is required to edit ring sets. You must assign the permission to the content sets of the deployment plans that use the ring sets. ◦ **Filter Group read** permission is required to change the filter groups for assigned endpoints or deferred endpoints in ring sets. You must apply **Filter Group read** permission to the content sets that contain the filter groups. • Delete deployment plans.

User role requirements for managing actions (continued)

Tasks	Tanium Console Administration pages	Roles and permissions

Manage ring deployments	**Actions > Ring Deployment Status**	**Deployment Plan read** permission is required to view deployments on the **Ring Deployment Status** page. These tasks are enabled only for deployments that use deployment plans in a content set to which you apply the permission.
		• Open the Deployment Details page for a single deployment. The following additional permissions determine which settings are visible:
		  ◦ **Progression Criteria Set read** permission is required to view progression criteria. You must assign the permission to the content sets of the deployment plans that use the criteria.
		  ◦ **Ring Set read** permission is required to view the ring set. You must assign the permission to the content sets of the deployment plans that use the ring sets.
		  ◦ **Filter Group read** permission is required to view the filter groups that are selected for assigned endpoints or deferred endpoints in the ring set. You must apply the permission to the content sets that contain the filter groups.
		The **Administrator** reserved role, **Deployment Plan Editor** role, and **Deployment Plan User** role have all the preceding permissions.
		You require additional permissions to view and manage the following deployment types on the **Ring Deployment Status** page. For all types, read permission enables viewing the deployments and write permission enables performing management tasks on them, such as pausing or stopping.
		• Tanium platform and Tanium Guardian deployments: **Action read/write** is required on the content sets of the deployments.
		• Tanium Deploy (software) deployments: **Deploy Deployment read/write** is required on the content sets of the deployments.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing actions (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage scheduled actions	**Actions > Scheduled Actions**	**Action read** permission is required to perform the following tasks on the **Scheduled Actions** page. These tasks are enabled only for actions that use packages in a content set to which **Action read** permission is assigned. • View actions. • Export actions in CSV format. **Export Content** (administration) permission is required to export scheduled actions in JSON format. • Copy action information to the clipboard. **Own Action read** permission enables the same tasks as **Action read** but only for actions that the user owns. **Action write** permission is required to perform the following tasks on the **Scheduled Actions** page. These tasks are enabled only for actions that use packages in a content set to which **Action write** permission is assigned. • View the status of, and re-download, packages that are associated with actions. • Disable or enable actions. • Change the action groups that actions target. • Create copies of action configurations. • Delete actions. **Sensor read** and **Saved Question read** permissions on the **Reserved** content set, in addition to **Action read** and **write** permissions (on the content sets of packages associated with the actions), are required to reissue or edit actions on the **Scheduled Actions** page. The **Reserved** content set includes content that is used to ask preview questions. **Action for Saved Question**: Write permission enables users to see and use the **Deploy Action** button on the **Question Results** page, but only for saved questions that are configured with an associated package. **Package read** permission is not required for the associated package. If the saved question is not configured with an associated package, the **Deploy Action** button does not appear. TIP Use **Action for Saved Question write** permission instead of **Action write** permission to limit use by action users who use Tanium to execute standard operating procedures that someone else created. **Import Signed Content**: This permission is required to import scheduled actions. The **Administrator** reserved role has all these permissions. The **Content Administrator** reserved role has all these permissions except the ability to export scheduled actions in JSON format or to import them in any format.

User role requirements for managing actions (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage action groups	**Actions > Action Groups**	**Action Group** (administration permission): • Read permission is required to view and export action group configurations.  NOTE **Action Group read** permission overrides the action group **Visibility** setting. A user who has **Action Group read** and action deployment permissions can select any action group when deploying an action. A user who has **Action Group read** and **Approve Action** permissions can approve actions that target any action group. However, the computer groups that are assigned to a user still control which endpoints run an action that the user deploys to the selected action group. • Write permission is required to create, edit, and delete action groups. The **Administrator** reserved role has these permissions.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing actions (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage action history	**Actions > Action History**	**Action read** permission is required to perform the following tasks on the **Action History** page. These tasks are enabled only for actions that use packages in a content set to which **Action read** permission is assigned. • View action configurations. • Export actions in CSV format. **Export Content** (administration) permission is required to export actions in JSON format. • Copy action information to the clipboard. • View action status on page 96, when combined with other content permissions. **Own Action read** permission enables the same tasks as **Action read** but only for actions that the user owns. **Action read** and **write** permissions are required to stop actions on the **Action History** page. The permissions must be assigned to the content sets of the packages that are associated with the actions. **Sensor read** and **Saved Question read** permissions on the **Reserved** content set, in addition to **Action read** and **write** permissions (on the content sets of packages associated with the actions), are required to reissue actions on the **Action History** page. The **Reserved** content set includes content that is used to ask preview questions. The **Administrator** and **Content Administrator** reserved roles have these permissions.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing actions (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
View action status	**Action Status**	The following permissions are required to View status for simple actions on page 352 on the **Action Status** page. For the permissions to view status for adaptive actions, see Manage ring deployments on page 92. • **Package**: Read permission on the content sets for packages that are associated with actions is required to view files in the **Action Status** page. • **Sensor** and **Saved Question**: Read permissions on the **Reserved** content set are required to use the **Show Client Status Details** button in the **Action Status** page. • **Sensor**: Read permission on the **Client Management** content set is required to use the **Get action log for selected machines** button in the **Action Status** page. • **Action**: Read permission is required to open the **Action Status** page from the **Action History** page. **Own Action read** permission enables the same ability but only for actions that the user owns. These permissions must be assigned to the content sets of the packages that the actions use. The **Administrator** and **Content Administrator** reserved roles have all these permissions.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing actions (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage action approval	**Actions > All Pending Approvals** **Actions > Actions I Can Approve**	**Action read** permission is required to perform the following tasks on the **All Pending Approvals** page. These tasks are enabled only for actions that use packages in a content set to which **Action read** permission is assigned. • View actions that require approval. • Export the actions in CSV format. **Export Content** (administration) permission is required to export actions in JSON format. • Copy the actions to the clipboard. **Own Action read** permission enables the same tasks as **Action read** but only for actions that the user owns. **Approve Action** permission is required to perform the following tasks on the **Actions I Can Approve** page. These tasks are enabled only for actions that use packages in a content set to which **Approve Action** permission is assigned. • View actions that require approval. Users cannot view their own actions on this page. • Approve actions that other users own, when combined with **Sensor** read permission. Users cannot approve their own actions. • Export the actions in CSV format. **Export Content** (administration) permission is required to export actions in JSON format. • Copy the actions to the clipboard. **Bypass Action Approval**: This permission enables users to bypass approval for their own actions. The permission does not apply retroactively. The permission must be assigned to the content sets of the packages that the actions use. The **Administrator** and **Content Administrator** reserved roles have all the preceding permissions except **Bypass Action Approval**. **Global Settings**: Write permission is required to enable or disable action approval. The **Administrator** reserved role has this permission.

Content management permissions

The following table summarizes the roles and permissions that are required to manage content such as sensors, packages, saved questions, and filter groups. The listed permissions are platform content permissions, except where otherwise noted. You apply the permissions to one or more content sets to manage the content that is assigned to those sets.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing content

Tasks	Tanium Console Administration pages	Roles and permissions
Manage sensors	**Content > Sensors** **Content > Quarantined Sensors**	**Sensor**: • Read permission on content sets is required to view the sensors that are assigned to those content sets, or to export those sensors in CSV format. • Write permission is required to create, edit, or delete sensors. **Export Content** (administration permission): This permission is required to export sensors in JSON format. **Import Signed Content**: This permission is required to import sensors. The **Administrator** and **Content Administrator** reserved roles have **Sensor read** and **write** permissions. The **Administrator** reserved role can import or export sensors in JSON format. **Global Settings** (administration permission): Write permission is required to enable or disable sensor quarantine enforcement. The **Administrator** reserved role has this permission. **Sensor read** permission or **Ask Dynamic Questions** permission is required to view quarantined sensors. Computer management group assignments determine on which endpoints users can manually quarantine or unquarantine sensors.
Manage packages	**Content > Packages**	**Package**: • Read permission on content sets is required to view the packages that are assigned to those content sets, or to export those packages in CSV format. • Write permission is required to create, edit, or delete packages. **Export Content** (administration permission): This permission is required to export packages in JSON format. **Import Signed Content**: This permission is required to import packages. **Action write** permission (on the content sets of packages associated with the actions), **Sensor read** permission (on the **Reserved** content set), and **Saved Question read** permission (on the **Reserved** content set) are required to deploy actions from the **Packages** page. The **Administrator** reserved role has all these permissions and can import packages. The **Content Administrator** reserved role has **Package read** and **write** permissions.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing content (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage saved questions	**Content > Saved Questions**	**Saved Question**: • Read permission on content sets is required to view the saved questions that are assigned to those content sets, or to export those saved questions in CSV format. • Write permission is required to create, edit, or delete saved questions. **Interact** show (module) permission is required to view any content types, including saved questions, on the Interact **Overview** page. **Export Content** (administration permission): This permission is required to export saved questions in JSON format. **Import Signed Content**: This permission is required to import saved questions. **Saved Question**, **Action** and **Package**: Write permissions are required to add associated packages to a new saved question. In addition to these three permissions, a user also requires owner permissions for the question to later edit or delete the associated packages. For more information about the **Visibility** setting, see Create a saved question. **Sensor**: Read permissions on content sets determine which sensors users can select for questions. The **Administrator** reserved role has all these permissions and can import saved questions. The **Content Administrator** reserved role has all these permissions except the ability to export saved questions in JSON format or to import them in any format.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing content (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage dashboards	Tanium **Home** page Interact **Overview** page	**Dashboard** permissions control access to Interact dashboards on the Interact **Overview** page and Tanium **Home** page: • Read permission is required to view dashboards. **Saved Question read** permission determine which saved questions are visible in dashboards. • Write permission is required to create, edit, or delete dashboards. NOTE For the permissions that control access to Tanium Reporting dashboards, see Tanium Reporting User Guide: User role requirements. **Interact show** (module) permission is required to view any content types, including dashboards, on the Interact **Overview** page. **Export Content** (administration) permission is required to export dashboards in JSON format. **Import Signed Content** (administration) permission is required to import dashboards. The **Administrator** reserved role has all these permissions and can import dashboards. The **Content Administrator** reserved role has all these permissions except the ability to export and import dashboards.
Manage categories	Tanium **Home** page Interact **Overview** page	**Dashboard Group** permissions control access to Interact categories on the Interact **Overview** page and Tanium **Home** page: • **Dashboard Group read** is required to view categories. **Dashboard** read permission determines which dashboards are visible in categories. • **Dashboard Group write** permission is required to create, edit, or delete categories. **Interact show** (module) permission is required to view any content types, including categories, on the Interact **Overview** page. **Export Content** (administration) permission is required to export categories in JSON format. **Import Signed Content** (administration) permission is required to import categories. The **Administrator** reserved role has all these permissions and can import categories. The **Content Administrator** reserved role has all these permissions except the ability to export and import categories.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing content (continued)

Tasks	Tanium Console Administration pages	Roles and permissions

Manage filter groups		**Filter Group**:
		• Read permission is required to view the **Filter Groups** page. Read permission on the content sets to which the filter groups are assigned is required to:
		  ◦ View the configuration (group membership) of specific filter groups. **Ask Dynamic Questions** permission is also required for this activity.
		  ◦ Export filter groups in CSV format.
		• Write permission is required to:
		  ◦ Create, clone, and edit filter groups. These abilities also require **Ask Dynamic Questions** permission.
		  ◦ Delete filter groups.
		Export Content (administration permission): This permission is required to export filter groups in JSON format.
		Import Signed Content: This permission is required to import filter groups.
		The **Administrator** reserved role has all these permissions and can import filter groups.

Export content files	Various **Content** and **Permissions** pages **Solutions** page	**Export Content** (administration permission): This permission is required to export the following content types: • Allowed URLs • Computer management groups • Filter groups • Packages • Saved questions • Scheduled actions • Sensors The **Administrator** reserved role has this permission.
Import content files	Various **Content** and **Permissions** pages **Solutions** page	**Import Signed Content** (administration permission): This permission is required to import digitally signed content files. The **Administrator** reserved role can import all content types.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing content (continued)

Tasks	Tanium Console Administration pages	Roles and permissions

Question history	**Content > Question History**	**Question History** (administration permission): Read permission is required to view and export information in the **Question History** page. To issue a question from the **Question History** page, users also require the following permissions:
		• **Interact** solution permissions:
		  ◦ **Interact show**
		  ◦ **Interact Module read**
		• **Platform Content Permissions**:
		  ◦ **Saved Question read** permission on the content sets that contain the questions that the user is allowed to issue.
		  ◦ **Sensor read** permission on the content sets that contain the sensors that are used in the questions that the user is allowed to issue.
		The **Administrator** reserved role has these permissions.

Manage question and sensor runtime indicator thresholds	**Content > Sensor Thresholds**	**Administrator** reserved role only
Manage content sets	**Permissions > Content Sets**	**Administrator** or **Content Set Administrator** reserved role only

RBAC management permissions

The following table summarizes the roles and permissions that are required to manage role-based access control (RBAC) configurations. The listed permissions are administration permissions except where otherwise noted.

User role requirements for managing RBAC

Tasks	Tanium Console Administration pages	Roles and permissions
Manage content sets	**Permissions > Content Sets**	**Administrator** or **Content Set Administrator** reserved role only
Manage roles	**Permissions > Roles**	**Administrator** or **Content Set Administrator** reserved role only. Note that a **Content Set Administrator** cannot manage the assignment of reserved roles to users and user groups.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing RBAC (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage computer management groups	**Permissions > Computer Groups**	**Computer Group**: Write permission is required to create, edit, or delete computer management groups. To create a computer management group in which membership is based on a sensor filter, the following permissions are required in addition **Computer Group write** permission: • **Sensor** (platform content permission): Read permission on the **Reserved** content set, which includes content that is used to ask preview questions • **Interact Module** (solution permission): Write permission Computer groups with manually defined membership do not require the **Sensor read** or **Interact Module write** permissions. The following permissions are required to edit the assignments of computer management groups: • **User**: Write permission is required to edit the computer management group assignments of users. • **User Group**: Write permission is required to edit the computer management group assignments of user groups. • **Persona**: Write permission is required to edit the computer management group assignments of personas. **Computer Group**: Read permission is required to export computer management groups in CSV format. **Export Content**: This permission is required to export computer groups in JSON format. **Import Signed Content**: This permission is required to import computer groups. The following permissions are required to view the assignments of computer management groups: • **User**: Read permission is required to view the computer management group assignments of users. • **User Group**: Read permission is required to view the computer management group assignments of user groups. • **Persona**: Read permission is required to view the computer management group assignments of personas. The **Administrator** reserved role has all these permissions and can import or export computer groups in JSON format.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing RBAC (continued)

Tasks	Tanium Console Administration pages	Roles and permissions

Manage users	**Permissions > Users**	**User**:
		• Read permission is required to:
		  ◦ View user configurations and export them in CSV format.
		  ◦ View the user group assignments of users. This ability also requires the **User Group read** permission.
		  ◦ View the computer management group assignments of a user.
		• Write permission is required to:
		  ◦ Add a user.
		  ◦ Manage user properties.
		  ◦ Edit the computer management group assignments of a user.
		  ◦ Save changes to a user.
		  ◦ Delete a user.
		  ◦ Edit the user group assignments of users. This ability also requires the **User Group write** permission.
		  ◦ Edit the persona assignments of users. This ability also requires the **Persona write** permission.
		The **Administrator** reserved role has all these permissions, and can also export user configurations in JSON format.
		The **Administrator** reserved role is required to change persona assignments and transfer the ownership of content.
		The **Administrator** or **Content Set Administrator** reserved role is required to change the role assignments of users. However, a **Content Set Administrator** cannot manage the assignment of reserved roles.
		Users cannot modify their own persona, computer group, or role assignments.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing RBAC (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage user groups	**Permissions > User Groups**	**User Group**: • Read permission is required to: ◦ Export user groups in CSV format. ◦ View the user assignments of user groups. This ability also requires the **User read** permission. ◦ View the computer management group assignments of user groups. • Write permission is required to: ◦ Add a user group. ◦ Edit a user group. ◦ Edit the computer management group assignments of a user group. ◦ Edit the user assignments of user groups. This ability also requires the **User** write permission. ◦ Edit the persona assignments of user groups. This ability also requires the **Persona write** permission. ◦ Set the default user group. This ability also requires the **Global Settings write** permission. ◦ Delete a user group. Only the **Administrator** reserved role has all these permissions and can export user groups in JSON format. The **Administrator** or **Content Set Administrator** reserved role is required to change the role assignments of user groups. However, a **Content Set Administrator** cannot manage the assignment of reserved roles. The **Administrator** reserved role is required to change persona assignments.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for managing RBAC (continued)

Tasks	Tanium Console Administration pages	Roles and permissions
Manage personas	**Permissions > Personas**	**Persona**: Write permission is required to add, edit, and delete personas, and to edit the computer management group and role assignments of personas. The following permissions are required to edit the user and user group assignments of personas: • **Persona write** and **User write** permissions are required to edit the user assignments of personas. • **Persona** write and **User Group write** permissions are required to edit the user group assignments of personas. **Persona**: Read permission is required to view and export persona configurations. The **Administrator** reserved role has all these permissions.
Import users and user groups from an LDAP server	**Configuration > LDAP/AD Sync Configuration**	**Administrator** reserved role only
Configure SAML authentication	**Configuration > SAML Configuration**	**Administrator** reserved role only
Manage API tokens	**Permissions > API Tokens**	**Token - View**: This permission is required to see the **API Tokens** page and to see the tokens of all users. **Token - Use**: This permission is required for a user to create, view, rotate, or revoke his or her own API tokens. This permission does not enable the user to perform these tasks for the tokens of other users. **Token - Revoke**: This permission is required to revoke the API tokens of any user. **Token - Rotate**: This permission is required to rotate the API tokens of any user. Rotation deletes the existing token and creates a new one. The expiration timer of the new token is reset and has the same interval as the deleted token. The **Administrator** reserved role has these permissions.

Troubleshooting permissions

The following table summarizes the roles and permissions that are required to perform troubleshooting tasks in Tanium Console. The listed permissions are platform content permissions except where otherwise noted.

© 2026 Tanium Inc. All Rights Reserved

User role requirements for troubleshooting your Tanium deployment

Tasks	Tanium Console Administration pages	Roles and permissions
Monitor Tanium Client registration and communication	**Configuration > Client Status**	**Client Status** (administration permission): Read permission is required to see the **Client Status** page and filter the table. The **Administrator** reserved role has this permission.
View date-times for activities related to user sign ins, user account configuration, and platform setting configuration	**Permissions > User** **Configuration > Settings**	**Audit** (administration permission): Read permission is required to view: • **Last Sign In** information on the **Users** page • **Last Modified** information on the user configuration page • **Last Modified** information on the **Settings** page
Configure server logging levels	**Configuration > Logging**	**Administrator** reserved role only
View plugins and plugin schedules	**Configuration > Plugins**	**Administrator** reserved role only
View cache usage	**Configuration > Package File Repository**	**Administrator** reserved role only
View the info page	`https://<Tanium_Server>/info`	**Server Status** (administration permission) read is required to view the `https://<Tanium_Server>/info` page.

© 2026 Tanium Inc. All Rights Reserved

Part 4: Managing Tanium solutions

Tanium solutions overview

Use the **Solutions** page to import, export, update, and otherwise manage Tanium solutions.

Tanium solutions include modules (such as Tanium Deploy), shared services (such as Tanium Client Management), and content-only solutions (such as Default Content). Each module and shared service comprises a *workbench* and content. A workbench is the user interface that you use to perform module operations. Users use the workbenches and content to perform their Tanium workflows, such as managing, monitoring, and protecting the endpoints in your environment.

For example, the workbench of the Tanium Comply module includes an **Assessments** page for monitoring the status of assessments, which evaluate endpoints for security configuration exposures and software vulnerabilities. In terms of content, the module includes **Comply - Run Assessment** packages for running the assessments.

For more information about each solution type, see:

- Modules on page 118
- Shared services on page 119
- Content-only solutions on page 120

To manage solution-provided content, see Solution content overview on page 418.

When you first sign in to Tanium Console after Tanium Server installation, the **Solutions** page opens if you are assigned the **Administrator** reserved role. You require that role to access the page and use it to manage Tanium solutions and content.



The **Import Signed Content** permission enables you to import content through other Console pages. For example, the combination of **Import Signed Content** permission and **Sensor read** permission enables you to import content through the **Administration > Content > Sensors** page. The **Administrator** reserved role has all the permissions for importing or exporting content and is the only role that allows access to the **Solutions** page.

To troubleshoot issues that occur when you manage and use solutions, see Troubleshoot solution issues on page 715.

If the Tanium license expires, you cannot import, export, or update any solutions, and the **Solutions** page does not show any solutions. For more information, see License expiration on page 206.

Solutions page contents and widgets

The following table describes the components of the **Solutions** page and describes how to use them for viewing information about solutions and for managing solutions.

© 2026 Tanium Inc. All Rights Reserved

Solutions page contents

Fields and sections	Description
Server Version	This field indicates the currently installed version of the Tanium Core Platform.
New release banner	A banner indicates if a new release for the Tanium Core Platform or Tanium solutions is available but not installed. For maintenance release updates, the banner also shows a button to start the update installation workflow, as described in Install a Tanium release update on page 128.
Custom manifest URL banner	If your Tanium environment is not air-gapped and a user has manually set the URL of the Tanium manifest on page 113, a banner provides the option to reset the URL to the default value and thereby revert the URL to Tanium management. The banner appears when a new Tanium release is available but not installed. Resetting the URL is not required to install updates. However, the reset simplifies installing future updates because it removes the need to manually configure the value for each update.
Installed Release	This section shows information about the currently installed semiannual release and maintenance release update. Click the Release Notes icon to view the release notes for a release.
Modules	This section shows a tile for each installed module. For more information about modules and working with the module tiles, see Modules on page 118.
Content	This grid shows a row for each Tanium solution that is a shared service or content-only solution. For more information about these solutions and the **Content** grid, see Shared services on page 119, Content-only solutions on page 120, and Content grid filters on page 109.
Buttons	The **Solutions** page provides buttons for managing solutions, as described in Solutions page buttons on page 110.

Content grid filters

On the **Solutions** page, the **Content** grid lists the available Tanium content-only solutions and shared services. You can filter the grid to find a particular solution.

Solutions page: Content grid filters

Filter	Description
Solution name	Enter a text string in the **Filter items** field to filter the grid by solution name.
Available updates	For the **Show** toggle, select **Available Updates** to show only solutions with pending updates or select **All** to show all solutions. To update solutions, see Install a Tanium release update on page 128.
Solution attributes	Expand the **Filters** section, select a solution attribute (such as **Available Version**), select an operator (such as **contains**), enter a text string that contains all or part of the attribute value, and click Apply. For each additional filter, click +, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.

© 2026 Tanium Inc. All Rights Reserved

Solutions page: Content grid filters (continued)

Filter	Description
Source	If your deployment uses a Tanium production license, only **Manifest** content is available. If you specified a Tanium lab license when installing the Tanium Server, you can filter the **Content** grid by **Source**: • **Manifest**: This is production content that includes the essential set of shared services and content-only solutions that you can manage. • **Labs**: This experimental set of content-only solutions is available only if you specified a Tanium lab license. • **All**: Both **Manifest** and **Labs** content.

Solutions page buttons

The **Import**, **Re-import**, **Update**, and **Uninstall** buttons appear in multiple places, and where you click a button determines the scope of its operation:

- **Solutions** page warning banner: If any installed solutions are incompatible with the current Tanium Console version, a warning banner lists those solutions. Clicking **Uninstall** in the banner uninstalls only the listed solutions, not any others that you select in the **Modules** or **Content** sections.
- **Solutions** page footer: Performs the operation for all the selected modules, services, and content-only solutions.
- **Modules** section header: Performs the operation only for the selected modules.
- **Modules** section tiles: Performs the operation only for a single module.
- **Content** section header: Performs the operation only for the selected services and content-only solutions.

The following table describes the page buttons that you use to manage solutions.

Solutions page buttons

Button	Operation
Tanium Recommended Installation	Initiate the workflow to import and automatically configure, in a single operation, all the modules and shared services that your Tanium license enables. After you import any modules or services, the page stops showing the **Tanium Recommended Installation** button. For more information, see Import all modules and services on page 123. NOTE Automatic configuration is not available for update or re-import operations.
Update	Initiate the workflow to update a solution to the latest version. The page uses **bold orange text** to indicate that one or more updates are available for a solution. The **Update** button is available only for **Labs** content and Emerging Issues Content. For more information, see Import or update specific solutions on page 125. Updates for other solutions are available only as part of a semiannual or maintenance release update that you install as a bundle for all solutions. For more information, see Install a Tanium release update on page 128.

© 2026 Tanium Inc. All Rights Reserved

Solutions page buttons (continued)

Button	Operation
Import	Initiate the workflow to import a solution for which no version is currently installed. The workflow includes an option to configure modules and shared services with the recommended default settings. For more information, see Import or update specific solutions on page 125.
Re-import	Initiate the workflow to re-import the currently installed version. For more information, see Import or update specific solutions on page 125. The **Re-import** button is available only for **Labs** content and Emerging Issues Content. For more information, see Import or update specific solutions on page 125.
Uninstall	Initiate the workflow to uninstall a solution. For more information, see Uninstall solutions on page 138.
Documentation 	Access the user guides for modules and shared services or access the release notes for content-only solutions.
Export 	Copy the URL of the source file for the currently installed version of a solution. For more information, see Export and import specific solution versions through URLs on page 132.

Tanium releases

A Tanium release provides new product versions as a bundle that you install to obtain the latest new features, enhancements, security fixes, and patch updates. Each bundle includes the latest available versions of the following Tanium components:

- Tanium Core Platform servers, including the Tanium Server, Tanium Module Server, Tanium Zone Server, and Tanium Zone Server Hub
- TanOS for Tanium Appliance deployments
- Tanium solutions, including modules, shared services, and content-only solutions

  New solution versions might provide updated versions of Tanium-managed content, such as sensors and packages.

  Tanium release bundles do not include Labs content on page 126.
- Tanium Clients
- Endpoint tools, such as client extensions

The procedure to install a release for these components depends on whether you are installing a new Tanium deployment (see Installing a new deployment on page 114) or updating an existing deployment (see Updating an existing deployment on page 114).

© 2026 Tanium Inc. All Rights Reserved

Tanium provides new feature releases twice per year (Semiannual releases on page 112) and patch releases once per month (Maintenance release updates on page 112). For an existing deployment, you can install a release as soon as it is available or defer installation to a more convenient time.

Semiannual releases

A semiannual release provides new features and enhancements for the Tanium components described in Tanium releases on page 111, as well as any security and bug fixes that applied to any previous semiannual release. Tanium provides a new semiannual release in May and November of each year.

RELEASE LIFECYCLE

Tanium supports each semiannual release for 18 months after the release date, regardless of when you install the release. Tanium provides maintenance release updates that contain critical security and bug fixes as necessary throughout the lifecycle of each semiannual release. For more information, see Maintenance release updates on page 112.

SKIPPING RELEASES

You can skip a semiannual release if you want to update your deployment at a yearly cadence instead of every six months. For example, if Tanium™ Semiannual Release 2024H1 is currently installed in your deployment, you can skip Semiannual Release 2024H2 and update directly to Semiannual Release 2025H1. You cannot skip more than one release.



Install each semiannual release when it becomes available. You cannot access new features or enhancements without installing a semiannual release.

TANIUM CLIENT AND ENDPOINT TOOLS SUPPORT

Each semiannual release supports the current endpoint toolset and the two previous toolset releases. If the installed toolset release is a version that is supported but is earlier than the semiannual release version, the tools are considered degraded because they do not support the latest features in Tanium solutions. You can review the list of new features in the release notes for the semiannual release. For more information, see Tanium Endpoint Configuration User Guide: Managing Tanium Client and endpoint tool upgrade rollouts.



Update the toolset release to match the installed semiannual release.

Maintenance release updates

A maintenance release update provides security and bug fixes for a semiannual release. The update applies to the Tanium components described in Tanium releases on page 111. Each update provides new versions only for the components that have fixes since the last update. Tanium typically provides a maintenance release update once per month but might skip an interval if no components require significant changes in a particular month.

© 2026 Tanium Inc. All Rights Reserved

SKIPPING RELEASES

You can skip any maintenance release updates that become available after a semiannual release. When you install a maintenance release update, it includes all the updates from any previous maintenance release update.



Install each maintenance release update when it becomes available to ensure your Tanium deployment has all the latest security and bug fixes.

INSTALLING AN UPDATE THAT IS NOT THE LATEST

You can install a maintenance release update that is not the latest as long as it is still supported. The semiannual release that is currently installed determines which maintenance releases are available to install. To install the same maintenance release in different Tanium environments, all the environments must have the same semiannual release installed.

The maintenance release that you install must be a higher version than the currently installed maintenance release because the Tanium Core Platform and Tanium solutions do not support downgrades. For example, if the currently installed release is 2025H1 Update 3, you can install 2025H1 Update 5 but not 2025H1 Update 1.



To preserve bug fixes and security fixes in the current installation and to add newer fixes, be sure the maintenance release that you select to install is newer than your current installation. For example, say 2024H2 Update 11 is currently installed and Tanium released it on August 19, 2025. Although you can install 2025H1 Update 3 because it is a higher version, it is an older update because Tanium released it on July 15, 2025. Therefore, 2025H1 Update 3 might not have fixes that Tanium included in maintenance releases between July 15 and August 19 for both the 2024H2 and 2025H1 semiannual release branches.

Installing a release that is not the latest might be useful in cases such as when you plan upgrades to your production environment based on testing in another environment. When testing finishes, you might choose to upgrade your production environment to the same release as the one in the test environment even if that release is not the latest. A gap between releases can occur if a new release becomes available while testing is in progress on an older release and your organization chooses not to restart testing with the new release. Keeping the production and test environments on the same release ensures that the Tanium solution versions you deploy to production are the versions that you tested.

Tanium manifest

A Tanium *manifest* is an XML file that specifies the versions of Tanium solutions and content that are available to install or update for a particular Tanium release. The Tanium Server retrieves the manifest from a URL that is specific to each semiannual release.

Some organizations, in consultation with Tanium Support, might override the default URL with a custom URL. A custom URL is required in air-gapped environments and is a rarely used option in non-air-gapped environments. If a custom URL is set in a non-air-gapped environment, Tanium Console provides the option to reset the URL to the default value, as described in Install the update on page 129. Resetting to the default value reverts the URL to Tanium management, which simplifies installing future updates because you no longer need to manually configure the value for each update. The reset option does not apply to air-gapped environments.

© 2026 Tanium Inc. All Rights Reserved

NOTE

If a module tile on the **Solutions** page shows the error `The manifest version cannot be installed because the currently installed version is newer`, see Installed Version Newer Than Manifest Version on page 715.

For more information about the configuration manifest that Tanium™ Endpoint Configuration distributes to endpoints, see Tanium Endpoint Configuration User Guide: Endpoint configuration overview.

Installing a new deployment

For a new deployment, the order in which you install Tanium components depends on your infrastructure:

- Tanium Appliance Deployment Workflow
- Tanium Deployment Workflow for Windows infrastructure

The following sections provide details about installing components in a new deployment.

FRESH INSTALLATION OF TANOS AND APPLIANCE

TanOS is pre-installed on the Appliance. Contact Tanium Support on page 724 for the items that you need to install the Appliance. After you acquire the items, install the Appliance as described in the Tanium Appliance Deployment Guide.

FRESH INSTALLATION OF TANIUM CORE PLATFORM SERVERS FOR WINDOWS

Contact Tanium Support on page 724 for the items that you need to install a platform servers release for Windows infrastructure. After you acquire the items, install the servers as described in Tanium Core Platform User Guide for Windows Deployments.

FRESH INSTALLATION OF TANIUM SOLUTIONS AND CONTENT

After you install Tanium Core Platform servers, the **Solutions** page provides a **Tanium Recommended Installation** button to install all your licensed Tanium modules and shared services in a single operation, along with any associated content. For more information, see Import all modules and services on page 123. You can also install specific solutions without installing others, and install any content-only solutions that the **Tanium Recommended Installation** workflow does not include. For more information, see Import or update specific solutions on page 125.

The recommended installation process for solutions automatically installs the latest solution versions. The latest versions include all the features in the current semiannual release and all the fixes that are available in the current maintenance release update.

FRESH INSTALLATION OF TANIUM CLIENT AND ENDPOINT TOOLS

To install Tanium Clients, see Tanium Client Management User Guide. When you perform a fresh installation of Tanium solutions and Clients, the solutions automatically use Tanium Endpoint Configuration to install endpoint tools.

Updating an existing deployment

Install a semiannual or maintenance release update for Tanium components in the following order:

© 2026 Tanium Inc. All Rights Reserved

- TanOS (Appliance only)
- Tanium Core Platform servers
- Tanium solutions
- Tanium Clients and endpoint tools



After you start installing a semiannual release for TanOS and the platform servers, solutions remain unavailable until the update process finishes for TanOS, the servers, and solutions. Therefore, notify users before you start installing a semiannual release for TanOS and the servers.

After you install a maintenance release update for TanOS and the servers, users can continue using solutions until you start installing the update for solutions. After you start the solutions update, solutions remain unavailable until the update process finishes.

The following sections provide details about updating components in an existing deployment.

TANOS UPDATES (APPLIANCE ONLY)

You must update TanOS before updating Tanium Core Platform servers. For more information, see Tanium Appliance Deployment Guide: Upgrade TanOS on Tanium Appliances.

TANIUM CORE PLATFORM SERVERS UPDATES

Contact Tanium Support on page 724 for the items that you need to update Tanium Core Platform servers. After you acquire the items, perform the procedure for your infrastructure:

- Tanium Appliance Deployment Guide: Upgrade Tanium Core Platform in an Appliance deployment
- Tanium Core Platform User Guide for Windows Deployments: Upgrading Tanium Core Platform servers in a Windows deployment.

TANIUM SOLUTIONS AND CONTENT UPDATES

You install each semiannual or maintenance release update as a bundle in a single operation that applies to all the currently installed solutions except **Labs** content. For more information about which solutions the updates include and exclude, see Install a Tanium release update on page 128.

After you install Tanium Semiannual Release 2024H1, you can import specific solutions at any time but you cannot re-import or update specific solutions other than the exceptions that are described in Import or update specific solutions on page 125.

Semiannual and maintenance release updates overwrite any customizations to Tanium-managed content. For example, if you moved the **Username** sensor from the original (Tanium-assigned) **Base** content set to a custom content set, the solutions update automatically reassigns that sensor to the **Base** content set during installation.

© 2026 Tanium Inc. All Rights Reserved

TIP

Before installing a release, you can clone content that has customizations you want to preserve. The solutions update does not overwrite cloned content or content that you created from scratch. For the procedures to clone content, see Managing content on page 419.

TANIUM CLIENT AND ENDPOINT TOOLSET UPDATES

Tanium releases can include updates to both Clients and endpoint tools. Each release bundles the tools in a versioned toolset that contains a specific version of each tool. When you install a Tanium release, it automatically updates the toolset on all endpoints but does not update Clients. You manage Client updates through Endpoint Configuration (best practice) or through the options described in the Tanium Client Management User Guide. For subsequent semiannual or maintenance release updates, you can use Endpoint Configuration to manage both toolset and Client updates independently from the solutions update. For more information, see Tanium Endpoint Configuration User Guide: Managing Tanium Client and endpoint tool upgrade rollouts.

Release status

Tanium Console shows information about a Tanium release for the Tanium Core Platform and solutions when the release becomes available. While you Install a Tanium release update on page 128, Console also displays information about the installation status. The information displayed, and the accessibility of solutions while a release is pending, depend on whether the release is a semiannual or maintenance release update and whether you sign in as an administrator or non-administrator. An administrator must be assigned the **Administrator** reserved role. Only administrators can see the **Solutions** page. The following sections describe the information displayed and the accessibility of Tanium solutions during various stages of a successful release installation:

- Installation not started on page 116
- Installation in progress on page 117
- Installation completed on page 118

If Console shows error messages during installation, see Troubleshoot release update issues on page 131.

NOTE

Tanium releases can also include updates to Tanium Clients and endpoint tools. To track the status of updates to these components, see Tanium Endpoint Configuration User Guide: Managing Tanium Client and endpoint tool upgrade rollouts.

While an update is in progress, you cannot switch to an alternative persona regardless of the roles and personas that are assigned to your account.

INSTALLATION NOT STARTED

The following tables describe the information displayed and the accessibility of Tanium solutions when a Tanium Information and solutions access when a semiannual release has not started on page 117 or Information and solutions access when a maintenance release update has not started on page 117 becomes available but you have not yet start installing it.

© 2026 Tanium Inc. All Rights Reserved

Information and solutions access when a semiannual release has not started

Components	Release information and solutions access
Platform	A banner appears on the Tanium **Home** page and **Solutions** page to indicate the availability of a platform update. The banner also shows the release version and a link to the associated release notes. An administrator must update the platform before updating solutions. Users of any type can access solutions as long as the platform update has not started.
Solutions	The **Semiannual Update** page is the only page that users can see when they sign in after the platform update finishes but before the solutions update starts. For administrators, the page shows a button to start the update. For non-administrators, the page indicates only that the update is available.

Information and solutions access when a maintenance release update has not started

Components	Release information and solutions access
Platform	A banner appears on the **Solutions** page to indicate the availability of a platform update. The banner also shows the release version and a link to the associated release notes. All solutions are accessible as long as the update has not started.
Solutions	The **Solutions** page shows a banner that indicates the availability of one or more solutions updates. Solutions are accessible as long as the update process has not started. Only administrators see the options to: • Reset the Tanium manifest on page 113 URL to the default value. This option appears only if a user previously set the URL to a custom value in a non-air-gapped environment. Resetting the value might initiate the solutions update process and lock users out of all other pages until the update is complete. • Install a maintenance release update. The release availability banner includes a button to start the update. For the steps to reset the manifest URL, compare updates, and install an update, see Install a Tanium release update on page 128.

INSTALLATION IN PROGRESS

The following tables describe the information displayed and the accessibility of Tanium solutions while installation is in progress for a Tanium Information and solutions access when a semiannual release is in progress on page 117 or Information and solutions access when a maintenance release update is in progress on page 118.

Information and solutions access when a semiannual release is in progress

Components	Release information and solutions access
Platform	No users can access solutions while a platform update is in progress.
Solutions	While the solutions update is in progress, users can see only the **Semiannual Update** page. For the administrator who started the update, the page shows the update progress. For other users, the page shows a banner that indicates solutions are unavailable until the update completes.

© 2026 Tanium Inc. All Rights Reserved

Information and solutions access when a maintenance release update is in progress

Components	Release information and solutions access
Platform	No users can access solutions while a platform update is in progress.
Solutions	While the solutions update is in progress, users can see only the **Maintenance Release Update** page. For the administrator who started the update, the page shows the update progress. For all other users, the page shows a banner that indicates solutions are unavailable until the update completes.

INSTALLATION COMPLETED

The following tables describe the information displayed and the accessibility of Tanium solutions after you finish installing a Tanium Information and solutions access when a semiannual release is complete on page 118 or Information and solutions access when a maintenance release update is complete on page 118.

Information and solutions access when a semiannual release is complete

Components	Release information and solutions access
Platform	When the platform update finishes, users can see only the **Semiannual Update** page. An administrator must then initiate the solutions update.
Solutions	After the solutions update finishes, the **Semiannual Update** page shows the release **Availability Date**, **Installed Date**, and **Version** to the administrator who initiated the update. That administrator can then click **Close** to dismiss the banner and resume using solutions. All other users can resume using solutions immediately after the solutions update finishes.

Information and solutions access when a maintenance release update is complete

Components	Release information and solutions access
Platform	After the platform updates finish, Console stops showing the banner that indicates the update is available. If a solutions update is available but not installed, the **Solutions** page still shows a banner for that update.
Solutions	After a solution update finishes, the **Maintenance Release Update** page shows the release **Availability Date**, **Installed Date**, and **Version** to the administrator who initiated the update. That administrator can then click **Close** to dismiss the banner and resume using solutions. All other users can resume using solutions immediately after the solutions update finishes. If a platform update is available but not installed, the **Solutions** page still shows a banner for that update.

Modules

Modules overview

Each Tanium module comprises a *workbench* and content. A workbench is the user interface that you use to perform module operations. For example, the Tanium Comply workbench includes an **Assessments** page for monitoring the status of assessments, which evaluate endpoints for security configuration exposures and software vulnerabilities. In terms of content, the module includes **Comply - Run Assessment** packages for running the assessments.

© 2026 Tanium Inc. All Rights Reserved

For more information about the operations that you can perform through a specific module, see the corresponding user guide at Tanium Resource Center: Product Modules.

View and manage modules

In the Main menu of Console, use the **Modules** menu to navigate the pages of module workbenches.

On the **Solutions** page, the **Modules** section shows a tile for each installed module. Each tile provides the following information and options:

- Currently installed module version (if any).
- Installation state, which can be `Installed`, `Not Installed`, `Available to Purchase`, `New Version Available`, or an error condition.

  TIP Hover over the message icon to see details about the versions to which you can update the module.

- Buttons for performing module operations, such as importing. For more information, see Solutions page buttons on page 110.

NOTE Contact Tanium Support if the **Solutions** page does not show tiles for certain modules or if a tile indicates the module is **Available for Purchase** and you want to add it to your Tanium license. For more information, see Contact Tanium Support on page 724.

Use the following widgets in the **Modules** section to filter the tiles:

- **Filter by module name**: Enter all or part of a module name to show only the tiles that match your entry.
- **Show**: Select **Available Updates** to show only the tiles of modules with pending updates or select **All** modules to show all the tiles. To update modules, see Install a Tanium release update on page 128.

NOTE The Tanium Console User Interface (UI) is also a module that you update when you install a semiannual or maintenance release update. However, the **Modules** section does not show a tile for the Console UI.

Shared services

Shared services overview

Each Tanium shared service includes a workbench and content that you use to enable or facilitate operations in other Tanium solutions. For example, you use the Tanium Direct Connect shared service to designate certain endpoints as satellites. The Tanium Comply and Tanium Discover modules can then run satellite scans for unmanaged endpoints.

© 2026 Tanium Inc. All Rights Reserved

For more information about the operations that you can perform through a specific shared service, see the corresponding user guide in the Tanium Resource Center

View and manage shared services

In the Main menu of Console, use the **Shared Services** menu to access the shared service workbenches.

On the **Solutions** page, the **Content** grid shows a row for each shared service (and each content-only solution) and shows various columns of information about the services. To filter the grid, see Content grid filters on page 109. To export or perform other operations for shared services, select the services in the grid and use the buttons described in Solutions page buttons on page 110.

TIP

The **Latest Version** column shows a message icon when newer versions are available for a solution. Hover over the icon to see details about the versions.

Content-only solutions

Overview of content-only solutions

Some Tanium solutions provide only content and have no workbench or service. The content enables users to perform certain operations through Tanium modules and shared services. For example, the Default Content solution provides utilities that enable users to deploy an action for changing Tanium Client settings on endpoints.

To see documentation for content-only solutions, see Tanium Core Content Documentation.

Default imports

After the Tanium Server is installed, it automatically imports the content-only solutions Default Content and Default Computer Groups (see Content-only solutions on page 48) when the first user signs in to Tanium Console. If you perform the **Tanium Recommended Installation** (see Import all modules and services on page 123), the Server automatically imports several more basic content-only solutions, but you must manually import any other content-only solutions (see Import or update specific solutions on page 125).

View and manage content-only solutions

On the **Solutions** page, the **Content** grid shows a row for each content-only solution (and each shared service) and shows various columns of information about the solutions. If your deployment uses a Tanium production license, only **Manifest** content is available. For more information, see Tanium manifest on page 113. If you specified a Tanium lab license when installing the Tanium Server, you can also see **Labs** content.

The **Content** grid shows a blank **Imported Version** for solutions that are not yet imported. If the **Imported Version** lags the **Available Version** for a solution, one or more updates are available. Tanium provides updates for content-only solutions only through semiannual and maintenance release updates, with the exceptions described in Import or update specific solutions on page 125. You must install the updates as a bundle in a single operation, as described in Install a Tanium release update on page 128.

© 2026 Tanium Inc. All Rights Reserved

To import or perform other operations for content-only solutions, select them in the grid and use the buttons described in Solutions page buttons on page 110. To filter the **Content** grid, see Content grid filters on page 109.

Imports and updates in active-active deployments

In a deployment with active-active Tanium Servers, the following features reduce the number of manual steps required to manage solutions:

- **Module synchronization**

  Peer Tanium Servers synchronize module operations, which include imports, re-imports, updates, and uninstallations. For example, if you manually import the Tanium™ Comply module on one Server, the peer imports Comply automatically.

- **Shared content**

  Shared services and content-only solutions that you import or update on any single Tanium Server are available in the peer because the Servers store content on the shared Tanium database. For example, if you manually import the Tanium™ Zero Trust shared service on one Server, you can also access that service on the peer.

BEST PRACTICE

Before importing solutions, replace the self-signed certificates on the Tanium Servers with certificates that a certificate authority (CA) has signed if you have not already done that. For the steps to replace certificates, see Securing Console and API access through certificates on page 220.

For more information about managing modules and certificates in an active-active deployment, see Tanium Server synchronization on page 141.

For more information about active-active deployments, see:

- Tanium Appliance Deployment Guide
- Tanium Core Platform User Guide for Windows Deployments: Tanium Server

Tools deployment and restricted targeting

If you select default configuration when importing modules and shared services, the ones that employ tools on managed endpoints create their own action groups and automatically deploy the tools to those groups. By default, those action groups target the **All Computers** filter group. However, you can set the **No Computers** computer group as the target by enabling the *restricted targeting* option. This option enables you to control tools deployment by preventing automatic deployment. For example, you might want to test Tanium™ Comply tools on a subset of endpoints before deploying the tools to all endpoints. In this case, you can manually deploy the tools to an action group that you configured to target only the subset. For more information, see Targeting actions through action groups on page 400.

To enable or disable restricted targeting:

1. Sign in to Tanium Console as a user who is assigned a role with the **Global Settings write** permission.
2. From the Main menu, go to **Administration > Configuration > Settings > Platform Settings**.
3. Set **Restricted Targeting** to **ON** (enable) or **OFF** (disable) and click **Save All**.

© 2026 Tanium Inc. All Rights Reserved

NOTE

After you enable or disable restricted targeting, the updated setting applies only to solutions that are subsequently imported, not to solutions that are already imported.

Dependencies and default settings

Some Tanium solutions cannot function unless you import dependent solutions. Tanium Console shows a warning if a solution is installed without its dependent solutions, and the warning lists the dependencies. Certain solutions support the automatic import of dependencies. For example, when you import Tanium Benchmark by itself, the Tanium Server automatically imports all the dependencies of Benchmark . To see a list of the dependencies for a solution and to see if it supports automatically importing them, click a link in the following table to go to the corresponding user guide. The user guides also list the default settings that are configured if you use the **Tanium Recommended Installation** button to import solutions.

Solution-specific settings and dependencies

Solution	Dependencies	Default Settings
Asset	Solution dependencies	Import and configure Asset with default settings
Automate	No solution dependencies	No default settings are configured for Automate.
Benchmark	Solution dependencies	Import Benchmark with default settings
Certificate Manager	Solution dependencies	Import Certificate Manager with default settings
Client Management	Solution dependencies	Import and configure Client Management with default settings
Cloud Workloads	Solution dependencies	
Comply	Solution dependencies	Import and configure Comply with default settings
Connect	Solution dependencies	Import and configure Connect with default settings
Criticality	Solution dependencies	Import Criticality with default settings
Deploy	Solution dependencies	Import and configure Deploy with default settings
Direct Connect	Solution dependencies	Import and configure Direct Connect with default settings
Directory Query	Solution dependencies	Configure satellite settings
Discover	Solution dependencies	Import and configure Discover with default settings
Endpoint Configuration	Solution dependencies	Import and configure Endpoint Configuration with default settings
End-User Notifications	Solution dependencies	Import and configure End-User Notifications with default settings
Enforce	Solution dependencies	Import and configure Enforce with default settings

© 2026 Tanium Inc. All Rights Reserved

Solution-specific settings and dependencies (continued)

Solution	Dependencies	Default Settings
Engage	Solution dependencies	Configuring Engage
Gateway	Solution dependencies	No default settings are configured for Gateway.
Guide	No solution dependencies	No default settings are configured for Guide.
Health Check	No solution dependencies	Import and configure Health Check with default settings
Impact	Solution dependencies	Import and configure Impact with default settings
Integrations Gallery	No solution dependencies	No default settings are configured for Integrations Gallery.
Integrity Monitor	Solution dependencies	Import and configure Integrity Monitor with default settings
Interact	Solution dependencies	Import and configure Interact with default settings
Investigate	Solution dependencies	Import Investigate with default settings
Jump Gate	Solution dependencies	Import Jump Gate with default settings
Patch	Solution dependencies	Import and configure Patch with default settings
Performance	Solution dependencies	Import and configure Performance with default settings
Provision	Solution dependencies	Installing Provision
Reporting	Solution dependencies	Import Reporting
Reputation	Solution dependencies	Import and configure Reputation with default settings
Reveal	Solution dependencies	Import and configure Reveal with default settings
Threat Response	Solution dependencies	Import and configure Threat Response with default settings
Trends	Solution dependencies	Import and configure Trends with default settings
Zero Trust	Solution dependencies	No default settings are configured for Zero Trust.

Import all modules and services

After you install the Tanium Server and sign in to Tanium Console for the first time, the **Solutions** page opens and shows a **Tanium Recommended Installation** button. To initiate the workflow for importing and configuring all your licensed modules and shared services in a single operation, you must click that button instead of selecting tiles in the **Modules** section or rows in the **Contents** grid. The import process automatically imports the latest solution versions. The latest versions include all the features in the current semiannual release and all the fixes that are available in the current maintenance release update. The **Tanium Recommended Installation** workflow also imports certain content-only solutions and configures default settings.

© 2026 Tanium Inc. All Rights Reserved

NOTE

After you finish the workflow, the **Solutions** page stops showing the **Tanium Recommended Installation** button. To update solutions, see Install a Tanium release update on page 128.

Default settings and content imports

The Tanium Server performs the following operations during the **Tanium Recommended Installation** workflow:

1. Imports the following content-only solutions:
   - **Client Maintenance**
   - **Core Content**
   - **Core Content - MSSQL**
   - **Initial Content - Python**
2. Imports the modules and shared services, and configures them with default settings. For more information, see Dependencies and default settings on page 122.
   The default settings including setting the service account for every solution to the user account that you use to perform the import. For more information, see Manage service accounts for solutions on page 144.
3. Sets the **Default - All Computers** action group as the target for all scheduled actions that previously targeted the **Default** action group. **Default - All Computers** specifies the **All Computers** computer group, whereas **Default** specifies the **No Computers** computer group. Five minutes after re-targeting the actions, the Tanium Server deploys them to **Default - All Computers** as a one-time event. The Server bases future deployments of the actions on their configured reissue interval. For more information, see Manage scheduled actions on page 342. If automatically deploying actions to the **Default - All Computers** action group is not appropriate for your deployment, enable restricted targeting before importing solutions. For more information, see Tools deployment and restricted targeting on page 121.

Before you begin

- Read the release notes for your licensed modules and shared services.
- (Best practice) Before importing modules in an active-active deployment, replace the self-signed certificates on the Tanium Servers with certificates that a certificate authority (CA) has signed if you have not already done that. For more information, see Tanium Server synchronization on page 141.
- (Optional) To avoid automatically deploying solution-specific tools to the **All Computers** filter group during automatic configuration, see Tools deployment and restricted targeting on page 121.

© 2026 Tanium Inc. All Rights Reserved

Import all solutions

1. Access Tanium Console by entering the fully qualified domain name (FQDN) of the Tanium Server in the browser URL field (`https://ts1.example.com`, for example).

   NOTE

   In an active-active deployment, Tanium Servers automatically synchronize module operations only if you specify the FQDN, not the IP address, and use the default port. In a Windows deployment, the default port is 443. In a Tanium Appliance deployment, the default port is 8443 but you can also use 443.

2. From the Main menu, go to **Administration > Configuration > Solutions** and click **Tanium Recommended Installation**.
   Tanium Console shows the progress of the import and configuration.

3. Click **Close** when Console indicates that the import and configuration succeeded.
   After you finish the operation, the Main menu shows the imported items under **Modules** and **Shared Services**.

Import or update specific solutions

When you first import solutions for a new Tanium deployment, you can import a subset of the solutions that your Tanium license includes instead of importing all of them.

BEST PRACTICE

For a new Tanium deployment, perform the **Tanium Recommended Installation** workflow to import all modules and shared services in a single operation (see Import all modules and services on page 123) because some cannot function unless you import dependent modules and shared services. For more information, see Dependencies and default settings on page 122.

You must install solution updates for any Tanium release as a bundle in a single operation (see Install a Tanium release update on page 128) that applies to all the currently installed solutions with the exceptions described in Labs content on page 126 and Tanium Emerging Issues Content on page 126. The bundle update automatically excludes solutions that are in your Tanium license but are not yet installed. You can use the same workflow (Import, re-import, or update solutions on page 126) to import solutions that are not yet installed and to update Emerging Issues Content or **Labs** content.

Solution versions

The import and re-import processes automatically import the solution versions that are associated with the currently installed Tanium semiannual release and maintenance release update. To import or re-import solution versions from another release, you must first install that release, as described in Install a Tanium release update on page 128.

IMPORTANT

After you import, re-import, or update solutions, you cannot downgrade them to earlier versions.

© 2026 Tanium Inc. All Rights Reserved

Labs content

The **Solutions** page lists **Labs** content only if your deployment uses a Tanium lab license instead of a production license. You can import, re-import, or update **Labs** content at any time. For more information about **Labs** content, see Content-only solutions on page 120.

Tanium Emerging Issues Content

Emerging Issues Content is a content-only solution that provides Guardian notifications and Tanium Reporting dashboards. For more information about the content that this solution provides, see Tanium Reporting User Guide: Emerging issue dashboards. For more information about Guardian notifications, see the Tanium Guide User Guide.

Updates to Emerging Issues Content can become available as part of a Tanium release (semiannual or maintenance release update) or between Tanium releases. For updates in a Tanium release, you update Emerging Issues Content as a bundle with other solutions, as described in Install a Tanium release update on page 128. For updates between Tanium releases, you can update Emerging Issues Content independently from other solutions, as described in Import, re-import, or update solutions on page 126.

Before you begin

Before you import, re-import, or update solutions:

- Read the release notes for each solution.
- (Best practice) In an active-active deployment, replace the self-signed certificates on the Tanium Servers with CA certificates if you have not already done that. For more information, see Tanium Server synchronization on page 141.
- Review solution dependencies. Certain Tanium solutions support the automatic import of dependencies. For example, when you import Tanium Benchmark, the Tanium Server automatically imports all the dependencies of Benchmark regardless of whether you select those dependencies for the import. For more information, see Dependencies and default settings on page 122.
- (Optional) To avoid automatically deploying solution-specific tools to the **All Computers** filter group, see Tools deployment and restricted targeting on page 121.

Import, re-import, or update solutions

You can combine imports, re-imports, and updates in a single operation. After you initiate an operation, it must finish before you can start another operation.

© 2026 Tanium Inc. All Rights Reserved

1. (Updates or re-imports only) Notify Tanium users not to use the modules or services that you are updating or re-importing until the update or re-import process finishes. Otherwise, users might lose work in progress.
2. Access Tanium Console by entering the fully qualified domain name (FQDN) of the Tanium Server in the browser URL field (`https://ts1.example.com`, for example).

   > **NOTE** In an active-active deployment, Tanium Servers automatically synchronize module operations only if you specify the FQDN, not the IP address, and use the default port. In a Windows deployment, the default port is 443. In an Appliance deployment, the default port is 8443 but you can also use 443.

3. From the Main menu, go to **Administration > Configuration > Solutions**.
4. In the **Modules** section, select the checkbox in the tile of each module to import.
5. In the **Content** section, select the shared services and content-only solutions to import. You can also select **Labs** content or Emerging Issues Content to update or re-import.
6. Click an action button (**Import**, **Re-import**, or **Update**) based on which solution types to include in the operation:
   - **All solution types**: To perform the operation for all the modules, services, and service packs that you selected, click the action button in the **Solutions** page footer.
   - **Modules**: To perform the operation only for selected modules, click the action button in the header of the **Modules** section. To perform the operation only for a single module, you can also click the action button in the module tile.
   - **Services and content-only solutions**: To perform the operation only for selected services and content-only solutions, click the action button in the header of the **Content** section.
7. (Fresh imports only) Optionally, clear **Apply All Tanium recommended configurations** for any modules or services that you want to configure manually instead of using the default settings:
   - **Manually configure all the listed solutions**: Deselect the checkbox above the list of solutions.
   - **Manually configure specific solutions**: Expand the solution entry and deselect the checkbox below its list of content.
8. Expand each solution, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts on page 135.
9. (Optional) To overwrite user-modified content set assignments with the default Tanium-defined assignments for objects that are imported with a solution, expand the solution entry and select **Include content set overwrite**. By default, the checkbox is clear and the Tanium Server preserves the existing content set assignments.
10. Click **Begin Import**.

    Tanium Console shows the progress of the operation.

    If you selected **Apply All Tanium recommended configurations** for any imports, click **Close** when Console indicates that the operation succeeded. Otherwise, the page automatically refreshes when the operation finishes. The Main menu then shows imported modules in the **Modules** menu and imported services in the **Shared Services** menu.

© 2026 Tanium Inc. All Rights Reserved

11. (Updates only) If the release notes for the updated solutions list changes to the Tanium™ Trends data, panels, or sources, perform the steps under Tanium Trends User Guide: Importing the initial gallery to re-import them.

12. (Updates only) From the Main menu, go to **Administration > Actions > Scheduled Actions** and set the **Source Package** filter to **Has Updates**. If the grid lists actions with that filter applied, it means the solutions that you updated include package updates. Update the affected actions as described in Update action packages on page 347.

Install a Tanium release update

Tanium provides new features, enhancements, security fixes, and patch updates for Tanium solutions and Tanium-managed content through Tanium releases on page 111. You install (import) the release as a bundle in a single operation that applies to all the currently installed solutions except **Labs** content. For the steps to update **Labs** content or install new solutions, see Import or update specific solutions on page 125.

When a new maintenance release update becomes available, Tanium Console provides the option to install that new update or any update that you skipped since you last installed an update. For more information, see Maintenance release updates on page 112.



After you install a release, you cannot downgrade solutions to versions that are earlier than the release versions. If the version of a currently installed solution is later than the version in a Tanium release bundle, the installation process skips that solution.

Solution dependencies in a release

If the release includes a solution version that requires other solutions, the other solutions are *dependencies*. The release installation process includes or excludes dependencies based on the following conditions.

- If the release contains an update for a solution that is already installed, the installation process includes dependencies of the solution if those dependencies are not already installed.
- If the release contains an update for a solution that is not already installed, the installation process excludes both the solution and its dependencies.
- If the release contains an update for a solution that is not already installed and is not a dependency, the installation process excludes that solution.

For more information, see Dependencies and default settings on page 122.

Before you begin

1. Read the release notes for the Tanium release. When a new release becomes available, you can see a link to the release notes in the banner that appears on the **Solutions** page and (for semiannual releases only) on the Tanium **Home** page.

   The banners appear only if your Tanium Core Platform servers are at version 7.6 or later.

© 2026 Tanium Inc. All Rights Reserved

2. Review Updating an existing deployment on page 114 to understand:

    - The order for installing prerequisite updates to other Tanium components.

      BEST PRACTICE

      If your Tanium Core Platform servers are at version 7.5 or earlier, Tanium strongly recommends that you update to the latest available versions of your installed solutions before updating to servers version 7.6 or later. For more information, see Import or update specific solutions on page 125. The best practice is to update your lab deployment (if you have one) before the production deployment. For more information, see Tip 3: Update the lab deployment first on page 137.

    - The timing for notifying Tanium users that solutions are unavailable during the update process.

3. Review Tanium solutions and content updates on page 115 to understand how release updates affect existing content (such as sensors or packages). The update process overwrites all Tanium-managed content. You can clone Tanium-managed content that users have customized if you want to preserve the customizations. For more information, see Managing content on page 419.

4. Verify that you have recent restore points and backups in case something goes wrong. For more information, see Tip 2: Verify restore points on page 137.

5. If you have a non-air-gapped Tanium environment that uses a custom Tanium manifest on page 113 URL, decide whether to continue managing the URL manually or revert the URL to Tanium management. Before you start a solutions update, you can click **Reset Manifest URL** to revert the URL to Tanium management if that is your preference. This option does not apply to air-gapped environments, which always require a custom URL.

6. (Best practice) In an active-active deployment, replace the self-signed certificates on the Tanium Servers with certificates that a CA has signed if you have not already done that. For more information, see Tanium Server synchronization on page 141.

Install the update

NOTE

For details about the information that Console shows for an update and details about solutions access during the update process, see Release status on page 116.

1. Access Tanium Console by entering the fully qualified domain name (FQDN) of the Tanium Server in the browser URL field (`https://ts1.example.com`, for example).

   NOTE

   In an active-active deployment, Tanium Servers automatically synchronize module operations only if you specify the FQDN, not the IP address, and use the default port. In a Windows deployment, the default port is 443. In a Tanium Appliance deployment, the default port is 8443 but you can also use 443.

© 2026 Tanium Inc. All Rights Reserved

2. (Optional) If a banner indicates that the Tanium manifest on page 113 URL has a custom value, click **Reset Manifest URL** to set the URL to the default value. Thereafter, Tanium manages the URL and you do not have to update it for future releases.

   IMPORTANT

   Resetting the manifest URL might automatically initiate the solutions update process and lock all users out of Tanium solutions until you complete the update workflow.

3. (Maintenance releases only) From the Main menu, go to **Administration > Configuration > Solutions**.

   NOTE

   If you are installing a semiannual release for which only one maintenance release is available, the **Semiannual Update** page opens automatically.

4. (Maintenance releases only) In the **Solutions** page banner, click the button to start the maintenance release review and installation process.
5. If multiple maintenance release updates are available, select an update in the dropdown list to compare the solution versions in that update to the versions that are currently installed. If only one update is available, skip this step.
6. Review the list of solutions that the release will update.
7. (Optional) Expand any solution in the **Module Updates** or **Content Updates** grids to see configuration and content details about the solution version that is in the update.
8. (Optional) Click **Release Notes** to see the release notes for the update.
9. (Optional) Clear **Apply recommended Tanium configurations to the installation of new solutions** if you plan to manually configure solutions instead of using the default settings. This option applies only to dependent solutions (dependencies) that are not already installed. The option does not appear if the update has no such dependencies. For more information, see Dependencies and default settings on page 122.
10. Click **Start Import** to begin the update.

    Console shows the progress of the operation. When the update successfully completes or stops because of errors, Console shows a banner to indicate the update status:

    - **Success**: Users can resume using solutions. Proceed to the next step.
    - **Failure**: Perform the steps in Troubleshoot release update issues on page 131 and then return to this step.

11. Update Tanium Clients and endpoint tools. For more information, see Tanium Endpoint Configuration User Guide: Managing Tanium Client and endpoint tool upgrade rollouts.
12. If the release notes for the updated solutions list changes to Tanium Trends data, panels, or sources, re-import them as described in Tanium Trends User Guide: Importing the initial gallery.
13. From the Main menu, go to **Administration > Actions > Scheduled Actions** and set the **Source Package** filter to **Has Updates**. If the grid lists actions with that filter applied, it means the solutions that you updated include package updates. Update the affected actions as described in Update action packages on page 347.

© 2026 Tanium Inc. All Rights Reserved

Troubleshoot release update issues

ERROR MESSAGES FOR UPDATES

If errors occur while you install a Tanium release, Tanium Console shows a banner that indicates additional update attempts are required before users can resume using solutions. The banner indicates which solutions have errors and any solutions that the update process skipped because they depend on the solutions with errors. For more information, see Resolve update errors on page 131.

The banner with update error messages appears only to the administrator who initiates the update and reattempts it in the same Console session. In the following cases, the banner shows only that the release is available instead of showing the errors that block the update. All administrators (users with the **Administrator** reserved role) can still click **Start Import** to reattempt the update. Non-administrators do not see the **Start Import** button.

- The administrator who initiated the update ends the current session and starts a new session before reattempting the update.
- The administrator who initiated the update refreshes the page before reattempting the update.
- Other administrators and non-administrators start a session while errors still block the update.

RESOLVE UPDATE ERRORS

1. **Close** the banner that shows the errors and click **Start Import** to reattempt the update.

   When you reattempt an update, the Tanium Server preserves your original choice for the **Apply recommended Tanium configurations to the installation of new solutions** option and you cannot change it. If the Server performed a fresh installation of dependencies but failed to configure them and you then abort the update due to errors, the Server uninstalls those dependencies and excludes them from subsequent attempts to install the update.

2. Perform one of the following steps based on the state of the update after your reattempt:

   - **Success** :

     Return to the last step that you completed under Install the update on page 129 before you began troubleshooting.

   - **Failure with errors in the same solutions as the previous attempt** :

     Close the error banner and click **Start Import** to reattempt the update.

     After you perform two reattempts for any particular solution, the page provides an option to exit the update process. Exiting enables users to resume using solutions in a degraded state. Console shows a banner to notify users of the degraded state until you resolve the errors and successfully complete the update.

     Contact Tanium Support on page 724 for help if reattempting the update does not resolve the errors. If Tanium Support provides a solution as an XML file to resolve errors, import the file as described in Import content files on page 134 and then reattempt the update.

© 2026 Tanium Inc. All Rights Reserved

- **Failure with errors in solutions that differ from the previous attempt** :

  Close the error banner and click **Start Import** to reattempt the update until it encounters one of the preceding states. Perform the task that is described for those states.

Export and import specific solution versions through URLs

IMPORTANT

Do not import a Tanium solution from another Tanium Server without guidance from Tanium Support. Any solution that you import without such guidance is unsupported.

You cannot downgrade solutions by importing from a URL.

For each solution, you can export a URL for the version that is currently installed on the Tanium Server. You can then sign in to Tanium Console on another Server and import that version from the URL. This option is useful for migrating a version other than the latest between Servers. For example, after testing a specific module version in your lab environment, you can export the URL for that version and then import the module from that URL into your production deployment.

Before you begin

- Read the release notes for the solution versions.
- (Best practice) In an active-active deployment, replace the self-signed certificates on the Tanium Servers with certificates that a CA has signed if you have not already done that. For more information, see Tanium Server synchronization on page 141.

Export a solution as a URL

1. Sign in to Tanium Console on the Tanium Server that already has the desired solution version.
2. From the Main menu, go to **Administration > Configuration > Solutions**.
3. In the **Modules** or **Content** section, click Copy URL in the tile or row of the solution that you want to export.

   TIP

   If you do not want to import the solution immediately, paste the URL into a text file to store it for later.

© 2026 Tanium Inc. All Rights Reserved

Import a solution from a URL

1. If you will replace an existing version of a module or service with another version, notify Tanium users not to use that module or service until the import process finishes. Otherwise, users might lose work in progress.
2. Sign in to Tanium Console on the Tanium Server where you want to import the solution. When you access Console, enter the FQDN of the Server in the browser URL field (`https://ts1.example.com`, for example).

   > **NOTE** In an active-active deployment, Tanium Servers automatically synchronize module operations only if you specify the FQDN, not the IP address, and use the default port. In a Windows deployment, the default port is 443. In an Appliance deployment, the default port is 8443 but you can also use 443.

3. Go to the **Content** section, select **Import > Import URL**, paste the URL in the **Import URL** field, and click **Import**.
4. Expand the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts on page 135.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, the **Include content set overwrite** checkbox is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Import** to proceed with the import.

Export content files

Export content in the format required for your workflow:

- **JSON**

  A JSON file contains the configurations of content objects. Exporting configurations is useful if you want to import them into another Tanium environment. For example, you might test custom sensors in a lab environment to ensure that they work as intended before importing the sensors into your production environment. You must be assigned a role with the **Export Content** permission to export a JSON file. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.

- **CSV**

  A CSV file contains all the attributes of content objects that you see in various grids in Tanium Console. For example, if you export in CSV format from the **Sensors** page, the CSV file contains all the sensor attributes (columns) that you see in the grid on that page. CSV exports are useful for reviewing content attributes in applications that support CSV. For example, you can use Microsoft Excel to create charts based on sensor attributes.

The steps to export content, and the supported file formats, vary by content type:

- Export and import specific solution versions through URLs on page 132
- Export action groups on page 402
- Export actions on page 347
- Export allowed URLs on page 170

© 2026 Tanium Inc. All Rights Reserved

- Export categories, dashboards, or questions on page 471
- Export computer groups on page 621
- Export content sets on page 566
- Export filter groups on page 478
- Export packages on page 451
- Export persona details on page 664
- Export roles on page 607
- Export saved questions on page 472
- Export sensors on page 430
- Export quarantined sensor details on page 436
- Export user group details on page 653
- Export user details on page 639

Import content files

A content file contains the configurations of content objects. Importing is useful if you want to copy content from another Tanium environment. For example, you might test custom sensors in a lab environment to ensure that they work as intended. You can then export the sensors from the lab environment and import them into your production environment.



Do not import a Tanium solution as a file without guidance from Tanium Support. Any solution that you import without such guidance is unsupported.

Tanium Support might provide a solution file to help you troubleshoot installation of a Tanium release. You can update solutions through file imports but you cannot downgrade solutions through any means.

You must be assigned a role with **Import Signed Content** permission to import content files through the following steps:

1. (Non-Tanium-provided content only) Digitally sign the content file and ensure a public key is in place to validate the signature. For more information, see Authenticating content files on page 482.



You do not have to generate keys or signatures for Tanium-provided solutions. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process.

If you plan to import a file that another user signed, you can first perform an integrity check on the file. For more information, see Verify content file signatures on page 487.

© 2026 Tanium Inc. All Rights Reserved

2. From the Main menu, go to any of the following **Administration** pages:
    - **Configuration > Solutions**
    - **Permissions > Filter Groups**
    - Under **Content**, select **Sensors**, **Packages**, or **Saved Questions**
    - Under **Actions**, select **Scheduled Actions**, **All Pending Approvals**, or **Actions I Can Approve**
3. Select an **Import** option based on the source of the content:
    - **Import > Import Files**: Perform one of the following steps to select one or more files:
        - Drag and drop files from your file explorer.
        - Click **Browse for File**, select the files, and click **Open**.
    - **Import > Import URL**: Enter the URL in the **Import URL** field, and click **Import**.
4. For each file, expand  the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts on page 135.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, **Include content set overwrite** is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Install**.
   Perform the next step only for imported packages that reference other files. You must manually download these files on the Tanium Server because the file that you imported contains only the package configurations, not associated files.
7. For each package that you imported, select the package, click **Status**, and click **Re-Download All** to download the referenced files.
   If the Tanium Server cannot access a file location, move the file to an accessible location, change the **File Address** in the package configuration (see Edit a package on page 450), and repeat this step.

Resolve import conflicts

When you import solution updates, or import a file that contains content (such as sensors), conflicts might occur with existing content. After you review the Best practices for resolving import conflicts on page 136, perform the following steps.



Import conflicts do not apply to updates in a Tanium release bundle. When you install a Tanium release bundle, it automatically overwrites any customizations to Tanium-managed content without the option to preserve customizations.

© 2026 Tanium Inc. All Rights Reserved

1. Perform the import workflow up to the point where Tanium Console lists the **New Items** and **Existing Items** to import:
   - **Modules, shared service, or content-only solutions**:
     - Import all modules and services on page 123
     - Import or update specific solutions on page 125
     - Export and import specific solution versions through URLs on page 132
   - **JSON/XML content file**: Import content files on page 134

2. Expand the items that you are importing and select a resolution for each conflict:
   - **Overwrite**: Replaces existing content with the imported content.
   - **Skip**: Skips the import for that item.
   - (Categories only) **Merge**: Unites objects that are included in the categories.

     BEST PRACTICE

     Select **Merge** and, after finishing the import, review the resulting configuration in the **Categories** panel on the Interact **Home** page.
   - (Actions only) **Overwrite and Disable Action**: This option is useful if you want the new action to be disabled by default. Later, when are ready to test the action, re-enable it: from the Main menu, go to **Administration > Actions > Scheduled Actions**, select the action, and select **More > Enable Action(s)**.

   BEST PRACTICE

   The solution or content file might include content set definitions. When you first establish your content sets, selecting **Include content set overwrite** ensures that content is assigned to the content sets that the content designer intended. After you implement your own role-based access control (RBAC) plan and move content to the content sets that you plan to use, do not select this option. Otherwise, the assignments defined in the imported file overwrite your content set assignment.

3. Click **Begin Import**. When the operation finishes, click **Close**.
4. (Updates only) If the release notes for the updated solutions list changes to the Tanium Trends data, panels, or sources, perform the steps under Tanium Trends User Guide: Importing the initial gallery to reimport them.

Best practices for resolving import conflicts

The following tips can inform your decisions regarding conflicts that might occur with existing content when you import new content.

© 2026 Tanium Inc. All Rights Reserved

Tip 1: Read release notes

Always read the release notes for every solution version that was released since your last update. The release notes alert you to the scope of changes and might include notes that can help you avoid issues. Release notes also indicate the release date, which is important if you plan to import multiple content-only solutions. Different content-only solutions might include updates to the same basic sensors or packages. In this case, it is best to import the older content-only solutions before the newer ones.

Tip 2: Verify restore points

Before you update Tanium solutions, verify that you have recent restore points and backups in case something goes wrong. The Tanium database stores content configuration objects. The installation folders for the Tanium Server and Tanium Module Server include important files, such as encryption keys, a license file, string files, and other data files.

As a best practice, schedule regular file system and database backups based on your Tanium infrastructure:

- **Tanium Appliance**: For more information, see Tanium Appliance User Guide: Backing up and recovering Tanium Appliances.
- **Windows**: For more information, see Tanium Core Platform User Guide for Windows Deployments: Back up Tanium Core Platform servers and databases.

Tip 3: Update the lab deployment first

Before you update Tanium Core Platform servers and solutions in your production environment, always update them in your lab first and perform the following tasks to evaluate how changes might affect endpoints:

- **Assess network utilization**: Assess the impact on network utilization when the Tanium Server distributes content to endpoints. For certain content types, an update might result in additional network traffic. Usually, this additional traffic is negligible.
- **Test functionality changes**: Test the changes or additions to Tanium functionality if a content update includes:
    - **Sensors**: Issue dynamic questions that use the sensors and review the results: see Issue a free-form question on page 241 or Issue a question through the Question Builder on page 245 and see Part 7: Analyzing question results in Console and Interact on page 255.
    - **Saved questions**: Issue the saved questions and review the results: see Issue a saved question on page 466.
    - **Dashboards**: Issue the dashboards and review the results: see Issue a dashboard of saved questions on page 467.
    - **Categories**: Review the categories: see Manage categories and dashboards on page 469.
    - **Packages**: Deploy the packages through actions: see Deploying actions and playbooks in Console and Interact on page 391.
    - **Scheduled actions**: Assign the correct action groups to the actions: see Edit action group assignments for scheduled actions on page 402.

After you qualify the updates on lab servers, import the updates on production servers and spot test the behavior of new or changed content.

© 2026 Tanium Inc. All Rights Reserved

Tip 4: Limit customizations to Tanium content

When you import Tanium updates, the configuration specified in the import overwrites the current configuration. In almost every case, overwriting is preferable to maintaining the current configuration because the updates include important changes that optimize performance, avoid issues, and make the associated tools more useful.

Limit customizations to Tanium content so that updates are minimally disruptive. Maintain notes of any changes you make. For example, record any changes to the **Max Sensor Age** setting, a package timeout, or a saved question reissue interval. Record a list of Tanium objects that you clone as a source for your custom objects. Recording these details enables you to redo customizations that the import overwrote. For the procedures to clone content, see Custom content development on page 418.

Tip 5: Recreate content that uses parameterized sensors or packages

When a content import overwrites a parameterized sensor or parameterized package, note the impact on existing saved questions, computer groups, and scheduled actions that reference the sensor or package:

- Questions with parameterized sensors on page 238
- Dynamic membership on page 614 (for computer groups with sensor-based membership)
- Scheduled action with parameterized package on page 443

Tip 6: Avoid bulk overwrites to Tanium content

Do not simply export the current configuration and then reimport it after the content update finishes. This practice overwrites the sensor code with old versions and often has unexpected consequences. For example, a Tanium content-only solution includes a scheduled action to distribute patch tools when the patch tools version, which the **Has Patch Tools** sensor reports, does not match a particular value. If the package that provides the patch tools and updates the version uses a different version than the **Has Patch Tools** sensor expects, the Tanium Server continuously distributes the patch tools until the **Has Patch Tools** sensor uses the correct version.

Uninstall solutions



Before performing these steps in an active-active deployment, replace the self-signed certificates on the Tanium Servers with CA certificates. For more information, see Tanium Server synchronization on page 141.



If Tanium removes a solution from the current Tanium manifest (as noted in the release notes), the **Uninstall** button is no longer available for that solution. In this case, uninstall the solution by importing the removal file that Tanium Support provides, as described in Import a solution from a URL on page 133. In an active-active deployment, import the removal file on each active Tanium Server and verify the result on each Tanium Server, for example by checking the **Solutions** page or the `workbenches.json` file.

© 2026 Tanium Inc. All Rights Reserved

1. Access Tanium Console by entering the FQDN of the Tanium Server in the browser URL field (`https://ts1.example.com`, for example).

   > **NOTE** In an active-active deployment, Tanium Servers automatically synchronize module operations only if you specify the FQDN, not the IP address, and use the default port. In a Windows deployment, the default port is 443. In an Appliance deployment, the default port is 8443 but you can also use 443.

2. From the Main menu, go to **Administration > Configuration > Solutions**.
3. (Deprecated solutions only) If a warning banner indicates that certain solutions are incompatible with the current Tanium Console version, click **Uninstall** in the banner to remove only those solutions. Uninstalling from the banner has no effect on other solutions that you select in the **Modules** or **Content** sections.
4. In the **Modules** section, select the checkbox in the tile of each module that you want to uninstall, or click **Select All** above the tiles.
5. In the **Content** section, select the services and content-only solutions that you want to uninstall.
6. Click an **Uninstall** button based on which solution types to include in the operation:
   - **All solution types**: To uninstall all the modules, services, and service packs that you selected, click **Uninstall** in the **Solutions** page footer.
   - **Modules**: To uninstall only the selected modules, click **Uninstall** in the header of the **Modules** section.
   - **Services and content-only solutions**: To uninstall only the selected services and content-only solutions, click **Uninstall** in the header of the **Content** section.

Completely uninstalling certain solutions requires additional steps. For example, to completely remove Tanium Comply from your Tanium deployment, you must remove Comply content and tools from endpoints. For more information about uninstalling specific solutions or Tanium Clients, see the user guides for those products:

- Tanium Client:
  - Tanium Client on Windows
  - Tanium Client on macOS
  - Tanium Client on Linux
  - Tanium Client on Solaris
  - Tanium Client on AIX
- Asset
- Automate
- Benchmark
- Certificate Manager
- Client Management

© 2026 Tanium Inc. All Rights Reserved

- Comply
- Connect
- Criticality
- Deploy
- Direct Connect
- Directory Query
- Discover
- Endpoint Configuration
- End-User Notifications
- Enforce
- Engage
- Gateway
- Guide
- Health Check
- Impact
- Integrations Gallery
- Integrity Monitor
- Interact
- Investigate
- Patch
- Performance
- Provision: Contact Tanium Support for the steps to uninstall Provision.
- Reporting
- Reputation
- Reveal
- Threat Response
- Trends
- Zero Trust

© 2026 Tanium Inc. All Rights Reserved

Tanium Server synchronization

If you deploy Tanium Servers in an active-active configuration, they automatically synchronize module operations to reduce the number of manual steps that you must perform to manage modules. The module operations include imports, re-imports, updates, and uninstallations. The Servers use digital certificates to authenticate to each other during synchronization. You might have to troubleshoot certificate issues or other issues to ensure synchronization works without disruption. The following table describes synchronization errors that might occur:

Tanium Server synchronization errors

Issue	Description and remediation
Certificate validation error	Your browser shows a certificate validation error when you try to sign in to Tanium Console. To resolve the error, see Manage certificates for Tanium Server synchronization on page 141.
Tanium Server settings	The **Solutions** page shows a message about an error that occurred when fetching Tanium Server settings from the peer Tanium Server. To resolve the error, ensure that the FQDNs for your Tanium Servers are accessible from any computer from which a user accesses Console. For more information specific to your Tanium infrastructure, see: • Tanium Appliance User Guide: Modify the host name • Tanium Core Platform User Guide for Windows Deployments: Installing the Tanium Server
Version disparity	The **Solutions** page shows a disparity between a module version installed on a Tanium Server and the version that is recorded in the Tanium database logs. The database and logs are shared between the Server peers. During a module operation, the module writes its workbench configuration to files on the Server where you perform the operation and adds an entry in the logs. To resolve version disparities, see Resolve Tanium Server synchronization errors on page 142.



In an active-active deployment, Tanium Servers automatically synchronize module operations only if you specify the FQDN (not the IP address) and use the default port when accessing Console. In a Windows deployment, the default port is 443. In an Appliance deployment, the default port is 8443 but you can also use 443.

Tanium Servers must have the same Tanium Core Platform version to support synchronization of module operations.

Manage certificates for Tanium Server synchronization

During Tanium Server synchronization, the browser on each Server must trust and access the peer Server. The Servers use their `SOAPServer.crt` certificates to establish that trust. If a CA signed the certificates, the Servers establish trust automatically. If the Servers use the self-signed certificates that they generated by default during installation, you must manually enable trust to avoid synchronization errors

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

To facilitate synchronization, replace the self-signed certificates with CA certificates before importing modules. For the steps to replace certificates, see Securing Console and API access through certificates on page 220.

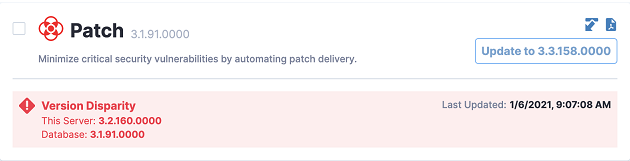
To prevent synchronization errors on Tanium Servers that use self-signed certificates:

1. Access Tanium Console on each Tanium Server and, when the browser shows a certificate validation error, select the option to ignore the error and proceed to the Server URL.
   This action enables the Servers to trust each other for the duration of the current browser session.
2. Complete the module operations (imports, updates, or uninstallations) within the current browser session.
   If the session times out during an operation, automatic synchronization fails and you must repeat the first step to re-enable trust.

Resolve Tanium Server synchronization errors

Module operations might succeed on one Tanium Server but fail to synchronize on the peer Server due to network or certificate issues. For example, in air-gapped deployments, deployments where Console is accessed through a CNAME alias, or deployments with unexpected certificate names, the browser on each Server might be unable to access the peer for Cross-Origin Resource Sharing (CORS). When such issues cause discrepancies in the module versions on the Servers, a message indicates the discrepancies when you access the **Solutions** page. The message appears in Tanium Console only on the Server that has discrepancies based on the database log entries. For example, updating Tanium™ Patch might succeed on Server `ts1.example.com` but not on Server `ts2.example.com`. In this case, the database logs will have an updated entry for `ts1.example.com` and Tanium Console for `ts2.example.com` will show a discrepancy message.

Mismatched module versions



Perform the following tasks to resolve module discrepancies between Tanium Servers. When you finish, repeat the import, update, or uninstallation operation on the Server where the module operation initially failed.

- Verify browser URL entry on page 142
- Verify Tanium Server port on page 143
- Enable CORS support on page 143 or, if you cannot enable CORS to work in your deployment, Disable synchronization for module operations on page 143

VERIFY BROWSER URL ENTRY

In the browser that you are using to access Tanium Console, verify that the URL field specifies the Tanium Server FQDN, not the Server IP address.

© 2026 Tanium Inc. All Rights Reserved

VERIFY TANIUM SERVER PORT

Verify that the Tanium Server uses the default port for Tanium Console access. If you specify a custom port, module operations are not automatically synchronized and you must repeat the operations on each active-active Server. The steps to view and edit the port (**ServerSOAPPort** setting) depend on your infrastructure:

- **Appliance deployment**: The default port is 8443 but you can also use 443. To view and edit the port, see Tanium Appliance User Guide: Reference: Deployment-related Tanium Core Platform settings or Tanium Core Platform User Guide for Windows Deployments: Reference: Deployment-related Tanium Core Platform settings.
- **Windows deployment**: The default port is 443. Use the Tanium Server CLI to view and edit the port. For more information, see Tanium Appliance User Guide: Reference: Tanium Core Platform command-line interface or Tanium Core Platform User Guide for Windows Deployments: Reference: Command-line interface.

VERIFY CERTIFICATE TRUST

Ensure that the browser on each Tanium Server trusts the `SOAPServer.crt` certificate of the peer Server. For more information, see Manage certificates for Tanium Server synchronization on page 141.

ENABLE CORS SUPPORT

Configure the **access_control_origin_servers** platform setting to ensure that the Tanium Servers support CORS.

In most deployments, Tanium Servers automatically enable CORS. However, if Server synchronization fails, manually configure **access_control_origin_servers** with the FQDNs or IP addresses that you use to access Tanium Console on each Server.

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings** and click **Add Setting**.
2. For the **Setting Type**, select **Server**.
3. For the **Platform Setting Name**, enter `access_control_origin_servers`.
4. Set the **Value Type** to **Text**.
5. For the **Value**, enter the Tanium Server FQDNs or IP addresses with a comma to separate each, such as `ts1.example.com,ts2.example.com` or `192.0.2.1,192.0.2.2`.

   NOTE

   If you specify FQDNs, enter the values in lowercase. If the Tanium Server uses a port other than the default SOAP port, preface the URL with `https://`.
6. Click **Save**.

DISABLE SYNCHRONIZATION FOR MODULE OPERATIONS

Perform this task only if no **access_control_origin_servers** value can enable CORS to work in your deployment. After disabling synchronization for module operations, you must perform all future module operations on both Tanium Servers in an active-active cluster.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings** and click **Add Setting**.
2. For the **Setting Type**, select **Server**.
3. For the **Platform Setting Name**, enter `console_disable_ha_workbench_install`.
4. Set the **Value Type** to **Numeric**.
5. For the **Value**, enter `1`.
6. Click **Save**.

Manage service accounts for solutions

Manage Tanium service accounts

Each Tanium solution (module or shared service) uses a service account that authenticates to the Tanium Server to run background processes, such as creating plugins on the Server. Most solutions automatically manage their accounts, but you can manually change account settings for Tanium Health Check and Tanium Reputation if necessary. For example, you can update service account passwords.



For more information about the service account that the Tanium Server might use if it synchronizes with a Lightweight Directory Access Protocol (LDAP) server, see LDAP User Name and Password on page 676.

SERVICE ACCOUNT PASSWORDS

If the password changes for a service account, the associated solution cannot create new plugins until you update the password in the account configuration on the Server, as described in Update Tanium service account settings on page 144. A solution authenticates to create a plugin when you import that solution and possibly when you upgrade it. Specific solutions also create plugins for other events.

Changes to service account passwords do not interrupt currently running processes. For example, if an administrator changes the password for the Reputation service account in the identity store of your organization, ongoing Reputation processes continue running without the need to re-authenticate to the Tanium Server.

MANUAL OR AUTOMATIC SERVICE ACCOUNT CONFIGURATION

When you import Tanium Health Check or Tanium Reputation, you can select automatic configuration of the service account for that solution (along with other settings) or manually configure the account after importing. Automatic configuration sets the service account to the user account that you use to perform the import. During manual configuration, you can specify any account that has permissions to run solution processes. Whether you select automatic or manual configuration, you can later specify different service accounts through Tanium Console.

UPDATE TANIUM SERVICE ACCOUNT SETTINGS

To update a service account password or other account settings, see the user guide for the corresponding solution:

© 2026 Tanium Inc. All Rights Reserved

- Health Check
- Reputation

Manage Windows service accounts (not applicable to the Tanium Appliance)

TANIUM SOLUTION SERVICE ACCOUNTS

In a Tanium deployment on Windows infrastructure, all Tanium solutions use a Windows service account to launch services on the Tanium Module Server. Windows service accounts are distinct, and managed independently, from the service accounts that Tanium solutions use to run processes on the Tanium Server. For example, Comply uses a Windows service account to launch the **Tanium Comply** service on the Module Server. If you do not use the default LocalSystem account, you might have to update the account password in certain cases.

Configuring a unique Windows service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization.

LOCALSYSTEM SERVICE ACCOUNT

By default, LocalSystem is the Windows service account that launches all Tanium solution services. LocalSystem is a predefined account that authenticates to the Windows operating system. Because LocalSystem has no password, you never need to update its credentials for running services. If you use any other Windows service accounts to launch Tanium services, and an administrator changes the account passwords on the LDAP or AD server, the services cannot restart until you enter the new passwords through the **Services** program on the Module Server. You can also use the **Services** program to select different service accounts for launching Tanium services. To update passwords or select a different account, see Update Windows service accounts on page 145.

TANIUM CORE PLATFORM SERVICE ACCOUNTS

Tanium Core Platform servers and the Tanium database use Windows service accounts to run processes during and after installation. You select the accounts during server installation. After installation, you can select different accounts or update their passwords, as described in Update Windows service accounts on page 145.

For more information about the service account requirements of platform servers and the database, see Tanium Core Platform User Guide for Windows Deployments: Administrator account permissions.

UPDATE WINDOWS SERVICE ACCOUNTS

1. Sign in as the Administrator user to the system that runs the service:
    - **Tanium solutions**: Sign in to the Module Server.
    - **Tanium Core Platform servers or Tanium database server**: Sign in to the system that hosts the server.
2. Open the Windows **Services** program and right-click the service that requires an update.
3. Select **Properties** and select the **Log On** tab.

© 2026 Tanium Inc. All Rights Reserved

4. (Optional) To select a different account, select **This Account** and enter the account name.
5. Enter the **Password**, re-enter it in the **Confirm Password** field, and click **OK**.
6. Restart the service. The account update does not apply until the service restarts.

© 2026 Tanium Inc. All Rights Reserved

Part 5: Customizing Console and Interact

Customize the appearance and behavior of Tanium Console and the Interact **Overview** page to achieve the following objectives:

- **Meet policy and network requirements**

  Your organization might have specific requirements such as a pre-login banner, a custom Console logo, password confirmations for Console operations, or an additional help URL.

- **Optimize Console ergonomics for specific users**

  Each Tanium user can configure certain settings that apply to their own user account but not others. For example, users might want to see Console text in different languages or change the contents (such as quick links) of solution **Overview** pages to reflect their own workflows.

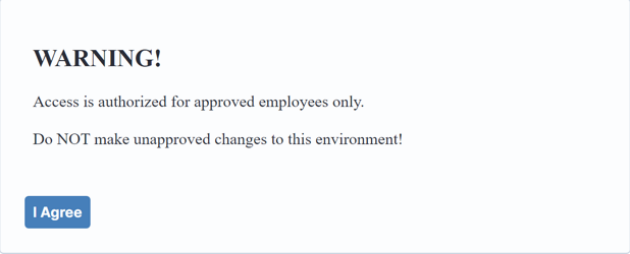
- **Identify Console instances**

  If your organization has multiple Tanium environments, each will have its own instance of Console. You can make it easy for users to identify which Tanium environment they are viewing by setting a unique color and text for the Console header in each environment.

Configure a pre-login banner

By default, the Tanium Console sign-in page (see Sign in to Console on page 49) is the first page that users see when they access the Console URL in a browser. However, you can configure a pre-login banner to provide information or warnings that users must read and acknowledge before accessing Console, as shown in the following example.

Example of Console pre-login banner



NOTE On the pre-login banner, the **I Agree** button appears by default and is not configurable.

Before you begin

Determine which of the following methods for configuring a pre-login banner best suits your needs based on the banner contents:

- Banner with only text and basic formatting on page 148
- Banner with images, links, or complex text formatting on page 148

© 2026 Tanium Inc. All Rights Reserved

NOTE

Both methods require a Tanium Console user account that has the **Administrator** reserved role or a role with **Global Settings write** permission.

Both methods also require some knowledge of HTML syntax. For more information, see https://html.spec.whatwg.org.

Configure and test the pre-login banner in a lab environment before adding the banner in your production environment.

BANNER WITH ONLY TEXT AND BASIC FORMATTING

The console_PreLoginBannerHTMLText setting provides the easiest method to configure a pre-login banner because this setting does not require you to copy an HTML file to the Tanium Server. However, the setting does not support CSS-based inline formatting or element attributes. The setting supports only basic HTML formatting elements, such as:

- Headings: `<h1>` through `<h6>`
- New lines: `<br>`
- **Bold** text: `<b></b>`
- *Italicized* text: `<i></i>`

To configure a pre-login banner that contains only text with basic formatting, skip to Enable the pre-login banner on page 150.

BANNER WITH IMAGES, LINKS, OR COMPLEX TEXT FORMATTING

The console_PreLoginBannerHTML setting supports any HTML content and formatting that you want, including images, links, element attributes, and CSS-based formatting. However, if you use this setting, you must first create an HTML file and copy it to the Tanium Server. The user requirements and procedure for creating the banner depend on the Tanium infrastructure:

- **Tanium Appliance**: The user must be able to use SSH File Transfer Protocol (SFTP) to upload files to the `/incoming` directory. You also require a user account that has the `tanadmin` role for TanOS console access. To start configuring the banner, go to Create the pre-login banner file for an Appliance deployment on page 148.
- **Windows Server host system**: The user must be able to copy files to the Tanium Server installation directory. To start configuring the banner, go to Create the pre-login banner file for a Windows deployment on page 150.

Create the pre-login banner file for an Appliance deployment

1. Use a text editor to create a text file with the following contents. Replace `PAGE TITLE` with the actual title that you want to use and replace `PAGE BODY` with the information or warnings that you want users to read.

```
<html>
<body>
<div>
   <h2>PAGE TITLE<br></h2>
      <p align=left>PAGE BODY</p>
```

© 2026 Tanium Inc. All Rights Reserved

```
</div>
</body>
</html>
```

The following example produces the pre-login banner in the figure Example of Console pre-login banner on page 147:

```
<html>
<body>
<div>
   <h2>WARNING!<br></h2>
      <p align=left>Access is authorized for approved employees
only.<br><br>Do NOT make unapproved changes to this environment!</p>
</div>
</body>
</html>
```

If any Tanium users access Tanium Console on a device with a small screen or low resolution and the pre-login banner has a lot of content, you might have to add a `style` attribute to the `<div>` element to ensure that those users can see the **I Agree** button. The following example shows the `style` attribute with properties that add a scroll bar (`overflow:auto`) for users to see content that exceeds 350px in vertical space (`max-height:350px`) on the pre-login banner.

```
<html>
<body>
<div style="max-height:350px;overflow:auto;">
   <h2>PAGE TITLE<br></h2>
      <p align=left>PAGE BODY WITH NUMEROUS LINES</p>
      <p align=left>...</p>
      <p align=left>...</p>
</div>
</body>
</html>
```

2. Save the file with the name `banner.html`.
3. Upload the HTML file to the Tanium Server:
   a. Use SFTP to upload the HTML file to the `/incoming` directory on the Appliance.
   b. Sign in to the TanOS console as a user with the `tanadmin` role.
   c. Enter `2` to go to the **Tanium Operations** menu.
   d. Enter `X` to go to the **Advanced Operations** menu.
   e. Enter `4` and follow the prompts to copy the HTML file to the appropriate location.

© 2026 Tanium Inc. All Rights Reserved

Create the pre-login banner file for a Windows deployment

1. Use a text editor to create a text file with the following contents. Replace `PAGE TITLE` with the actual title that you want to use and replace `PAGE BODY` with the information or warnings that you want users to read.

```
<div>
   <h2>PAGE TITLE<br></h2>
      <p align=left>PAGE BODY</p>
</div>
```

   The following example produces the pre-login banner in the figure Example of Console pre-login banner on page 147:

```
<div>
   <h2>WARNING!<br></h2>
      <p align=left>Access is authorized for approved employees
only.<br><br>Do NOT make unapproved changes to this environment!</p>
</div>
```

   If any Tanium users access Tanium Console on a device with a small screen or low resolution and the pre-login banner has a lot of content, you might have to add a `style` attribute to the `<div>` element to ensure that those users can see the **I Agree** button. The following example shows the `style` attribute with properties that add a scroll bar (`overflow:auto`) for users to see content that exceeds 350px in vertical space (`max-height:350px`) on the pre-login banner.

```
<div style="max-height:350px;overflow:auto;">
   <h2>PAGE TITLE<br></h2>
      <p align=left>PAGE BODY WITH NUMEROUS LINES</p>
      <p align=left>...</p>
      <p align=left>...</p>
</div>
```

2. Save the file with a name that reflects its purpose and use `.html` as the suffix (for example, `banner.html`).
3. Copy the HTML file to the *<Tanium Server installation directory>*`\http` directory on the Tanium Server host.

Enable the pre-login banner

1. Sign in to Tanium Console as a user with the **Administrator** reserved role or a role with **Global Settings write** permission.
2. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings** and click **Add Setting**.
3. Configure the following attributes of the console_PreLoginBannerHTMLText setting (basic banner) or console_PreLoginBannerHTML setting (complex banner) based on the banner contents (see Before you begin on page 147), and then click **Save**:

© 2026 Tanium Inc. All Rights Reserved

Pre-login banner attributes

Attribute	Basic banner	Complex banner
Setting Type	`Server`	`Server`
Platform Setting Name	`console_PreLoginBannerHTMLText`	`console_PreLoginBannerHTML`
Value Type	`Text`	`Text`
Value	Enter the HTML content of the pre-login banner as described under Banner with only text and basic formatting on page 148.	Enter the name of the HTML file that you created for the pre-login banner. The name must be `banner.html` on the Appliance.

NOTE

Users who are currently signed in to Console do not see the pre-login banner until they sign out, wait for the Tanium Server refresh interval (default 60 seconds), and sign in again. If the banner still does not appear, instruct users to perform a hard refresh on their browser.

Select the Console color

If your organization deployed multiple Tanium environments, each environment has a separate instance of Tanium Console. To help users identify which environment they are signed in to for the current session, customize the color of the top border and of the Environment details on page 56 section of Console header. For example, you might set different colors to distinguish between lab and production environments.

Console header color



In an active-active cluster, the Console instances for both Tanium Servers use the same color configuration. You cannot specify a different color for each Server in the cluster.

NOTE

Users require the **Administrator** reserved role to manage the Console color.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Configuration > Appearance**.
2. In the **Console Color** section, use the **Current Color** selector to pick a color and then click **Submit**.
3. Perform one of the following steps:
    - Click **Refresh Now** to apply the change immediately by refreshing your web browser.
    - If you plan to customize other aspects of Console (for example, Configure Console header text on page 152), submit each change and then click **Refresh Now** to apply all the changes simultaneously.

Configure Console header text

By default, the Tanium Console displays no custom text in the Environment details on page 56 section of the Console header. If your organization deployed multiple Tanium environments, adding custom text can help users identify which environment they are signed in to for the current Console session. For example, if your organization established separate Tanium deployments for separate customers, the Console implementation for each customer can have text that identifies the customer.

Console header custom text



In an active-active cluster, the Tanium Console instances for both Tanium Servers use the same text configuration. You cannot specify different text for each Server in the cluster.

> NOTE
> Users require the **Administrator** reserved role to manage the custom text in the header.

Perform the following steps to add or edit the custom text:

1. From the Main menu, go to **Administration > Configuration > Appearance**.
2. Enter the new text in the **Header Text** field and click **Submit**.
3. Perform one of the following steps:
    - Click **Refresh Now** to apply the change immediately by refreshing your web browser.
    - If you plan to customize other aspects of Console (for example, Select the Console color on page 151), submit each change and then click **Refresh Now** to apply all the changes simultaneously.

> TIP
> To revert to the default of no text, return to the **Appearance** page, go to the **Console Header Text** section, and click **Reset**.

© 2026 Tanium Inc. All Rights Reserved

Select the task confirmation prompt

Many tasks that users initiate in Tanium Console require responding to a confirmation prompt before the tasks proceed. Select the prompt type based on whether you want to optimize Console security (password prompt) or user ergonomics (**Yes/Cancel** prompt).

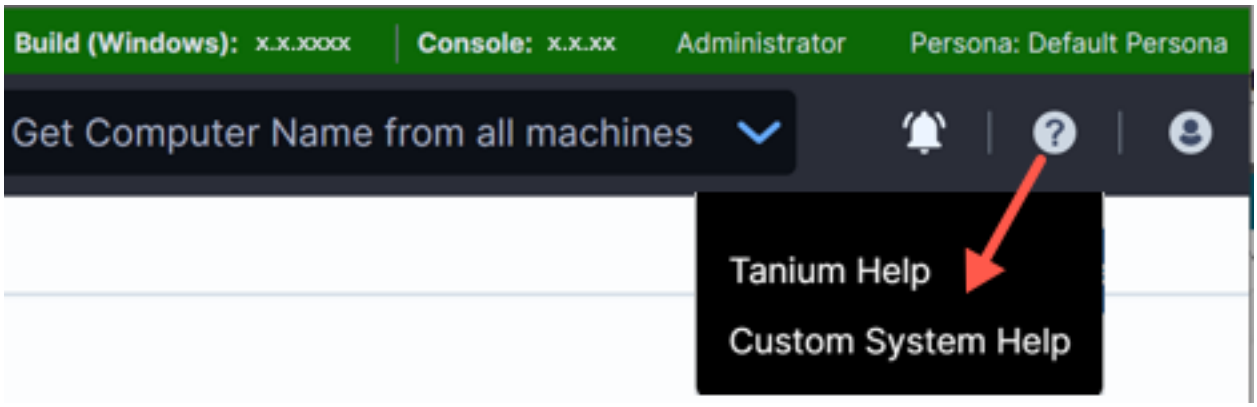
> NOTE
>
> Only users who are assigned the **Administrator** reserved role can manage the confirmation prompt.
>
> If you enable Security Assertion Markup Language (SAML) single sign-on, the Tanium Server automatically changes the prompt to a **Yes/Cancel** prompt. For more information, see Enabling SSO through SAML on page 684.

1. From the Main menu, go to **Administration > Configuration > Appearance**.
2. In the **Choose which type of Confirmation Prompt to display** section, select one of the following options and click **Submit**:
   - **Show a password prompt (default)**
   - **Show a prompt with "Yes" and "Cancel" options**
3. Perform one of the following steps:
   - Click **Refresh Now** to apply the change immediately by refreshing your web browser.
   - If you plan to customize other aspects of Console (for example, Select the Console color on page 151), submit each change and then click **Refresh Now** to apply all the changes simultaneously.

Add a help URL

Clicking Help in the Console header opens the Tanium Resource Center in a new browser tab or window. Optionally, you can add a link to a custom help source. For example, you might create an internal help source in deployments where the Tanium Resource Center is inaccessible because the Tanium Server has no Internet connection. If you add a help link, the Help menu shows a **Tanium Help** option for the Tanium Resource Center and a **Custom System Help** option for the added link.

Tanium Console Help links



© 2026 Tanium Inc. All Rights Reserved

NOTE

Users require the **Administrator** reserved role to manage the Console help URL.

1. From the Main menu, go to **Administration > Configuration > Appearance**.
2. Enter the custom **Help URL**, including the protocol prefix, `http://` or `https://`.
3. Click **Submit** and perform one of the following steps:
   - Click **Refresh Now** to apply the change immediately by refreshing your web browser.
   - If you plan to customize other aspects of Console (for example, Select the Console color on page 151), submit each change and then click **Refresh Now** to apply all the changes simultaneously.
4. Select > **Custom System Help** to verify that the URL works.

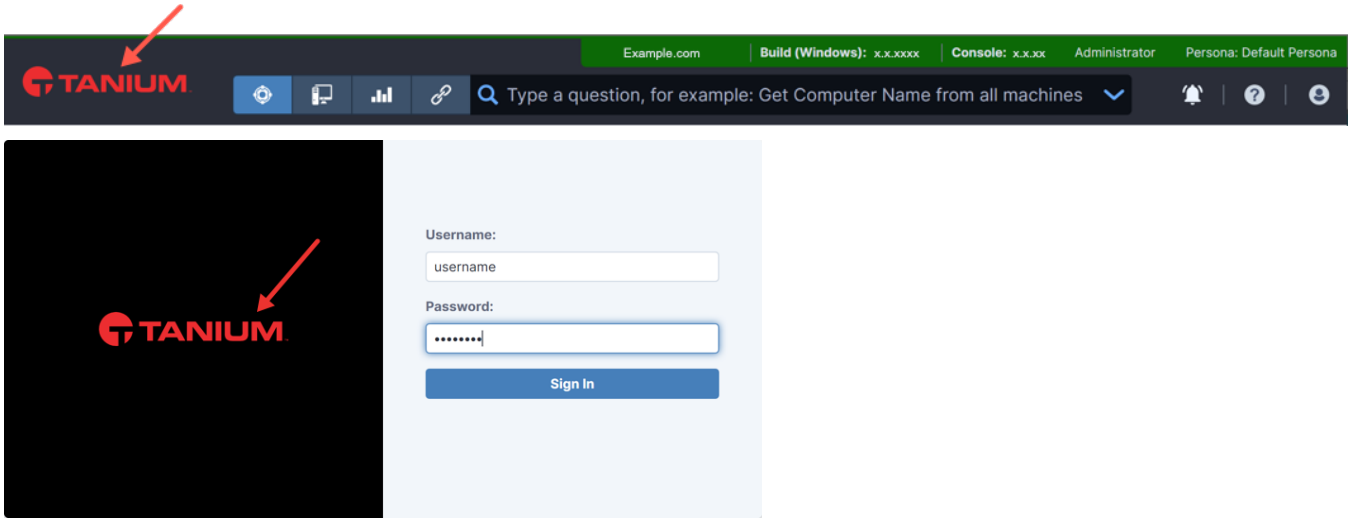
TIP

To revert to the default of no text, return to the **Appearance** page, go to the **Console Header Text** section, and click **Reset**.

Customize the Console logo

You can replace the default Tanium logo in the Tanium Console header and in the sign-in page with the logo of your organization. Console supports all the standard image formats that your browser supports, such as PNG, JPG, and SVG. The maximum file size is 2 MB. You can also adjust the logo height, which is 24 pixels by default. Console automatically scales the logo width proportionately.

Logo in header and sign-in page



NOTE

Users require the **Administrator** reserved role to manage the Console logo.

Perform the following steps to replace the logo or adjust its height:

© 2026 Tanium Inc. All Rights Reserved

1. (New logo only) Create your own logo file.
2. From the Main menu, go to **Administration > Configuration > Appearance**.
3. (New logo only) In the **Console Logo** section, click **Upload**, select the logo file, and click **Open**.
4. (Optional): In the **Logo height** field, specify the logo height in pixels.
5. Click **Submit** and perform one of the following steps:
    - Click **Refresh Now** to apply the change immediately by refreshing your web browser.
    - If you plan to customize other aspects of Console (for example, Select the Console color on page 151), submit each change and then click **Refresh Now** to apply all the changes simultaneously.

To revert to the original, default logo, return to the **Appearance** page, go to the **Console Logo** section, and click **Reset**.

Configure Console user preferences

You can configure certain Tanium Console settings to suit your own ergonomic preferences without affecting those settings for other user accounts. For example, you might want to see Console text in a certain language or view the UI in dark mode instead of light mode.

The Tanium Server applies your preferences when you sign in to Console. Changes that you make to the preferences apply to any persona that you select for a Console session, but the changes do not affect the personas of other users.

All users can update their preferences regardless of their role assignments.

Perform the following steps to update preferences for the user account that you are using for the current Tanium session:

1. In the Console header, hover over  and select **Preferences**.
2. Configure the following settings and click **Save**. The changes apply immediately.
    - Consider question results complete at on page 156
    - Suspend console automatically if no activity detected for on page 156
    - Theme on page 156
    - Language on page 157
    - Hide error results from questions on page 157
    - Open Search Bar Results in New Tab on page 157
    - Show Environment Details on page 157

© 2026 Tanium Inc. All Rights Reserved

Consider question results complete at

Console pages that show results from Tanium Clients indicate that all Clients have responded when the number of responding Clients reaches the threshold specified in the **Consider question results complete at** setting in your Console user preferences. For example, the Interact **Question Results** page starts showing results upon reaching this threshold. The default threshold is 99%.

The Tanium Server calculates the number of registered Clients based on when it initiated the operation, such as when it issued a question or deployed an action. However, the actual number of registered Clients might fluctuate during the period between the initiation and timeout of the operation. For example, several end users might close their laptops soon after a question is issued and before it times out (default 10 minutes).

For cases where the calculated and actual numbers of registered Clients might never match, setting the value at less than 100% prevents Console users from waiting indefinitely for an indication that all Clients have answered.

Suspend console automatically if no activity detected for

By default, Console automatically ends your session and displays the sign-in page if you perform no activity on Console for 10 minutes. In your Console user preferences, you can set the **Suspend console automatically if no activity detected for** setting to a minimum of 2 minutes. The maximum value that you can set is equal to the **max_console_idle_seconds** platform setting (rounded down to minutes), which applies to all users. The platform setting has a default of 3,600 seconds (60 minutes). If the user preference is less than the platform setting, the Tanium Server applies the user preference. To edit platform settings, see Edit advanced settings on page 165.



Initiating a solution import or update operation suspends the inactivity timer. The timer resets to zero and resumes at the moment the operation finishes.

By default, Console displays a warning 60 seconds before the activity timeout to give users a chance to preserve their current session. The **console_idle_warning_seconds** platform setting controls the timeout warning interval.

For more information about how other events and platform settings affect the duration of a user session, see Session validity and timeouts on page 53.

Theme

In your Console user preferences, select the user interface color scheme that is most comfortable for you when using Console and Tanium solution workbenches:

- **Dark** (default): Pages have a dark background and white text.
- **Light**: Pages have a white background and dark text.
- **Auto**: On the device that you use to access Console, the operating system (OS) settings automatically set the color scheme to light or dark. If the OS settings specify automatically changing the theme based on the time of day (such as switching to the dark theme at sunset), the Tanium user interface automatically changes accordingly. To change the color scheme, you can change the OS settings or override them by selecting another option in the **Theme** dropdown list.

© 2026 Tanium Inc. All Rights Reserved

NOTE

Not all versions of Tanium solutions support the **Dark** theme.

Language

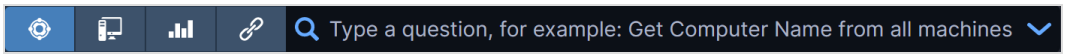
In your Console user preferences, select a language for user interface text that appears in the workbenches of Tanium solutions such as Console. The default option **(Browser Language)** is the language that is selected for the browser that you use to access solution workbenches. For more information, see Reference: Language support on page 761.

Hide error results from questions

In your Console user preferences, the **Hide error results from questions** option is enabled by default and makes the **Questions Results** grid omit null or error values, such as `[no results]` or `[results currently unavailable]`. Hiding such values provides clarity in that the grid shows only the answers that are likely to be useful. However, this option also prevents the grid from showing the complete set of answers received from all endpoints. For more information, see Troubleshoot question results issues on page 709.

Open Search Bar Results in New Tab

In your Console user preferences, select whether the results of the Quick Search bar open in a new browser tab (default) or in the current tab. For more informatio, see Quick Search bar on page 55.



Show Environment Details

In your Console user preferences, select whether to display environment details in the Console header:



For more information, see Environment details on page 56.

Customize solution overview pages

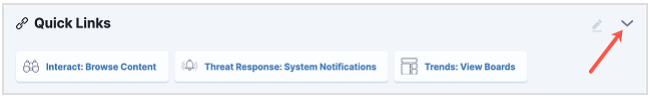
Each Tanium solution (module or shared service) has an **Overview** page that opens when you access the solution workbench. These **Overview** pages, and also the Tanium Home page on page 62, are organized into sections, such as guidance on getting started and reports related to solution health. You can show, hide, or reorder sections on an **Overview** page to reflect your own preferences.

For example, on the Interact **Overview** page, you might move the **Learn to Use Tanium Interact** section to the bottom of the page if you seldom use the links in that section.

Your changes to **Overview** pages apply across all the personas that are assigned to your user account but do not apply to other users.

© 2026 Tanium Inc. All Rights Reserved

1. Open the page that you want to customize by selecting a Main menu option:
   - Tanium **Home** page: click .
   - Module **Overview** page: Select **Modules > *<module name>***.
   - Shared service **Overview** page: Select **Shared Services > *<shared service>***.
2. (Optional) Collapse or expand page sections based on what you want to see. By default, all the sections are expanded.



3. Click **Customize Page**, select or clear checkboxes to show or hide page sections, drag the sections to the order you want, and click **Save**.
   The following example is for the Interact **Overview** page.



4. (Tanium **Home** page only) Optionally, modify the contents of the following sections on the Tanium **Home** page:
   - **Quick links**: For more information, see Work with Quick Links on page 67.
   - Reporting **Dashboards** and **Dashboard Lists**: For more information, see Work with Reporting dashboards on page 68.
   - Favorite Interact content: For more information, see Work with favorite Interact categories, dashboards, and saved questions on page 71.

© 2026 Tanium Inc. All Rights Reserved

Configuring the Tanium Core Platform

Use Tanium Console to maintain the health and optimize the efficiency of your Tanium environment by configuring settings that affect the behavior of various Tanium Core Platform on page 43 components. For example, you can configure bandwidth throttles for the data that platform servers send to Tanium Clients to ensure that data bottlenecks do not interfere with the operations of Tanium users.



For the user roles and permissions required to configure the settings, see Tanium Core Platform configuration permissions on page 77.

Settings for Tanium Core Platform servers

Perform the following tasks during the initial deployment of Tanium Core Platform servers:

- Synchronizing active-active Tanium Servers on page 224 is required only if you have an active-active deployment on Windows infrastructure. In a Tanium Appliance deployment, the array setup automatically manages trust between Tanium Servers.
- Enabling communication between Zone Servers and Hubs on page 226 is required only if your deployment includes Tanium Zone Servers.

You can also perform the following tasks for optional settings as part of Day One provisioning. Update the settings anytime after Day One if necessary to accommodate changes in your deployment or network.

- Manage platform settings on page 163, such as the default user group for new users.
- Allowing Tanium Client downloads from Internet URLs on page 168 to control how the Tanium Server handles file downloads that the Tanium Client requests from Internet URLs.
- Enabling authentication between platform servers and remote systems on page 173 from remote sources, such as for package files.
- Configuring Internet access through proxy servers on page 181 if your organization deploys a proxy server for traffic between internal servers and the Internet.
- Encrypt the root keys database on page 217 to prevent unauthorized access to the Tanium root keys.

The Tanium license and Tanium digital keys are included automatically when you install Tanium Core Platform servers. However, you can perform the following tasks to manage the license and keys when necessary:

- Replace the license on page 207 if you receive a new license for changes to your entitlements, such as the purchase of additional Tanium solutions.
- Securing Tanium connections and operations through digital keys on page 209 if you need to replace or download the Tanium root keys.

To configure Tanium Core Platform settings that Tanium Console does not expose, see the guide for your deployment:

© 2026 Tanium Inc. All Rights Reserved

- Tanium Core Platform User Guide for Windows Deployments
- Tanium Appliance Deployment Guide

Settings for Tanium Clients

As part of Day One provisioning, you can perform the following tasks for optional settings that affect Tanium Clients. Update the settings anytime after Day One if necessary to accommodate changes in your deployment or network.

- Manage platform settings on page 163, such as the options that control action deployment to Clients.
- Throttling bandwidth and connections to Tanium Clients on page 187 to limit the bandwidth and the number of concurrent connections that Tanium Servers or Zone Servers use to send data to Clients.
- Optimizing Tanium Client peering through subnets on page 196 to create separated subnets, intentional subnets, and isolated subnets that modify the default peering behavior of Clients.

To configure Tanium Client settings that Tanium Console does not expose, see Tanium Client Management User Guide: Managing Client settings and Index configurations.

© 2026 Tanium Inc. All Rights Reserved

Configuring the Tanium Core Platform

Use Tanium Console to maintain the health and optimize the efficiency of your Tanium environment by configuring settings that affect the behavior of various Tanium Core Platform on page 43 components. For example, you can configure bandwidth throttles for the data that platform servers send to Tanium Clients to ensure that data bottlenecks do not interfere with the operations of Tanium users.



For the user roles and permissions required to configure the settings, see Tanium Core Platform configuration permissions on page 77.

Settings for Tanium Core Platform servers

Perform the following tasks during the initial deployment of Tanium Core Platform servers:

- Synchronizing active-active Tanium Servers on page 224 is required only if you have an active-active deployment on Windows infrastructure. In a Tanium Appliance deployment, the array setup automatically manages trust between Tanium Servers.
- Enabling communication between Zone Servers and Hubs on page 226 is required only if your deployment includes Tanium Zone Servers.

You can also perform the following tasks for optional settings as part of Day One provisioning. Update the settings anytime after Day One if necessary to accommodate changes in your deployment or network.

- Manage platform settings on page 163, such as the default user group for new users.
- Allowing Tanium Client downloads from Internet URLs on page 168 to control how the Tanium Server handles file downloads that the Tanium Client requests from Internet URLs.
- Enabling authentication between platform servers and remote systems on page 173 from remote sources, such as for package files.
- Configuring Internet access through proxy servers on page 181 if your organization deploys a proxy server for traffic between internal servers and the Internet.
- Encrypt the root keys database on page 217 to prevent unauthorized access to the Tanium root keys.

The Tanium license and Tanium digital keys are included automatically when you install Tanium Core Platform servers. However, you can perform the following tasks to manage the license and keys when necessary:

- Replace the license on page 207 if you receive a new license for changes to your entitlements, such as the purchase of additional Tanium solutions.
- Securing Tanium connections and operations through digital keys on page 209 if you need to replace or download the Tanium root keys.

To configure Tanium Core Platform settings that Tanium Console does not expose, see the guide for your deployment:

© 2026 Tanium Inc. All Rights Reserved

- Tanium Core Platform User Guide for Windows Deployments
- Tanium Appliance Deployment Guide

Settings for Tanium Clients

As part of Day One provisioning, you can perform the following tasks for optional settings that affect Tanium Clients. Update the settings anytime after Day One if necessary to accommodate changes in your deployment or network.

- Manage platform settings on page 163, such as the options that control action deployment to Clients.
- Throttling bandwidth and connections to Tanium Clients on page 187 to limit the bandwidth and the number of concurrent connections that Tanium Servers or Zone Servers use to send data to Clients.
- Optimizing Tanium Client peering through subnets on page 196 to create separated subnets, intentional subnets, and isolated subnets that modify the default peering behavior of Clients.

To configure Tanium Client settings that Tanium Console does not expose, see Tanium Client Management User Guide: Managing Client settings and Index configurations.

© 2026 Tanium Inc. All Rights Reserved

Customizing the Tanium environment through platform settings

You can customize the Tanium environment to suit policies and operations that are specific to your organization by editing settings that control Tanium Core Platform behaviors for all users. For example, if your organization requires two-person integrity for actions, you can enable the **Require Action Approval** setting. Thereafter, actions that any user initiates do not deploy to endpoints until another user approves those actions.

The **Administration > Configuration > Settings** page lists settings in two tabs based on the level of expertise that is required to manage them effectively:

- **Platform Settings**

  You can manage these settings effectively without guidance from Tanium Support. However, you cannot create or delete settings on the **Platform Settings** tab; you can only view and edit them. Platform settings are a subset of the **Advanced Settings** and therefore appear in both tabs, but the **Platform Settings** tab simplifies configuring them.

- **Advanced Settings**

  Contact Tanium Support on page 724 for guidance before you edit, create, or delete these settings unless they are also **Platform Settings**. Advanced settings are listed alphabetically for easy scanning. Some advanced settings are hidden by default and you must create them before they appear in the tab. Settings that are hidden by default have default values even if you do not add those settings to the tab.

For descriptions of the settings that are most commonly viewed or configured when you set up or customize a Tanium deployment, see Reference: Tanium Core Platform settings on page 765.



Platform Settings and **Advanced Settings** include server and Client settings that appear only to users who have **Global Settings read** permission. **Global Settings write** permission provides **Global Settings read** permission and also enables users to create, edit, or delete server and Client settings. The **Administrator** reserved role has these permissions.

Only the **Administrator** reserved role can view and manage **Local** Tanium Server settings.

Manage platform settings

The **Platform Settings** page contains settings that you can manage effectively through Tanium Console without guidance from Tanium Support. Assess the impact of your planned changes before you edit settings. For example, enabling **Restricted Targeting** prevents the automatic deployment of solution-specific tools to endpoints by making the **No Computers** computer group the target for the action groups of solutions that you later import. Therefore, before enabling the setting, assess the impact of preventing automatic tools deployment.

Perform the following steps to view setting values and descriptions, and to change the values:

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Configuration > Settings** and select the **Platform Settings** tab.
   For each setting, the page shows the current value, whether that value is the **Default**, and a brief description. Settings with non-default values have a **Reset** button for reverting to the default values.
2. (Optional) Expand the setting that you plan to edit to see additional information about the platform behavior that it controls.
3. Change the setting value as follows and click **Save All**:
   - Click the **ON** or **OFF** widget for settings that are enabled or disabled.

   - Enter values in the text-entry fields for settings that have numeric or string values.

     NOTE You must expand some settings to see their text-entry fields.

Manage advanced settings

IMPORTANT Contact Tanium Support for guidance before you edit advanced settings. For more information, see Contact Tanium Support on page 724.

The **Advanced Settings** page contains all the settings that you can view and edit through Tanium Console.

Types of Tanium Core Platform settings

The setting type determines which platform component the setting affects:

Types of Tanium Core Platform settings

Type	Description
Server	Server settings affect the behavior of all Tanium Core Platform servers and Console.
Local	Tanium Server settings that you configure locally on each Server control aspects of the connections between the Server and other Tanium Core Platform components or external servers. Local settings also control features such as logging and Tanium Client peering. Most local settings are automatically configured during Server installation, but you can change the settings when necessary. During troubleshooting, Tanium Support might ask you to review or confirm local settings, but rarely asks you to change them. NOTE You must update local settings on each Tanium Server in an active-active deployment because the Servers do not synchronize those settings.
Client	Client settings affect the behavior of all Tanium Clients.

© 2026 Tanium Inc. All Rights Reserved

Hidden settings

Some advanced settings are hidden by default: they do not appear in Console or in the server or Client command-line interface (CLI) unless you manually add those settings. However, hidden settings have default values that apply even if you do not add them. After you add a setting through Console or the CLI, the value that you set overrides the default value.

Override settings on individual servers and Clients

Server and Client settings that you configure locally on a Tanium Core Platform server or Client through its CLI override the settings that you configure through Tanium Console. To configure server settings locally, see:

- Tanium Appliance User Guide: Reference: Deployment-related Tanium Core Platform settings
- Tanium Core Platform User Guide for Windows Deployments: Reference: Deployment-related Tanium Core Platform settings

To configure Client settings locally, see Tanium Client Management User Guide: Tanium Client CLI and Client settings.

View advanced settings

The **Advanced Settings** page displays the setting properties described in Advanced settings properties on page 166, as well as who last modified a setting and when. However, the page does not show the **Value** of **protected** settings. After you configure a **protected** setting, you cannot see its value in Tanium Console.

1. From the Main menu, go to **Administration > Configuration > Settings** and select the **Advanced Settings** tab.
2. (Optional) Filter the settings by:
   - **Type**: The page displays **All** settings by default but you can click **Server**, **Client**, or **Local** to display only settings of that type.
   - **Name** or **Value**: Enter a search string in the **Filter items** field.
3. (Optional) Click **Show More** in the **Note** column to see the full text for settings that are configured with a **Note** value.

Edit advanced settings

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.
2. Click the **Name** of the setting that you want to edit.
3. Enter a new **Value**, optionally update the **Note** (server and Client settings only), and click **Save**.

A **Note** can help other users understand why you changed the setting.



Updates to most **Server** and **Local** settings apply immediately but some require a Tanium Server restart. Contact Tanium Support on page 724 for information about which settings require a Server restart. To restart the Server, see:

© 2026 Tanium Inc. All Rights Reserved

NOTE

- **Tanium Appliance**: Tanium Appliance User Guide: Start, stop, and restart Tanium services.
- **Windows Server**: Tanium Core Platform User Guide for Windows Deployments: Manage Windows services for core platform servers.

Updates to Tanium **Client** settings apply only after you manually restart the Clients or wait for the automatic Client reset, which occurs at a random interval typically in the range of two to six hours.

Create advanced settings

Some advanced settings are hidden by default. When you create a setting through Tanium Console, the setting becomes visible and you can change its default value.

1. From the Main menu, go to **Administration > Configuration > Settings** and select the **Advanced Settings** tab.
2. Click **Create Setting**, configure the following properties, and click **Save**:

Advanced settings properties

Property	Description
Setting Type	Specify the Tanium Core Platform components to which the setting applies: • **Server**: Applies to one or more Tanium Core Platform servers • **Client**: Applies to Tanium Clients • **Local**: Applies to the Tanium Server that you are currently logged into through Tanium Console
Name	Enter a name of up to 255 characters to identify the setting.
Value Type	Specify the type of value: • **Text**: The value is a text string. Note that the string might include both letters and numbers, such as an IP address or URL. • **Numeric**: The value is a number. • **Protected**: This type applies only to **Local** settings (such as passwords) for which you want to hide the value in the **Advanced Settings** page. After you configure a **protected** setting, you cannot see its value in Tanium Console.
Value	Enter the setting value.
Note	(Server or Client settings only) Optionally, enter any notes that might help other users understand the purpose of the setting.

© 2026 Tanium Inc. All Rights Reserved

NOTE

Most **Server** and **Local** settings apply as soon as you create them, but some require a Tanium Server restart. Contact Tanium Support on page 724 for information about which settings require a Server restart. To restart the Server, see:

- **Tanium Appliance**: Tanium Appliance User Guide: Start, stop, and restart Tanium services.
- **Windows Server**: Tanium Core Platform User Guide for Windows Deployments: Manage Windows services for core platform servers.

New Tanium **Client** settings apply only after you manually restart the Clients or wait for the automatic Client reset, which occurs at a random interval typically in the range of two to six hours.

© 2026 Tanium Inc. All Rights Reserved

Allowing Tanium Client downloads from Internet URLs

The URL expressions that you configure on the **Allowed URLs** page enable Tanium Clients to successfully run content that requires file downloads from Internet URLs. For example, a package that you deploy through an action, or a sensor that you include in a question, might run a script that requests a file download. The Client API uniquely identifies the download by URL, including file name. For security, the Client sends a message to the Tanium Server, which checks the requested URL against its lists of package file URLs and allowed URLs. The URLs of package files are known URLs that the package author specified. You use the allowed URLs to account for dynamic URLs, such as URLs that a Client script computed. If the URL does not match either list, the request fails.

The first time the Tanium Server handles a Tanium Client file download request that passes the allowed URLs check, the Server downloads the file and stores a temporary package file and metadata so that it can distribute the file to endpoints. For more information, see Tanium Client Management User Guide: File distribution. The allowed URLs configuration includes settings that affect how often the Server checks for changes to the requested URL files and how often the Server clears temporary files.



Allowed URLs read permission is required to view allowed URLs configurations. **Allowed URLs write** permission is required to create, modify, or delete allowed URLs configurations. The **Administrator** reserved role has these permissions.

The Tanium Server and Tanium Module Server also access Internet URLs to download content. If your enterprise network uses SSL intercept technologies, such as man-in-the-middle (MITM) proxies, you must configure them so that they do not prevent the servers from downloading files from these locations. For more information, see Tanium Appliance User Guide: Internet URLs or Tanium Core Platform User Guide for Windows Deployments: Internet URLs.

View allowed URLs

1. From the Main menu, go to **Administration > Permissions > Allowed URLs**.
   The page displays the settings that are described in Allowed URL settings on page 169.
2. (Optional) To displays the identifier for each allowed URL, click Customize Columns and select **ID**.
3. (Optional) Enter a text string in the **Filter items** field to filter the grid by **URL Expression**.

© 2026 Tanium Inc. All Rights Reserved

Add allowed URLs

1. From the Main menu, go to **Administration > Permissions > Allowed URLs**.
2. Click **New URL Expression**.
3. Configure the following settings and click **Save**.

Allowed URL settings

Setting	Description
URL	Specify a URL. To allow multiple files from a base URL, select **Treat the above text as a regular expression** and specify the regular expression (regex). For example, the following regex allows any download from `www.microsoft.com`: `http\:\/\/www\.microsoft\.com\/.*` Note that the value is case sensitive. For example, the regex `https\:\/\/192\.0\.2\.1\/abc\.csv` allows `https://192.0.2.1/abc.csv` but not `https://192.0.2.1/ABC.csv`. The regex to allow both files is `https\:\/\/192\.0\.2\.1\/abc|ABC\.csv`. When Tanium Clients initiate a download that passes this check, the Tanium Server downloads the file so that it can distribute it to Clients through the linear chain.
Download Interval	(Optional) Select **Check for changes after** and specify an interval at which the Tanium Server checks the URL for changes to the requested file. The default is every six hours. If the check indicates there are changes to the file, the Server updates its copy of the file and restarts the expiration clock. For **URL** definitions that specify a regular expression, the Server maintains a timer for each match.
Expiration	(Optional) Select **Clean up downloaded files after** and specify the interval for clearing stale files. The default is seven days. This means that the Tanium Server deletes files that it has not downloaded and that Tanium Clients have not requested in the past seven days. If a Client subsequently requests the URL, the Server downloads it again and resumes the update checks. For **URL** definitions that specify a regular expression, the Server maintains a timer for each match. TIP To troubleshoot issues that relate to clearing stale files, see Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform.

Edit allowed URLs

1. From the Main menu, go to **Administration > Permissions > Allowed URLs**.
2. Select an allowed URL configuration and click **Edit**.
3. Update the settings that Allowed URL settings on page 169 describes and click **Save**.

© 2026 Tanium Inc. All Rights Reserved

Delete allowed URLs

1. From the Main menu, go to **Administration > Permissions > Allowed URLs**.
2. Select an allowed URL configuration and click Delete.

Export or import allowed URLs

Export allowed URLs

Export allowed URLs as a file in the format required for your workflow:

- **CSV**

  You can use any application that supports CSV format to display the same allowed URL attributes (columns) as the Console **Allowed URLs** grid shows and then customize the display. For example, you can use Microsoft Excel to create charts based on allowed URL attributes.

- **JSON**

  You can export multiple allowed URL configurations as a JSON file. Exporting configurations is useful if you want to import them into another Tanium environment. For example, you might test allowed URLs in a lab environment to ensure that they work as intended before importing them into your production environment. You must be assigned a role with the **Export Content** permission to export a JSON file. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.

Perform the following steps to export allowed URLs:

1. From the Main menu, go to **Administration > Permissions > Allowed URLs**.
2. (Optional, CSV exports only) To add or remove attributes (columns) for the CSV file, click Customize Columns in the grid and select the attributes.
3. Select rows in the grid to export only specific allowed URLs. If you want to export all allowed URLs, skip this step.
4. Click Export.
5. (Optional) Edit the default export **File Name**.

   NOTE

   The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.

6. Select an **Export Data** option: **All** allowed URLs in the grid or just the **Selected** allowed URLs.
7. Select the file **Format**:
   - **List of Allowed URLs - CSV**
   - **Allowed URL Definitions - JSON** (requires **Export Content** permission)

© 2026 Tanium Inc. All Rights Reserved

8. Click **Export**.

   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

Import allowed URLs

Importing is useful if you want to copy allowed URL configurations from another Tanium environment. For example, you might test allowed URLs in a lab environment to ensure that they work as intended. You can then export the allowed URLs from the lab environment and import them into your production environment. You can import allowed URLs and other content as a JSON or XML file.

You must be assigned a role with **Import Signed Content** permission to import content files through the following steps.

1. (Non-Tanium-provided content only) Digitally sign the content file and ensure a public key is in place to validate the signature. For more information, see Authenticating content files on page 482.

   You do not have to generate keys or signatures for Tanium-provided solutions. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process.

   If you plan to import a file that another user signed, you can first perform an integrity check on the file. For more information, see Verify content file signatures on page 487.

2. From the Main menu, go to any of the following **Administration** pages:
   - **Configuration > Solutions**
   - **Permissions > Filter Groups**
   - Under **Content**, select **Sensors**, **Packages**, or **Saved Questions**
   - Under **Actions**, select **Scheduled Actions**, **All Pending Approvals**, or **Actions I Can Approve**
3. Select an **Import** option based on the source of the content:
   - **Import > Import Files**: Perform one of the following steps to select one or more files:
     - Drag and drop files from your file explorer.
     - Click **Browse for File**, select the files, and click **Open**.
   - **Import > Import URL**: Enter the URL in the **Import URL** field, and click **Import**.
4. For each file, expand the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, **Include content set overwrite** is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Install**.

© 2026 Tanium Inc. All Rights Reserved

Copy allowed URL details

Copy information from the **Allowed URLs** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the content that you copy.

1. From the Main menu, go to **Administration > Permissions > Allowed URLs**.
2. Perform one of the following steps:
    - **Copy row information**: Select one or more rows and click Copy .
    - **Copy cell information**: Hover over the cell, click Options , and click Copy .

© 2026 Tanium Inc. All Rights Reserved

Enabling authentication between platform servers and remote systems

Use the **Downloads Authentication** page to specify the credentials and certificates that Tanium Core Platform servers and remote systems use for authentication to support the operations of Tanium solutions and Tanium Clients.

When the Tanium Server or Tanium Module Server connects to a remote system for solution or Client operations, the remote system and server must trust each other. If the remote system regards the server as untrusted, then the server must authenticate. If the server regards the remote system as untrusted, that system must authenticate. For example, the following operations might require authentication:

- The Tanium Server downloads action package files from a remote system.
- Tanium™ Patch scans Linux endpoints to download available patches from repositories such as the Red Hat Content Delivery Network.
- Tanium™ Connect sends data to a security information and event management (SIEM) system.

The Tanium Server or Module Server uses a client certificate or account credentials to authenticate, depending on which authentication method the remote system requires.

A remote system authenticates by presenting a server certificate for the Tanium Server or Module Server to validate. The Tanium Server or Module Server validates using a *trusted certificate*, which is a CA certificate or pinned certificate. A CA certificate can validate any certificate that the CA digitally signed. A pinned certificate can validate only the certificate for a particular domain (such as `cdn.redhat.com`) and port. Some proxy servers require both an intermediate certificate and a CA certificate.



Only users who are assigned the Administrator reserved role can see and configure remote authentication settings.

To troubleshoot issues related to remote authentication for downloads, check the Tanium Downloader (TDL) log. For more information, see Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform.

The figure Remote authentication in the Tanium Core Platform on page 175 illustrates an example deployment where the Tanium Server and Module Server connect through a proxy server (optional) and firewall (optional) to download files from the following remote systems:

- **Remote System A**: The Tanium Server and Module Server use a client certificate to authenticate to the system and use a CA certificate to verify the server certificate of that system.
- **Remote System B**: The Tanium Server and Module Server use a client certificate to authenticate to the system and use a pinned certificate to verify the server certificate of that system.

© 2026 Tanium Inc. All Rights Reserved

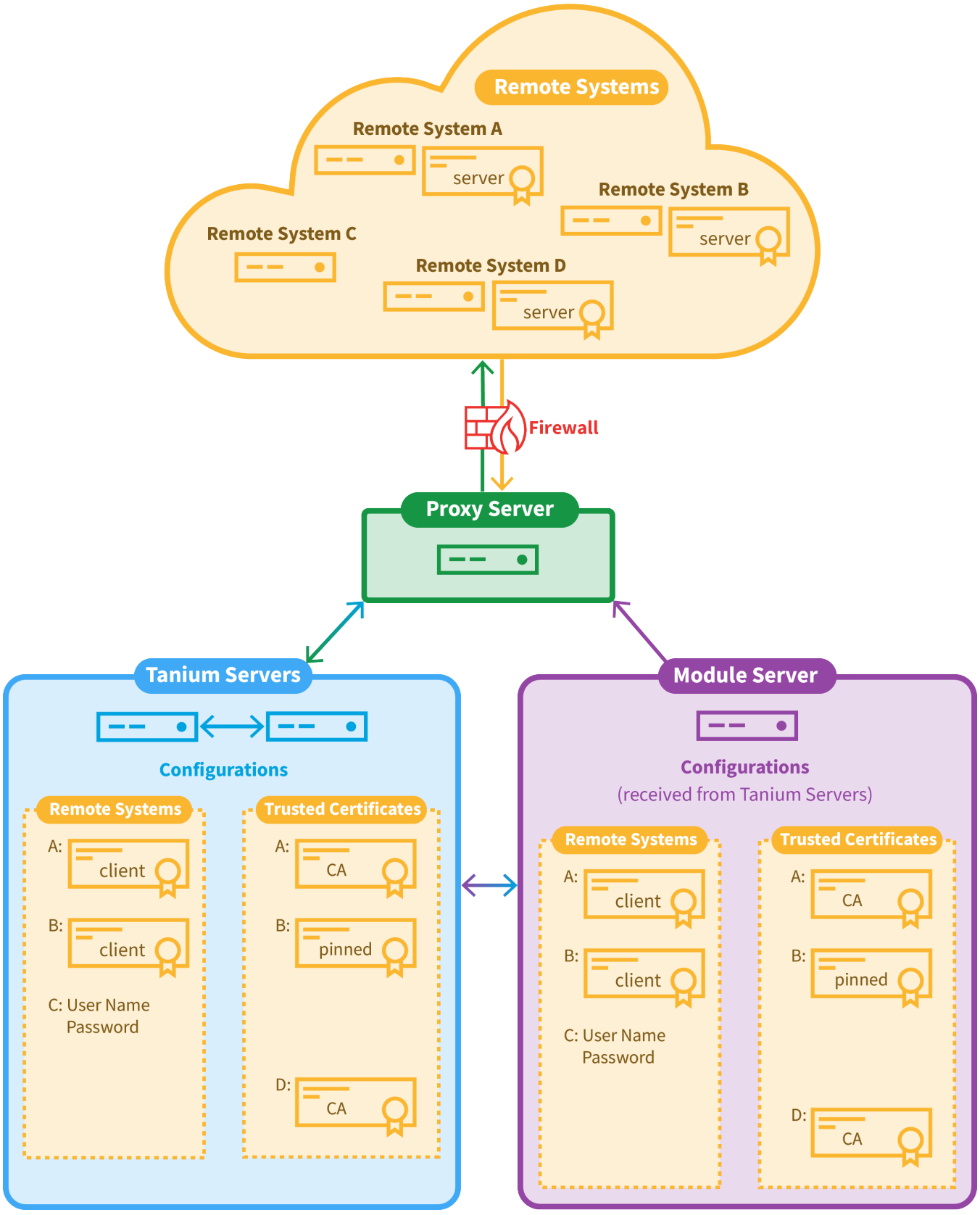
- **Remote System C**: The Tanium Server and Module Server use credentials to authenticate to the system and do not require the system to present a server certificate.
- **Remote System D**: The Tanium Server and Module Server do not need to authenticate to the system but use a CA certificate to verify the server certificate of that system.



For information about the ports for these connections, see URI on page 178.

© 2026 Tanium Inc. All Rights Reserved

© 2026 Tanium Inc. All Rights Reserved



© 2026 Tanium Inc. All Rights Reserved

Manage remote systems

Remote system configurations determine how the Tanium Server and Module Server authenticate to remote systems.

View remote systems

To see the details of remote systems that are already configured:

1. From the Main menu, go to **Administration > Configuration > Downloads Authentication > Remote Sources**.
   The tab displays the following information:
   - **Name**: The **Display Name** appears if one was configured for the system. Otherwise, the Uniform Resource Identifier (**URI**) of the system appears.
   - **Validity details**: Icons indicate which systems have certificates that are valid, expired, or valid but expiring in less than 30 days. These states do not apply to credentials.
   - **Modification details**: These values indicate which user last modified the certificates or credentials and when.
2. Expand a remote system to see the following additional details:
   - **Authentication type**: Certificate or credentials
   - **URI** of the system. This field shows the port only if the URI uses a non-standard port. For more information, see URI on page 178.
   - **Username** of the account that is used to access the system (credential authentication only)
   - **Expiration** date of the certificate (certificate authentication only)
3. Click Edit in the row for a system to see its **Description**, if that setting was configured.

Add remote systems

BEFORE YOU BEGIN

Determine how the Tanium Server and Tanium Module Server must authenticate to each remote system:

- **Certificate authentication**: Obtain a valid client certificate and matching private key, both in PEM format, from the remote system. Each system has its own methods for processing certificate and key requests. The Tanium Server and Tanium Module Server support password-protected private keys.

  IMPORTANT For the minimum bit size of the keys, see Communication with external systems on page 210.

- **Credential authentication**: Determine the user name and password that are required to authenticate to the remote system. Each system has its own methods for processing requests for access credentials.

© 2026 Tanium Inc. All Rights Reserved

ADD A REMOTE SYSTEM

1. From the Main menu, go to **Administration > Configuration > Downloads Authentication > Remote Sources** and click **Add Entry**.
2. Configure the following settings and click **Save**.

Remote system settings

Setting	Description
URI	The value depends on the **Authentication Type**: • **Certificate Authentication**: The remote system domain, such as `cdn.redhat.com` • **Credential Authentication**: The remote system URL, such as `\\server\share` Include the port number in the value only if the remote system specifies a non-standard port. For example, `example.com:17500` specifies port 17500. The standard ports are: • 443 if the remote system uses HTTPS • 80 if the remote system uses HTTP • 445 if the remote system uses a UNC path, such as Windows system that use Server Message Block (SMB) protocol
Display Name	(Optional) Enter a name to identify the remote system on the **Remote Sources** tab. If you omit this setting, the tab displays the system URI instead.
Description	(Optional) Enter text for other users to understand why Tanium Core Platform servers connect to this remote system.
Authentication Type	Select **Certificate Authentication** or **Credential Authentication**. After you save the remote system configuration, you cannot change this setting.
Authentication Certificate	(Certificate authentication only) When you add a remote system, this section appears only after you click **Upload Certificate**, select the certificate, and click **Open**. If you later edit the system configuration, you can click **Update Certificate** to select another certificate. The **Authentication Certificate** section displays the certificate **Subject** (common name) and **Expiration** date-time.
Private Key	(Certificate authentication only) When you add a remote system, this field displays the file name of the private key only after you click **Upload Private Key**, select the key, and click **Open**. If you later edit the system configuration, you can click **Update Private Key** to select another key.
Username	(Credential Authentication only) Enter the user name that is required to access the remote system.
Password	(Credential Authentication only) Enter the password that is required to access the remote system.

© 2026 Tanium Inc. All Rights Reserved

Edit remote systems

You can edit remote system configurations to replace expired certificates or update credentials that have changed. All the system settings are editable except the **Authentication Type**.

1. From the Main menu, go to **Administration > Configuration > Downloads Authentication > Remote Sources** and click Edit in the row for the system that you want to edit.
2. Update the settings in Remote system settings on page 178 and click **Save**.

Delete remote systems

1. From the Main menu, go to **Administration > Configuration > Downloads Authentication > Remote Sources**.
2. Click Delete in the row for the system that you want to remove.

Manage trusted certificates

The Tanium Server and Tanium Module Server require untrusted remote systems to authenticate. You must upload the trusted CA or pinned certificates that the Tanium Server and Tanium Module Server use to validate the certificates that systems present for authentication. If your deployment uses a proxy server that requires an intermediate certificate, upload the CA certificate and its associated intermediate certificate as a bundle.

BEST PRACTICE

Not all proxy servers require an intermediate certificate to be installed. Add the intermediate certificate only if the Tanium Core Platform and Tanium solutions cannot connect through a proxy server to external servers or to `content.tanium.com` without the certificate.

IMPORTANT

For the minimum bit size of the certificate keys, see Communication with external systems on page 210.

View trusted certificates

To see the details of certificates that are already uploaded:

1. From the Main menu, go to **Administration > Configuration > Downloads Authentication > Trusted Certificates**.
   The tab displays the following information:
   - **Name**: The **Display Name** if one was configured for the certificate.
   - **Modification details**: Which user last modified the certificate and when
   - **Expiration**: The date-time when the certificate expires. The **Trusted Certificates** tab displays warnings if certificates have expired or will expire in less than 30 days.
2. Click Edit in the row for a certificate if you want to see the **Subject**, **Domain**, and **Port** settings that Trusted certificate settings on page 180 describes.

© 2026 Tanium Inc. All Rights Reserved

Add trusted certificates

1. Obtain the CA, intermediate, or pinned certificate of the remote system.

   > **NOTE** If the certificate is in Privacy Enhanced Mail (PEM) format, open it in a text editor and verify that the certificate has no text before the `BEGIN CERTIFICATE` marker or after the `END CERTIFICATE` marker. Otherwise, Tanium Console generates a parsing error because it does not support PEM certificates with text outside those markers.

2. From the Main menu, go to **Administration > Configuration > Downloads Authentication > Trusted Certificates** and click **Add Trusted Certificate**.

3. Select the certificate file and click **Open**.

   > **NOTE** Upload the CA and intermediate certificates as a single file if an intermediate certificate is required.

4. Configure the following settings and click **Save**.

   Trusted certificate settings

Setting	Description
Subject	This read-only setting shows the common name of the certificate.
Expiration	This read-only setting shows the date-time when the certificate expires.
Update Certificate	Click the button if you need to upload a different certificate.
Display Name	(Optional) Enter a name to identify the certificate on the **Trusted Certificates** tab.
Domain	(Pinned certificates only) The domain for which the certificate is trusted.
Port	(Pinned certificates only) The port for which the certificate is trusted.

Edit trusted certificates

Replace certificates when they expire or change other settings when necessary.

1. From the Main menu, go to **Administration > Configuration > Downloads Authentication > Trusted Certificates** and click Edit in the row for the certificate that you want to edit.

2. Update the Trusted certificate settings on page 180 and click **Save**.

Delete trusted certificates

1. From the Main menu, go to **Administration > Configuration > Downloads Authentication > Trusted Certificates**.

2. Click Delete in the row for the certificate that you want to remove.

© 2026 Tanium Inc. All Rights Reserved

Configuring Internet access through proxy servers

Overview of proxy servers

Some organizations use proxy servers for traffic between internal servers and the Internet. If your organization uses proxies and its security policy does not allow Tanium Core Platform Servers to access Internet locations directly, configure access through the proxies. The Tanium Server and Tanium Module Server connect to the Internet to download content and module software updates from Tanium, and to download necessary files from other remote sources. Individual Tanium solutions might also have requirements to access the Internet.



Only users who have the **Administrator** reserved role can see and use the **Administration > Configuration > Proxy Settings** page.

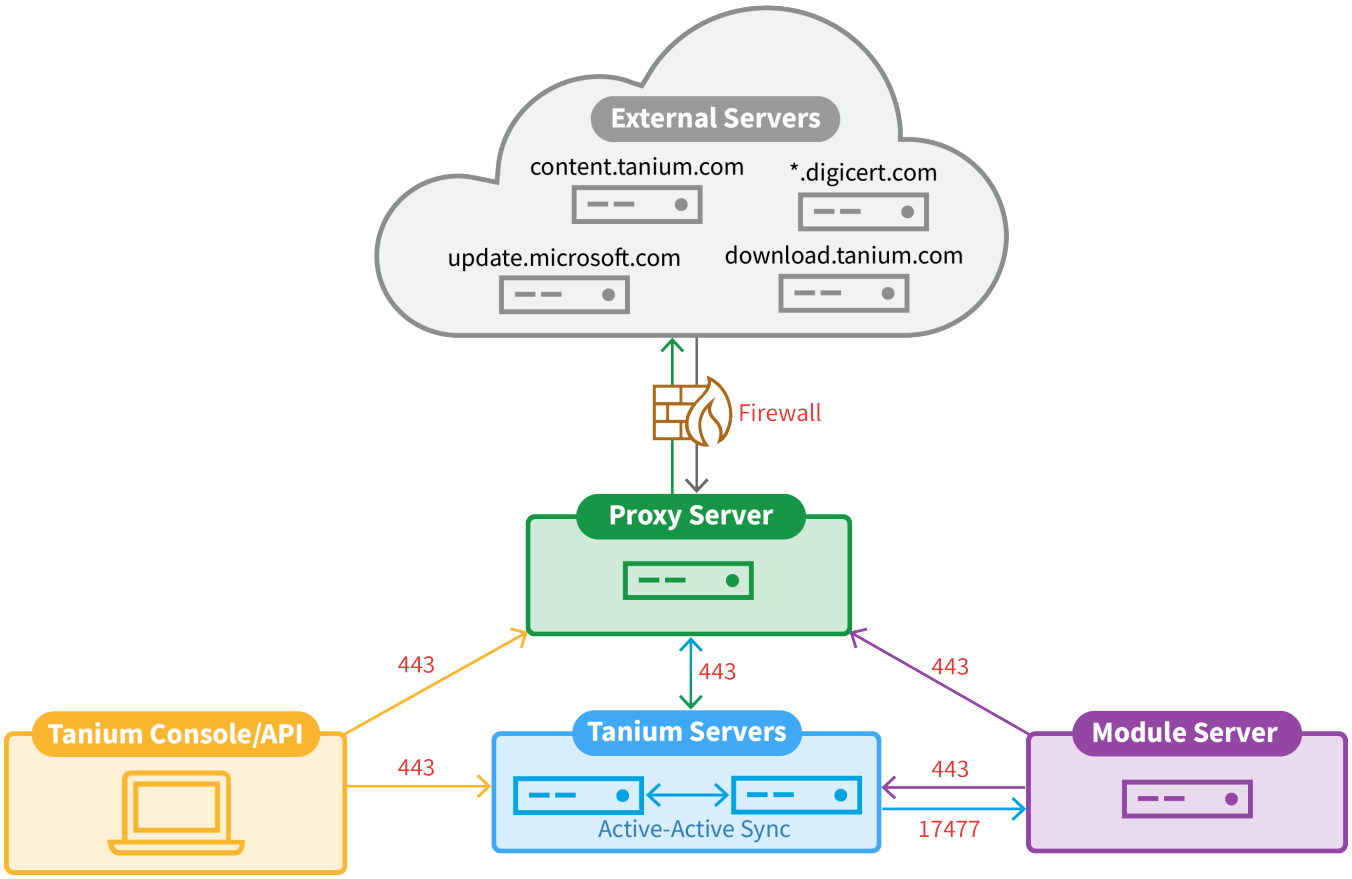
To configure the Tanium Client to connect through an HTTPS proxy server to the Tanium Server or Tanium Zone Server, see Tanium Client Management User Guide: Connect through an HTTPS proxy server.

For a list of external sites that Tanium Core Platform servers access, see Tanium Appliance User Guide: Internet URLs or Tanium Core Platform User Guide for Windows Deployments: Internet URLs.

A remote source might have its own requirements, such as certificate authentication or user authentication. For more information, see Enabling authentication between platform servers and remote systems on page 173.

© 2026 Tanium Inc. All Rights Reserved

Tanium deployment with proxy server



Types of proxy servers

The Tanium Core Platform supports two types of proxies, depending on the deployment:

- **Basic (Appliance or Windows deployments)**: A strictly IP address-based proxy server allows a specified list of servers to traverse the proxy and access the network or Internet. Add the IP addresses or fully qualified domain names of the Tanium Server and Module Server to the access list of the proxy server. If the proxy server requires authentication, configure the account ID and password.
- **NTLM (Windows deployments only)**: If the proxy server is set up to use Microsoft NT LAN Manager (NTLM), and you configure the Tanium Server service to run in the context of a service account that has sufficient permissions to traverse the proxy server, you do not have to configure an account ID and password.

Configure proxy server settings

In most cases, the best practice is to use Tanium Console to configure proxy settings, as follows. However, if you need to configure proxy settings before you have access to Tanium Console, you can configure proxy settings on the Tanium Server or Module Server host as described in the Tanium Appliance User Guide: Configuring proxy server settings or Tanium Core Platform User Guide for Windows Deployments: Configuring proxy server settings.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

The proxy server configuration is stored in configuration files on the Tanium Server host. Tanium Servers do not automatically synchronize the configuration files in an active-active deployment. If you change these settings, be sure to perform the procedure on both Tanium Servers in the active-active cluster.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Configuration > Proxy Settings**.
2. Configure the following **Tanium Server Proxy Settings** and click **Save**.

Tanium Server proxy settings

Setting	Description
Proxy Type	Select the proxy type: • **None** (disables the proxy server settings) • **Basic** • **NTLM**
Proxy Server	IP address of the proxy server.
Port Number	Port number of the proxy server.
Proxy User ID	Account username that is used to establish the connection with the proxy server. This field is required if the **Proxy Type** is **Basic**. NTLM proxies use the credentials of the user context that runs the Tanium Server service.
Proxy Password	Password that is used to establish the connection with the proxy server. The password is stored in clear text within the registry.
Bypass Proxy Host List	If you configure a proxy server, you might need to configure exceptions so that connections to specified hosts do not go through the proxy server. Enter the hosts as a comma-separated list of FQDNs or IP addresses. Enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). You do not have to enter `127.0.0.1`, `localhost`, or the Tanium Module Server, but enter the active-active Tanium Servers if necessary. All supported Tanium Core Platform versions allow wildcards.
Bypass CRL Check Host List	Use this setting to list servers that the Tanium Server can trust without checking the Certificate Revocation List (CRL). Unless a server is specified in this list, the Tanium Server performs a CRL check and does not download files from a server that does not pass. Enter the servers as a comma-separated list of FQDNs or IP addresses. Enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`).

© 2026 Tanium Inc. All Rights Reserved

Tanium Server proxy settings (continued)

Setting	Description
Trusted Host List	By default, the Tanium Server validates the SSL/TLS certificate of remote servers when establishing connections to them, such as for downloading files. To bypass certificate validation for specific servers, enter their FQDN or IP address. Enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). You do not have to enter `127.0.0.1`, `localhost`, the Tanium Module Server, or Tanium Servers (standalone or active-active). All supported Tanium Core Platform versions allow wildcards.  Contact Tanium Support before modifying this setting. For more information, see Contact Tanium Support on page 724.
Mirror all changes to Module Server except Trusted Host List and Bypass CRL Check Host List	This option appears only if the Module Server is on a dedicated host that is not shared with the Tanium Server. Enable the option if you want to copy the values for Tanium Server proxy settings to the **Module Server Proxy Settings**. The only values that are not copied are **Bypass CRL Check Host List** and **Trusted Host List**.

3. Configure the **Module Server Proxy Settings** and click **Save**.
4. Test the settings by configuring the **Validate Proxy Settings** fields and clicking **Start Download**.

Proxy settings for validation

Setting	Description
Component	Tanium Server or Module Server.
File Source	• **From Tanium**—Use predefined settings for a connection to content.tanium.com. • **From Random Site**—Use predefined settings for a connection to www.msftncsi.com. • **Specify URL/Hash**—Configure your own test settings.
URL	If you selected **Specify URL/Hash**, specify the URL.
Hash	If you selected **Specify URL/Hash**, specify the hash.
Download Time	If you selected **Specify URL/Hash**, specify a maximum download time before returning a failure message.

Tanium Console returns a message that indicates success or failure. If the test fails, check that the proxy server is up and is configured as expected. Also, check that Tanium Console settings you specified match the settings that the proxy server expects. The TDownloader log has detailed event messages. For more information, see Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform.

© 2026 Tanium Inc. All Rights Reserved

5. Enable the global setting **authenticate_api_token_with_x_forwarded_for_ip** only if all API token access to the Tanium Server must go through a reverse proxy server. If the setting is disabled in such deployments, you cannot restrict which systems are allowed token access.

   a. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.

   b. In the **Name** column, click **authenticate_api_token_with_x_forwarded_for_ip**.

   c. Set the value to `1` and click **Save**.

   To configure which systems have API token access to the Tanium Server, see Enable API token authentication behind a reverse proxy on page 699.

6. If the proxy server has an IPv6 address, configure the **ForceIPV6** setting.

   Contact Tanium Support for guidance before configuring this setting. For more information, see Contact Tanium Support on page 724.

   a. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.

   b. Click **Add Setting**, specify the following values, and click **Save**:

      - **Setting Type**: **Server**
      - **Value Type**: **Numeric**
      - **Value**: `1`

© 2026 Tanium Inc. All Rights Reserved

Throttling bandwidth and connections to Tanium Clients

Bandwidth throttling overview

Use the **Bandwidth Throttles** page to configure throttles that limit the bandwidth and the number of concurrent connections that Tanium Servers or Tanium Zone Servers use to send data to Tanium Clients. The data includes sensor configurations, Tanium™ Connect exports, Tanium™ Jump Gate data, package configurations, and package files. In deployments where numerous Clients connect with the servers at the same time to download data, spikes in bandwidth usage might occur. Throttles prevent the spikes from degrading network performance by ensuring that the servers never exceed a specific bandwidth or number of connections across your entire network or in specific subnets when sending Tanium data. To enforce the limits, the servers delay sending data that would exceed the maximum bandwidth and reject connections beyond the allowed maximum number.

You can also use the **Bandwidth Throttles** page to monitor changes in bandwidth usage and the count of connections over time. Monitoring these metrics can help you determine if you need to adjust throttle configurations.



For the user role permissions to view and manage bandwidth throttle configurations and bandwidth usage, see Manage bandwidth throttling on page 79.

Bandwidth throttles control only the rate at which Tanium Servers or Zone Servers send data to Tanium Clients. The data that Clients send to the servers is not subject to throttles. Bandwidth throttles do not affect data exchanges between any other Tanium components, such as Tanium Console traffic between user systems and Tanium Servers.

In an active-active Tanium Server deployment, throttle limits are not cumulative across the Server cluster. For example, if you configure a global throttle of 1,600 Mbps and 500 connections, each Server applies those limits instead of load balancing the limits between them.



Bandwidth throttles apply to the cumulative updates that Tanium Clients download through the Microsoft Unified Update Platform (UUP).

Before you begin

When you configure throttles, strike a balance between providing enough resources (bandwidth and concurrent connections) for Tanium Clients to complete tasks in a reasonable time frame and mitigating the impact of those tasks on your network. Setting limits too low might prevent Clients from receiving all the sensors and packages that Clients need in time to respond to questions and perform actions. Setting limits too high might allow spikes in Tanium traffic to hinder other tasks that the endpoints must perform. Evaluate the default throttle settings and the bandwidth requirements of your network to determine if custom throttle settings are necessary.

© 2026 Tanium Inc. All Rights Reserved

Evaluate default throttle settings

After you set up your Tanium environment, Monitor bandwidth and connection usage on page 195 over time to determine if the default values for the global throttles suffice for the bandwidth and connection limits of your network. By default, no site throttles are configured.



The **Global Throttle for Connect Data** applies to data exports from Tanium solutions to external destinations and to data that is transferred during a Tanium Jump Gate session. For more information, see Tanium Connect exports on page 190 and Jump to endpoints on page 250.

DEFAULT THROTTLES FOR BANDWIDTH

- **Global Throttle for All Data**, which is all the data types combined: `0` (no limit)
- **Global Throttle for Package Files**: `800` Mbps
- **Global Throttle for Sensors**: `160` Mbps
- **Global Throttle for Connect Data**: `0` (no limit)

DEFAULT THROTTLES FOR CONCURRENT CONNECTIONS

- **Global Throttle for All Data**, which is all the data types combined: `0` (no limit)
- **Global Throttle for Package Files**: `1600`
- **Global Throttle for Sensors**: `40`
- **Global Throttle for Connect Data**: `0` (no limit)

Evaluate network bandwidth requirements

Evaluate the following aspects of your network to determine if you must customize the global throttles or configure subnet-specific throttles (site throttles):

- Bandwidth trends on page 188
- Global throttles on page 189
- Site throttles on page 189
- Zone Server throttles on page 190
- Tanium Connect exports on page 190
- Overlapping IP address ranges on page 190

BANDWIDTH TRENDS

Evaluate bandwidth trends for data that Tanium Server or Zone Servers send to endpoints. The trends will enable you to gauge how much the traffic affects your network and determine the maximum resources that are required to send the data. For example, if you observe that actions often expire before they can finish, the bandwidth throttles for packages might require higher values. You can

© 2026 Tanium Inc. All Rights Reserved

configure separate throttles for sensor data, package data, and all data combined. Note that the throttles for all data must accommodate every type of outbound data (such as Client registration information), not just sensor and package data. Contact Tanium Support on page 724 for help determining the throttles that are required for all data types.



The best practice is leave the all-data throttle unconfigured so that no limit applies to it. If configuring the all-data throttle is necessary, set it to at least 150 megabits per second (Mbps) above the sum of the sensor and package throttles. For example, if you set the sensors bandwidth throttle to 1,600 Mbps and the packages throttle to 1,800 Mbps, set the all-data throttle to 3,550 Mbps or higher to accommodate all additional data types.

GLOBAL THROTTLES

Determine the appropriate bandwidth and connection throttles for the data that Tanium Servers or Zone Servers send to all the subnets in your network. If specific sites require more restrictive limits than the global throttles, you can configure exceptions through *site throttles*.



Review global throttles on a monthly basis and update them if necessary. For more information, see Tanium Maintenance User Guide: Review and update global bandwidth throttles.

SITE THROTTLES

Determine whether you need subnet-specific throttles that are more restrictive than the throttles for the rest of your network. Site throttles are useful if lower limits are required for Tanium traffic in sites that are dedicated to high priority tasks or that experience more non-Tanium traffic.



The global throttles are always the maximum allowed bandwidth and number of connections, and limit any site throttles that have higher values than the global throttles.

The Tanium Server balances the available bandwidth across sites on a first-request, first-serve basis. For example, consider a deployment that applies the following bandwidth limits for packages. In this example, NAM refers to a specific site in North America and APAC refers to a specific site in the Asia-Pacific region.

- Global throttle = 3,000 Mbps
- NAM site throttle = 2,000 Mbps
- APAC site throttle = 1,600 Mbps
- Headquarters = no site-specific throttle is configured

As long as the aggregate bandwidth across all the sites does not exceed the global throttle limit of 3,000 Mbps, the NAM site or APAC site supports the maximum bandwidth that is specified in their site-specific throttles, while the Tanium Clients at Headquarters support the maximum bandwidth of the global throttle. However, if the aggregate bandwidth reaches the global limit of 3,000 Mbps,

© 2026 Tanium Inc. All Rights Reserved

the Tanium Server prevents additional bandwidth even for sites that have not reached their individual limits. For example, if the NAM site requests bandwidth first and reaches 2,000 Mbps, the APAC site and Headquarters subsequently can use no more than 1,000 Mbps between them.



Review site throttles on a quarterly basis and update them if necessary. For more information, see Tanium Maintenance User Guide: Review and update site bandwidth throttles.

ZONE SERVER THROTTLES

In a deployment with Tanium Zone Servers, determine whether they require throttles that differ from the Tanium Servers. For example, the connections between a Zone Server and Tanium Clients in external networks might support and need more or less bandwidth than the connections between Tanium Servers and Clients in internal networks.

TANIUM CONNECT EXPORTS

You use Tanium Connect to configure data exports from other Tanium solutions to external destinations, such as SQL servers, SIEMs, and email. If the destination is an on-premises server that is not accessible from the external internet, Connect first sends the data to a Tanium Client that functions as a satellite. The satellite can access the on-premises server and forward the data to it. When you configure bandwidth throttles for Connect data, they apply only to the traffic from Tanium Cloud (solutions) to satellites, not from satellites to the external destinations. Before you configure throttles for Connect data, review the connections that use satellites to assess the amount of traffic. For details about satellite connections, see Tanium Connect User Guide: Managing connections.

OVERLAPPING IP ADDRESS RANGES

Determine whether the sites that require separate throttles have overlapping IP address ranges. Only the throttle for the site with the smallest IP address range applies to an endpoint that has an address within the ranges of multiple sites. For example, the endpoints in subnet 192.168.2.0/26 are a small subset of the endpoints in subnet 192.168.2.0/24. Therefore, the 192.168.2.0/26 site throttle override the 192.168.2.0/24 site throttle for an endpoint that is in both subnets, such as IP address 192.168.2.1. If multiple subnets throttles have overlapping IP address ranges that are equal in size, the throttle that was configured most recently overrides the other throttles for the overlapping IP addresses.

Configure global throttles

Configure global throttles on the bandwidth and number of connections for each data type that requires a distinct throttle: all data combined (packages, sensors, and all other types), just package files, or just sensors. By default, global throttles apply to both Tanium Servers and Zone Servers, but you can configure Zone Server-specific throttles if necessary. Existing settings are preserved after upgrades.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Configuration > Bandwidth Throttles** and select the **Configure Throttles** tab.
2. In the **Global Throttles** section, click **Add** or Edit  beside the data type that you want to throttle.
3. Enter the maximum bandwidth in Mbps.

   To delete a throttle, enter `0` to specify unlimited bandwidth.
4. Enter the maximum number of concurrent connections between Tanium Clients and Tanium Server.

   To delete a throttle, enter `0` to specify unlimited connections.
5. Click **Save**. Your throttle updates apply immediately.
6. (Zone Server only) For each Zone Server that requires global throttles that differ from those you configured for the Tanium Server, create a JSON file named `server-throttles.json`. The file must be in the Zone Server installation folder. Contact Tanium Support on page 724 for the steps to move the file to the Tanium™ Appliance. The file contents must match the following format, including the comma after each value except the last one. The bandwidth and connection limit values are always numbers (not enclosed in quotation marks) and the bandwidth units are bytes per second. To convert from megabits per second (Mbps), multiply Mbps values by 1,000,000 and divide by 8. For example, the value to enter for 1,600 Mbps is `200000000`.

   ```
   { "data": [{
      "bandwidth_bytes_limit" : <maximum bandwidth for all data>,
      "connection_limit" : <maximum number of concurrent connections for all
   data>,
      "download_bandwidth_bytes_limit" : <maximum bandwidth for packages>,
      "download_connection_limit" : <maximum number of concurrent connections
   for packages>,
      "sensor_bandwidth_bytes_limit" : <maximum bandwidth for sensors>,
      "sensor_connection_limit" : <maximum number of concurrent connections for
   sensors>
   }]}
   ```

   When this file is present, the Zone Server does not inherit any global or site throttle settings from the Tanium Server. Any settings that you omit from the file have a default value of 0 (no limit). After you add, edit, or delete the file, the changes apply immediately and you do not have to restart the Zone Server service.

Configure site throttles

Configure site throttles for the data that Tanium Servers or Zone Servers send to specific Tanium Client subnets. By default, site throttles apply to both Tanium Servers and Zone Servers, but you can configure Zone Server-specific throttles if necessary. Site throttles cannot exceed global throttles.

© 2026 Tanium Inc. All Rights Reserved

Base throttles on local or NAT IP addresses

Use the **IP address type** setting to specify whether all the sites in your environment use local or NAT IP addresses. You cannot specify both types. By default, Tanium Servers and Zone Servers treat the IP addresses as NAT-translated. Perform the following steps if you need to change this setting:

1. From the Main menu, go to **Administration > Configuration > Bandwidth Throttles** and select the **Configure Throttles** tab.
2. Go to the **Site Throttles** section and Edit the **IP address type**.
3. Select NAT or local as the type, and click **Save**.

Add sites

Add a site for each group of Tanium Client subnets that require the same bandwidth throttles for data received from Tanium Servers.

> NOTE
>
> For subnets that receive data from Zone Servers, you configure the sites when you Add site throttles on page 192.

1. From the Main menu, go to **Administration > Configuration > Bandwidth Throttles** and select the **Configure Throttles** tab.
2. Go to the **Site Throttles** section, click **Add Site**, configure the following settings, and click **Save**. Tanium Console then displays each subnet that you added to the site.

Site settings

Setting	Description
Site Name	Enter a name to identify the site.
Subnets	Enter one or more subnets in CIDR format, such as `192.168.2.0/24` or `2001:db8::/32`. Enter one subnet per line.
Apply Throttles To	Select whether to apply throttles for the site to the: • **Total bandwidth shared across all subnets in bundle** • **Individual bandwidth of each subnet in bundle**
Monitor site usage	Select this option to track data for this site on the **Monitor Usage** tab. You can track data for up to 100 sites. For more information, see Monitor bandwidth and connection usage on page 195.

Add site throttles

Configure site-specific bandwidth throttles that apply to all data types combined, just package files, just Connect and Jump Gate data, or just sensors.

1. From the Main menu, go to **Administration > Configuration > Bandwidth Throttles** and select the **Configure Throttles** tab.
2. Go to the **Site Throttles** section, which has a ***<site_name>*** subsection for each site that you added.
3. For each data type that you want to throttle, click **Add** in the ***<site_name>*** subsection.

© 2026 Tanium Inc. All Rights Reserved

4. Enter the maximum bandwidth in Mbps and enter the maximum number of concurrent connections. For all settings, the default `0` specifies no limit.

   If a limit is configured for any setting, you can enter `0` to delete the throttle and revert its value to unlimited.

5. Click **Save**. Your throttle updates apply immediately.

6. (Zone Server only) For each Zone Server that requires site throttles that differ from those you configured for the Tanium Server, create a JSON file named `site-throttles.json`. The file must be in the Zone Server installation folder. (Contact Tanium Support on page 724 for the steps to move the file to the Tanium Appliance.) The file contents must match the following format, including commas. The bandwidth and connection limit values are always numbers (not enclosed in quotation marks) and the bandwidth units are bytes per second. To convert from megabits per second (Mbps), multiply Mbps values by 1,000,000 and divide by 8. For example, the value to enter for 1,600 Mbps is `200000000`. This example specifies two sites: one with three subnets and one with two subnets. The `all_subnets_flag` controls whether the throttles apply individually to each subnet (`0`) or apply to the total bandwidth that is shared across all the subnets (`1`).

```
{ "data": [
   {
      "all_subnets_flag" : [0 | 1],
      "bandwidth_bytes_limit" : <maximum bandwidth for all data>,
      "connection_limit" : <maximum number of concurrent connections for all
data>,
      "download_bandwidth_bytes_limit" : <maximum bandwidth for packages>,
      "download_connection_limit" : <maximum number of concurrent connections
for packages>,
      "sensor_bandwidth_bytes_limit" : <maximum bandwidth for sensors>,
      "sensor_connection_limit" : <maximum number of concurrent connections
for sensors>,
      "subnets" : [
         {
           "range" : "<subnet CIDR>"
         },
         {
           "range" : "<subnet CIDR>"
         },
         {
           "range" : "<subnet CIDR>"
         }
      ]
   },
   {
      "all_subnets_flag" : [0 | 1],
      "bandwidth_bytes_limit" : <maximum bandwidth for all data>,
      "connection_limit" : <maximum number of concurrent connections for all
```

© 2026 Tanium Inc. All Rights Reserved

```
data>,
      "download_bandwidth_bytes_limit" : <maximum bandwidth for packages>,
      "download_connection_limit" : <maximum number of concurrent connections
for packages>,
      "sensor_bandwidth_bytes_limit" : <maximum bandwidth for sensors>,
      "sensor_connection_limit" : <maximum number of concurrent connections
for sensors>,
      "subnets" : [
         {
           "range" : "<subnet CIDR>"
         },
         {
           "range" : "<subnet CIDR>"
         }
      ]
   }
]}
```

When this file is present, the Zone Server does not inherit any global or site throttle settings from the Tanium Server. Any settings that you omit from the file have a default value of 0 (no limit). After you add, edit, or delete the file, the changes apply immediately and you do not have to restart the Zone Server service.

Verify throttle delays

You can view the current delays (**Queue delay** values) that the Tanium Server applies to enforce throttles to determine if the throttles require updates. Review global throttles as part of monthly maintenance and site throttles as part of quarterly maintenance for your Tanium environment.

1. From the Main menu, go to **Administration > Configuration > Bandwidth Throttles** and select the **Configure Throttles** tab.
2. Go to the page section that shows the type of throttles for which you want to see information about delays.
   For example, if you set the bandwidth limit for the **Global Throttle for All Data** to 1,600 Mbps and the Tanium Server starts sending 1,600 megabits of data, the **Global Throttle for All Data** section initially displays a **Queue delay** of 1,000 milliseconds (ms). After the download completes, the **Queue delay** drops to 0 ms until the Server sends more data.



Tanium Console displays queue delays only for the Tanium Server. For the queue delays associated with Zone Servers, contact support@tanium.com.

Tanium Console uses the following icons to indicate the severity level of a **Queue delay**. The severity levels indicate the likelihood that the delay will prevent Tanium Clients from receiving all the sensors and packages that the Clients need in time to respond to questions and perform actions.

© 2026 Tanium Inc. All Rights Reserved

- 0 to 9,999 ms: Little or no risk of disrupting Tanium functions.
- 10,000 to 44,999 ms: Moderate risk of disrupting Tanium functions.
- 45,000 ms or more: High risk of disrupting Tanium functions.

Monitor bandwidth and connection usage

Monitor bandwidth usage and Tanium Client connection usage over time to determine if the throttles require adjustment. On the **Bandwidth Throttles** page, the **Monitor Usage** tab shows the data as a line chart for each data type. In each chart, the red line represents the throttle value and the blue line represents your network usage. The tab tracks global usage by default but tracks site-specific usage only for sites that have the Monitor site usage on page 192 option selected.

> **NOTE** A chart does not show a red line (throttle data) for periods when the throttle is set to `0` (no limit). During such periods, the chart shows only the usage data.

1. From the Main menu, go to **Administration > Configuration > Bandwidth Throttles** and select the **Monitor Usage** tab.
2. Select the usage and throttle data that you want to view:
   - **Throttles**: Select one of the following options:
     - **Global Usage**: View usage across your environment and compare it to the global throttles.
     - ***<Site>***: View usage for the subnets of a specific site and compare that usage to the site throttle.
   - **Timeframe**: View data for the past:
     - **Hour**: The charts show data points at 15-minute intervals.
     - **Day** (24 hours): The charts show data points at 6-hour intervals.
     - **Week**: The charts show data points at 24-hour intervals.
     - **Month**: The charts show data points at 1-week intervals.
   - ***<Data type>***: Expand a section to see the chart for a data type. The **All Data Types** section is expanded by default.

   > **TIP** Click Refresh to update the charts if you think their data might have changed after you opened the **Monitor Usage** tab.
3. (Optional) Hover over the chart to open a popup window that shows the usage and throttle data at a specific time. The bandwidth values are in Mbps.

© 2026 Tanium Inc. All Rights Reserved

Optimizing Tanium Client peering through subnets

Overview of Client subnets

Client peering

Tanium Clients interconnect within linear chains to exchange Tanium messages and files, such as for questions and actions. Peering settings define the subnet boundaries of the linear chains. The default setting values are designed to optimize network resource usage by ensuring that most of the data exchange is among the low-latency, high-bandwidth links of local area networks (LANs). Separated subnets, intentional subnets, and isolated subnets provide methods for modifying the peering behavior of Clients in subnets where the default settings are not applicable or not optimal. For example, you can configure separated subnets to segregate their peering from a parent subnet, configure isolated subnets for VPN Clients, or configure intentional subnets to account for network address translation (NAT).

Before configuring subnets, be sure that you understand the behavior that the default settings define and the impact of your changes. For more information, see Tanium Client Management User Guide: Configuring Tanium Client peering.

NOTE

To troubleshoot Client peering issues, see Troubleshoot Tanium Client issues on page 717.

BEST PRACTICE

Review the Client subnet configurations on a monthly basis to account for any subnets that are added to or removed from your network. For more information, see Tanium Maintenance User Guide: Review and update Tanium Client subnets.

Topology of Client subnets

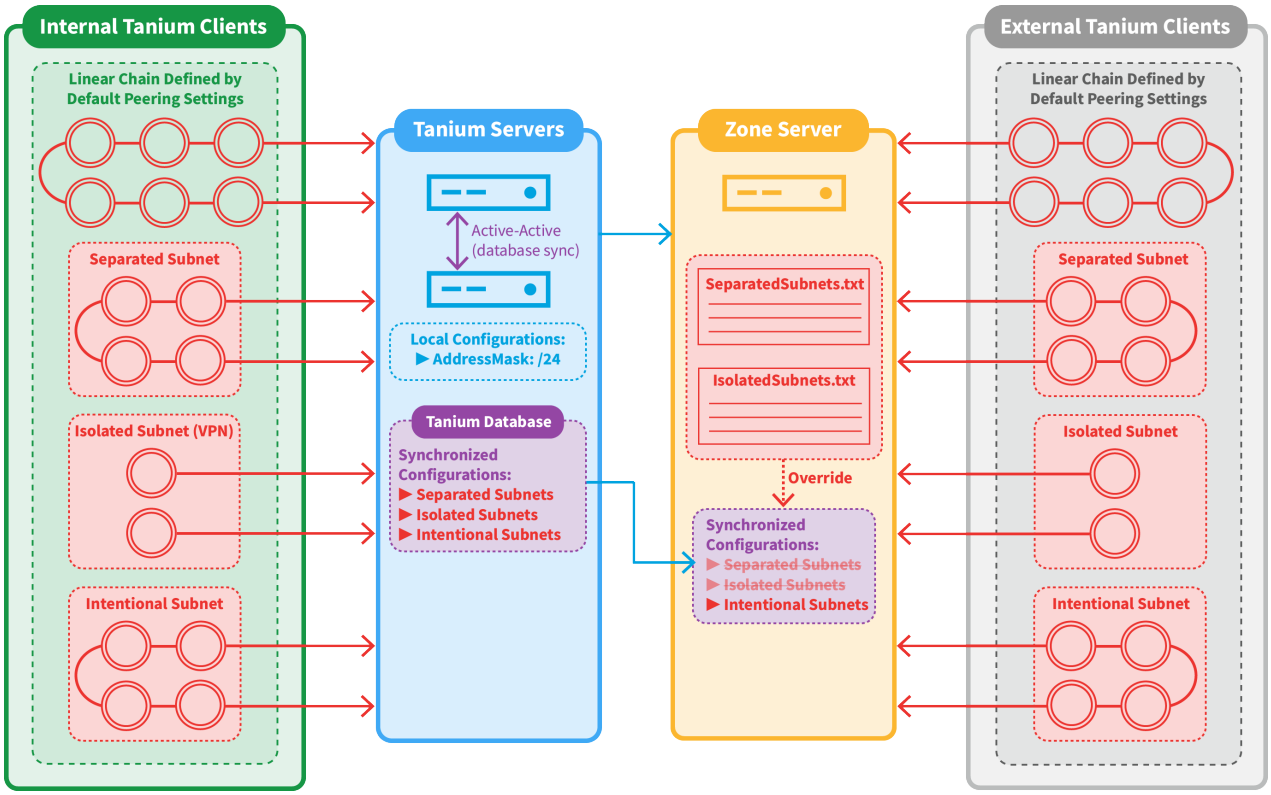
The following figure illustrates a deployment where internal Tanium Clients connect with Tanium Servers in an active-active deployment and external Clients connect with the Zone Server. This example shows separated subnets, intentional subnets, and isolated subnets within the linear chains that the default peering settings define.

NOTE

The following figure shows the Tanium database on the same host as the Tanium Servers in a Tanium Appliance deployment. However, in a Windows deployment, the database is on a dedicated host.

Tanium Client peering in subnets

© 2026 Tanium Inc. All Rights Reserved



Configure separated subnets

Tanium Clients in a *separated subnet* can peer only with other Clients that are within that subnet. Configure separated subnets to specify more granular exceptions for Client peering than the subnet boundaries that the address mask or prefix settings define (see Tanium Client Management User Guide: Address mask and prefix settings). Clients use the separated subnets configuration for peering based on whether they connect to the Tanium Server or Zone Server. Each Server uses the configuration to manage the peer lists for Clients that register through it.

After you configure separated subnets, you do not have to restart the Tanium Servers or Zone Servers. Tanium Clients might take up to two to six hours (the randomized Client-reset interval) to finish applying all the changes associated with the new configuration. To verify that the separated subnets work as expected after the Clients register, see Tanium Client Management User Guide: Verify Tanium Client peering and leader connections.

The figure Tanium Client peering in subnets on page 196 shows an example deployment with separated subnets.

BEST PRACTICE

In most environments, the separated subnets configuration is the same for all Zone Servers and Tanium Servers, and the best practice is to keep the configuration synchronized across Servers to avoid confusion. In complex environments with overlapping subnets, you might have to segregate subnets differently for Zone Servers. In such cases, you can modify `SeparatedSubnets.txt` on each Zone Server that requires a unique configuration.

© 2026 Tanium Inc. All Rights Reserved

NOTE

A user role with the **Read Separated Subnets** permission is required to view the separated subnets configuration. The **Write Separated Subnets** permission is required to create, modify, or delete the separated subnets configuration. The Administrator reserved role has these permissions.

Tanium Core Platform 7.3 or later supports IPv6 subnets, such as: `2001:db8::/32`. Contact Tanium Support for details.

Configure separated subnets that are the same for Tanium Servers and Zone Servers

ADD SUBNETS

1. From the Main menu, go to **Administration > Configuration > Subnets**.
2. In the **Separated Subnets** section, click **New Subnets**.
3. Enter each subnet in CIDR format using separate lines or commas as delimiters. Use the semicolon `;` or hash `#` character before any optional comments, as shown in the following example. You cannot use a comma `,` within the comment text because that character is reserved as a subnet delimiter.

```
192.168.0.0/26 #This is a data center subnet.
192.168.2.0/26 ;This is a branch office subnet.
2001:db8::/32
```

TIP

If your deployment includes Zone Servers that require different separated subnets than the Tanium Servers, copy entries from the text field to the clipboard to use when you configure separated subnets that are specific to Zone Servers.

4. Click **Save**.

EDIT SUBNETS

1. From the Main menu, go to **Administration > Configuration > Subnets**.
2. Select one of the **Separated Subnets** and click **Edit**.
3. Edit the subnet (**CIDR**) and **Comment**, and click **Save**.

Configure separated subnets that are specific to Zone Servers

If a deployment includes Zone Servers that require different separated subnets than the Tanium Servers, perform the following steps based on your Tanium infrastructure to add a custom separated subnets configuration to each Zone Server. Because Zone Servers do not synchronize custom subnet configurations, each Zone Server can have a unique configuration.

© 2026 Tanium Inc. All Rights Reserved

WINDOWS INFRASTRUCTURE

1. Create a plain text file named `SeparatedSubnets.txt`.
2. Enter the subnets and optional comments that you entered for the Tanium Server into `SeparatedSubnets.txt`. Use the formatting described in Add subnets on page 198.
3. Move `SeparatedSubnets.txt` to the installation directory of each Zone Server (the default installation directory is `\Program Files (x86)\Tanium\Tanium Zone Server`). If necessary, you can modify the file contents for each Zone Server that requires a unique configuration.

NOTE

If you remove `SeparatedSubnets.txt` from the Zone Server, it reverts to using the separated subnets that are configured on the Tanium Servers.

TANIUM APPLIANCE INFRASTRUCTURE

1. On the Zone Server Appliance, sign in to the TanOS console as a user with the `tanadmin` role.
2. From the **tanadmin menu**, enter `2-2` (Tanium Operations > Configuration Settings).
3. Enter `12` to edit the `SeparatedSubnets.txt` file.
4. Use the menu to specify subnets in CIDR format.

Configure isolated subnets

Configure *isolated subnets* to disable Client peering for a specified list of subnet and endpoint IP addresses. If the IP address of a Tanium Client is in an isolated subnet, the Tanium Server or Zone Server sends that Client an empty peer list to prevent the Client from participating in peering. Each Server uses the configuration to manage the peer list for Tanium Clients that register through it.

After you configure isolated subnets, you do not have to restart the Tanium Servers or Zone Servers. Tanium Clients might take up to two to six hours (the randomized Client-reset interval) to finish applying all the changes associated with the new configuration. To verify that the isolated subnets work as expected after the Clients register, see Tanium Client Management User Guide: Verify Tanium Client peering and leader connections.

The figure Tanium Client peering in subnets on page 196 shows an example deployment with isolated subnets.

IMPORTANT

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

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

- Configure isolated subnets for virtual desktop infrastructure (VDI) instances in a high-density environment with shared storage or for any other virtual endpoints where concurrent disk I/O operations must be limited. Endpoints cache file chunks to share distributed files with peers, which requires multiple endpoints in the linear chain to concurrently read and write file chunks. Isolating an endpoint reduces the concurrent disk I/O that normally occurs when this cache is used to share files with peers. For more information, see Tanium Client Management User Guide: File distribution.
- You might find it convenient to use isolated subnets to disable peering in other cases, such as for testing or debugging peering when you have to troubleshoot network issues. Note that disabling peering causes Tanium Clients to consume more network resources in terms of bandwidth and Client-server connections over the WAN. For troubleshooting cases, after you resolve the network issues, the best practice is to remove the Clients from the isolated subnets configuration so that they resume peering.
- In most environments, the isolated subnets configuration is the same for all Zone Servers and Tanium Servers, and the best practice is to keep the configuration synchronized across Servers to avoid confusion. In complex environments with overlapping subnets, you might have to segregate subnets differently for Zone Servers. In such cases, you can modify the subnets configuration on each Zone Server that requires a unique configuration.

NOTE

A user role with the **Read Isolated Subnets** permission is required to view the isolated subnets configuration. The **Write Isolated Subnets** permission is required to create, modify, or delete the isolated subnets configuration. The Administrator reserved role has these permissions.

Tanium Core Platform 7.3 or later supports IPv6 subnets, such as: `2001:db8::/32`. Contact Tanium Support for details.

Configure isolated subnets that are the same for Tanium Servers and Zone Servers

ADD SUBNETS

1. From the Main menu, go to **Administration > Configuration > Subnets**.
2. In the **Isolated Subnets** section, click **New Subnets**.
3. Enter each subnet in CIDR format using separate lines or commas as delimiters. Use the semicolon `;` or hash `#` character before any optional comments, as shown in the following example. You cannot use a comma `,` within the comment text because that character is reserved as a subnet delimiter.

```
192.168.0.0/26 #This is a data center subnet.
192.168.2.0/26 ;This is a branch office subnet.
2001:db8::/32
```

© 2026 Tanium Inc. All Rights Reserved

If your deployment includes Zone Servers that require different isolated subnets than the Tanium Servers, copy entries from the text field to the clipboard to use when you configure isolated subnets that are specific to Zone Servers.

4. Click **Save**.

EDIT SUBNETS

1. From the Main menu, go to **Administration > Configuration > Subnets**.
2. Select one of the **Isolated Subnets** and click **Edit**.
3. Edit the subnet (**CIDR**) and **Comment**, and click **Save**.

Configure isolated subnets that are specific to Zone Servers

If a deployment includes Zone Servers that require different isolated subnets than the Tanium Servers, perform one of the following procedures based on your Tanium infrastructure and whether you want to isolate all Clients or Clients on specific subnets. Because Zone Servers do not synchronize custom subnet configurations, each Server can have a unique configuration.



The Zone Server applies the most restrictive rule to determine the subnet for a Client. If you configure the **zs_address_mask** or **AddressMask** setting to isolate Clients, that setting overrides any subnet-based isolation that is configured in an `IsolatedSubnets.txt` file.

ISOLATE ALL CLIENTS CONNECTED TO ANY ZONE SERVER

Set the **zs_address_mask** platform setting on the Tanium Server (**Administration > Configuration > Settings > Advanced Settings**) to `4294967295`, which specifies /32 subnet boundaries (single hosts) for all Zone Servers.

For more information, see Tanium Client Management User Guide: Address mask and prefix settings.

ISOLATE ALL CLIENTS CONNECTED TO A PARTICULAR ZONE SERVER

1. Sign in to the Zone Server host as an administrator user.
2. Access the CLI. For more information, see:
   - Tanium Appliance User Guide: Reference: Tanium Core Platform command-line interface
   - Tanium Core Platform User Guide for Windows Deployments: Reference: Command-line interface
3. Navigate to the Zone Server installation folder:

```
> cd <Zone Server>
```

© 2026 Tanium Inc. All Rights Reserved

4. Configure the **AddressMask** local setting to specify /32 subnet boundaries (single hosts):

```
> TaniumZoneServer config set AddressMask 4294967295
```

For more information, see Tanium Client Management User Guide: Address mask and prefix settings.

ISOLATE CLIENTS ON SPECIFIC SUBNETS WITH WINDOWS INFRASTRUCTURE

1. Create a plain text file named `IsolatedSubnets.txt`.
2. Enter the subnets and optional comments that you entered for the Tanium Server into `IsolatedSubnets.txt`. Use the formatting described in Add subnets on page 200.
3. Move `IsolatedSubnets.txt` to the installation directory of each Zone Server (the default installation directory is `\Program Files (x86)\Tanium\Tanium Zone Server`). If necessary, you can modify the file contents for each Zone Server that requires a unique configuration.

NOTE

If you remove `IsolatedSubnets.txt` from the Zone Server, it reverts to using the isolated subnets that are configured on the Tanium Servers.

ISOLATE CLIENTS ON SPECIFIC SUBNETS WITH TANIUM APPLIANCE INFRASTRUCTURE

1. On the Zone Server Appliance, sign in to the TanOS console as a user with the `tanadmin` role.
2. From the **tanadmin menu**, enter `2`-`2` (Tanium Operations > Configuration Settings).
3. Enter `11` to edit the `IsolatedSubnets.txt` file.
4. Use the menu to specify subnets in CIDR format.

Configure intentional subnets

Overview of intentional subnets

In a network configuration that uses network address translation (NAT), the local IP addresses of Tanium Clients in the same local area network (subnet) might be mapped to different NAT IP addresses for communication with the Tanium Server or Tanium Zone Server. The default Tanium peering settings allow Clients in that subnet to peer with each other only if they share the same NAT IP address. If Clients in the same subnet are assigned to different NAT IP addresses, they can peer with each other only if you assign them to an *intentional subnet* that specifies the full range of NAT IP addresses for that subnet. Without an intentional subnet, each Client with a different NAT IP address establishes a leader connection to the Server. Network traffic is higher in a deployment with more leader connections, especially when Clients download package files for running actions. Therefore, configuring intentional subnets can increase peering and reduce traffic, particularly in deployments where many Clients use NAT when connecting to the Server over the Internet.

The figure Tanium Client peering in subnets on page 196 shows an example deployment with intentional subnets.

© 2026 Tanium Inc. All Rights Reserved

NOTE

A user role with the **Read Intentional Subnets** permission is required to view the intentional subnets configuration. The **Write Intentional Subnets** permission is required to create, modify, or delete the intentional subnets configuration. The Administrator reserved role has these permissions.

You can configure IPv6 subnets, such as `2001:db8::/32`. Contact Tanium Support for details.

The following table shows examples of Tanium Clients that do or do not require intentional subnets to enable peering. The example IP addresses are listed as they would appear on the **Administration > Configuration > Client Status** page, where the **Network Location (from Client)** column shows the pre-NAT IP addresses and the **Network Location (from Server)** column shows the NAT IP addresses. In this example, the **AddressMask** platform setting specifies a /24 address mask, which is the default peering range (see Tanium Client Management User Guide: Overview of Tanium Client peering settings).

Example of Tanium Client peering requirements

Tanium Client	Network Location (from Client)	Network Location (from Server)	Intentional subnet required for peering?
TC-UK-1	31.0.0.11	31.0.0.11	**No**: The Clients do not use NAT. Therefore, even though their IP addresses differ, they can peer because they are in the same subnet within the default peering range (**AddressMask** = `/24`).
TC-UK-2	31.0.0.12	31.0.0.12	
TC-US-1	172.16.0.11	14.0.0.11	**No**: The Clients can peer because they use the same NAT address.
TC-US-2	172.16.0.12	14.0.0.11	
TC-HQ-1	10.0.0.11	98.0.0.1	**Yes**: The Clients are in the same subnet within the default peering range, but the **AddressMask** setting does not apply because their NAT IP addresses differ. Without an intentional subnet, the Tanium Server interprets the different NAT IP addresses as an indication that the Clients are in different subnets and therefore prevents peering.
TC-HQ-2	10.0.0.12	98.0.0.2	

Before you begin

You can define intentional subnets using either of the following methods:

- **Intentional subnet sites:** In Tanium Console, you can specify a **Site** name for an *intentional subnet site* and the subnets that belong to that **Site**. Clients in the subnets that belong to a single site can peer with one another.
- **PeerNeighborhood Client setting:** You can configure the same *neighborhood name* for the **PeerNeighborhood** setting on each Client that can peer. You can use this setting to define intentional subnets in the following scenarios:
    - You want to allow Clients that have a wide variety of NAT IP addresses to peer, and the variety of IP addresses makes subnets difficult to define, or subnets overlap among sites that need to remain isolated.
    - You want to deploy Clients that are always allowed to peer, regardless of NAT IP addresses, such as virtual machines in a cloud environment.
    - You want to manually allow specific Clients to peer.

© 2026 Tanium Inc. All Rights Reserved

To determine the appropriate method to define intentional subnets, and the appropriate **Site** names and subnet CIDR values or **PeerNeighborhood** names:

1. From the Main menu, go to **Administration > Configuration > Client Status** and identify endpoints that are in the same subnet [based on their **Network Location (from Client)**] but are not peering because their NAT IP addresses [**Network Location (from Server**)] differ.

   The Tanium Server considers pre-NAT IP addresses to be in the same subnet based on the **AddressMask** (IPv4) or **AddressPrefixIPv6** setting.

2. Choose appropriate **Site** or **PeerNeighborhood** names for the endpoints that you identified. For example, you might have a `HeadQuarters` site for endpoints in the headquarters subnet and a `NAM` site for endpoints in a North America branch office subnet.

3. Inventory the NAT IP addresses of each site to determine the appropriate method to define the intentional subnets and, if applicable, the CIDR values to enter.

   - If the subnets are reasonable to define and do not overlap among sites that need to remain isolated, use the NAT IP addresses to determine the appropriate subnets in intentional subnet sites.

     The best practice is to enter the smallest subnet ranges possible that include the identified endpoints while allowing for potential changes to their NAT IP addresses. As an example, for the Clients TC-HQ-1 (98.0.0.1) and TC-HQ-2 (98.0.0.2) in the table Example of Tanium Client peering requirements on page 203, you might configure a **Site** named `HeadQuarters` with one of the following subnets, which are listed in descending order in terms of the size of their IP address range:

     - **98.0.0.0/24**: Peering is allowed for all Tanium Clients with NAT IP addresses in the range 98.0.0.0 to 98.0.0.255. If TC-HQ-1 and TC-HQ-2 are assigned to new NAT IP addresses within that range, they can still peer.
     - **98.0.0.0/30**: Peering is allowed for all Tanium Clients with NAT IP addresses in the range 98.0.0.0 to 98.0.0.3. If the NAT IP address of TC-HQ-1 changes to 98.0.0.3 and TC-HQ-2 stays at 98.0.0.2, they can still peer. However, if TC-HQ-1 changes to 98.0.0.4, it cannot peer with TC-HQ-2.
     - **98.0.0.1/32 and 98.0.0.2/32**: Peering is allowed only for Tanium Clients with NAT IP addresses 98.0.0.1 and 98.0.0.2. TC-HQ-1 and TC-HQ-2 cannot peer if their NAT IP addresses change.

     After you determine the appropriate subnet ranges, follow the steps in Define intentional subnets using Sites on page 205.

   - If the IP addresses are too varied to define reasonable subnets, or if subnets overlap among sites that need to remain isolated, see Define intentional subnets using the PeerNeighborhood Client setting on page 205.

4. Consider whether newly deployed Clients in certain networks might have different NAT IP addresses but are allowed to peer. If so, see Define intentional subnets using the PeerNeighborhood Client setting on page 205.



After you configure intentional subnets, Tanium Clients might take up to two to six hours (the randomized Client-reset interval) to finish applying all the changes associated with the new configuration.

© 2026 Tanium Inc. All Rights Reserved

NOTE

Intentional subnet configurations are always synchronized across all Zone Servers and Tanium Servers.

Define intentional subnets using Sites

The Tanium Server can identify an intentional subnet by a **Site** name that you specify and allow peering among all Tanium Clients that are in the subnets you add to that **Site**.

ADD SUBNETS

1. From the Main menu, go to **Administration > Configuration > Subnets**.
2. In the **Intentional Subnets** section, click **New Subnets**.
3. Enter a name to identify the **Site** that comprises the intentional subnets.
4. (Optional) Enter a comment to help other users understand the function of the subnet in your organization.
5. In the **New subnet CIDRs** field, enter each subnet in CIDR format (`a.b.c.d/x`) using separate lines or commas as delimiters.
6. Click **Save**.

EDIT SUBNETS

1. From the Main menu, go to **Administration > Configuration > Subnets**.
2. Select one of the **Intentional Subnets** and click **Edit**.
3. Edit the subnet (**CIDR**) and **Comment**, and click **Save**.

Define intentional subnets using the PeerNeighborhood Client setting

Use the **PeerNeighborhood** Client setting to designate certain Clients that are allowed to peer with one another. You can apply the setting during or after Client deployment. The Tanium Server allows these Clients to peer, regardless of the NAT IP of each Client.

Set the same **PeerNeighborhood** name for all Clients in each site that are allowed to peer. For example, if you have lab sites "Lab East" and "Lab West," you can set the **PeerNeighborhood** Client setting for all Clients in each site to `Lab-East` and `Lab-West` respectively.

For methods to modify the **PeerNeighborhood** Client setting, see Tanium Client Management User Guide: Modify Client settings.

Verify intentional subnets

After you configure intentional subnets, wait for the next Client-reset interval before verifying that the subnets work as expected. For more information, see Verify or remediate Tanium Client peering and leader connections. In the **Administration > Configuration > Client Status** page, the **Network Location (from Client)** column shows the pre-NAT IP addresses and the **Network Location (from Server)** column shows the NAT IP addresses.

© 2026 Tanium Inc. All Rights Reserved

Managing the Tanium license

The Tanium™ license file (`tanium.license`) enables the entitlements for your deployment, such as the Tanium solutions that you can use. Use the **Tanium License** page to view the license details and to replace a license.



The **Administrator** reserved role is required to see and manage the Tanium license.

License expiration

The Tanium license validity period starts when Tanium generates the license, regardless of when your organization activates it. Console shows a warning when the license will expire within 30 days, but only if you sign in as a user who is assigned the **Administrator** role. Your Tanium or partner account team will contact the procurement department of your organization well before the license expires to start the renewal process.

If the license expires, you cannot import, export, or update any Tanium solutions. The following user guides list additional effects of license expiration. After you upload a new license, full functionality is restored for all solutions.

- Comply
- Provision

View license details

1. From the Main menu, go to **Administration > Configuration > Tanium License**. This page shows most of the details about your Tanium license, including:
    - Maximum number of managed endpoints:
      The Tanium Server considers an endpoint to be *managed* if its Tanium Client has registered in the past 30 days. For the current count of unique managed endpoints, see View the count of managed endpoints on page 207.
    - License validity period:
      The page displays the license **Duration**, **Days Left**, and (for each solution) the **Start Date** and **Expiration Date**.
    - Licensed solutions:
      The grid displays entitlements for each Tanium solution. A zero indicates solutions that are not licensed.
2. (Optional) To see all the IP addresses and FQDNs that the license authorizes for accessing Tanium Console:
    a. Enter `https://<tanium_server>/info` in your browser URL field, where *<tanium_server>* is the Tanium Server FQDN or IP address.
    b. Sign in as a user who is assigned the **Administrator** reserved role.
    c. See the **licensed_server_name** setting.

© 2026 Tanium Inc. All Rights Reserved

Replace the license

Use the **Tanium License** page to apply a new license if the current one expires soon or your entitlements change.

> BEST PRACTICE
>
> In an active-active deployment, replace the license on each Tanium Server in case one Server becomes unavailable for a long time.

1. Contact Tanium Support on page 724 to obtain a new license. You must provide the FQDNs or IP addresses of the physical or virtual devices that host your Tanium Servers.
2. Copy the new license to a location that is accessible from the system that you use to access Tanium Console.
3. (Optional) Back up the current license. The steps depend on the infrastructure of your Tanium Core Platform:
   - **Windows**: Go to the Tanium Server installation directory and rename the current Tanium license.

     > BEST PRACTICE
     >
     > Include the current date in the file name (such as `tanium.license_2022-02-30`) in case you repeat this procedure at a later date.

   - **Tanium Appliance**: To run an automatic or manual backup, see Tanium Appliance User Guide: Backing up and recovering Tanium Appliances.
4. From the Main menu, go to **Administration > Configuration > Tanium License**.
5. Click **Upload**, select the new license file, and click **Open**.
   The Tanium Server automatically activates the new license after a few minutes.

View the count of managed endpoints

The Tanium license determines the maximum number of endpoints that you can manage through the Tanium Client. The Tanium Server considers an endpoint to be managed if its Client has registered in the past 30 days. Perform the following steps to see the current tally of managed endpoints:

1. From the Main menu, go to **Administration > Configuration > Client Status**.
2. Set the filter **Show systems that have reported in the last** to `30 Days`.
3. Select **Hide Duplicate Host Names** (it is selected by default) to show only one row for each **Host Name**, containing only the information from the last time the Client registered.

> TIP
>
> To see the most accurate count of managed endpoints for purposes other than license usage, go to the Tanium **Home** page, **Environment Status** section, and check the **Total Endpoints**. For more information, see View environment status on page 65.

© 2026 Tanium Inc. All Rights Reserved

Troubleshoot license issues

The following table lists alerts and issues related to the Tanium license. If conditions trigger an alert, Tanium Console displays it whenever you sign in. The listed corrective actions are independent options to consider, not sequential steps.

You can also see the alerts in the Tanium Server logs. For more information, see Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform.

Tanium license alerts and common issues

Issues and alerts	Corrective actions
Common issue: Tanium features unavailable Some Tanium features that you expected to access are unavailable. This might happen if you: • Activated the wrong license. • Accessed the wrong Tanium Server. • Renamed or moved the license file. • Did not wait for long enough (one minute) for the license to activate after you replaced the license.	• Verify that your license authorizes the expected features. In the **Tanium License** page, the **Solution** grid shows zero **Maximum Managed Endpoints** for features that are not licensed. For more information, see View license details on page 206. • (Windows infrastructure only) Verify that the license file has the correct name (`tanium.license`) and is in the Tanium Server installation directory. • Restart the Tanium Server service to activate the license immediately: ◦ **Tanium Appliance**: For more information, see Tanium Appliance User Guide: Start, stop, and restart Tanium services. ◦ **Windows Server**: For more information, see Tanium Core Platform User Guide for Windows Deployments: Manage Windows services for core platform servers.
Alert: license expired Tanium Console displays an alert indicating the number of days since the license expired. For more information, see License expiration on page 206.	Replace the license on page 207.
Alert: Maximum Managed Endpoints exceeded If the number of managed endpoints exceeds the **Maximum Managed Endpoints** in the license, Tanium Console displays a warning and indicates the current number of managed endpoints. If the count exceeds the maximum by more than 10 percent, Console also directs you to contact Tanium Support.	Contact Tanium Support for a new license that supports more managed endpoints and then Replace the license on page 207.

© 2026 Tanium Inc. All Rights Reserved

Securing Tanium connections and operations through digital keys

Tanium keys overview

Use the **Key & Trust Management** page to manage the digital keys that the Tanium Core Platform uses to secure various connections and operations. For example, your organization might have a policy for periodic key rotation or you might distribute keys to install Tanium Clients on new endpoints that join your network. The following connections and operations use Tanium keys:

- **Platform server and Tanium Client connections**

  Tanium Core Platform servers and Tanium Clients secure their interconnections using the Tanium™ Protocol, which uses TLS 1.3 as described in TLS communication on page 209. The Tanium Core Platform also supports TLS for connections that various Tanium solutions require. For more information, see the user guides for your solutions at the Tanium Resource Center.

- **External server and client connections**

  Tanium Core Platform servers communicate with external servers and clients, as described in Communication with external systems on page 210. External clients include the user systems that connect to Tanium Console and the Tanium™ API over HTTPS. To manage the certificates for Console and API access, see Securing Console and API access through certificates on page 220.

- **Content file imports**

  Keys are used to sign and authenticate content files that you import into the Tanium Server, as described in Authenticating content files on page 482.

NOTE

You require the **Administrator** reserved role to manage Tanium keys.

To troubleshoot issues that relate to Tanium keys and certificates, see Troubleshoot certificate and key issues on page 706.

TLS communication

The Tanium Protocol uses TLS 1.3 to encrypt communication among the following Tanium Core Platform components, as illustrated in the figure Tanium Protocol communication on page 210:

1 Tanium Server to Tanium Server in an active-active deployment

NOTE

For some communications between active-active Servers, such as Tanium database traffic and Lightweight Directory Access Protocol (LDAP) synchronization traffic, Tanium Appliances use IPsec instead of the Tanium Protocol.

© 2026 Tanium Inc. All Rights Reserved

2 Tanium Servers to Zone Server Hub

> **NOTE** The figure Tanium Protocol communication on page 210 shows the Zone Server Hub installed on a host that is separate from the Tanium Server hosts to illustrate that the connection is encrypted. However, in most Windows deployments and all Appliance deployments, you install the Hub on the same host(s) as the Tanium Servers.

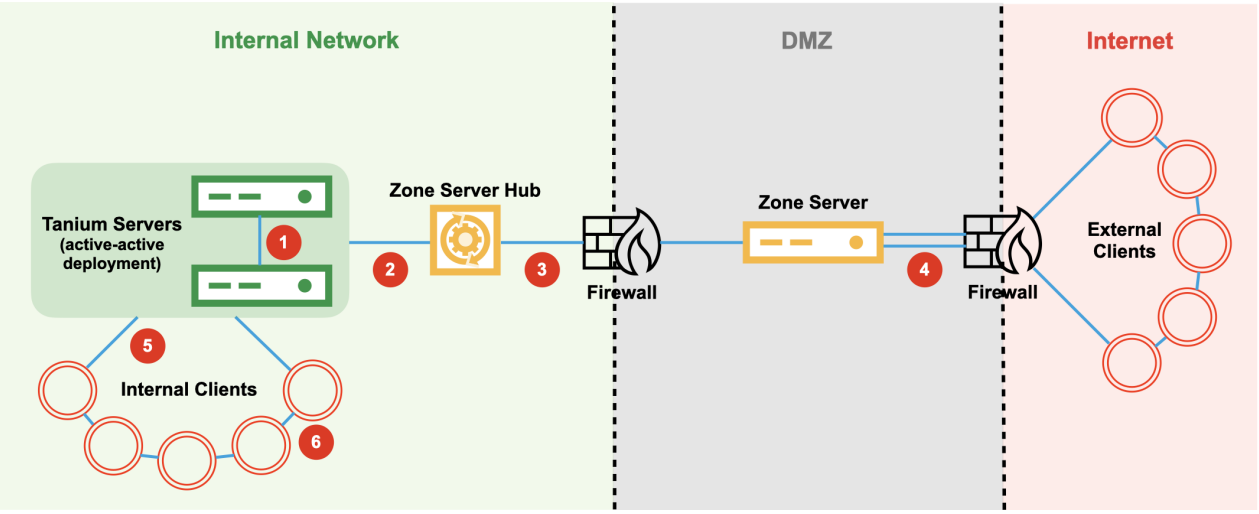
3 Zone Server Hub to Zone Server

4 Tanium Clients (external) to Zone Server

5 Tanium Clients (internal) to Tanium Servers

6 Tanium Client to Tanium Client (external and internal)

Tanium Protocol communication



TLS is enabled by default for communication among platform components. For more information about TLS, and the steps to enable or disable it, see:

- Tanium Appliance User Guide: Securing Tanium Server, Zone Server, and Tanium Client access
- Tanium Core Platform User Guide for Windows Deployments: Securing Tanium Server, Zone Server, and Tanium Client access

Communication with external systems

Tanium keys secure only Tanium traffic. Your enterprise public key infrastructure (PKI) governs the security of non-Tanium traffic among the endpoints in your network.

Tanium Core Platform servers might communicate with external servers for operations such as downloading packages (see Enabling authentication between platform servers and remote systems on page 173) or synchronizing with LDAP servers (see Importing and authenticating users through LDAP on page 666). The Tanium Server also communicates with external client systems when users access Console. External servers and clients require digital keys with a minimum bit size of 2048 for RSA and 256 for ECDSA to

© 2026 Tanium Inc. All Rights Reserved

communicate with Tanium Core Platform servers. If your Tanium license includes Tanium Certificate Manager, see Tanium Certificate Manager: View short keys for the steps to check the key sizes in your environment. Otherwise, use OpenSSL from a CLI to check the key sizes.

Root keys

When you install the Tanium Server, it automatically generates a public-private root key pair. These root keys are at the top of the Tanium key infrastructure and are required for all subordinate keys to secure connections among Tanium Core Platform components. You deploy the root public key to the Zone Server, Zone Server Hub, and Tanium Clients during installation or upgrade so that these components can secure communication with the Tanium Server. In an active-active deployment, each Tanium Server has its own root key pair that it uses to secure communication with its peer.

The Tanium Server uses separate root key pairs for TLS communication with Tanium Clients based on their version. Initially after a fresh installation or upgrade, Tanium Client 7.6 or later uses the root public key that has the name ***<Tanium Server FQDN>* Root 0**, as shows in the figure Tanium root public keys on page 216. Each new root public key that you create for version 7.6 or later has a unique name in the format ***<Tanium Server FQDN>* Root *<#>***.

> **NOTE** The name **legacy-root** identifies the root keys for Tanium Client 7.2. Tanium release 2026H1 or later does not support Client 7.2 and you cannot create new keys for that Client version. Upgrade any Client 7.2 installations to a new Client version. For more information, see Tanium Client Management User Guide: Upgrading Tanium Clients.

To view details about the root keys, see View root key information on page 216.

Subordinate keys

The Tanium Server, Zone Server, Zone Server Hub, and Tanium Clients generate subordinate keys locally and request a digital signature for each key pair. The responding server uses a private key to generate the signatures and returns the associated public key along with the signatures to enable TLS communication among the requesting servers and Clients.

Subordinate key types

The Tanium Core Platform uses the following subordinate keys, as shown in the figure Digital keys in the Tanium Core Platform on page 212:

Subordinate key types

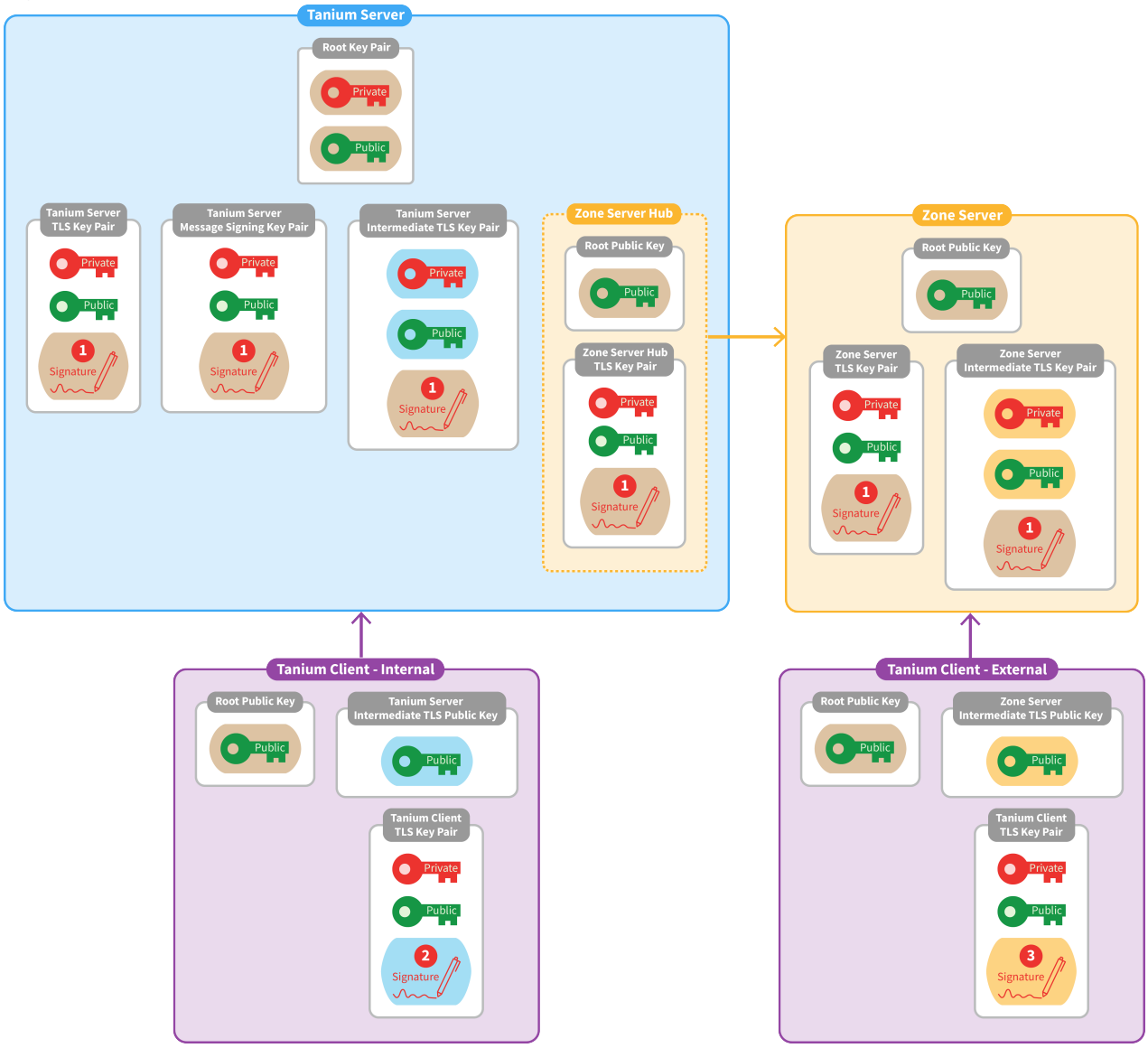
Type	Description
TLS keys	Each Tanium Core Platform server and Tanium Client uses TLS keys to enable TLS communication with other servers and Clients. The Tanium Server uses the root private key to generate signatures for the platform server TLS keys (1).
Message-signing keys	The Tanium Server uses this key pair to sign messages (such as for action packages) that it sends to Tanium Clients. The Tanium Server uses the root private key to generate a signature for the message-signing key pair (1).

© 2026 Tanium Inc. All Rights Reserved

Subordinate key types (continued)

Type	Description
Intermediate TLS keys	TheTanium Server uses an intermediate TLS private key to generate signatures for the TLS keys of internal Tanium Clients that report to that Server (2). Each Zone Server also has an intermediate TLS private key to generate signatures for the TLS keys of external Clients that report to that Zone Server (3). The servers return the intermediate TLS public key along with the signatures to enable TLS for Client communications. Using intermediate TLS keys instead of the root keys for generating signatures makes Client registration faster and less CPU intensive. For security, you can rotate the intermediate keys independently of the root keys. The Tanium Server uses the root private key to generate a signature for the intermediate key pairs on the Tanium Server and Zone Server (1).

Digital keys in the Tanium Core Platform



© 2026 Tanium Inc. All Rights Reserved

NOTE

A copy of the root public key resides in the Zone Server Hub installation directory regardless of whether the Hub is installed on the same host as the Tanium Server (as shown in the figure Digital keys in the Tanium Core Platform on page 212) or on a dedicated host.

In an active-active deployment, each Tanium Server has its own root key pair.

To enable communication among the Tanium Core Platform servers, you must also enable trust. For more information, see Synchronizing active-active Tanium Servers on page 224 and Enabling communication between Zone Servers and Hubs on page 226.

Rotation intervals for subordinate keys

Tanium Core Platform components automatically generate new subordinate key pairs when it is time to rotate them. For example, Tanium Clients renew their TLS keys four hours (the renewal window) before the end of each seven-day validity period (expiration interval) by default. The renewal windows ensure components have enough time to re-establish trust in the Tanium environment before the current keys expire.

Rotation intervals for subordinate keys

Key	Purpose	Rotation properties and settings
Tanium Server TLS keys	The Tanium Server uses this key pair for communication with another Tanium Server (in an active-active deployment), the Zone Server Hub, or Tanium Clients.	Rotation interval: 60 days Setting: pki_server_tls_key_duration_days Renewal window: 4 hours Setting: pki_server_tls_key_renewal_window_hours
Message Signing Keys	The Tanium Server uses this key pair to sign messages (such as for action packages) that it sends to Tanium Clients.	Rotation interval: 180 days Setting: pki_message_signing_key_duration_days Renewal window: 4 hours Setting: pki_message_signing_key_renewal_window_hours
Tanium Zone Server Hub TLS keys	The Zone Server Hub uses this key pair for TLS communication with the Tanium Server and Zone Server.	Rotation interval: 60 days Setting: pki_hub_tls_key_duration_days Renewal window: 4 hours Setting: pki_hub_tls_key_renewal_window_hours

© 2026 Tanium Inc. All Rights Reserved

Rotation intervals for subordinate keys (continued)

Key	Purpose	Rotation properties and settings
Tanium Zone Server TLS keys	The Zone Server uses this key pair for TLS communication with the Zone Server Hub and Tanium Clients.	Rotation interval: 60 days Setting: pki_zoneserver_tls_key_duration_days Renewal window: 4 hours Setting: pki_zoneserver_tls_key_renewal_window_hours
Tanium Client CA TLS keys	The Zone Server or Tanium Server uses this key pair to provide digital signatures for Tanium Clients when the Clients generate new TLS key pairs.	Rotation interval: 180 days Setting: pki_client_tls_ca_key_duration_days Renewal window: 168 hours (7 days) Setting: pki_client_tls_ca_key_renewal_window_hours
Tanium Client TLS keys	Tanium Clients use this key pair for TLS communication with each other and with the Zone Server or Tanium Server.	Rotation interval: 7 days Setting: pki_client_tls_key_duration_days Renewal window: 4 hours Setting: PKIClientTLSKeyRenewalWindowHours

Key rotation

Although root keys never expire, you can rotate them, which means generating new keys and revoking the old keys. Rotating keys is useful if your organization has a policy for periodic key rotation or the security of the active keys is in doubt. If the security of the active root keys is in doubt, rotate them immediately.



If your organization does not have a key rotation policy, rotate the root keys at least once every year but no more than once every six months.



Tanium Clients that are offline when you rotate keys acquire the new keys and resume regular operations upon coming online as long as those Clients were initialized with the correct `tanium-init.dat` file. For more information, see Download infrastructure configuration files (keys) on page 218.

On the **Key & Trust Management** page, the name **legacy-root** identifies the root keys for Tanium Client 7.2. You cannot rotate the **legacy-root** keys and Tanium release 2026H1 or later does not support Client 7.2. Upgrade any Client 7.2 installations to a new Client version as described in Tanium Client Management User Guide: Upgrading Tanium Clients.

© 2026 Tanium Inc. All Rights Reserved

To ensure the security of root private keys, Tanium Console exposes only root public keys. However, when you generate or revoke a public key, the Tanium Server automatically generates and revokes the private key. Furthermore, when you rotate the root keys, the Tanium Core Platform automatically rotates all subordinate keys. Regardless of whether you rotate the root keys, the subordinate keys automatically rotate at configurable intervals.

The following steps summarize the workflow for rotating keys:

1. (Optional best practice) On each Tanium Server, encrypt the `pki.db` file that contains the root keys, Tanium Server TLS keys, and message-signing keys. This is a one-time only task that you perform to prevent unauthorized access to the keys. For more information, see Encrypt the root keys database on page 217.
2. If your organization has a key rotation policy, configure automatic rotation for subordinate keys to match the policy. This is a one-time only task, unless your policy changes. For more information, see Rotation intervals for subordinate keys on page 213.
3. Generate a new root public key. The Tanium Server automatically generates a new corresponding private key and triggers the creation of new subordinate keys. For more information, see Generate root keys on page 218.

   As a best practice, wait one week before revoking the old root keys to ensure that the process of generating new keys finishes for all Tanium Core Platform components. When you revoke, any components that did not finish this process expend more processing resources and network traffic to generate new keys. However, if the security of the root keys is in doubt, revoke the old keys immediately after generating the new keys.
4. Revoke the old root public key. The Tanium Server automatically revokes the associated private key and propagates the revocation directive for the old root keys and subordinate keys to all Tanium Core Platform components. For more information, see Revoke root keys on page 218.
5. (Best Practice) Back up the Tanium deployment immediately before and after revoking the root keys. If recovery becomes necessary, you must restore the deployment from the post-revocation backup. However, the pre-revocation backup might contain information that is useful for recovery planning. The backup steps depend on your Tanium infrastructure:
   - Tanium Appliance User Guide: Backing up and recovering Tanium Appliances (a core backup is sufficient)
   - Tanium Core Platform User Guide for Windows Deployments: Back up Tanium Core Platform servers and databases

   If you configure the Tanium Server to integrate with a hardware security module (HSM), you cannot use a backup of `pki.db` to install a cryptographically identical duplicate of the Server.

HSM integration

If you configure the Tanium Server to integrate with a hardware security module (HSM) for storing and managing keys, all key operations occur on the HSM even when you use Tanium Console to initiate those operations. For more information, see Tanium Core Platform User Guide for Windows Deployments: Securing keys with an HSM.

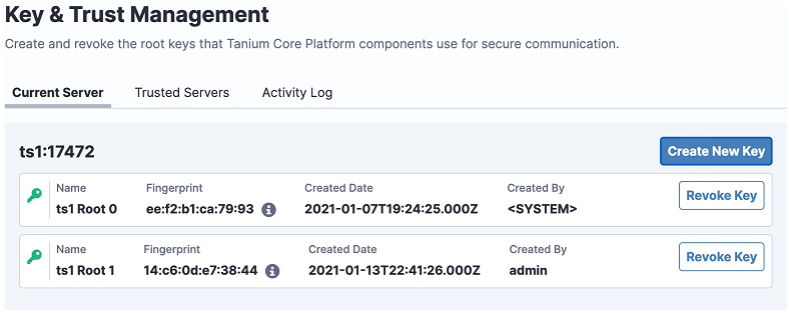
© 2026 Tanium Inc. All Rights Reserved

View root key information

The **Administration > Configuration > Key & Trust Management > Current Server** page shows a tile for each root public key that is active, as shown in figure Tanium root public keys on page 216. In an active-active deployment, the page displays the keys for both Tanium Servers, but only after you approve trust between them. For more information, see Synchronizing active-active Tanium Servers on page 224. You can identify keys by their **Fingerprint**, which is the hash digest of the key, and by the Tanium Server **Name**.

> **NOTE**
>
> The name **legacy-root** identifies the root keys for Tanium Client 7.2. Tanium release 2026H1 or later does not support Client 7.2. Upgrade any Client 7.2 installations to a new Client version. For more information, see Tanium Client Management User Guide: Upgrading Tanium Clients.

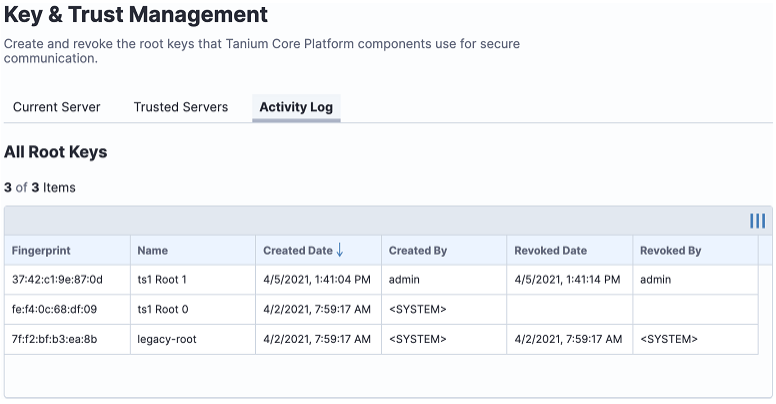
Tanium root public keys



You can also see details about root key operations, such as who generated or revoked a key and when:

1. From the Main menu, go to **Administration > Configuration > Key & Trust Management > Activity Log**.
2. Review the entries in the **All Root Keys** grid, as shown in figure Tanium keys activity log on page 216.

Tanium keys activity log



© 2026 Tanium Inc. All Rights Reserved

Encrypt the root keys database

As a best practice to prevent unauthorized access, specify a password to encrypt the root keys that the Tanium Server stores in the `pki.db` file.

Tanium Console displays the values of most settings that you configure. However, for security, Console does not display the encryption password.

Set the encryption password

Encrypt the root keys by adding the **PKIDatabasePassword** setting.



In an active-active deployment, perform the following steps on each Tanium Server.

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings** and click **Add Setting**.
2. For the **Setting Type**, select **Local**.
3. For the **Platform Setting Name**, enter `PKIDatabasePassword`.
4. Set the **Value Type** to **Protected**.
5. Enter the password **Value** and click **Save**.



Store the password in a safe location.

Change the encryption password

After adding the **PKIDatabasePassword** setting, you can later change the password.



In an active-active deployment, perform the following steps on each Tanium Server.

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.
2. In the **Name** column, click **PKIDatabasePassword**.

   The **Value** field displays `(protected)` instead of the actual value.
3. Enter a new **Value** and click **Save**.

© 2026 Tanium Inc. All Rights Reserved

Generate root keys

You can generate additional active public-private root key pairs for each Tanium Server. Perform this task on each Server in an active-active deployment.

1. From the Main menu, go to **Administration > Configuration > Key & Trust Management > Current Server**.
2. Click **Create New Key**. The page shows the root public key details in a new tile.

Revoke root keys

To prevent communication disruptions among Tanium Core Platform components, you cannot revoke a root key pair until you first generate a new key pair to replace it. Review the Key rotation on page 214 workflow before revoking the old root key pair. You must revoke keys on both Tanium Servers in an active-active deployment.



Back up the Tanium deployment immediately before and after revoking the root keys. If recovery becomes necessary, you must restore the deployment from the post-revocation backup. However, the pre-revocation backup might contain information that is useful for recovery planning. The backup steps depend on your Tanium infrastructure:

- Tanium Appliance User Guide: Backing up and recovering Tanium Appliances (a core backup is sufficient)
- Tanium Core Platform User Guide for Windows Deployments: Back up Tanium Core Platform servers and databases



If you configure the Tanium Server to integrate with an HSM, note that you cannot use a backup of the `pki.db` file containing the root keys to install a cryptographically identical duplicate of the Server.

Revoke keys as follows:

1. From the Main menu, go to **Administration > Configuration > Key & Trust Management > Current Server**.
2. Click **Revoke Key** in the tile of the public key.

Download infrastructure configuration files (keys)

The Tanium Zone Server, Tanium Zone Server Hub, and Tanium Client must authenticate to the Tanium Server to enable communication with it. The Zone Server, Hub, and Client authenticate by using keys (including the root public key) that are inside the initialization bundle (`tanium-init.dat`). After you download the initialization file from the Tanium Server, you can deploy the file to every Zone Server, Hub, and Client.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

Be careful not to allow the `tanium-init.dat` file to be distributed or stored outside of your organization, such as in a publicly accessible source code repository or any other location accessible from the public internet. Limit the distribution to specific use in the deployment of Tanium Clients.

Though this file does not contain private keys and cannot be used to provide control over a Tanium environment, a user with malicious intent could use it to connect an unapproved Client and use this unauthorized access to learn how your organization is using Tanium.

TIP

If you download `tanium-init.dat` through Tanium Client Management, certain settings (such as **ServerNameList**) are preconfigured in the file. For more information, see Tanium Client Management User Guide: Download the installation bundle or tanium-init.dat file for alternative deployment.

1. (Active-active deployment only) Enable trust between the Tanium Servers in an active-active deployment if you haven't already, as described in Synchronizing active-active Tanium Servers on page 224. Upon establishing trust, the Servers exchange the necessary keys so that the `tanium-init.dat` file on each Server contains the public key of both Servers.
2. From the Main menu, go to **Administration > Configuration > Infrastructure** and click **Download**.

   The file appears in the `Downloads` folder on the system that you use to access Tanium Console.

To deploy `tanium-init.dat`, see the relevant user guide:

- **Tanium Clients**: Tanium Client Management User Guide.
- **Zone Server and Hub**:
  - Tanium Appliance User Guide:
    - Installing and managing an Appliance Array
    - Install individual Zone Servers
  - Tanium Core Platform User Guide for Windows Deployments: Install the Tanium Zone Server

© 2026 Tanium Inc. All Rights Reserved

Securing Console and API access through certificates

Overview of SSL/TLS certificates

You can replace the Tanium Server certificate that secures user access to Tanium Console or the Tanium API in accordance with the certificate rotation policy of your organization. Console and the API communicate over HTTPS, which uses TLS certificates to secure client-server connections.

In the context of Console and API access, the user system is the client and the Tanium Server is the server. As part of the TLS handshake that secures the connection, the Tanium Server proves its identity to the client by presenting its server certificate. By default, the server certificate is the self-signed certificate that the Tanium Server generates during installation. The security best practice is to replace the self-signed certificate with one that a certificate authority (CA) has signed. In an active-active deployment, you can use Console to replace the certificate that is specific to each Tanium Server, but you cannot use Console to apply a single certificate to both Servers.



For Console and API access, clients do not have to prove their identity to secure connections with the Tanium Server.

For more information about the certificate requirements and TLS connection process, see;

- Tanium Appliance User Guide: Securing Tanium Console, API, and Module Server access
- Tanium Core Platform User Guide for Windows Deployments: Securing Tanium Console, API, and Module Server access

To manage the certificates that enable the Tanium Core Platform and Tanium solutions to connect with remote systems, see Enabling authentication between platform servers and remote systems on page 173.

Users require a role with **Https Certificates read** permission to view SSL/TLS certificates and certificate signing requests (CSRs). The **Administrator** reserved role has this permission and is the only role with permission to generate CSRs and upload new certificates.

Before you begin

- Replacing the Tanium Server certificate involves the following tasks. This guide describes only the first and last tasks. To perform the other tasks, you must first work with your CA to establish a process for submitting certificate signing requests (CSRs) and receiving signed certificates.

© 2026 Tanium Inc. All Rights Reserved

1. Generate and download a CSR. For more information, see Generate and download a CSR on page 222.
2. Submit the CSR to your CA.
3. The CA returns a signed certificate and any intermediate certificates.
4. Upload the signed certificates to Tanium Console. For more information, see Upload certificates on page 223.

- The CA has a signing certificate and associated private key that it uses to sign the requested Tanium Server certificate. For certificate validation to succeed during a TLS handshake, the CA signing certificate must be present on the systems from which users access the Console or API. If the CA provides a certificate chain along with the signed certificate, the chain includes the CA signing certificate. If the CA does not provide a chain, ensure the CA signing certificate exists in the required location:
  - **Console**: The CA signing certificate must be in the trusted certificates store of user browsers.

    NOTE

    Browser certificate stores typically contain the CA signing certificates of many third-party CAs without users needing to manually copy the certificates there.

  - **API**: The CA signing certificate must be in the location specified in API calls, as shown in the `--cacert <file path>` option of the following example:

    ```
    $ curl -s --cacert <file path> -X POST --data-binary @<sign in>.json
    https://localhost/api/v2/session/login
    ```

View details for the current certificates or CSR

Perform the following steps to view details about the certificate or CSR for a Tanium Server. In an active-active deployment, perform the steps on each Server.

1. From the Main menu, go to **Administration > Configuration > SSL Certificates**.

   The page shows the status (such as `Current` or `Expired`), validity period (**Issued Date** to **Expiration Date**), and identifying attributes (such as fingerprint) of the current Tanium Server certificate. Icons in the following locations indicate additional information about the certificate or CSR:

   - **SSL Certificates** menu option: An icon indicates if the current certificate expires within 60 days or has already expired .
   - **SSL Certificates** page: A banner at the top of the **Certificate** section indicates if the current Server certificate is self-signed , a CSR is pending , or the uploaded certificate is invalid .
2. Go to the **Certificate Chain** section to see the details of any intermediate certificates. The section appears only if the Server certificate is part of a certificate chain.

© 2026 Tanium Inc. All Rights Reserved

Generate and download a CSR

Perform the following steps to generate and download a CSR. In an active-active deployment, repeat the steps on each Tanium Server to generate a separate CSR for each Server. After you submit the CSRs to the CA, it returns signed certificates that you then upload on the Servers.

1. From the Main menu, go to **Administration > Configuration > SSL Certificates** and click **Generate CSR**.
2. Enter the following certificate attributes and click **Submit**.

   Certificate attributes

Attribute	Description
Common Name	Enter the fully qualified domain name (FQDN) or IP address of the Tanium Server.
Subject Alternative Names	Enter the FQDN or IP address of the Tanium Server. Web browsers typically require a **Subject Alternative Names** value.
Organization Name	(Optional) Enter the legal name of your organization.
Organization Unit/Department	(Optional) Enter the unit, department, or division of your organization for which you are creating the CSR. For example, this might be the department responsible for maintaining the Tanium Core Platform.
City/Locality	(Optional) Enter the name of the municipality where your organization resides.
State/Province	(Optional) Enter the name of the state, province, region, or county where your organization is located. Do not abbreviate the name. For example, enter `New York` instead of `NY`.
Country/Region	(Optional) Enter the two-letter ISO code for the country where your organization resides.

   The Tanium Server automatically copies the CSR file, `csr.txt`, to the downloads directory on the system that you use to access the Console.

   TIP

   If you later need to re-download the CSR, click **Download CSR** on the **SSL Certificates** page.

3. Click **Close** when the Tanium Server finishes generating and downloading the CSR.

   NOTE

   When the Server generates a CSR, it also generates a private key that never leaves the Server. When you upload certificates, the Server uses the key to determine the validity of the signed certificate that the CA returns. The Server uses both the certificate and key to perform the TLS handshake when securing connections to the systems of Console or API users.

© 2026 Tanium Inc. All Rights Reserved

4. Submit the CSR to your CA and notify the CA of the supported hashing algorithms for signing the certificate:
    - RSA-SHA256
    - RSA-SHA384
    - ECDSA-SHA256
    - ECDSA-SHA384

Upload certificates

After your CA processes the CSR and returns a signed certificate and any intermediate certificates, upload all the certificates. In an active-active deployment, perform the following steps on each Tanium Server.

1. Move the certificates to a system where you can copy files to the Tanium Server.
2. From the Main menu, go to **Administration > Configuration > SSL Certificates** and click **Upload Files**.
3. Drag and drop all the certificates to the **Drag and drop files** field or click **Browse for Files** and select all the certificates. Click **Upload** when you finish selecting files.

    The Tanium Server uses the private key that it generated at the same time as the CSR to verify that the uploaded certificates are valid.
4. In the **Certificate** and **Certificate Chain** sections, verify that the identifying attributes of the certificate (such as **Common Name**) are correct.

© 2026 Tanium Inc. All Rights Reserved

Synchronizing active-active Tanium Servers

Overview of Tanium Server trust

In a Windows deployment, you must enable trust between Tanium Servers in an active-active cluster to enable them to communicate with each other for synchronization. Enable trust to address the following situations:

- You completed a fresh installation of Tanium Servers and must enable trust between them.
- You initially deployed a Tanium Server in a standalone configuration, but now you want to deploy a second Server for an active-active configuration.
- You need to replace one of the Tanium Servers in an active-active deployment. In this case, you must revoke the trust state for the old Server and enable trust for the new Server.

The **Administration > Configuration > Key & Trust Management** page, **Trusted Servers** tab, displays details about the state of trust (enabled or revoked) between Tanium Servers.



You require the **Administrator** reserved role to manage trust for Tanium Servers.

In a Tanium Appliance deployment, the array setup automatically manages trust between Tanium Servers.

To troubleshoot issues related to Server trust, see:

- View Tanium Server trust history on page 225
- Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform

Enable trust between Tanium Servers

Before you begin

- Install both Tanium Servers in the active-active cluster. For the procedure, see the deployment guide for your Tanium infrastructure under Tanium Core Platform Servers. When you add a second Server, both Servers automatically discover the presence of the other through the Tanium database and appear in the **Administration > Configuration > Key & Trust Management > Trusted Servers** page.
- (Tanium Appliance deployment only) Check the TanOS version of your Appliances. If the version is TanOS 1.6.5 or later, you can skip this procedure because the array installation process automatically establishes trust between Appliances in the array. For more information, see Tanium Appliance User Guide: View version information and Tanium Appliance User Guide: Installing an Appliance Array.

© 2026 Tanium Inc. All Rights Reserved

- Record the fingerprints of the root public keys that are active on each Tanium Server. You use the fingerprints to verify Server identities. To see the fingerprints, sign in to Tanium Console on each Server and select **Administration > Configuration > Key & Trust Management > Current Server**.

Approve trust

1. Sign in to Tanium Console on a Tanium Server.
   A message appears at the top of Console indicating trust approval is required for the Server that is the peer of the Server you signed into.
2. From the Main menu, go to **Administration > Configuration > Key & Trust Management > Trusted Servers**.
   The page contains information about the Tanium Server that requires trust in relation to the Server you signed into.
3. Verify the identity of the Tanium Server that requires trust by its **Root Key Fingerprint** and **IP Address**.

   If the identifiers of a Tanium Server are wrong, decommission the Server before denying trust. Denied trust is irreversible for any particular instance of a Server. To subsequently approve trust, you must uninstall and reinstall the Server so that it generates a new root key pair.
4. Click **Accept** to initiate the trust approval workflow and click **Confirm** to proceed with the operation.
   The **Trust Status** remains `Awaiting trust from other server` until you enable trust on the other Tanium Server.
5. You must repeat the same preceding steps on the other Tanium Server. When you finish, the **Trust Status** changes to `Trusted`.

Revoke trust between Tanium Servers

To replace one of the Tanium Servers in an active-active deployment, revoke the current trust state for the old Server as follows, before enabling trust for the new Server.

1. Sign in to Tanium Console on the Tanium Server that currently trusts the Server that you will revoke.
2. From the Main menu, go to **Administration > Configuration > Key & Trust Management > Trusted Servers**.
3. In the tile of the Server for which you want to revoke trust, click **Revoke Trust**, and then click **Confirm**.

View Tanium Server trust history

You can see details about Tanium Server trust operations, such as who approved or revoked trust, when, and whether the operation succeeded.

1. From the Main menu, go to **Administration > Configuration > Key & Trust Management > Activity Log**.
2. Review the entries in the **Server Trust History** grid.

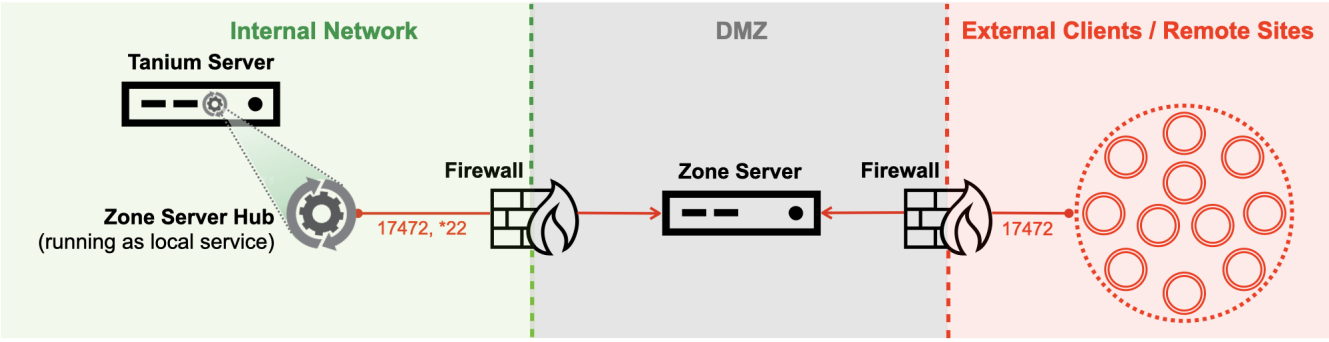
© 2026 Tanium Inc. All Rights Reserved

Enabling communication between Zone Servers and Hubs

Overview of trust and mappings among Zone Servers and Hubs

Deploy a Tanium Zone Server if the network security policies of your organization prohibit Tanium Clients in an external, untrusted network from initiating connections with the Tanium Server. You deploy the Zone Server in the DMZ to proxy communication between the Clients and Tanium Server. The Tanium Server communicates with the Zone Server through a Tanium Zone Server Hub. You must enable trust between each Tanium Server and Hub so that they can communicate. You must also map each Zone Server to a Hub so that only trusted Zone Servers communicate with Hubs. In an active-active deployment, enable trust and configure mappings for each Tanium Server, Zone Server, and Hub.

Zone Server deployment



* Port 22 is required only for a Tanium Appliance Array.

NOTE

In Tanium™ Appliance deployments, the Zone Server Hub is always installed on the Tanium Server. In Windows deployments, the Hub is typically installed on the Tanium Server but can also be on a dedicated host.

For more information about the Zone Server and Hub and the procedures to install them, see:

- Tanium Appliance User Guide: Installing an individual Tanium Zone Server
- Tanium Core Platform User Guide for Windows Deployments: Tanium Zone Server

The procedures to establish or revoke trust and to configure or delete mappings address the following situations:

- You completed the fresh installation of the Tanium Servers, Zone Servers, and Zone Server Hubs, and now you must enable trust and configure mappings.
- You must add a Zone Server or Hub to an existing deployment.
- You must replace a Zone Server or Hub. In this case, you must revoke the trust state and delete the mappings for the old Hub and then enable trust and configure mappings for the new Hub.

© 2026 Tanium Inc. All Rights Reserved

NOTE

You require the **Administrator** reserved role to manage trust and mappings among Zone Servers and Hubs.

To troubleshoot issues related to server trust and mappings, see Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform:

Establish trust and configure mappings

Before you begin

- Install the Tanium Servers, Zone Servers, and Zone Server Hubs. For the procedures, see the deployment guide for your Tanium infrastructure under Tanium Core Platform Servers. When you install a Zone Server Hub, Tanium Console automatically displays it as a tile in the **Administration > Configuration > Zone Servers > Zone Server Hubs** page.
- (Tanium Appliance deployment only) Check the TanOS version of your Appliances. If the version is TanOS 1.6.5 or later, you can skip this procedure because the array installation process automatically establishes trust between Appliances in the array. For more information, see Tanium Appliance User Guide: View version information and Tanium Appliance User Guide: Installing an Appliance Array.

In an active-active deployment, perform the following tasks in sequence on each Tanium Server.

Approve trust for Zone Server Hubs

Perform the following steps for each Zone Server Hub.

NOTE

If you upgraded the Zone Server Hub from version 7.3, the Hub migrates the `ZoneServerList.txt` file into Zone Server mappings after you approve trust for the Hub.

1. Display the registration fingerprint of the Zone Server Hub so that, in a later step, you can verify its identity before establishing trust.

   Appliance deployment:

   a. Sign in to the TanOS console of the Zone Server Hub Appliance as a user with the `tanadmin` role.

   b. Enter `@` to open the **About the Appliance** page and note the value of the **TZS Hub Registration Fingerprint** field.

   Windows deployment:

   a. Sign in to the Zone Server Hub and access the CLI.

   b. Navigate to the Zone Server Hub installation directory (such as `\Program Files (x86)\Tanium\Tanium ZoneServer`):

   ```
   > cd <Zone Server>
   ```

© 2026 Tanium Inc. All Rights Reserved

c. Display the registration fingerprint of the Zone Server Hub:

```
> TaniumZoneServer pki show-registration-fingerprint
```

2. Sign in to Tanium Console on a Tanium Server.
3. From the Main menu, go to **Administration > Configuration > Zone Servers > Zone Server Hubs**.
   The page displays a tile for each **Zone Server Hub** that you installed.
4. Verify the identity of each Zone Server Hub by its **Fingerprint** and its IP address or FQDN.

   If the identifiers of a Zone Server Hub are wrong, decommission the Hub before denying trust for it. Denied trust is irreversible for any particular instance of a Hub. To subsequently approve trust, you must uninstall and reinstall the Hub so that it generates a new fingerprint.
5. In the **Zone Server Hub** tile, click **Accept** and **Confirm**.
   The tile shows the trust **Status** is `Approved`.

Map Zone Servers to a Zone Server Hub

After approving trust for Zone Server Hubs, perform the following steps for each Zone Server. In an active-active deployment, map both Zone Servers to each Zone Server Hub.

1. Display the registration fingerprint of the Zone Server so that, in a later step, you can verify its identity before establishing trust.

   Appliance deployment:

   a. Sign in to the TanOS console of the Zone Server Appliance as a user with the `tanadmin` role.

   b. Enter `@` to open the **About the Appliance** page. Note the value of the **TZS Registration Fingerprint** field.

   Windows deployment:

   a. Sign in to the Zone Server and access the CLI.

   b. Navigate to the Zone Server installation directory (such as `\Program Files (x86)\Tanium\Tanium ZoneServer`):

   ```
   > cd <Zone Server>
   ```

   c. Display the registration fingerprint of the Zone Server:

   ```
   > TaniumZoneServer pki show-registration-fingerprint
   ```
2. Sign in to Tanium Console.
3. From the Main menu, go to **Administration > Configuration > Zone Servers > Zone Servers Hubs**.
4. In a **Zone Server Hub** tile, click **Add Zone Server**.

© 2026 Tanium Inc. All Rights Reserved

5. Enter the Zone Server **FQDN, Host Name, or IP address**.
6. Enter the **Port** that the Zone Server uses for traffic from the Zone Server Hub. The default is 17472.

   BEST PRACTICE

   Configure separate ports for traffic from Zone Server Hubs and Tanium Clients to improve the security of the Zone Server. For more information, see Tanium Core Platform User Guide for Windows Deployments: Configure ports for traffic from Zone Server Hubs and Tanium Clients.
7. Click **Save**.

   Below the Zone Server Hub tile, Tanium Console displays a tile for the Zone Server that you added.
8. Click the **Zone Servers** tab.

   The page displays a tile with a **Status** of `Pending` for each Zone Server that you added.
9. Verify the identity of each Zone Server by its **Fingerprint** and its IP address or FQDN.

   NOTE

   If the identifiers of a Zone Server are wrong, decommission the Server before denying trust for it.
10. In the Zone Server tile, click **Accept** and **Confirm**.

    The tile shows the mapping **Status** is `Approved`.

Revoke trust and delete mappings

If you need to replace one of the Zone Server Hubs, revoke the trust state and Zone Server mappings for the old Hub before establishing trust and mappings for the new Hub. If you need to replace a Zone Server, delete its Hub mapping before creating a mapping for the new Zone Server.

IMPORTANT

You cannot undo the revocation of server trust without reinstalling the revoked Zone Server or Zone Server Hub.

In an active-active deployment, perform these tasks on each Tanium Server.

Revoke a Zone Server Hub

1. Sign in to Tanium Console on a Tanium Server.
2. From the Main menu, go to **Administration > Configuration > Zone Servers > Zone Server Hubs**.

   The page displays a tile for each **Zone Server Hub**.
3. In the **Zone Server Hub** tile, click **Revoke** and **Confirm**.

© 2026 Tanium Inc. All Rights Reserved

Revoke a Zone Server

1. Sign in to Tanium Console on a Tanium Server.
2. From the Main menu, go to **Administration > Configuration > Zone Servers > Zone Servers**.
   The page displays a tile for each **Zone Server**.
3. In the **Zone Server** tile, click **Revoke** and **Confirm**.

Delete a Zone Server Hub-to-Zone Server mapping

1. Sign in to Tanium Console on a Tanium Server.
2. From the Main menu, go to **Administration > Configuration > Zone Servers > Zone Server Hubs**.
   The page displays a Zone Server tile for each mapping.
3. In the Zone Server tile, click **Delete Mapping**.

© 2026 Tanium Inc. All Rights Reserved

Part 6: Exploring and accessing endpoints in Console and Interact

Tanium Interact provides the following methods to explore and manage endpoints:

- **Issue questions**

  Use the free-form question fields or **Question Builder** to issue questions that retrieve information from endpoints. For example, you can ask a question that determines if any endpoints are missing critical security patches. Based on the question results that the endpoints return, you can then deploy actions, such as installing security patches.

  > NOTE
  >
  > To issue saved questions, see Issue a saved question on page 466 and Issue a dashboard of saved questions on page 467.
  >
  > For more information about manipulating and analyzing question results, see Part 7: Analyzing question results in Console and Interact on page 255.
  >
  > For the user roles and permissions required to ask questions, see Interact permissions on page 81.

- **Search endpoints on page 249**

  Use the **Search Endpoints** feature to quickly retrieve a lot of information about a single endpoint instead of constructing a long question with many sensors.

- **Jump to endpoints on page 250**

  Use Tanium Jump Gate to access a PowerShell session on a Windows endpoint or a Bash session on a macOS or Linux endpoint.

What is a question?

A Tanium *question* is a query that you issue through Tanium solutions to managed endpoints. Tanium Clients running on the endpoints process the question and return answers that you can view on the **Question Results** page. Questions enable you to explore endpoints in the course of various Tanium operations for managing, monitoring, and protecting your environment.

For example, you can issue the question `Get Computer Name and Last Logged In User from all machines with Last Logged In User contains <user name>` to determine which endpoints a particular user is accessing.

A *dynamic question* is one that you create from scratch and issue through the Interact features **Ask a Question** and **Question Builder**. For more information, see Issue a free-form question on page 241 and Issue a question through the Question Builder on page 245.

A *saved question* is a configuration object that enables you to reissue a question without recreating it. For more information, see Saved questions overview on page 455.

All questions include the following elements:

© 2026 Tanium Inc. All Rights Reserved

- `get` clause

  In the `get` clause, one or more sensors (such as `Last Logged In User`) specify the information to retrieve from endpoints. You can add filters to the sensor results by using an operator, such as **matches** or **is greater than**. Use the `and` operator to separate multiple sensors. For more information, see What is a sensor? on page 232, Filters in get clause on page 731, and Questions with multiple sensors on page 238.

- `from` clause

  The `from` clause specifies the target endpoints that must answer the question. For example, the default value `from all machines` specifies all endpoints that host the Tanium Client. To target fewer endpoints, add filters to the `from` clause. For more information, see Filters in from clause on page 731.

  To return results, endpoints must be members of computer groups assigned to the user account or persona that you use to issue the question, regardless of the `from` clause targeting. For more information, see Computer groups in questions on page 612.

Advanced questions include reserved words or characters (such as `match` or `$`), regular expressions, filters, or advanced options. For more information, see Reference: Advanced question syntax in Console and Interact on page 731.



For examples of questions, see Reference: Example questions in Console and Interact on page 725.

What is a sensor?

A *sensor* configuration includes a script that the Tanium Client runs on an endpoint to compute an answer to a Tanium question. The Tanium Server distributes sensors to endpoints managed using Tanium Client during Client registration. Sensors enable you to ask questions that collect information such as:

- Hardware and software inventory and configuration
- Running applications and processes
- Files and directories

After all the sensors in a question compute answers, Tanium Clients return the answers to the Tanium Server. Interact then shows the answers, called results, in grid format on the **Question Results** page. Each sensor result provides one or more rows and columns of information that the grid aggregates according to whether you issued a counting or non-counting question. For examples, see:

- Example: Single row of results on page 233
- Example: Multiple rows of results on page 233
- Example: Multiple rows and columns of results on page 234

The **Question Results** page also shows a **Count** column that indicates how many endpoints returned each result. For more information, see Counting and non-counting questions on page 235.

© 2026 Tanium Inc. All Rights Reserved

NOTE

The **Count** column is hidden by default if its value is `1` for every result.

The Tanium Server automatically imports content-only solutions that include sensors for a wide range of common questions. Other Tanium solutions that you import might provide more sensors. If you cannot find a sensor that you need within Tanium-provided content, you can create custom sensors.

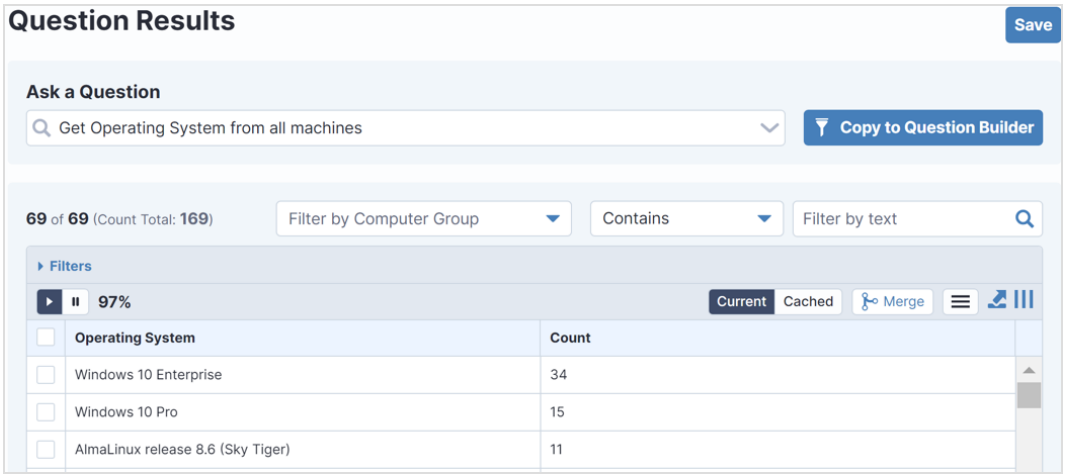
For more information, see:

- Content-only solutions on page 48 for information about the initial content that the Tanium Server provides automatically.
- Managing sensors for collecting endpoint data on page 421 for the steps to view, create, or edit sensor configurations.
- Part 7: Analyzing question results in Console and Interact on page 255 for the steps to perform operations on sensor results, such as filtering and analyzing.
- Virtual sensors on page 422 for information about sensors for which Tanium solutions generate data instead of collecting it from endpoints.
- Solution-generated sensor attributes on page 423 for details about sensor attributes (columns) for which Tanium solutions generate data instead of collecting it from endpoints.

Example: Single row of results

Operating System is an example of a sensor that returns a single row for each unique result from endpoints.

Single row for each unique question result

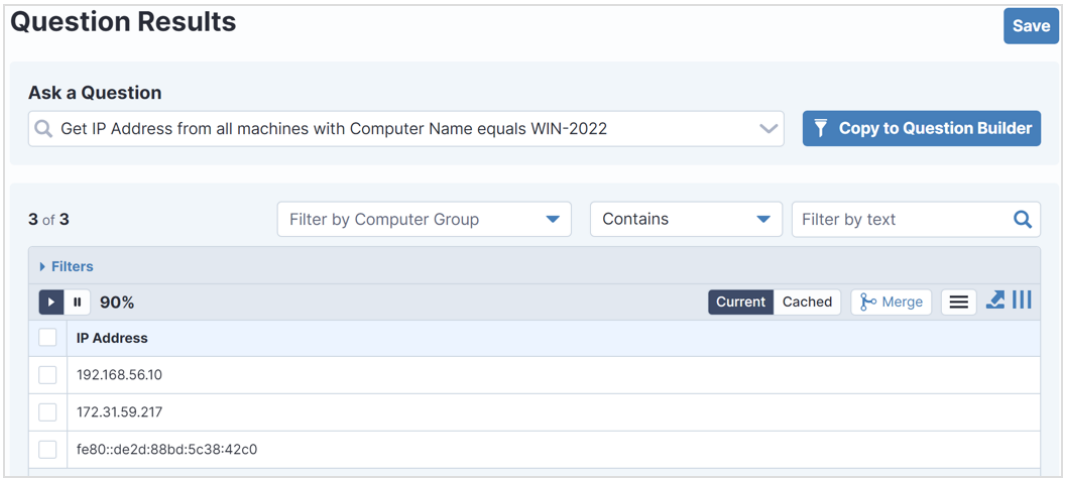


Example: Multiple rows of results

IP Address is an example of a sensor that can return multiple rows for one endpoint if the endpoint has multiple interfaces and a mix of IPv4 and IPv6 addresses.

Question results with multiple rows per endpoint

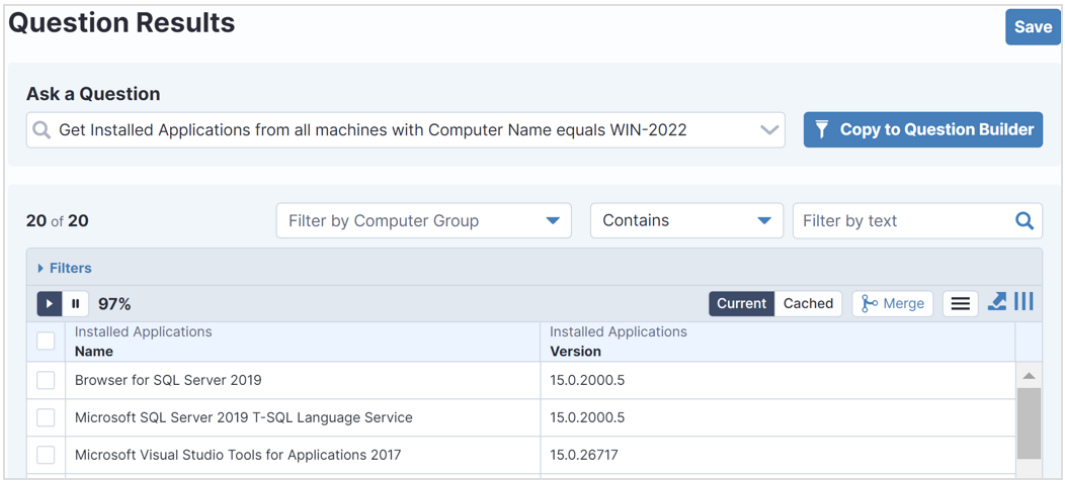
© 2026 Tanium Inc. All Rights Reserved



Example: Multiple rows and columns of results

Installed Applications is an example of a sensor that returns multiple rows and columns for each endpoint: one row for each application on the endpoint and two columns to indicate the application name and version. For more information, see Example: Multi-column sensors on page 492.

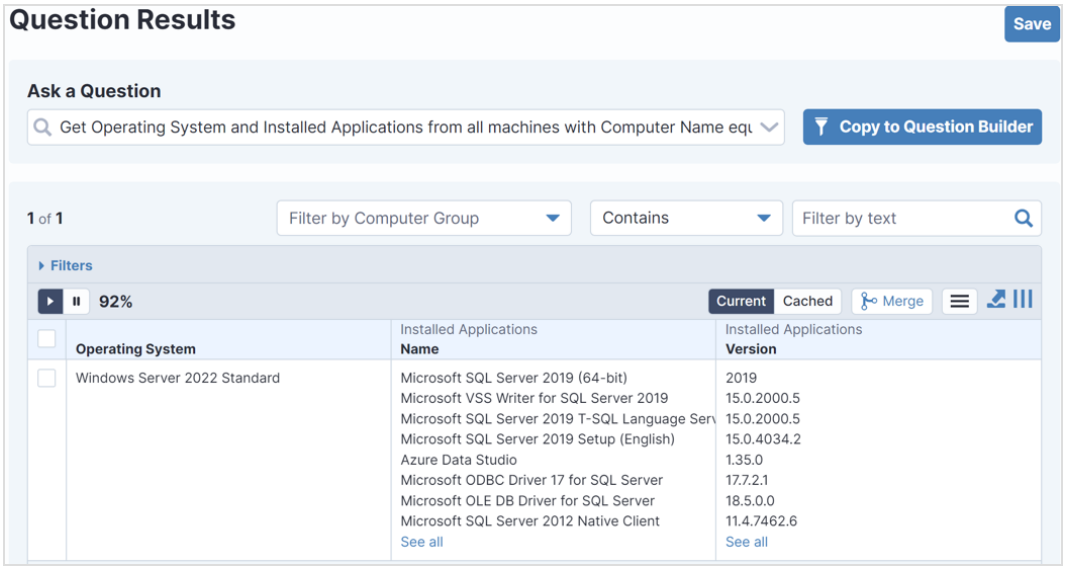
Question results with multiple rows and columns per endpoint



If the question has multiple sensors, the **Question Results** grid shows their results in separate columns. If one of the sensors provides multiple columns, the column headings show the sensor name above the column names. In the following example, the **Installed Applications** sensor provides the application **Name** and **Version** columns. For more information about multi-sensor questions, see Questions with multiple sensors on page 238.

Results for a question with multiple sensors

© 2026 Tanium Inc. All Rights Reserved



NOTE

To filter multi-column sensors by the values in a particular column, see Use sensor column filters on page 742.

Counting and non-counting questions

The Interact **Question Results** grid aggregates results differently based on whether you issued a counting or non-counting question. For a counting question, the **Count** column shows how many endpoints returned the same unique value in a result that has one or more values for a single sensor. For a non-counting question, the **Count** shows how many endpoints returned all the same values in all the results of one or more sensors. Results aggregation on page 235 describes this **Count** distinction in detail.

NOTE

The **Question Results** page automatically shows a **Count** column if its value exceeds `1` for any row and hides the column otherwise. To manually show or hide the column, click Customize Columns in the **Question Results** toolbar and select (show) or clear (hide) the **Count** checkbox.

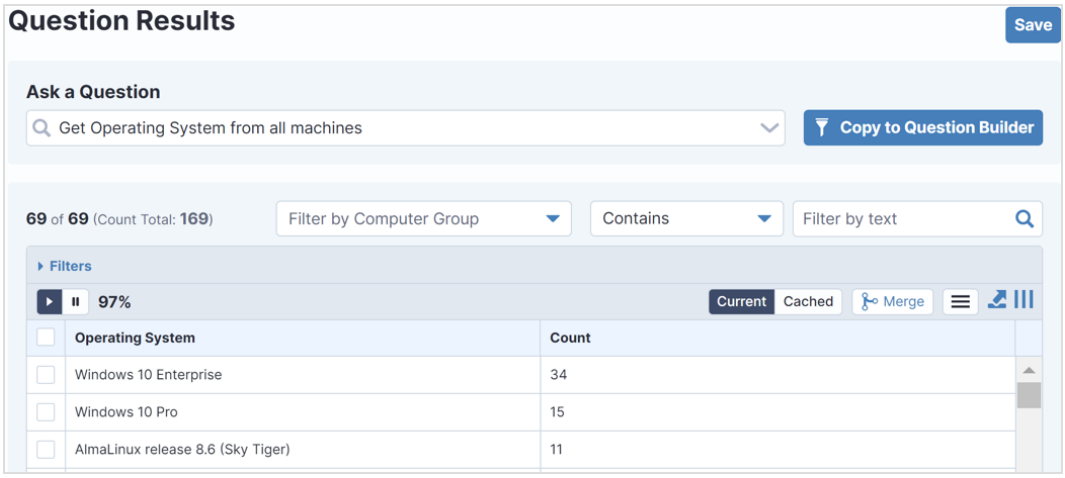
A question with multiple sensors in its `get` clause is always a non-counting question. A question with one sensor in its `get` clause is a counting question by default but you can convert it to a non-counting question. For more information, see Convert counting questions to non-counting questions on page 237. Before you issue a single-sensor question, consider the following ramifications of counting and non-counting questions.

Results aggregation

The **Question Results** grid presents results the same way for a counting or non-counting question if each endpoint provides only one value for the result of a single sensor. Each grid row shows one unique value and the **Count** of endpoints that returned the value. **Operating System** is an example of a single-value sensor.

© 2026 Tanium Inc. All Rights Reserved

Count for a sensor with one value per endpoint

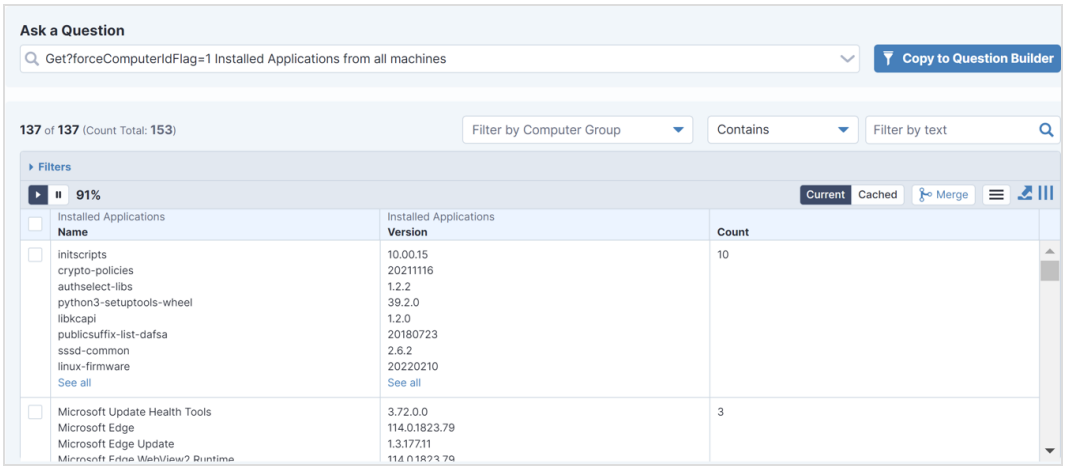


The **Installed Applications** sensor is an example of a sensor that includes multiple sets of values from each endpoint. Each set is the name and version of an application and the result includes as many sets as the endpoint has applications. The **Question Results** grid presents the results of a multi-value sensor differently for non-counting and counting questions:

- **Non-counting question**

  Each grid row shows the **Count** of endpoints that return all the same value sets in a result. In the following example, a non-counting question is useful if you want to know how many endpoints have all the same application versions.

  Non-counting question

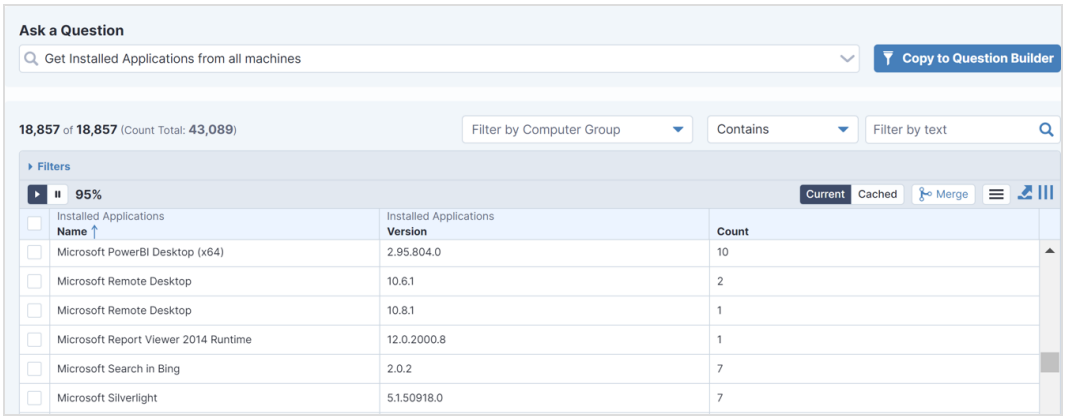


- **Counting question**

  Each grid row shows the **Count** of endpoints that return the same unique value set. In the following example, a counting question is useful if you want to know how many endpoints have a particular application version, regardless of whether any endpoints share all the same application versions. The grid shows how many endpoints have Microsoft Remote Desktop version 10.6.1 and how many have Microsoft Silverlight 5.1.5.0918.0, but the grid does not show how many endpoints have both.

© 2026 Tanium Inc. All Rights Reserved

Counting question



Results readability and network traffic

The **Question Results** grid might show more rows than you can effectively review for a non-counting question. For example, if your network has five operating systems (OSs) across 10,000 endpoints, the grid would show 10,000 rows for the non-counting question `Get?forceComputerIdFlag=1 Operating System from all machines` because each result includes the **Computer ID** along with the **Operating System** of each endpoint. In this case, if the only important information is the count of endpoints that run each OS, you could issue the counting question `Get Operating System from all machines` and the grid would be more readable with only five rows to review. In this example, the counting question would also generate much less network traffic for the Tanium Server to process because the endpoints return only five result strings.

Merge questions

You can select only a non-counting question for a merge operation on question results. For more information, see Merge questions on page 264.

Recent results

The Tanium Server stores question results as *recent results* only for non-counting saved questions. The **Question Results** page shows recent results when live results are unavailable, such as when the answering endpoints are offline. For more information, see Display results for online and offline endpoints on page 258.

[too many results] message

The **Question Results** page shows `[too many results]` to indicate that more results are available but Tanium Clients will not return the additional results. If a counting question returns this message, converting it to a non-counting question might resolve the issue. For more information, see Too many results on page 710.

Convert counting questions to non-counting questions

Specify the **Force Computer ID** option to issue a single-sensor question as a non-counting question. This option compels endpoints to return results for the **Computer ID** sensor along with the results for the sensor that you specify in the question. The Tanium Server stores the **Computer ID** results but the **Question Results** page shows only the results for the sensor that you specify in the

© 2026 Tanium Inc. All Rights Reserved

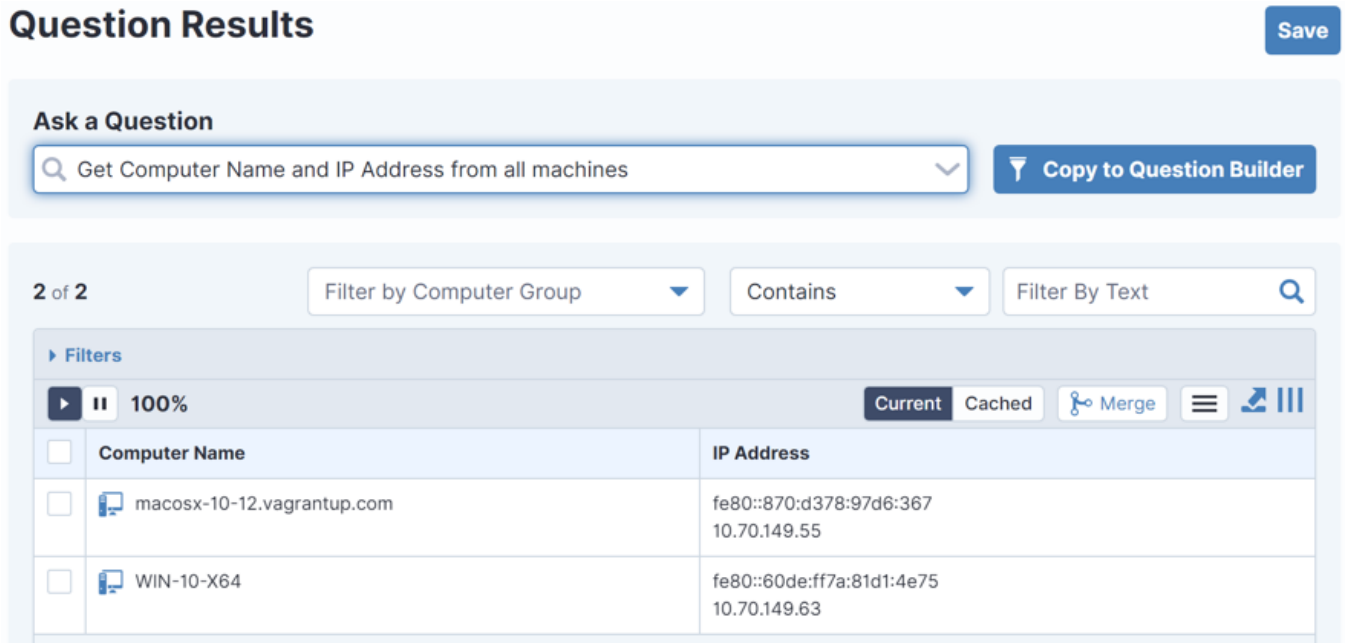
question. Specify the **Force Computer ID** option through one of the following methods:

- **Ask a Question field**: Use the `Get?forceComputerIdFlag=1` statement instead of `Get`. For more information, see Issue a free-form question on page 241.
- **Question Builder**: Specify the **Force Computer ID** option in the **Advanced Question Options**. For more information, see Issue a question through the Question Builder on page 245.
- **Saved question configuration**: Select the option **Yes, turn into non-counting question**. For more information, see Create a saved question on page 463.

Questions with multiple sensors

When you construct a question, use the `AND` operator in the `get` clause to specify multiple sensors. The **Question Results** page groups results by the first sensor, then by the next sensor, and so on, as the following example illustrates. For more information about how the **Question Results** page shows sensor results across multiple columns, see What is a sensor? on page 232.

Question with multiple sensors

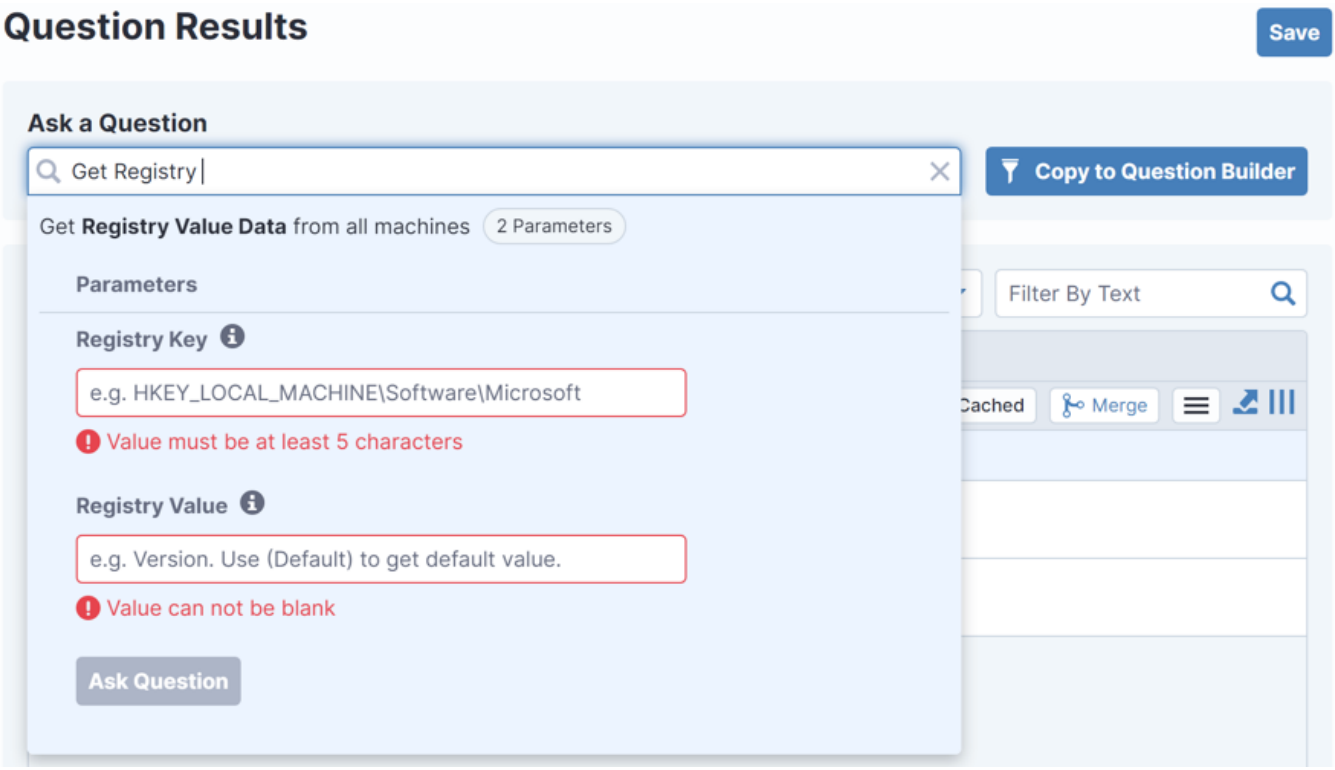


Questions with parameterized sensors

A *parameterized sensor* uses a value that you specify when entering the question in the **Ask a Question** field or **Question Builder**. The following example shows the **Registry Value Data** sensor. Interact prompts you to specify a registry path and value.

© 2026 Tanium Inc. All Rights Reserved

Parameterized sensor



Another example is the **High CPU Processes** sensor. You can specify a parameter that is the number of CPU processes to return from each machine. For example, you might want to get the top 5 highest CPU utilizing processes. The question has the following syntax:

```
Get High CPU Process[5] from all machines
```

For sensors with multiple parameters, you can specify an ordered list of comma-separated parameters. For example, to see the first 10 lines from the action log for the action with ID 1, specify a parameter list as follows:

```
Get Tanium Action Log[1,10] from all machines
```

For more information, see Example: Parameterized sensors on page 495.

IMPORTANT

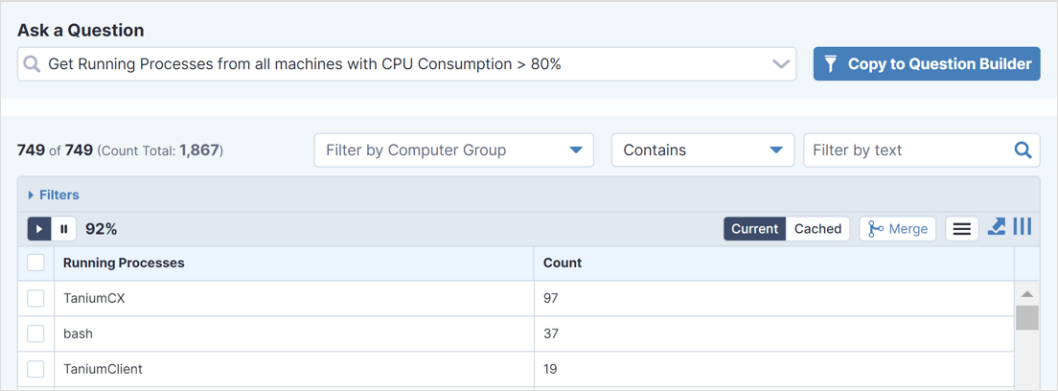
When you issue a question that has a parameterized sensor, the Tanium Server creates an object called a *temporary sensor*, which contains the substituted parameter values and a link to the actual sensor. The Tanium Client runs the temporary sensor to respond to a dynamic or saved question that uses the sensor. If the sensor definition changes on the Server, the Client receives the new definition after its next registration interval. The Client then applies the parameter values to the updated sensor definition for subsequent responses to the saved question.

© 2026 Tanium Inc. All Rights Reserved

Questions with target filters

You can use a filter in the `from` clause of a question to target fewer endpoints than the default `all machines`. For example, the following question targets only endpoints managed using Tanium Client where CPU consumption exceeds 80%.

Question with target filter



NOTE

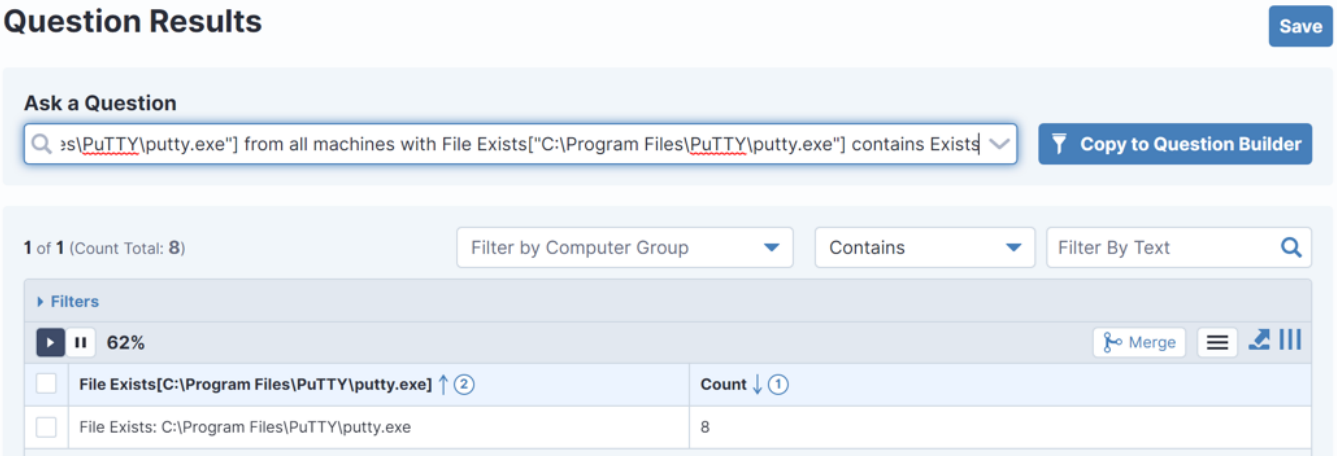
To filter the `get` clause of a question, see Use question filters on page 731.

Filters in the `from` clause are the first part of a question that an endpoint processes. If the endpoint data does not match the filter, the endpoint does not process the question any further. If the question has multiple filters, the endpoint evaluates each filter. The filter expression must evaluate to a Boolean true or false. For example, the expression `from all machines with CPU Consumption > 80%` evaluates to true if CPU consumption exceeds 80% on the endpoint and evaluates to false otherwise. If a filter evaluates to true, the endpoint runs the sensors in the `get` clause of the question and returns the results.

A parameterized sensor like **File Exists[]** returns the result `File Exists: <file name>` or `File does not exist`, so be careful how you enter the sensor in a filter expression. The filter expression `from all machines with File Exists ["C:\Program Files\PuTTY\putty.exe"] contains "Exists"` evaluates to true when the result is `File Exists: C:\Program Files\PuTTY\putty.exe` and false when the result is `File does not exist`, so you can use it to filter the set of responses.

© 2026 Tanium Inc. All Rights Reserved

Question filter with parameterized sensor



Filter expressions can match strings or regular expressions. For more information, see Reference: Advanced question syntax in Console and Interact on page 731.

Issue a free-form question

Overview of free-form questions

Interact provides text-entry fields where you can quickly construct dynamic questions, such as `Get Last Logged In User from all machines`. These fields are particularly useful when you want to issue simple questions, or when you understand Tanium question syntax sufficiently to manually enter advanced questions. For example, an advanced question might contain filters in the `get` clause (such as `Get Last Logged In User matches "(root|reboot)"`) or `from` clause (such as `from all machines with CPU Consumption > 80%`).

NOTE

For more information about `get` and `from` clause usage in basic question syntax, see What is a question? on page 231. For more information about filters and other advanced syntax, see Reference: Advanced question syntax in Console and Interact on page 731.

When you start typing a free-form question in one of the question fields, Interact evaluates your entry through a natural language parser instead of a specialized query language. The parser enables you to enter text in natural English that does not require complete sentences, case sensitivity, or strictly correct spelling. Based on the evaluation of your entry, Interact opens a dropdown list with proposed questions in valid syntax. If the list shows multiple proposed questions, they appear in top-to-bottom order based on how closely they approximate the text that you entered. The parser uses Valid syntax matching on page 242 or Enhanced search on page 243 to generate proposed questions. For the steps to issue a question or select other options in the dropdown list of proposed questions, see Issue a question on page 244.

NOTE

For examples of questions that you can issue, see Reference: Example questions in Console and Interact on page 725.

© 2026 Tanium Inc. All Rights Reserved

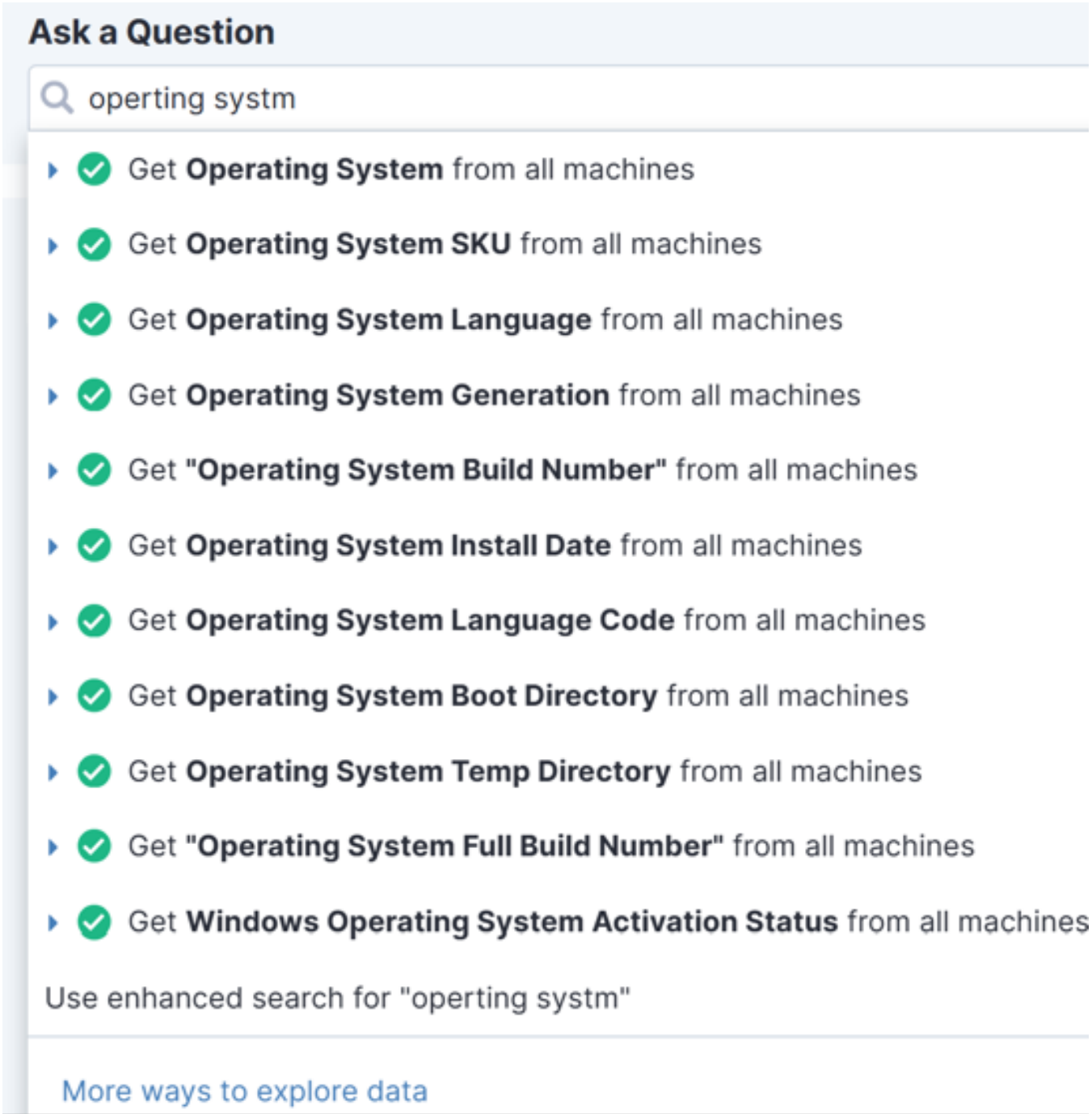
If you want more structured guidance when issuing a question, the Interact **Question Builder** provides widgets that enable you to precisely select all the components of a question. For more information, see Issue a question through the Question Builder on page 245.

VALID SYNTAX MATCHING

If you enter only text that matches, or closely approximates, the valid syntax of a question in an Interact question field, Interact proposes questions with corresponding syntax. For example, Interact proposes similar questions if you enter the exact sensor name `operating system` or the approximate words `operting systm`:

© 2026 Tanium Inc. All Rights Reserved

Question that approximates valid syntax



ENHANCED SEARCH

If some of the words that you enter in an Interact question field are too ambiguous to match with valid question syntax, you can select the **Use enhanced search for "*<text>*"** option to make Interact re-parse your entry based on a more expansive interpretation of the text and then propose additional questions.

© 2026 Tanium Inc. All Rights Reserved

Issue a question

Perform the following steps to issue a free-form question. When Tanium Clients return answers, the **Question Results** page shows the answers in grid format. For more information, see Part 7: Analyzing question results in Console and Interact on page 255.

1. Go to the question field in one of the following locations:
   - Console header: Select the Question option to show the text field. The **Question Results** page shows the answers in a new browser tab.
   - Tanium **Home** page: Select the **Ask a Question** tab to show the text field. The **Question Results** page shows the answers in the current browser tab.
   - **Modules > Interact > Overview** page: The **Explore Data** section contains the **Ask a Question** field. The **Question Results** page shows the answers in the current browser tab.
2. Perform one of the following steps in the question field:
   - **Issue a new question**: Start typing the question text to see a list of proposed questions that best match your entry, then go to Step 3. on page 245

     NOTE

     If you enter sensor names that contain reserved words or characters, add quotation marks around the names. For more information, see Use reserved words or characters on page 735.
   - **Re-issue a recently issued question**: Click inside the question field to open a dropdown list and select the question. If the question does not have parameterized sensors, Interact issues it immediately and no further steps are necessary. If you must specify parameter values, skip to Step 4. on page 245

     NOTE

     If you are a new user who never issued questions before, the dropdown list shows common questions instead of recently issued questions.

     TIP

     When the question field lists proposed questions, icons indicate the average runtime of each question. You can Expand any question to show details about the sensors that the question uses and the sensor runtimes. For more information, see Assessing question impacts on endpoints through sensor runtime indicators on page 438.

© 2026 Tanium Inc. All Rights Reserved

3. Select one of the following options in the list of proposed questions:

   - Select a question to issue it. If the question does not have parameterized sensors, no further steps are necessary. If you must specify parameter values, go to Step 4. on page 245

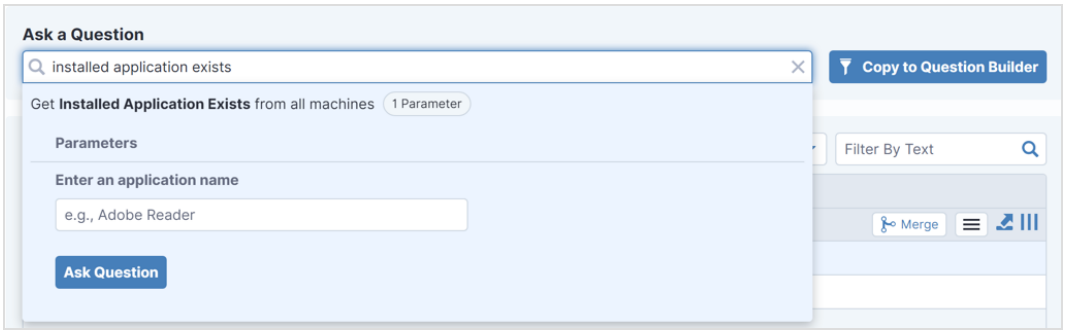
     The remaining options are useful if the proposed questions do not match your expectations.

   - Select **Use enhanced search for "*<text>*"** to make Interact re-parse your entry based on a more expansive interpretation of the text. Interact then proposes additional questions.

   - Select **More ways to explore data** to open the **Question Builder**. You can then construct the question exactly as you want it.

   For more information about using the **Question Builder**, see Issue a question through the Question Builder on page 245.

4. Enter the parameter values for parameterized sensors and click **Ask Question** to issue the question. For more information, see Questions with parameterized sensors on page 238.

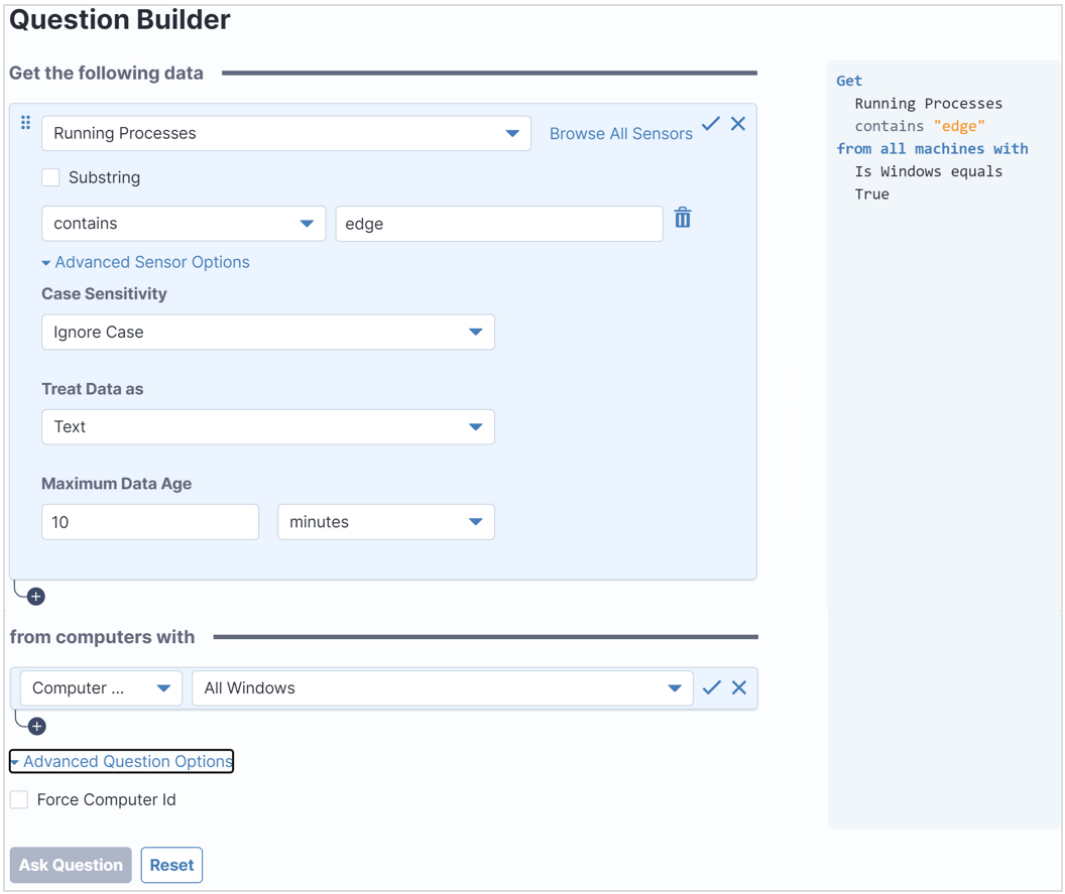


Issue a question through the Question Builder

The **Question Builder** provides a guided method for creating a dynamic question. It has form fields to help you complete the `get` statement and the `from` clause, including any filters.

Question Builder

© 2026 Tanium Inc. All Rights Reserved



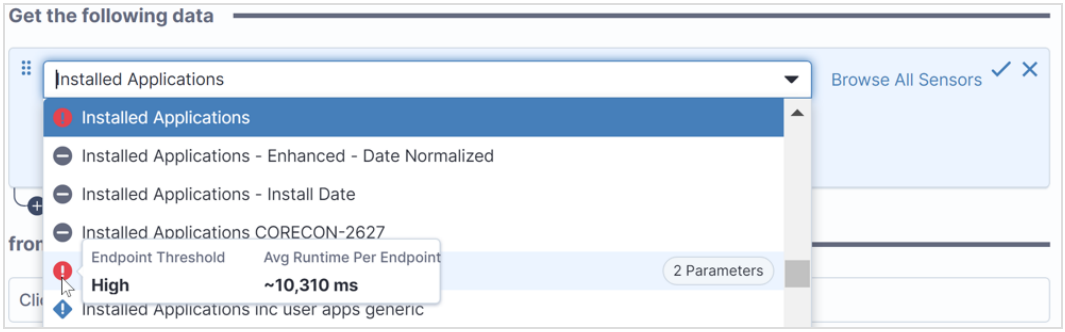
1. Open the **Question Builder** page from any of the following locations:
    - Tanium Home page: Click **Build Question** beside the **Ask a Question** field. If you start typing a question in that field, the **More ways to explore data** option also opens the **Question Builder**.
    - Interact Overview page: Select **Modules > Interact > Overview** and click **Build Question** beside the **Ask a Question** field.
    - Interact menu: Select **Modules > Interact > Question Builder**.
    - Question Results page: To refine a question that you already issued, click **Copy to Question Builder** beside the **Ask a Question** field

© 2026 Tanium Inc. All Rights Reserved

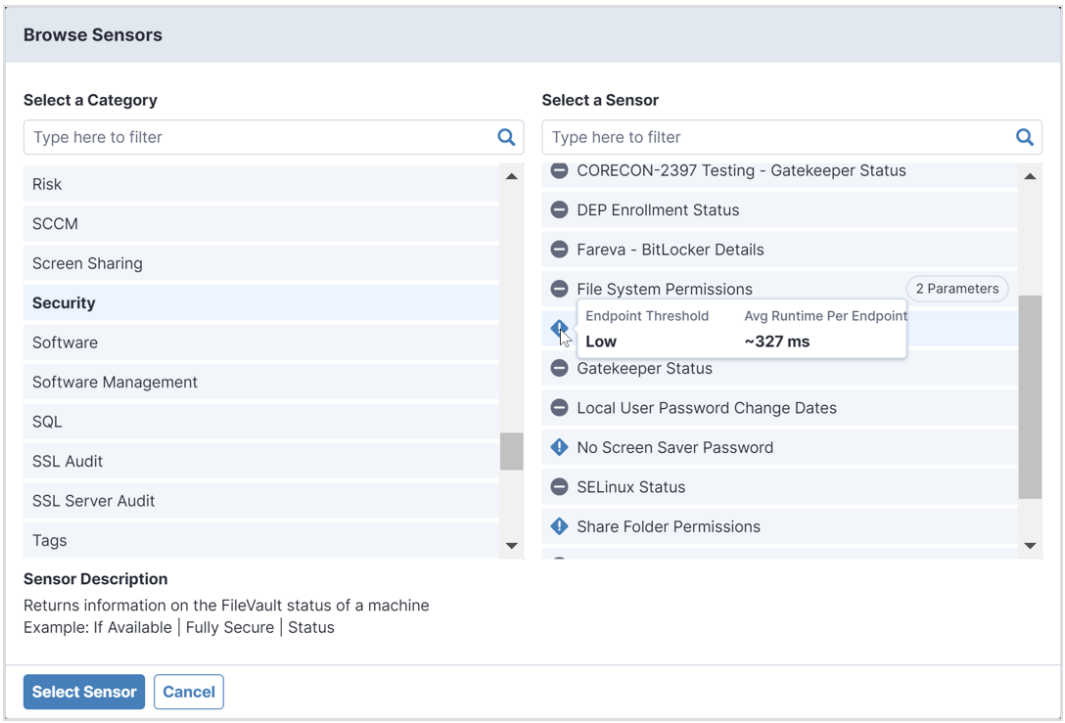
2. In the **Get the following data** section, perform the following sub-steps for each sensor in the `get` statement of the question:

   a. Click **Add Row** to add the first sensor and click + to add each additional sensor. Then perform one of the following sub-steps to specify each sensor:

   - Start typing the sensor name in the **Filter by Name** text field. The typeaheads dropdown list below the field shows a list of sensors that match your entry. Select a sensor and click Apply ✓.



   - Click **Browse All Sensors** to open the **Browse Sensors** dialog and select a sensor. The bottom of the dialog displays the **Sensor Description**.



© 2026 Tanium Inc. All Rights Reserved

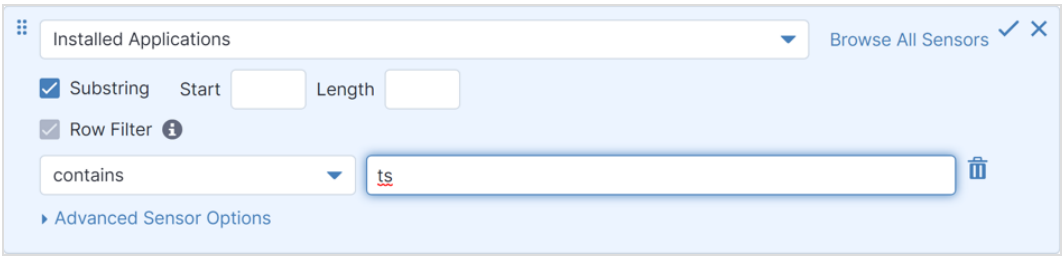
TIP

In the typeaheads dropdown list or **Browse Sensors** dialog, hover over a runtime icon (, , ,) to see the average runtime (in milliseconds) for a sensor. For more information, see Assessing question impacts on endpoints through sensor runtime indicators on page 438.

b. (Optional) To filter the sensor results, click **Add filter**, select an operator (such as **matches**), and specify a regular expression to match result strings. For more information, see Use question filters on page 731.

You can configure the following filter options:

- **Column matching**: If a sensor produces data across multiple **Question Results** columns, filter matching applies only to the selected column by default. For example, you can filter the **Name** column or **Version** column of the **Installed Applications** sensor. For more information, see Use sensor column filters on page 742. To apply matching to all the columns for a sensor, select **Row Filter**.
- **Substring matching**: To match only part of a result string, select the **Substring** checkbox, enter the **Start** position (where `0` is the first position), and enter the number of characters (**Length**). The following example matches results from the **Installed Applications** sensor where the first two characters match the string `ts`. For a multi-column sensor, you cannot apply the **Substring** filter to a specific column, only across all the columns (**Row Filter**).



c. (Optional) Click **Advanced Sensor Options** below the filter to configure additional settings. For more information, see Use advanced sensor options on page 746.

d. Specify parameter values if you added a parameterized sensor. For more information, see Questions with parameterized sensors on page 238.

3. (Optional) In the **from computers with** section, perform the following sub-steps to add targeting filters in the `from` clause of the question. If you omit filters, the question targets all computers.

NOTE

For more information about targeting filters, see Questions with target filters on page 240.

Interact processes nested filters (group filters) and applies Boolean **AND**/**OR** logic for question targeting in the same way as for question results. For more information, see Overview of advanced filters on page 261.

© 2026 Tanium Inc. All Rights Reserved

a. Click **Add Row** or **Add Group**.

b. (Group filter only) Select whether to apply a Boolean **AND** or **OR** to all the filters in the group.

c. Select an option for the first or only filter:

- **Sensor**: Specify a sensor using the same methods and options as in the **Get the following data** section.
- **Computer Group**: The dropdown lists all the computer management groups and filter groups that you have permissions to access. You can type a string in the typeaheads field to filter the list if it is long. Select a computer group and click Apply.

Perform the remaining sub-steps only if additional targeting filters are required.

d. Click and select one of the following options for each additional filter:

- **Add Row**: Configure the filter as you did for the first row. Then select a Boolean **AND** or **OR** to apply to this filter and other filters that are at the same level.
- **Add Group**: Configure a group of nested filters. Then select a Boolean **AND** or **OR** for filters within the group and a separate **AND** or **OR** for the relationship between the entire group and other filters at the same level as the group.

e. (Optional) Expand the **Advanced Question Options** and enable **Force Computer Id** to convert a counting question into a non-counting question. This option works only if the `get` statement has a single sensor; a `get` statement with multiple sensors is automatically a non-counting question. The option forces Tanium Clients to include the **Computer ID** sensor results in their answers. Note that the **Question Results** page does not show the **Computer ID** results when you select this option. For more information, see Counting and non-counting questions on page 235.

4. Click **Ask Question** to issue the question.
   The **Question Results** page opens to show the answers from endpoints.

TIP

For more information, see Part 7: Analyzing question results in Console and Interact on page 255.

Search endpoints

Use the Interact **Search Endpoints** field to view comprehensive information about a single endpoint as an alternative to issuing a long, complex question in the **Ask a Question** field. Interact quickly retrieves and displays information for the **Search Endpoints** feature, even if the target endpoints are currently offline. This quick retrieval is possible because most of the sensors that collect the information are registered by default with Tanium Data Service (TDS), which collects the information through recurring questions and stores the results.

NOTE

The permissions that are required to use the **Search Endpoints** field are available to the **Administrator** reserved role, **Interact Power User**, and **Interact Basic User** role.

© 2026 Tanium Inc. All Rights Reserved

NOTE For more information about TDS, see Tanium Interact User Guide: Managing Tanium Data Service.

The **Search Endpoints** field provides two levels of information:

- **Basic information**: This includes the results of the following sensors:
  - **Computer Name**
  - **Tanium Client IP Address**
  - **OS Platform**
  - **Last Logged in User**
  - **Online** status: online or offline
- **Detailed information**: You can open the Endpoint Details page, which shows comprehensive details from dozens of sensors and provides additional options for exploring and managing the endpoint. For more information, see Tanium Reporting User Guide: Working with a single endpoint.

TIP You can also access the basic and detailed information through the Interact **Question Results** page. For more information, see View details for a single endpoint on page 270.

1. Perform one of the following steps to access the **Search Endpoints** field:
   - In the Quick Search bar of the Console header, click to display the search field.
   - Go to the Tanium **Home** page and click the **Search Endpoints** tab.
2. Display basic information about an endpoint by typing its computer name, Tanium Client IP address, or last logged-in user name without pressing **Enter**.

   TIP Type a partial string to see basic information about multiple endpoints. For example, if you type `10.20.21`, a dropdown list shows information about all the endpoints with an IP address that contains those digits.
3. Click the **Computer Name** to open the Endpoint Details page.

Jump to endpoints

Jump Gate overview

Tanium Jump Gate provides secure, controlled, just-in-time access to critical systems and data in your environment. An access session is called a *jump*. After you request a jump and the request is approved, you can access a PowerShell session on a controlled Windows endpoint or a Bash session on a controlled macOS or Linux endpoint.

A Jump Gate operator defines the access policies that determine:

© 2026 Tanium Inc. All Rights Reserved

- Which endpoints can be jump targets
- Which users or user groups can request jumps
- Whether jump requests require approval and for which users or user groups
- Which users can approve or reject jump requests



For an overview of Jump Gate concepts, the role permissions to request and approve jumps, and the steps to configure access policies, see Tanium Jump Gate User Guide.

Jump to an endpoint

You can jump to an endpoint without issuing a question (**Search Endpoints** feature) or from the **Question Results** page. In both cases, the jump option appears only for endpoints that support jumps.

	Search Endpoints	Question Results
1.	Perform one of the following steps to access the **Search Endpoints** field: • In the Quick Search bar of the Console header, click to display the search field. • Go to the Tanium **Home** page and click the **Search Endpoints** tab.	Issue a dynamic or saved question that includes the **Computer Name**, **Computer ID**, or **Tanium Client IP Address** sensor.
2.	Specify an endpoint to target for the jump by typing the endpoint computer name, Tanium Client IP address, or last logged-in user name without pressing **Enter**.	In the **Question Results** grid, click the endpoint icon.
3.	In the **Access Endpoint** column, click Create Jump.	Click **Create Jump**.

© 2026 Tanium Inc. All Rights Reserved

	Search Endpoints	Question Results
4.	Select the **Access Type**, enter a **Justification** for the request, and click **Submit**. The **Request Details** page opens in a new browser tab and shows the approval status. If approval is automatic or not required, proceed immediately to the next step. If another user must approve the request, wait until the approval status changes to `Completed` before proceeding to the next step. For more information, see: • Tanium Jump Gate User Guide: View your own open requests • Tanium Jump Gate User Guide: View and approve jump requests TIP Tanium™ Guide provides a notification when a user approves a jump request. You can click **View request** in this notification to open the **Request Details** page.	
5.	In the **Request Details** page, click **Jump**. The window for the jump session appears on the **Request Details** page. TIP You can enlarge or shrink the session window. In the **Endpoint Details** section, click the **Name** of the target endpoint to open the Endpoint Details page in Tanium Reporting, where you can view comprehensive information about the endpoint and manage the endpoint. For more information, see Tanium Reporting User Guide: Working with a single endpoint.	
6.	Click **Close Jump** to end the session when you finish the work that requires access to the endpoint.	

BEST PRACTICE

Use a method or program to detach any long-running processes from the terminal to prevent those processes from terminating if the session ends unexpectedly. For example, you can use the `START /B` command on Windows or the `tmux` program for Linux and macOS. For more information about troubleshooting disconnected sessions, see Tanium Jump Gate User Guide: Troubleshooting disconnected jump sessions.

Question expiration

When the Tanium Server issues a dynamic or saved question, it remains open (not expired) for 10 minutes on the targeted endpoints. Upon receiving a question, the Tanium Client on each endpoint runs the sensors in the question, stores the results in its Client cache, and returns the results to the Server. If the Client reruns a sensor from the question during the 10-minute expiration interval, the Client returns the fresh result of that sensor to the Server. The frequency at which the Client reruns any particular sensor depends on the **Max Sensor Age** setting in the sensor configuration. The setting determines the maximum time for which the Client returns a cached result when answering questions, instead of rerunning the sensor for a fresh result.

© 2026 Tanium Inc. All Rights Reserved

For example, if the **Max Sensor Age** is 8 minutes, the Tanium Client runs the sensor twice: first upon receiving the question and then again after 8 minutes. If the Client receives another question between those two instances, the Client returns a cached result instead of rerunning the sensor. If the **Max Sensor Age** exceeds 10 minutes, the Client runs the sensor only once before the question expires.

For more information, see Max Sensor Age on page 428.

> NOTE
>
> The expiration interval is 2 hours instead of 10 minutes for questions that the Tanium Server issues to collect results for sensors that are registered with Tanium Data Service (TDS). For more information, see Tanium Interact User Guide: Sensor results caching and updates.

For each question, the Tanium Server assigns an identifier (ID) that appears in the URL field of your browser when the **Question Results** page opens. For example, in the URL `https://10.20.30.40/#/interact/q/376`, the question ID is 376. The question and its ID expire 10 minutes after the question is issued, at which point the URL becomes invalid. This means you can refresh the page or share a link to its URL only within that 10-minute period. If you navigate to the URL after 10 minutes, Interact displays a `Question Expired` message and **Copy Question** button. Clicking the button reissues the question.

Question history

Use the **Question History** page to manually reissue questions or view a chronology of issued questions, as well as their syntax and other details (such as issuer and expiration time stamp). By default, the **Question History** page shows questions that were issued in the past 24 hours. You can change the date range to show more entries, or apply filters to limit the entries that appear.

By default, question **Expiration** date-times are based on the **Local Time** of the system that you use to access Tanium Console, but you can switch to Coordinated Universal Time (**UTC**).

> NOTE
>
> Users require a role with the **Question History read** permission to see the **Question History** page. For the permissions that are required to load questions from the page, see Question history on page 102.

Reissue a question

To reissue a question, select the question in the grid and click **Load**. Console displays the results in the **Question Results** page.

Export question history

Export information from the **Question History** grid as a CSV file to view the information in an application that supports that format. If you have the **Administrator** reserved role, you can also export the information as a JSON file.

1. From the Main menu, go to **Administration > Content > Question History**.
2. Select rows in the grid to export information only for specific questions. If you want to export information for all questions, skip this step.
3. Click Export .

© 2026 Tanium Inc. All Rights Reserved

4. (Optional) Edit the default export **File Name**.

   
   NOTE

   The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.

5. Select an **Export Data** option: export information for all **All** questions in the grid or just for the **Selected** questions.
6. Select the file **Format**: **CSV** (default) or **JSON** (**Administrator** reserved role only).
7. Click **Export**.

   The Tanium Server exports the file to the downloads folder on the system that you used to access Console.

Copy question history details

Copy question history details to your clipboard to paste them into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string.

1. From the Main menu, go to **Administration > Content > Question History**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy .
   - **Copy cell information**: Hover over the cell, click Options , and click Copy .

Saved questions

After issuing a dynamic question, you can click **Save** above the question field to save the question syntax as a configuration object with associated settings. You can then reissue the question without reconstructing it in the **Ask a Question** field or **Question Builder**. Tanium solutions provide predefined saved questions. You can issue saved questions manually or based on a configurable schedule. You can also issue saved questions through Tanium modules or custom applications that use the Tanium XML API. For more information, see Managing saved questions in Console and Interact on page 455.

© 2026 Tanium Inc. All Rights Reserved

Part 7: Analyzing question results in Console and Interact

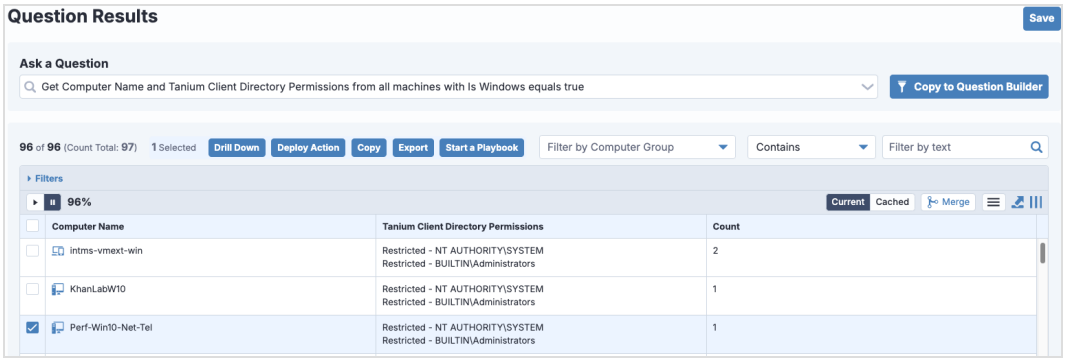
Question results overview

After you issue a question, the Interact **Question Results** page opens and shows a grid with the answers (sensor results) from endpoints. The page provides the following options for analyzing the results and addressing any issues that they reveal:

- Grid customizations, such as wrapping or unwrapping text that is too wide to fit on one line in the cells. For more information, see Data grid viewing options on page 61 and Filter question results on page 259.
- Continuous live updates to the results from online endpoints. For more information, see Enable or disable live updates on page 257
- Viewing cached results for offline endpoints. For more information, see Display results for online and offline endpoints on page 258.
- Collection of additional results that relate to the current results. For more information, see Merge questions on page 264, Drill down into results on page 267, and View details for a single endpoint on page 270.
- Reviewing results in another application. For more information, see Copy question results to the clipboard on page 262 and Export question results on page 262.
- Endpoint access and management to address issues that the results reveal. For example, you might want to deploy an action that updates access permissions for the Tanium Client installation directory if results show that too many users can access that directory. For more information, see Jump to endpoints on page 250 (opening shell sessions) and Deploying actions and playbooks in Console and Interact on page 391.

Several of the preceding options become available only after you select one or more rows of results. For more information, see Selecting rows on page 256.

Question Results page



For more information about how the **Question Results** page shows sensor results across multiple columns, see What is a sensor? on page 232.

© 2026 Tanium Inc. All Rights Reserved

TIP

To refine the original question, update your entry in the **Ask a Question** field (see Issue a free-form question on page 241) or click **Copy to Question Builder** to open the **Question Builder** (see Issue a question through the Question Builder on page 245).

NOTE

The user roles and permissions that are required to ask questions also enable you to view the results. For more information, see Tanium Interact and TDS permissions on page 80.

You can view question results only from computer groups that are assigned to your user account or persona. For more information, see Assign computer groups on page 618.

If endpoints do not answer questions, see Troubleshoot question results issues on page 709.

Results aggregation

If more than one endpoint returned the same answer for a question, the results grid shows a **Count** column to indicate the number of endpoints for each answer. For more information, see Counting and non-counting questions on page 235.

Results for saved questions and dashboards

When you issue a saved question or a dashboard of questions, Interact opens the saved question results page or dashboard results page respectively. These pages resemble the **Question Results** page for dynamic questions but have additional options. For more information, see Issue a saved question on page 466 and Issue a dashboard of saved questions on page 467.

BEST PRACTICE

Use Tanium Reporting instead of Interact saved questions or dashboards if you want to review results from sensors that are registered with Tanium Data Service (TDS). For more information, see Part 7: Analyzing question results in Console and Interact on page 255.

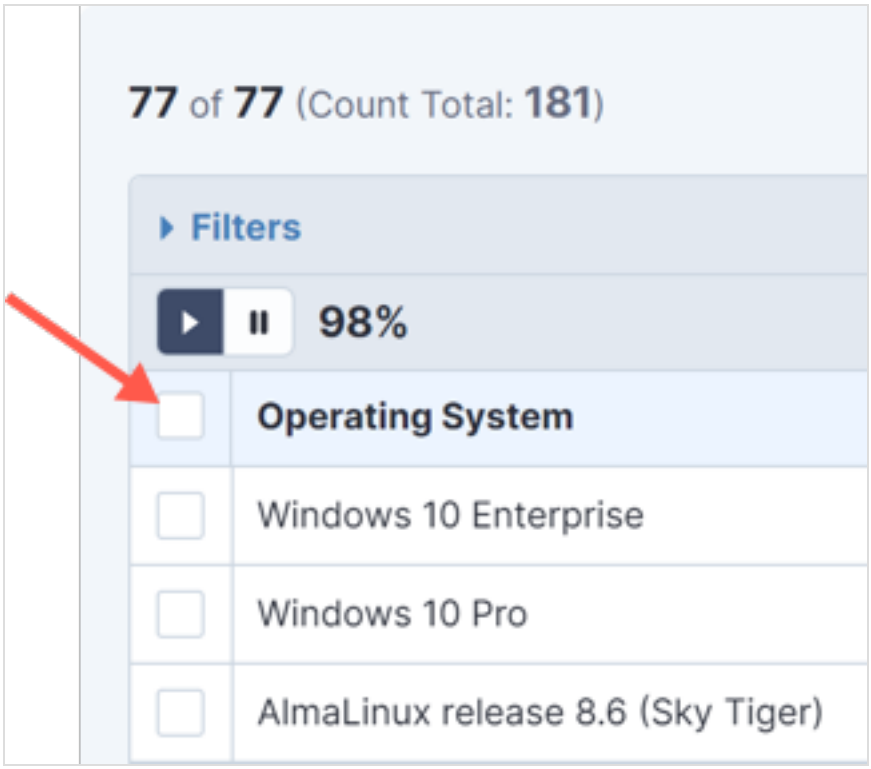
Selecting rows

After you manipulate the **Question Results** grid to show the results that you want, you can select result rows to perform additional operations, such as deploying actions. You can select up to 100 rows in the grid. The following options facilitate selecting multiple rows:

- To quickly select multiple consecutive result rows for drilling down, copying, exporting, or deploying actions, click the checkbox in the first row to include, hold down the **Shift** key, and then click the checkbox in the last row to include.
- Select the check box in the header row to select 100 rows, starting with the first row in the grid. If you already selected rows before selecting the check box, Interact only selects enough additional rows to reach the 100 limit. Clear the check box to clear any selected rows.

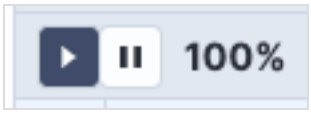
© 2026 Tanium Inc. All Rights Reserved

Check boxes for selecting question results



Enable or disable live updates

On the **Question Results** page, the results grid has a toolbar that shows the percentage of Tanium Clients that reported results. The live updates feature is enabled by default, which means Interact updates the grid as more Tanium Clients report results.



Click Pause to stop the grid from updating and click Play to resume updating.

TIP

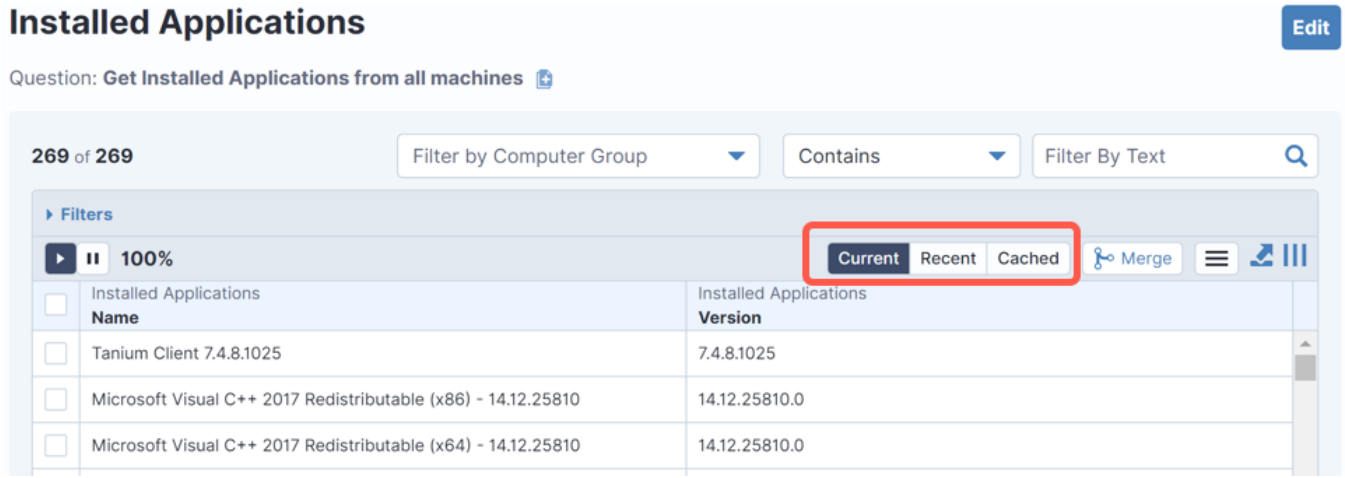
Even after 100% of Tanium Clients have reported, some answer rows might indicate incomplete results. To investigate incomplete results, see Troubleshoot question results issues on page 709.

© 2026 Tanium Inc. All Rights Reserved

Display results for online and offline endpoints

When the **Question Results** page opens, it initially displays only current results, which are answers from endpoints that were online at the moment you issued the question. However, you can also display recent or cached results that the Tanium Server stored when it queried endpoints that were previously online but are currently offline.

Current, recent, and cached results for questions



The option to display stored results enables you to have a more complete view of your managed endpoints. For example, to evaluate the security state of both online and offline endpoints, you can display both current and stored results for questions about which endpoints have a critical patch applied or a particular third-party application installed. Click the button for the type of results that you want to display:

Current, recent, and cached results for questions

Results options	Description
Current	The grid shows results from endpoints managed using Tanium Client that are currently online.
Recent	This option is available only for the results of saved questions and only users who have permissions to create saved questions can view recent results. For more information, see Managing saved questions in Console and Interact on page 455. In addition to results from online endpoints managed using Tanium Client, this option includes results from offline endpoints managed using Tanium Client if those results still reside on the Tanium Server after the last time the Server issued that question. The Server stores the results of saved questions for seven days by default. The Tanium Server associates recent results with specific saved questions, not with sensors. This means that even if multiple saved questions share the same sensor, the results grid might show different recent results for that sensor based on which question you issue and your computer management group permissions. For more information, see Recent results and computer group assignments on page 756

© 2026 Tanium Inc. All Rights Reserved

Current, recent, and cached results for questions (continued)

Results options	Description
Cached	The grid displays results that the Tanium Server collects by periodically querying all managed endpoints for specific sensors. The option appears only for questions in which all the sensors are registered for collection with Tanium Data Service (TDS). For more information, see Tanium Interact User Guide: Managing Tanium Data Service. The Server stores the results for 30 days by default. The grid displays only the most recent collected results. The Server saves the results on a per-sensor basis. Consequently, the grid shows the same results for a particular sensor when you issue any dynamic or saved question that uses that sensor.



For offline endpoints, view **Cached** results instead of **Recent** results. For cached results, the Tanium Server more accurately identifies the responding endpoints, allows all users to view the results, and returns results for both dynamic and saved questions.

Filter question results

Use the following filter options in the header of the **Question Results** grid to show only results that match the criteria you specify:

- Filter by text on page 260
- Filter by computer group on page 260
- Filter by advanced conditions on page 261

Interact applies a Boolean AND if you configure multiple types of filters. For example, if you select a computer group filter and configure an advanced filter, Interact shows only the results that match both filters.

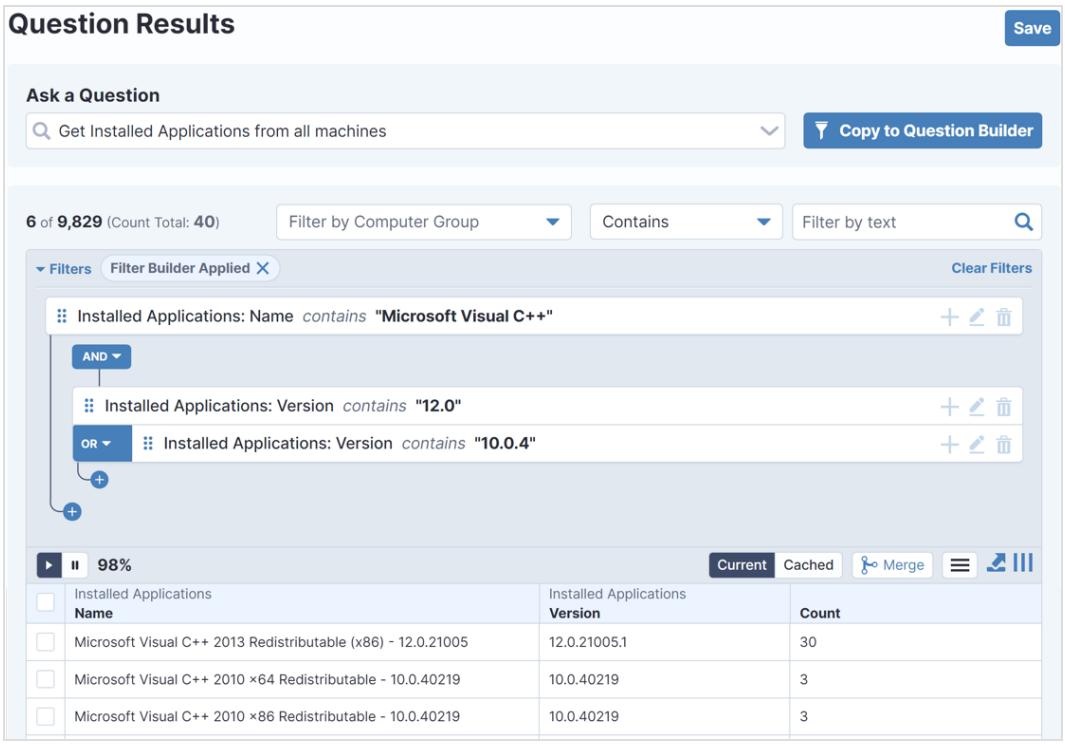


If you save a question, the question text does not include any filters that you added on the **Question Results** page.

To apply filters to a question instead of its results, see Use question filters on page 731.

Question Results grid filters

© 2026 Tanium Inc. All Rights Reserved



Filter by text

On the **Question Results** page, use the **Filter by text** field to filter results based on their values. The Tanium Server filters the grid without reissuing the question.

1. Select **Contains** or **Does not contain** in the dropdown list beside the **Filter by text** field.
2. Enter a search string in the **Filter by text** field and click Search.

TIP

For most questions, the text filter shows matching results in any grid column. If you filter on certain cached results, the text filter ignores the **Count** column values.

Filter by computer group

On the **Question Results** page, select a **Filter by Computer Group** option to issue a new question with the added filter. If the dropdown list shows many computer groups, you can enter part or all of a group name in the text field to filter by that name.

NOTE

The **Filter by Computer Group** dropdown list shows only computer management groups that are assigned to your user account. The list also shows filter groups that are assigned to a content set for which your account has role permissions. For more information, see Controlling endpoint management rights through computer groups on page 610.

© 2026 Tanium Inc. All Rights Reserved

Filter by advanced conditions

OVERVIEW OF ADVANCED FILTERS

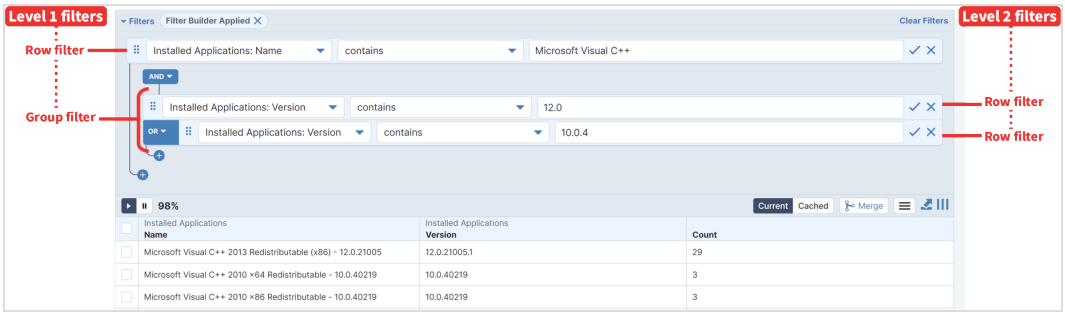
On the **Question Results** page, you can configure a filter that is based on conditions for matching sensor results. Interact evaluates the filter to a Boolean true or false and shows only the results that evaluate to true. For example, if you issue a question with the **Installed Applications** sensor and configure the filter `application name contains Microsoft Visual C++`, the **Question Results** grid shows only results in which an application name contains the string `Microsoft Visual C++`.

If you configure multiple filters, Interact shows results only if their true/false evaluations collectively match your Boolean AND/OR selection:

- **AND**: The grid shows only results for which all the filters evaluate to true.
- **OR**: The grid shows results for which any filter evaluates to true.

The AND/OR selection cannot differ among filters that are at the same level (not nested). If you configure multiple levels of filters through nested groups, you select a Boolean AND/OR for each level. Interact evaluates filters in ascending order, from the row filters in the lowest-level group to the highest level of row and group filters. The following figure shows two levels of filters: the first (highest) level has a row filter and group filter, and the second (lowest) level comprises the row filters within the group.

Row and group filters for question results



Interact evaluates these example filters in the following sequence:

1. Interact evaluates each row filter within the group: `application version contains 12.0` and `application version contains 10.0.4`.
2. Interact evaluates the group filter to a collective true if either filter inside the group evaluates to true because the Boolean OR is selected for those filters. Interact also evaluates the first-level row filter: `application name contains Microsoft Visual C++`.
3. Interact applies a Boolean AND to the first-level filters, which means they collectively evaluate to true only if both the row filter and the group filter evaluate to true.

© 2026 Tanium Inc. All Rights Reserved

CONFIGURE ADVANCED FILTERS

1. In the header of the **Question Results** grid, expand the **Filters** section.
2. Select an attribute (sensor column), select an operator (such as **contains**), enter a value to match against (`Microsoft Visual C++` in the figure Row and group filters for question results on page 261), and click Apply. Interact evaluates the filter and refreshes the results grid as soon as you apply the filter.
   Results filters support the same operators as filters in the `get` statement of a question. Results filters do not support the **in** operator. For more information, see Filter operators on page 733.
   Perform the following steps only if you want additional filters. Repeat the steps for each filter.
3. Click Add and select an option:
   - **Add Row**: Specify the attribute, operator, and value as you did for the first filter.
   - **Add Group**: Specify the attribute, operator, and value for the first filter in the group. Then, for the next filter in the group, click Add and select a row or another group.
4. For each level of filters, select a Boolean **AND** or **OR**.

Copy question results to the clipboard

On the **Question Results** page, copy information from the results grid to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the copy.

- To copy specific results along with the sensor names (column headers), select the corresponding checkboxes and click **Copy**.
- To copy the contents of a grid cell, perform one of the following steps:
  - Hover over the cell, click Options, and click Copy Cell Value.
  - Press the **Alt** key (Windows) or **Option** key (macOS) and click in the grid cell. This operation works for most grids in Interact.

Export question results

You can use any application that supports CSV format to display the same columns of information as the grid on the **Question Results** page. For example, you can use Microsoft Excel to create charts based on results.

1. Select one of the following export options:
   - To export specific results, select the corresponding checkboxes and click **Export**.
   - To export the complete results, click Export in the header of the grid.
2. Enter a **File Name** for the CSV file.
3. To include sensor names (grid column headers) in the .csv file, select **Include headers in export**.
   If you selected only a subset of the results to export, click **Export** and skip the remaining steps, which describe options that are available only if you are exporting the complete results.

© 2026 Tanium Inc. All Rights Reserved

4. Select how the CSV file displays results for questions where one sensor generates multiple results for each responding endpoint. As an example, for the question `Get Computer Name and High CPU Processes[5] from all machines`, the High CPU Processes sensor returns five processes for each endpoint. By default, the file displays one row for all the results that the sensor generated for an endpoint. For the example question, this would mean each row lists all the top five processes for each endpoint (identified by Computer Name).

Computer Name	High CPU Processes[5]
SQL1.tam.local	sqlservr.exe TaniumClient.exe cmd.exe conhost.exe cscript.exe
TS1.tam.local	TaniumReceiver.exe chrome.exe svchost.exe cmd.exe conhost.exe

   To display a row for each result that a sensor generates, select **Flatten rows**. For the example question, a flattened export results in five rows per endpoint: one row for each process that the High CPU Processes sensor returned. Note that this option works only if just one sensor in the question has multiple results.

Computer Name	High CPU Processes[5]
SQL1.tam.local	sqlservr.exe
SQL1.tam.local	TaniumClient.exe
SQL1.tam.local	cmd.exe
SQL1.tam.local	conhost.exe
SQL1.tam.local	cscript.exe

   If you select **Flatten rows**, the **Fail on errors** checkbox appears. Selecting **Fail on errors** causes the export to fail for all results if any result includes multiple columns (sensors) with more than one value. In the example, it would be an error if a single endpoint returned multiple results for both Computer Name and High CPU Processes. By default, **Fail on errors** is disabled, which means the export proceeds despite such errors. However, the output includes errors without flattening the affected results; the output does not use separate lines to account for multiple columns with multiple values.

5. Click **Export**.

© 2026 Tanium Inc. All Rights Reserved

Merge questions

Question results often lead to additional questions. For example, the results of a question that returns computer names and running processes might indicate that some endpoints are running a suspicious process. You can *merge* the initial question with another question to learn more information, such as the last logged-in user. The Tanium Server issues the merge question in the background, and Interact re-displays the **Question Results** grid with one or more additional columns containing results for the sensors that the merge question specified.



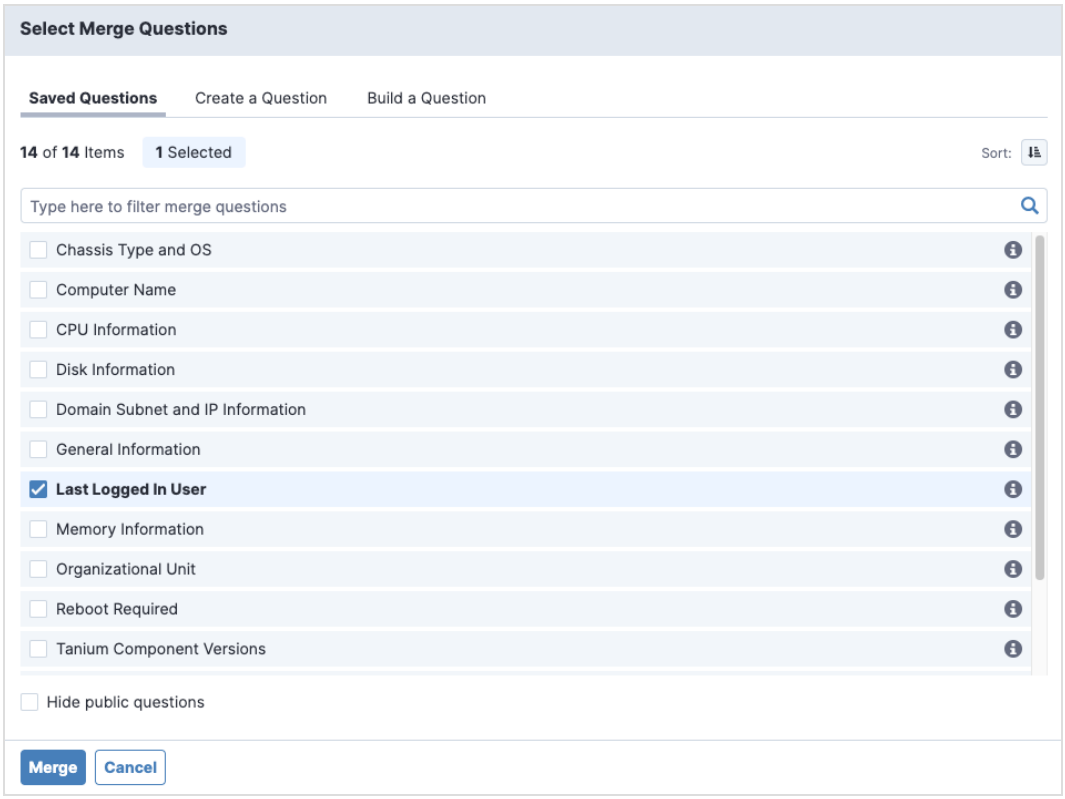
Merge operations automatically apply to all results. You do not need to select grid rows before merging.

You can use only non-counting questions in merge operations. For more information, see Counting and non-counting questions on page 235.

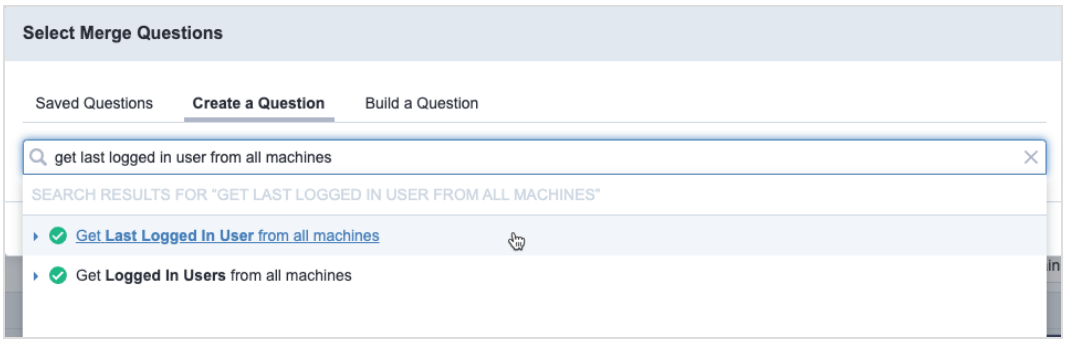
1. On the **Question Results** page, click **Merge** in the grid toolbar.
2. Use one of the following tabs to add questions and then click **Merge**:
   - **Saved Questions**: Lists saved questions that are assigned to content sets for which you have **Saved Question read** permission. The questions must also have the Display this question in the list of questions that are available to merge on page 465 setting enabled.

     To filter the list so that it includes only saved questions with **Visibility** is set to **Only the Owner and Admins can see this object**, select **Hide public questions**.

© 2026 Tanium Inc. All Rights Reserved

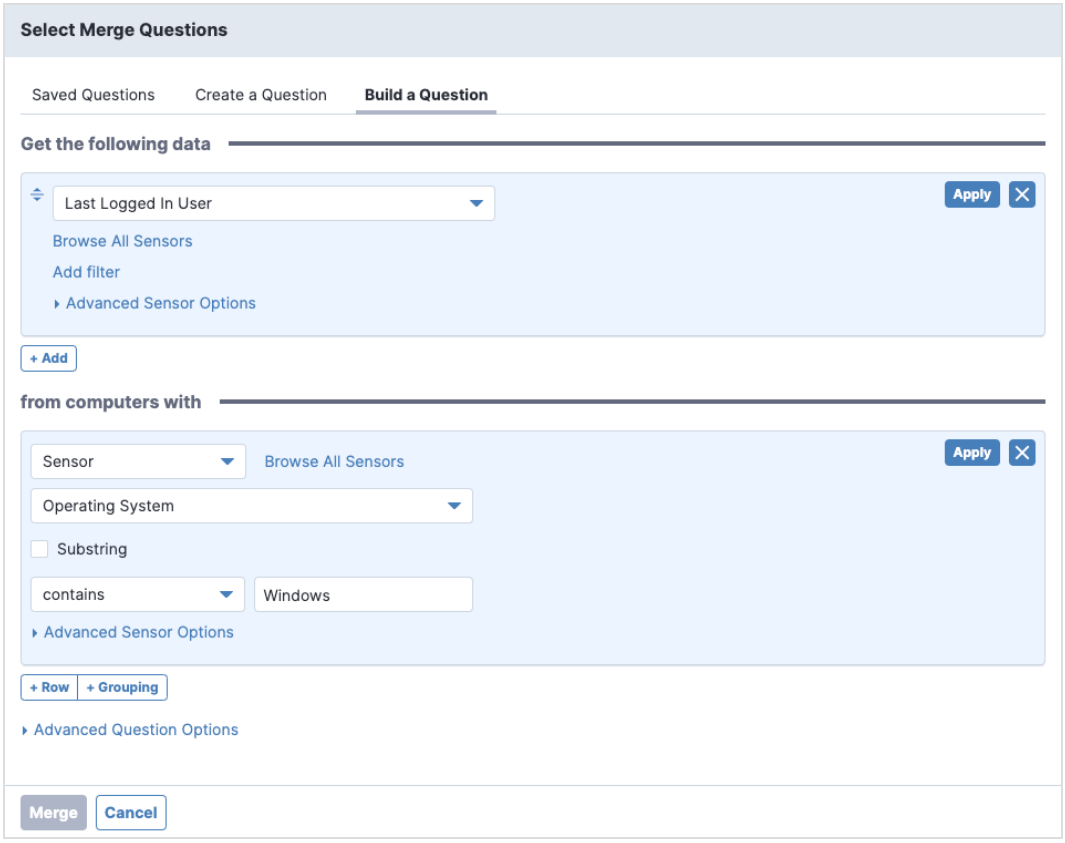


- **Create a Question**: Enter a question using the same syntax as in the Interact **Ask a Question** field. For more information about the syntax, see Issue a free-form question on page 241.



© 2026 Tanium Inc. All Rights Reserved

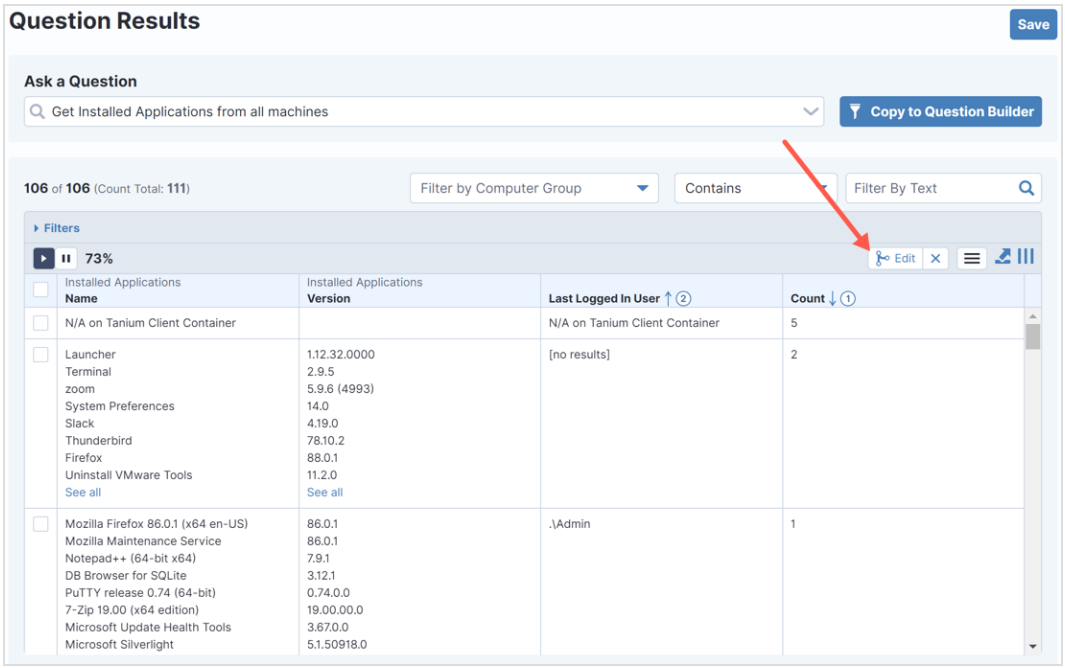
- **Build a Question**: Construct a question using the same fields as in the Interact **Question Builder**. For more information, see Issue a question through the Question Builder on page 245.
  Notice that you add sensors to the `get` clause but you do not add filters to the `from` clause. The `from` clause is automatically based on the rows that you selected in the **Question Results** grid when you clicked **Merge**.



After you click **Merge**, the **Question Results** grid displays the updated results. You can use the **Edit** button in the grid header to modify the merge settings.

Question results after a merge operation

© 2026 Tanium Inc. All Rights Reserved



Drill down into results

In the **Question Results** grid, you can drill down into selected results to retrieve more information from the associated endpoints. Adding a drill-down question effectively means using its sensors to filter the selected results. A typical scenario is targeting a smaller group of endpoints for an action. For example, you might initially issue a question that returns a list of chassis types and operating systems for all endpoints. To see the identities of endpoints that return specific results, you can drill down into those results with the **Computer Name** sensor.

1. In the **Question Results** grid, select the results for which you want more information and then click **Drill Down**.
2. Use one of the following tabs to specify a drill-down question and then click **Drill Down**.

   TIP

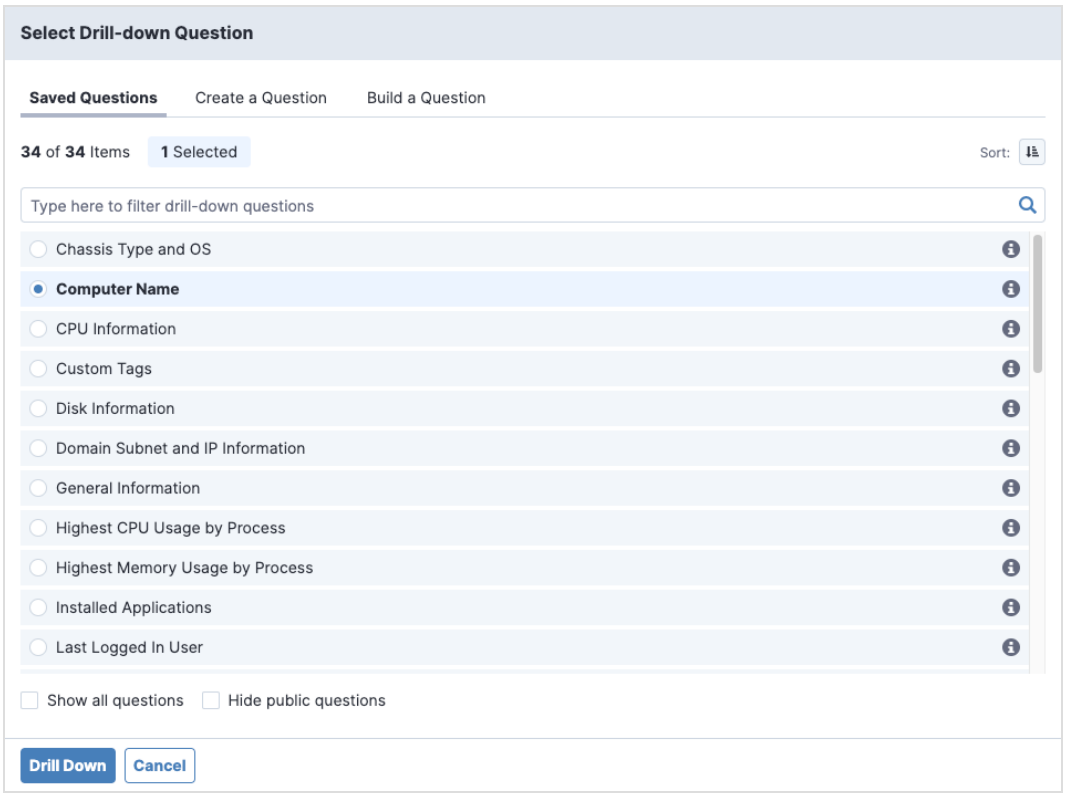
   If the selected **Question Results** include the value of a parameterized sensor and your drill-down question uses a sensor with a matching parameter, the **Select Drill-down Question** dialog automatically populates that parameter with the value from the selected results.

   - **Saved Questions**: Lists saved questions that are assigned to content sets for which you have **Saved Question read** permission. By default, the list includes only questions that have the Display this question in the list of questions that are available for drilling down on page 464 setting enabled. To include questions that do not have the setting enabled, select **Show all questions**.

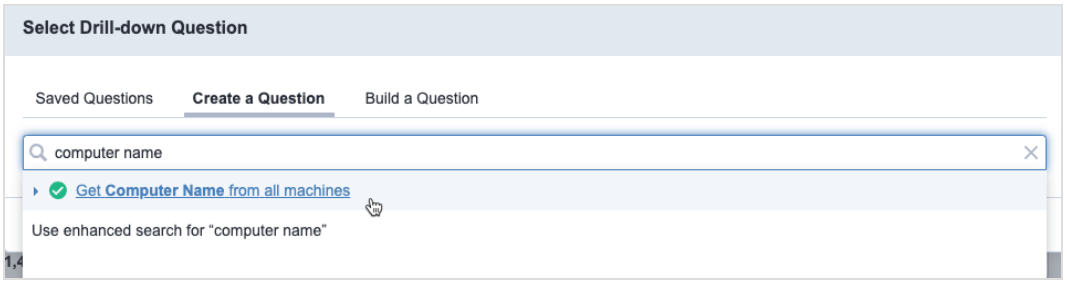
© 2026 Tanium Inc. All Rights Reserved

TIP

To filter the list so that it includes only saved questions with **Visibility** is set to **Only the Owner and Admins can see this object**, select **Hide public questions**.

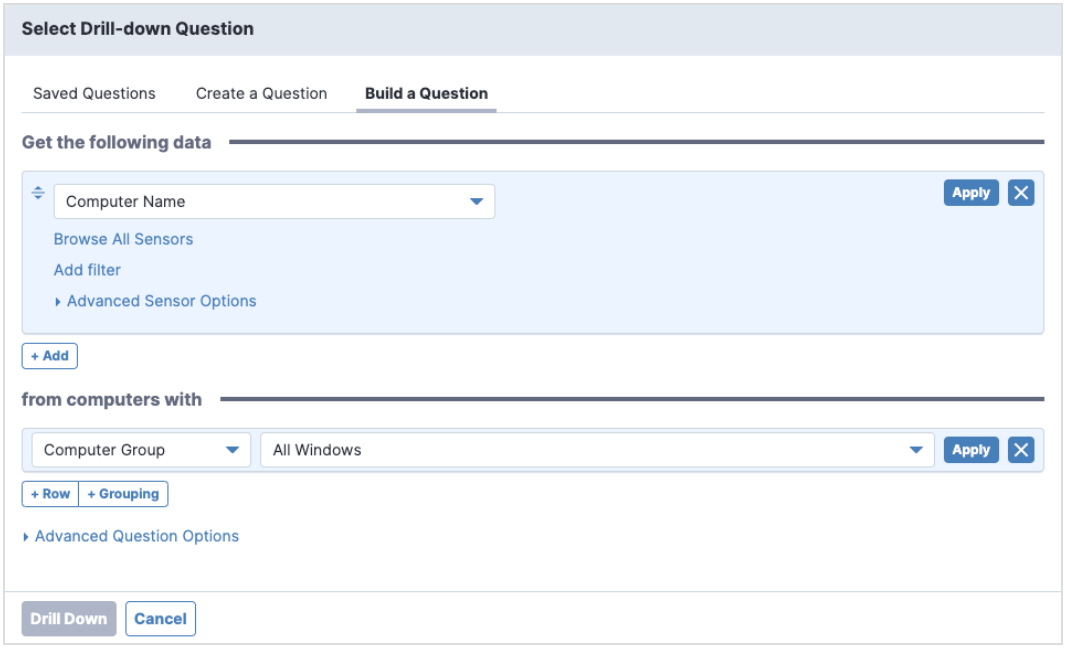


- **Create a Question**: Enter a question using the same syntax as in the Interact **Ask a Question** field. For more information about the syntax, see Issue a free-form question on page 241).



© 2026 Tanium Inc. All Rights Reserved

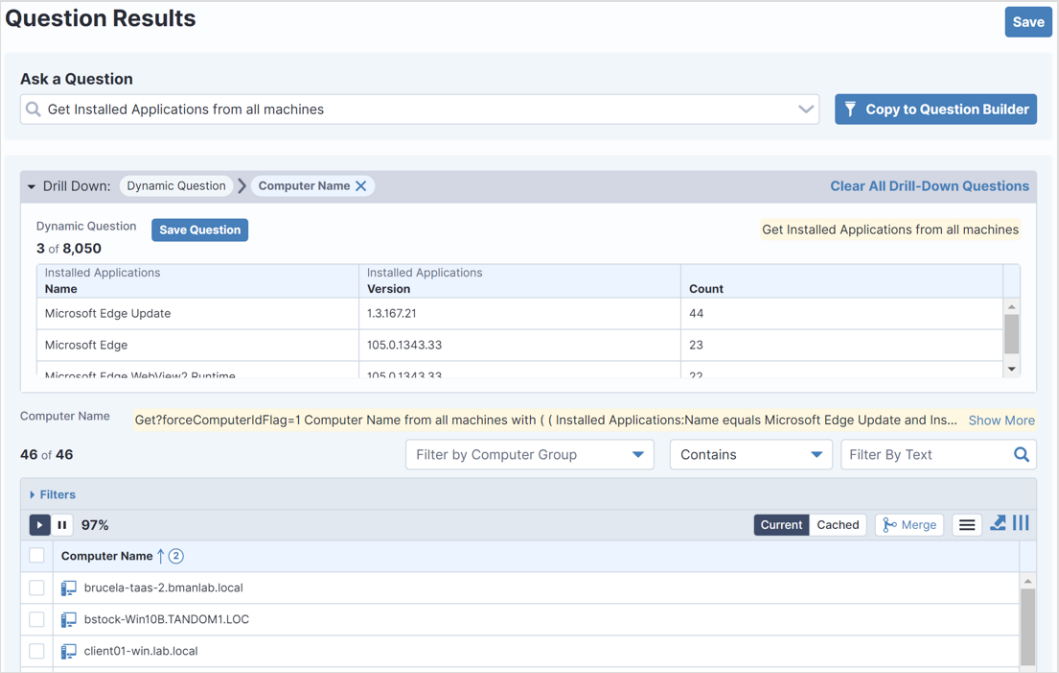
- **Build a Question**: Construct a question using the same fields as in the Interact **Question Builder**. For more information, see Issue a question through the Question Builder on page 245.



After you click **Drill Down**, Interact shows the progression of results, including a new **Question Results** grid for the drill-down question. You can then drill down further, deploy an action, save the question, or click **Copy to Question Builder** for further refinement.

Question results after drill-down operation

© 2026 Tanium Inc. All Rights Reserved



View details for a single endpoint

When you analyze question results from endpoints, you might want to explore additional information about a particular endpoint. For example, if an endpoint returns `100%` for a question with the **CPU Consumption** sensor, you might want to see details about the processors on that endpoint. Interact provides a single endpoint view feature that quickly retrieves and displays the information, even for endpoints that are currently offline. This quick retrieval is possible because most of the sensors that collect the information are registered by default with Tanium Data Service (TDS), which collects the information through recurring questions and stores the results.

> NOTE
>
> For more information about about TDS, see Tanium Interact User Guide: Managing Tanium Data Service.
>
> The permissions that are required to view endpoint details are available to the **Administrator** reserved role, **Interact Power User** role, and **Interact Basic User** role.

From the Interact **Question Results** page, you can access two levels of information about an endpoint:

- **Basic information**: This includes the results of the following sensors:
  - **Computer Name**
  - **Tanium Client IP Address**
  - **OS Platform**

© 2026 Tanium Inc. All Rights Reserved

    - **Last Logged in User**
    - **Online** status: online or offline

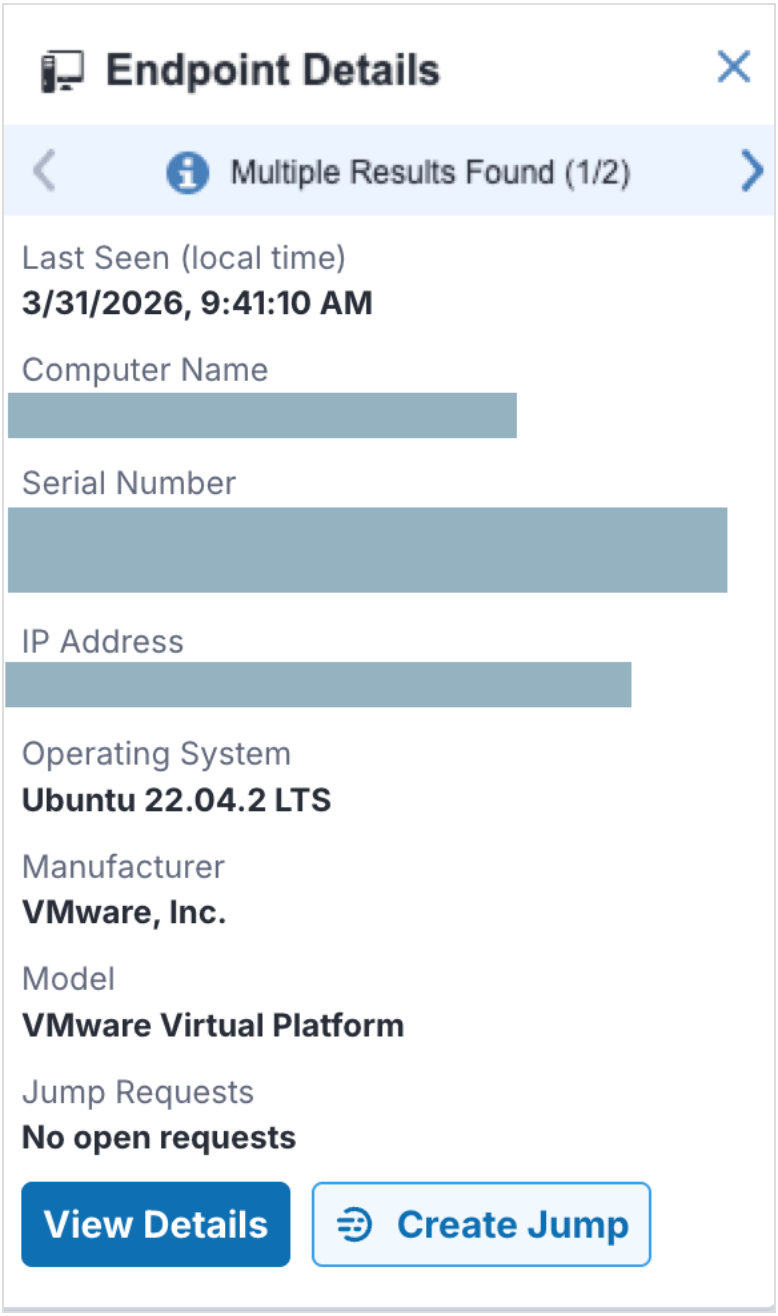
- **Detailed information**: You can open the Endpoint Details page, which shows comprehensive details from dozens of sensors and provides additional options for exploring and managing the endpoint. For more information, see Tanium Reporting User Guide: Working with a single endpoint.

You can access basic or detailed information about an endpoint without first issuing a question by using the **Search Endpoints** field in the Tanium Console header or Tanium **Home** page. For more information, see Search endpoints on page 249.

1. Issue a question that includes the **Computer Name**, **Computer ID**, or **Tanium Client IP Address** sensor. For more information about issuing questions, see Issue a free-form question on page 241 or Issue a question through the Question Builder on page 245.
2. In the **Question Results** grid, click an endpoint icon to see the details for that endpoint.

© 2026 Tanium Inc. All Rights Reserved

An **Endpoint Details** dialog opens to display the basic information. If multiple endpoints have the same **Computer Name**, **Tanium Client IP Address**, or **Last Logged in User**, click Previous or Next in the **Multiple Results Found** banner to find the details for a specific endpoint.



3. Click **View Details** to open the Endpoint Details page.

© 2026 Tanium Inc. All Rights Reserved

Optimizing and automating workflows through the Autonomous IT Platform

Overview of Tanium Autonomous IT Platform

Tanium Autonomous IT Platform comprises a set of interrelated features across multiple Tanium solutions that collect real-time intelligence about conditions in your environment. The Autonomous IT Platform provides guidance based on that intelligence, along with actions and cross-solution workflows (playbooks) to act on the guidance. You can automate workflows to improve the security posture of your organization, avoid costly IT disruptions due to malware or human error, and reduce overhead for IT support. The Autonomous IT Platform provides these capabilities through the following elements.

Guided initial configuration

Tanium Threat Response provides common configuration workflows to expedite the time to value and to simplify the initial configuration experience. The configuration workflows include samples of functionality and scenarios to accelerate learning for new users. For more information, see Tanium Threat Response User Guide: Getting started with Tanium Threat Response.

Proactive guidance

Tanium Guide automatically aggregates and analyzes data from millions of endpoints across all Tanium Cloud environments. Based on the analysis, Guide identifies trends, anomalies, and emerging issues that are relevant to your environment. Tanium Guardian provides dashboards that alert you to emerging issues and provides predefined actions that mitigate the impacts of the issues before they happen. For more information, see

- Tanium Reporting User Guide: Emerging issue dashboards
- Tanium Guide User Guide: Viewing and managing notifications

Adaptive actions and playbooks

You can deploy each Tanium platform or Deploy (software) action through a sequence of progressive phases called rings. For each ring, you define the target endpoints and progression criteria to ensure safe, reliable change management for endpoints. Adaptive (ring-based) actions are designed for autonomous deployment, but you can customize, monitor, and control their deployment as necessary. Tanium Automate playbooks enable you to automate reusable, event-driven workflows that run actions and other tasks across multiple Tanium solutions. Playbooks streamline your business processes, improve productivity, and reduce human errors by minimizing or eliminating the manual effort to create, perform, and monitor routine tasks. For more information, see:

- Deploying actions and playbooks in Console and Interact on page 391
- Tanium Automate User Guide

© 2026 Tanium Inc. All Rights Reserved

Action oversight

Tanium Console provides centralized oversight for viewing the history and current state of all adaptive actions that users or Tanium solutions deploy. From a single Console page, you can track deployment progress, troubleshoot unexpected results, and intervene before or during deployment. For more information, see Managing ring deployments on page 359.

Autonomous IT Platform across Tanium solutions

Autonomous IT Platform features work seamlessly across Tanium solutions such that you can quickly achieve their benefits without comprehensive knowledge of all solutions or the Platform mechanisms. You can customize the Autonomous IT Platform to fit your environment by configuring the following Tanium solutions:

- Automate on page 274
- Benchmark on page 274
- Comply on page 275
- Console on page 275
- Deploy on page 275
- Enforce on page 275
- Guide on page 275
- Interact on page 276
- Patch on page 276
- Threat Response on page 276



Certain Tanium solution features that the Autonomous IT Platform provides are currently unavailable in Tanium Cloud for U.S. Government. For specific information, see the solution user guides in the Tanium Resource Center.

Automate

- **Playbooks**: Playbooks contain a series of steps, each representing a single task, that run Tanium functionality automatically. You can create custom reusable playbooks and run the playbook on an ad-hoc basis or on a schedule. For more information, see Tanium Automate User Guide: Building playbooks and Tanium Automate User Guide: Reference: Steps.

Benchmark

- **Guide notifications**: Benchmark can generate Guide observations related to risk score and benchmark metric changes. Tanium operators who receive these observations can view the risk score or benchmark metrics and remediate the situation. For more information, see Tanium Benchmark User Guide: Evaluating your risk score, Tanium Benchmark User Guide: Reviewing benchmark metrics, and Tanium Guide User Guide: Viewing and managing notifications.

© 2026 Tanium Inc. All Rights Reserved

Comply

- **Remediation Visibility**: Remediation visibility uses Tanium Comply to scan for vulnerabilities on endpoints and Tanium Patch or Tanium Deploy to remediate discovered vulnerabilities as part of one workflow. For more information, see Tanium Comply User Guide: Remediating findings.

Console

- **Deployment plans**: A deployment plan defines the sequence of rings (ring set) for an adaptive action. You can create a plan for each type of deployment that must progress through the same rings with the same progression criteria. For more information, see Managing deployment plans for ring deployments on page 384.
- **Ring deployment status**: The **Ring Deployment Status** page provides a central location for you to view the current state of adaptive actions across multiple solutions, track action progress, troubleshoot deployment issues, and intervene when necessary. For more information, see Managing ring deployments on page 359.

Deploy

- **Confidence score**: The confidence score rates the probability that a Predefined Package Gallery package deployment will succeed. Tanium assigns a confidence score to most unedited Predefined Package Gallery packages. Use the confidence score to determine when to deploy a software package. For more information, see Tanium Deploy User Guide: Gallery package confidence score and Confidence score.
- **Deployment plans**: A deployment plan defines the sequence of rings (ring set) for a ring-based deployment. You can assign a deployment plan to manual ongoing deployments or automatic deployment configurations. For more information, see Tanium Deploy User Guide: Deployments and ring deployment plans and Managing ring deployments.
- **Automatic deployment configurations**: An automatic deployment configuration automates the creation of Predefined Package Gallery package deployments based on rule triggers. Rule triggers can either use the latest available software package version or age of the software package in the gallery. For more information, see Tanium Deploy User Guide: Automatically deploying software package.

Enforce

- **Guide notifications**: Enforce can generate Guide observations and guidance related to endpoint security configuration. Tanium operators that receive these observations and guidance can view the affected endpoints and remediate the situation, or update Enforce configuration to enable Defender Platform updates. For more information, see Tanium Enforce User Guide: Manage anti-malware settings and Tanium Feed User Guide: Viewing and managing notifications.

Guide

- **Guide notifications**: Guide notifications enable you to stay informed of important updates and actions you might need to take. Tanium operators can receive Guide notifications in Tanium Console. For more information, see Tanium Guide User Guide: Viewing and managing notifications.



Tanium Guide was previously named Tanium™ Feed.

© 2026 Tanium Inc. All Rights Reserved

Interact

- **Adaptive actions**: An adaptive action applies changes to endpoints through a sequence of progressive phases called rings. Actions apply the changes by running content such as packages on the endpoints. Ring-based deployment enables you to safely test action impacts, mitigate disruptions to your environment, and protect sensitive resources when rolling out endpoint changes. For more information, see Deploying actions and playbooks in Console and Interact on page 391.

Patch

- **Confidence score**: The confidence score rates the probability that a Windows patch deployment will succeed and not cause post-installation downtime. Tanium assigns confidence scores to Windows patches released within the last 365 days or that are applicable in your environment. Use the score to determine if a patch is reliable enough for deployment or if you must first edit the endpoint targeting in the deployment. For more information, see Tanium Patch User Guide: Patch confidence score.

Threat Response

- **Tanium Automate playbook steps**: Tanium Automate implements endpoint quarantine and quarantine removal in playbook steps. For more information, see Tanium Threat Response User Guide: Quarantining endpoints, Tanium Automate User Guide: Building playbooks, and Tanium Automate User Guide: Reference: Steps.
- **Default configuration**: Threat Response provides common configuration workflows to expedite the time to value and to simplify the initial configuration experience. Configuration categories that target specific end-to-end scenarios decrease the number of steps required to operationalize Threat Response without having a comprehensive knowledge of all of the functionality of the module.

Ring-based deployment

Deployment *rings* enable you to deploy an action through a sequence of progressive phases instead of through a single phase. A ring defines the target endpoints for each phase and the criteria that the deployment must meet on those endpoints to progress to the next phase. You configure each ring and the ring set (sequence) in a deployment plan. When you create a deployment for an action that must progress through a ring set, you then assign a deployment plan to the deployment. An *adaptive (ring-based) action* is any action that has a deployment plan assigned, in contrast with *simple (non-ring-based) actions* that deploy in a single phase.

Consider the following aspects and components of adaptive actions before you configure and deploy them:

- Advantages of adaptive actions on page 277
- Deployment types on page 277
- Deployment plans on page 278
- Endpoint targeting on page 278
- First ring on page 292
- Last ring on page 292

© 2026 Tanium Inc. All Rights Reserved

- Ring progression criteria on page 292
- Deployment timing factors and maintenance windows on page 295
- Deferred endpoints on page 298

Advantages of adaptive actions

Adaptive actions provide the following advantages over simple actions.

TESTING AND RESTRICTION OF ACTION IMPACTS

You can limit any adverse impacts that an action might have on your environment by assigning endpoints to rings based on progressive levels of importance. For example, the first ring might target only test endpoints that do not affect regular operations in your organization. You can configure stricter progression criteria in subsequent rings to ensure that a deployment is safe before it reaches more critical or sensitive endpoints. Progression criteria control automatic promotion through the rings, but you can manually pause or stop promotion for the sake of troubleshooting, as described in Stop, pause, or resume deployments on page 375. You can also manually progress a deployment to the next ring if circumstances warrant overriding progression criteria failures, as described in Manually progress deployments through rings on page 377.

MITIGATION OF ACTION-RELATED DISRUPTIONS

An action might require unavoidable disruptions. An adaptive action staggers the deployment one ring at a time to minimize the overall disruption to your environment. Rings also provide control over the timing of progression. For example, if installing an application has an impact on endpoints that might take up to two hours to accurately measure, you can specify a Wait on page 293 interval of two hours before the Tanium Server evaluates the progression criteria.

PROTECTION FOR SENSITIVE ENDPOINTS

Adaptive actions enable you to defer action deployment for specific endpoints until the last ring. You can configure the strictest progression criteria before the last ring to ensure it is the safest ring with respect to action impacts. Deferral is useful for endpoints that you consider sensitive from a security viewpoint or that serve critical functions in your environment. For more information, see Deferred endpoints on page 298.

Deployment types

You can use ring-based deployment for the following deployment types by assigning a deployment plan to the associated action:

- **Deploy**: Packages that install, update, or remove software. This deployment type is available only if Tanium Deploy is installed in your environment. For more information, see Tanium Deploy User Guide.
- **Platform action**: Actions that you deploy through the following Tanium solutions:
    - **Interact**: For example, you can deploy actions from the **Question Results** page. For more information, see Deploying actions and playbooks in Console and Interact on page 391.
    - **Console**: For example, you can deploy actions from the **Packages** page or **Client Status** page.
    - **Reporting**: You can deploy actions from reports, dashboards, and the Endpoint Details page. Dashboard actions are also available in workbenches outside of Reporting. For example, Tanium Guide provides access to Tanium Guardian dashboards for resolving emerging issues. For more information, see Tanium Reporting User Guide.

© 2026 Tanium Inc. All Rights Reserved

Deployment plans

A deployment plan defines the sequence of rings (ring set) that an action must progress through to complete successfully, along with the target endpoints and progression criteria for each ring. You assign the plan when you configure an action deployment, such as for remediating an emerging issue. For more information, see Managing deployment plans for ring deployments on page 384.

Endpoint targeting

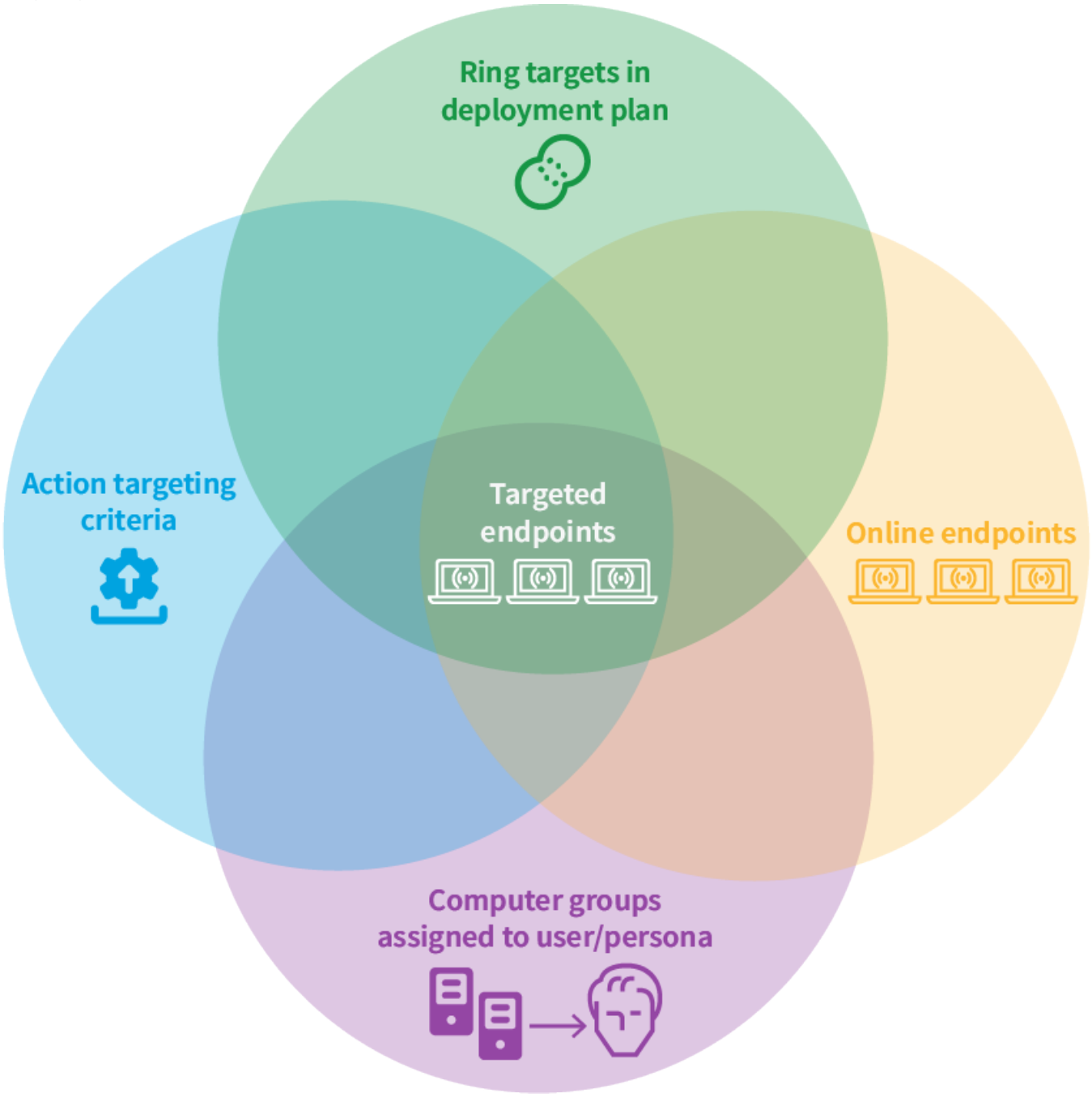
The following factors determine which endpoints are the targets for an adaptive action in any single ring:

- Ring-defined targets on page 279
- Online and offline endpoints on page 281
- Action targeting criteria on page 283
- Computer group assignments on page 289

The following diagram illustrates how an action targets only the endpoints for which all the preceding factors apply during deployment in any particular ring.

© 2026 Tanium Inc. All Rights Reserved

Targeting for adaptive actions



RING-DEFINED TARGETS

In a deployment plan, you assign endpoints managed using Tanium Client to each user-defined ring based on filter group membership (custom plans) or a percentage of the total endpoints in your environment (dynamic plans). When a deployment starts in a user-defined ring, it targets assigned endpoints that also meet the Action targeting criteria on page 283, minus any Deferred endpoints on page 298. In the predefined Last ring on page 292 (**All Targeted Computers**), the deployment targets all endpoints that the action targeting criteria specify, including any deferred endpoints.

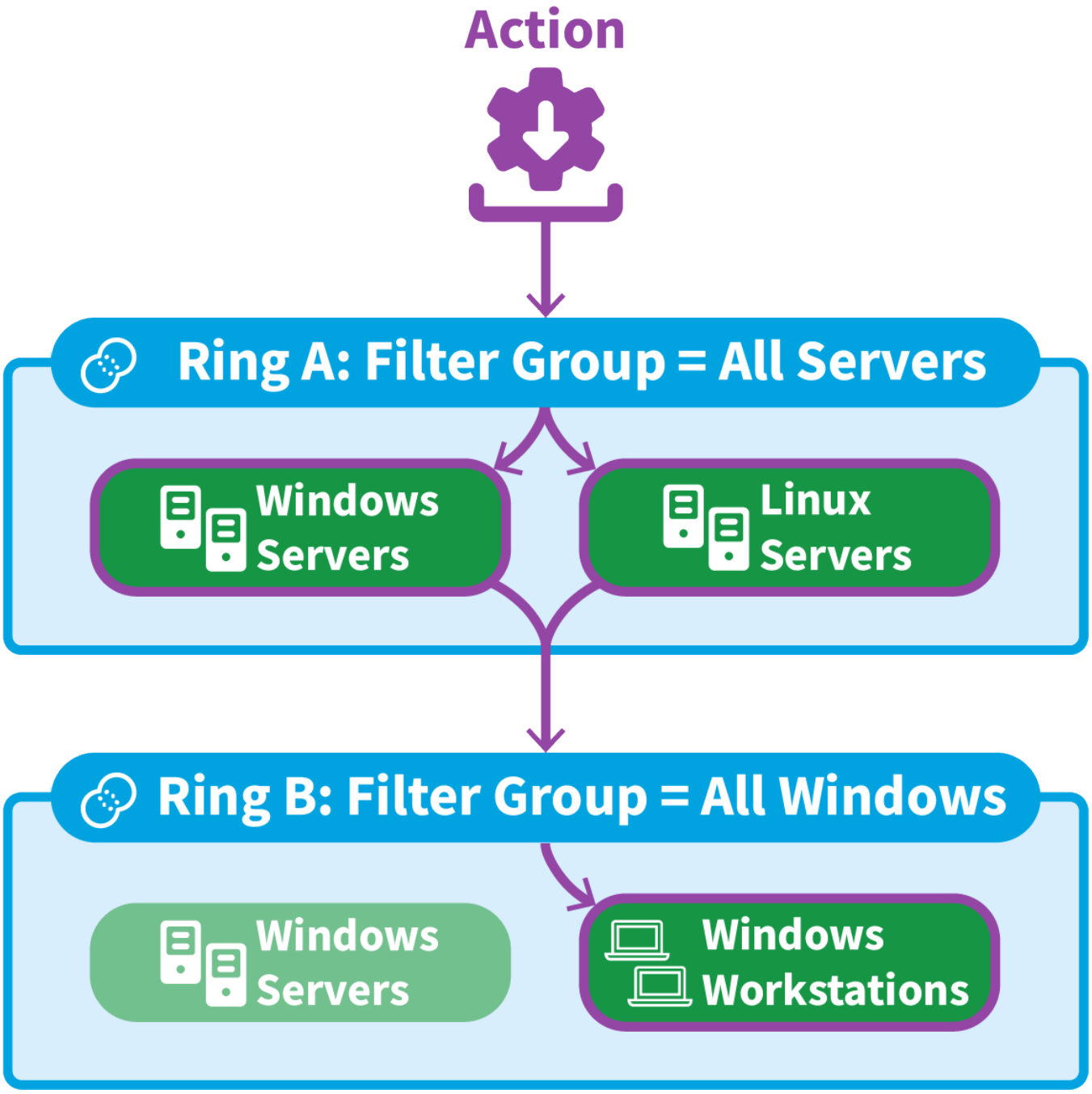
© 2026 Tanium Inc. All Rights Reserved

NOTE

For more information about custom and dynamic plans, see Deployment plan types on page 384.

In any single deployment, an action deploys only once to each endpoint across all rings. For example, consider a deployment plan in which you assign the **All Servers** filter group to Ring A and the **All Windows** group to Ring B. When deployment starts in Ring B, the action runs on Windows workstations but not on Windows servers because the servers already ran the action in Ring A.

Action targeting based on ring assignments



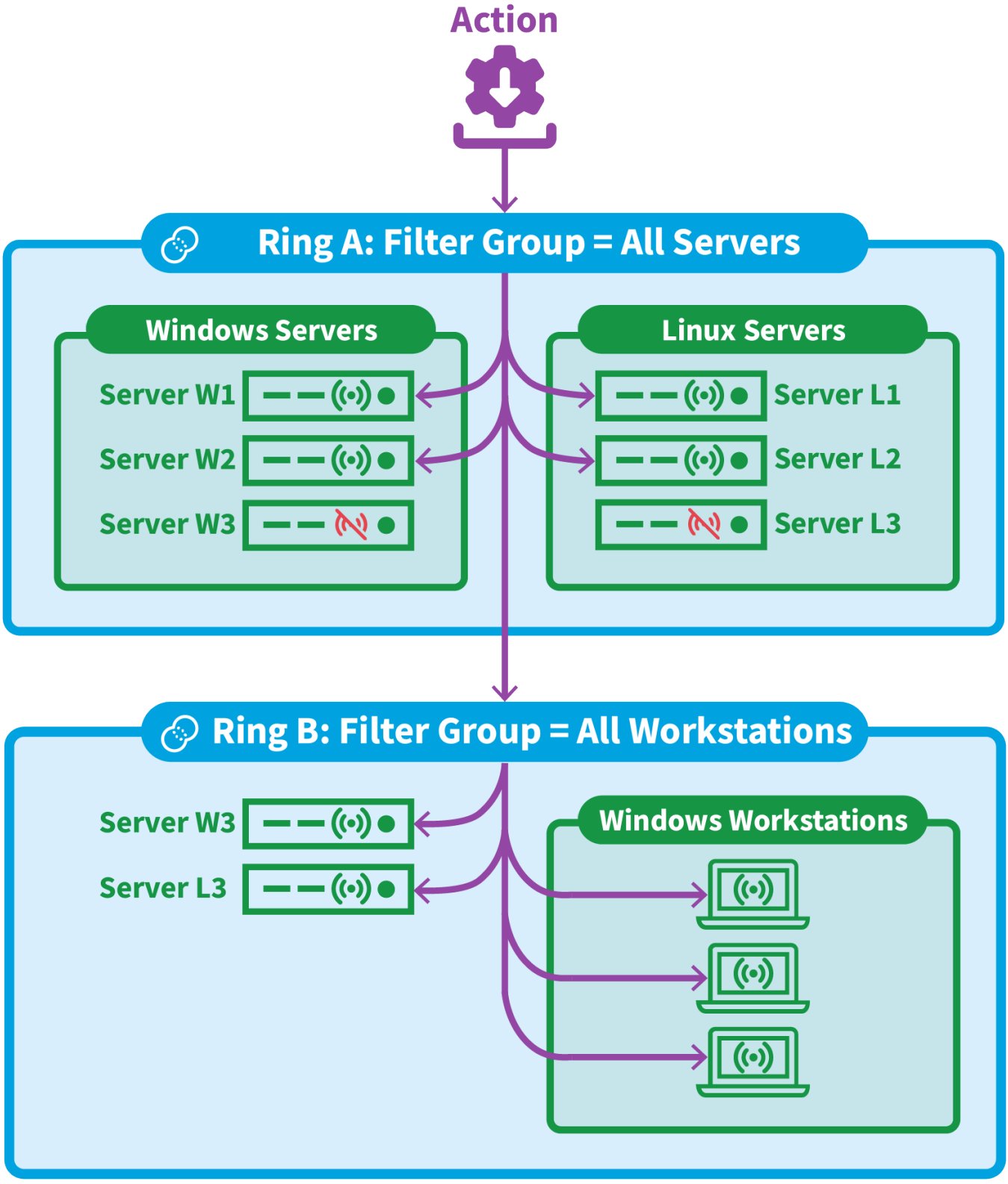
© 2026 Tanium Inc. All Rights Reserved

ONLINE AND OFFLINE ENDPOINTS

During deployment in a ring, an action excludes any offline endpoints that are assigned to the ring. If the offline endpoints go online in a subsequent ring, the action deploys to those endpoints then. For example, consider a deployment plan in which you assign the **All Servers** filter group to Ring A and the **All Workstations** filter group to Ring B. If servers W3 and L3 are offline during deployment in Ring A but come online during deployment in Ring B, the action runs on W3 and L3 in Ring B even though those servers are not members of the **All Workstations** group.

© 2026 Tanium Inc. All Rights Reserved

Action targeting based on the online or offline status of endpoints



© 2026 Tanium Inc. All Rights Reserved

When you view endpoint counts for rings in a deployment plan configuration, those counts also exclude offline endpoints. The counts in a deployment plan might differ from the counts during deployment if some endpoints go online or offline between the times when you view the deployment plan and when deployment starts.



Environments with many virtual desktop infrastructure (VDI) endpoints are particularly susceptible to fluctuations in the number of online endpoints.

ACTION TARGETING CRITERIA

The Deploying actions and playbooks in Console and Interact on page 391 in an action applies as a filter to endpoint targeting during deployment. However, the filter does not apply when you view a deployment plan configuration. The following examples illustrate how action targeting can create discrepancies in the endpoint counts that you see in custom or dynamic deployment plans compared to the counts during deployment.

EXAMPLE: CUSTOM DEPLOYMENT PLAN

If you assign the **All Windows** filter group to Ring A in a custom plan, the plan shows the count for all Windows endpoints in Ring A. If you select the plan for an action that targets the **All Servers** computer group, the action deploys in Ring A only to Windows servers because only Windows servers are members of both the **All Windows** and **All Servers** groups.

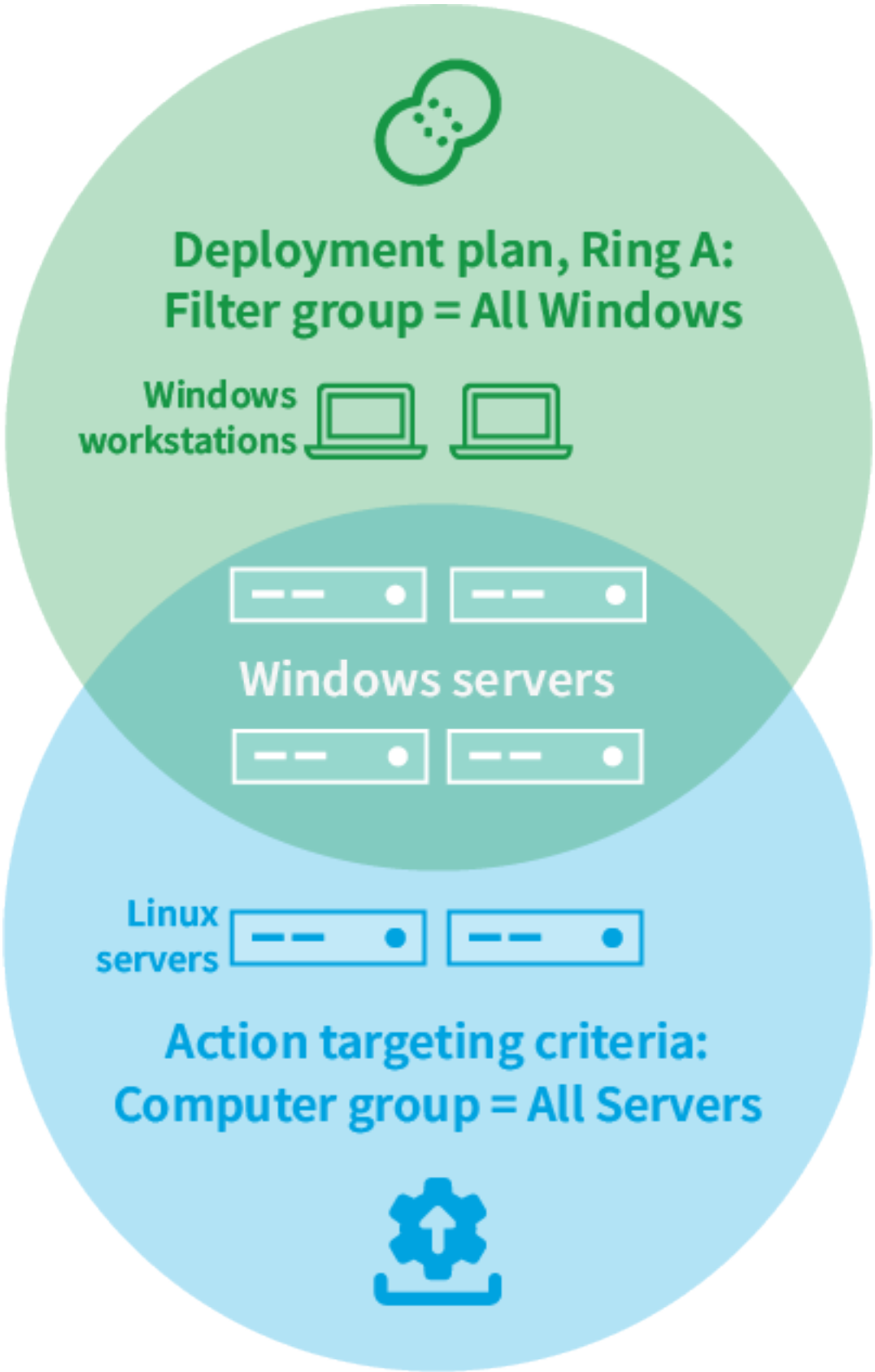


For more information, see Custom deployment plans on page 384.

© 2026 Tanium Inc. All Rights Reserved

Action targeting for a custom deployment plan

© 2026 Tanium Inc. All Rights Reserved



© 2026 Tanium Inc. All Rights Reserved

EXAMPLE: DYNAMIC DEPLOYMENT PLAN

If you configure a dynamic plan with Ring A targeting 25% of endpoints, in an environment that has a total of 1,000 endpoints, for an action that targets the **All Servers** computer group containing 100 endpoints (10% of the total), the Tanium Server applies targeting logic in the following sequence:

1. The Tanium Server randomly selects 250 endpoints as the Ring A targets. The number of servers among the 250 might be more or less than 25 (10% of 250) because the selection is random. The endpoint selection applies only to the current instance of the Ring A deployment. If you deploy the same action in the future, the endpoint selection is again randomized and not based on selections in the earlier deployment. For example, the 25% of selected endpoints might include 15 servers and 235 non-servers when the deployment first runs in Ring A but then include 50 servers and 200 non-servers in the next deployment to that ring.
2. The Server applies the action targeting criteria as a filter to the endpoints selected for Ring A in the previous step. In this example, if only 15 of the randomly selected 250 endpoints are servers, then the action deploys to only 15 endpoints in Ring A. A key point is that, due to the variability of random selection, each instance of the deployment in this example might target from 0 to 100 servers in Ring A.

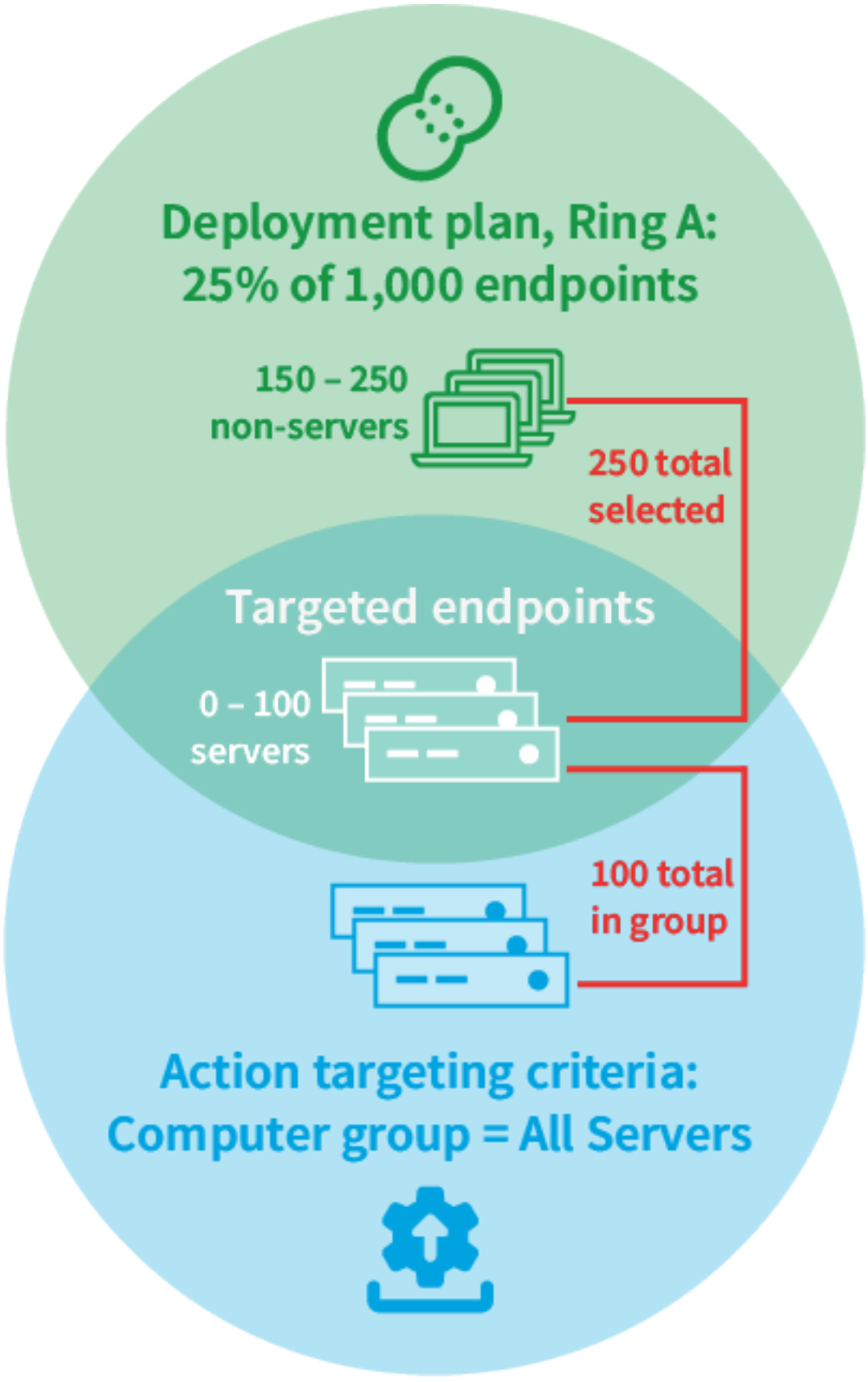


For more information, see Dynamic deployment plans on page 384.

© 2026 Tanium Inc. All Rights Reserved

Action targeting for a dynamic deployment plan

© 2026 Tanium Inc. All Rights Reserved



© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

When you configure progression criteria for a dynamic deployment plan, specify the Execution Success Rate on page 294 instead of the Minimum Endpoints on page 294. The randomness of targeting in a dynamic plan makes it hard to predict how many endpoints a ring will target at deployment time. Consequently, a minimum number that seems reasonable when you preview the deployment plan might result in progression criteria failures at deployment time even if all the targeted endpoints in the ring successfully run the action. Alternatively, if you decide you want the **Minimum Endpoints** condition despite this drawback, you can Manually progress deployments through rings on page 377 in cases where the progression fails because the current ring targeted too few endpoints.

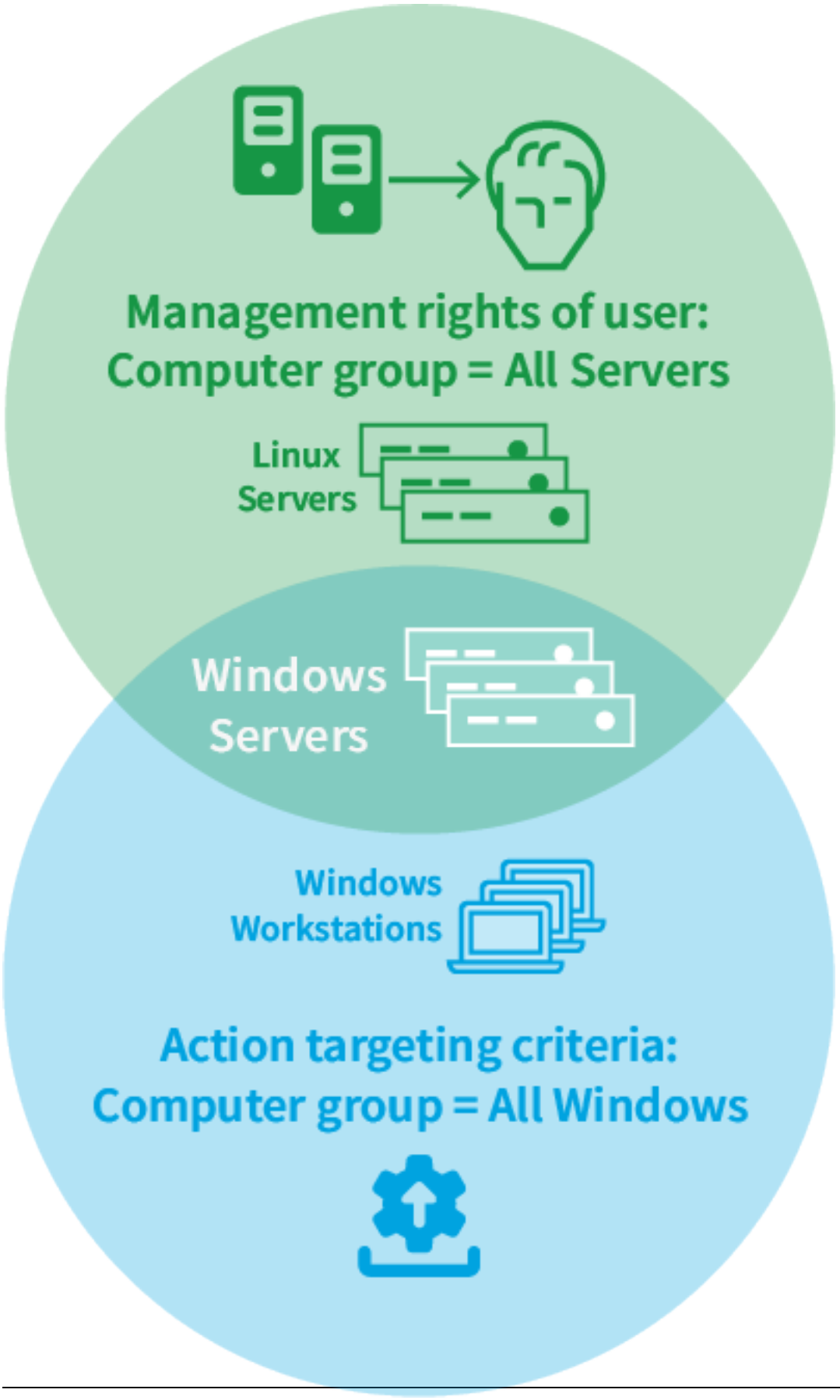
COMPUTER GROUP ASSIGNMENTS

The computer management groups that are assigned to your user account or persona also control which endpoints a deployment targets. For example, if you sign in as a user who is assigned only the **All Servers** group and you deploy an action that targets the **All Windows** group, the action deploys only to Windows servers, not Windows workstations.

© 2026 Tanium Inc. All Rights Reserved

Action targeting based on computer group assignments

© 2026 Tanium Inc. All Rights Reserved



© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

Optimize computer group assignments and configurations for action targeting as described in Resource usage for actions and questions on page 557.

First ring

When an action starts, it does not have to meet any progression criteria to deploy to endpoints in the first ring of a deployment plan. Therefore, when you configure the first ring, consider assigning only endpoints on which unforeseen action impacts cannot disrupt your production environment.

Last ring

In every deployment plan, a predefined ring named **All Targeted Computers** is always the last ring regardless of how many custom rings you add. You cannot edit or delete **All Targeted Computers**, or change its position in the ring sequence. The targeting criteria that you configure in an action applies as a filter to **All Targeted Computers**. **All Targeted Computers** includes any Deferred endpoints on page 298 that are configured in the deployment plan.

NOTE

For more information about all the factors that determine which endpoints an action targets, see Endpoint targeting on page 278.

Ring progression criteria

In a deployment plan, you configure progression criteria in each ring definition except the last ring, as described in Rings and progression criteria on page 387. The criteria define the action results that endpoints must return for the deployment to progress to the next ring. Endpoint results must meet all the criteria to progress. However, for the sake of modularizing deployment plans, you can add criteria that apply only to a specific deployment type without affecting other types. For example, if a plan has criteria that are specific to Tanium Deploy (software) deployments and you assign the plan to a Tanium platform deployment, the deployment ignores the Deploy-specific criteria. For more information, see Deployment plan types on page 384.

NOTE

You can Manually progress deployments through rings on page 377 if circumstances warrant bypassing progression criteria failures.

PROGRESSION CRITERIA EVALUATION

Progression criteria are not cumulative across rings. After deployment ends in the current ring, the Tanium Server evaluates action results only for that ring to determine if the deployment can progress to the next ring. The evaluation applies to all endpoints that ran the action in the ring, even if some of those endpoints subsequently go offline by the time the evaluation occurs. The evaluation also includes endpoints that the current ring targets because they were offline during deployment in the previous ring, as described in Endpoint targeting on page 278.

© 2026 Tanium Inc. All Rights Reserved

For platform actions, The Tanium Server evaluates progression criteria for each ring only once after the **Wait** interval ends. Some endpoints might run the action, evaluate the progression criteria, and return evaluation results after the **Wait**. However, the Server does not re-evaluate the criteria or change whether the deployment progresses based on post-**Wait** results.

For Tanium Deploy (software) deployments, you can select whether The Tanium Server evaluates progression criteria for each ring only once or periodically after the **Wait** interval ends. For more information, see Default Criteria for Progression on page 388.

PROGRESSION CRITERIA DESCRIPTIONS

The following tables describe the progression criteria:

- Progression criteria for all deployment types on page 293
- Optimizing and automating workflows through the Autonomous IT Platform on page 273

Percentage values are relative to the total number of online endpoints that a ring targets.



All the criteria evaluate as passed if none of the targeted online endpoints attempt the action and the **Minimum Endpoints** criterion is set to 0 or is not specified.

Progression criteria for all deployment types

Criteria	Description
The following progression criteria have an impact on the time limits for deployments. For more information, see Deployment timing factors and maintenance windows on page 295.	
Wait 	This is the amount of the time that a deployment must wait in a ring before the Tanium Server evaluates the other criteria. A **Wait** value is required in every deployment plan, but you can enter `0` to specify no wait before the Server starts evaluating the criteria. Criteria evaluation is more likely to accurately represent endpoint states if the wait is longer. The Server evaluates the other criteria based on data that Tanium Clients return after measuring the impact of an action. Setting a wait interval gives Clients time to return more accurate data because not all action impacts are instantaneous. For example, if an action installs an application, CPU and memory usage might spike during installation but then return to normal later. Also, the application might run normally at the moment installation finishes but then crash after extended use. The deployment type determines when the wait interval starts: • **Tanium platform deployments**: The wait begins after the Action runtime on page 295 ends. • **Tanium Deploy (software) deployments**: The wait begins as soon as the action starts in the ring. When the wait ends, the Tanium Server evaluates the other criteria even if the action is still in progress. NOTE: You can Skip the wait intervals during deployment on page 378 if you decide an action is urgent.

© 2026 Tanium Inc. All Rights Reserved

Progression criteria for all deployment types (continued)

Criteria	Description
Execution Success Rate 	The percentage of endpoints that successfully completed the action must equal or exceed the specified value. When you configure a deployment plan, you can select the **Ignore pending endpoints** option to evaluate results only from endpoints that have returned a `Completed` (successful) or `Failed` status for the action. This option is useful if certain actions might take longer than expected to complete on some endpoints and you don't want the delay to prevent ring promotion. For example, you might want to exclude results from endpoints that return `Pending` status because they are waiting for a maintenance window to complete an action.
Minimum Endpoints 	The number of endpoints that attempted the action must equal or exceed the specified value. An action counts as attempted regardless of whether it is completed (successful), failed, or pending (such as when endpoints are waiting for a maintenance window). When you configure a deployment plan, you can select the **Ignore pending endpoints** option to evaluate results only from endpoints that have returned a `Completed` or `Failed` status for the action. This option is useful if the number of endpoints that return another status, such as `Pending`, might skew the evaluation results for other progression criteria. For example, you might issue a deployment in which 5 endpoints return `Failed`, 0 endpoints return `Completed`, and 100 endpoints return `Pending`. If the evaluation includes pending endpoints and the **Execution Success Rate** is set to 90%, the deployment still progresses to the next ring even though the probability is high that the action will fail on many of the 100 endpoints that return `Pending`.

Progression criteria for Patch deployments

Criteria	Description
No Unexpected Reboots	The percentage of endpoints that unexpectedly rebooted after patch installation must not exceed the specified value. This setting enables you to evaluate the impact of an action in the following scenarios: • One reboot is expected after patch installation but the endpoint reboots multiple times. • No reboots are expected after patch installation but the endpoint reboots anyway.

PROGRESSION CRITERIA STATUS

When you Analyze and manage a single deployment on page 362, you can see the progression criteria status for each endpoint and for all the endpoints in a ring.

Progression criteria status

Status	Description
Failed 	• **Endpoint**: The endpoint failed the progression criteria. • **Ring**: Not enough endpoints meet the progression criteria to qualify the deployment for promotion to the next ring. In this case, the deployment is in a failed state.

© 2026 Tanium Inc. All Rights Reserved

Progression criteria status (continued)

Status	Description
Passed 	• **Endpoint**: The endpoint passed the progression criteria. • **Ring**: Enough endpoints meet or exceed the progression criteria to qualify the deployment for promotion to the next ring.
Pending 	This status applies only at the ring level and indicates that the evaluation has not yet started or is in progress. Endpoints do not return criteria status until they finish evaluating the criteria.
Not Applicable 	This status applies only at the ring level and indicates that specific criteria do not apply to the current deployment. For example, if you add the **Memory Usage High** criterion to a deployment plan and assign the plan to a Tanium platform deployment, that criterion does not apply because platform actions do not deploy software. Endpoints do not evaluate non-applicable criteria.

Deployment timing factors and maintenance windows

Consider the following timing factors before you configure rings in a deployment plan or assign a plan to actions.

Deployment timing factors and maintenance windows

Time factors	Description
Maintenance windows	Endpoints can run Deploy (software) deployments only within a maintenance window if you configure windows for those deployment types. For more information, see: • Tanium Deploy User Guide: Managing maintenance windows Maintenance windows might cause a deployment to enter a `Failed` state and require a user to manually progress the deployment to the next ring. For more information, see Example: Deploy (software) deployment timing on page 296.
Maximum deployment time	The maximum period for a ring-based deployment is 90 days regardless of how many rings are in the associated deployment plan. If the deployment expires after starting in a ring, it continues deploying to endpoints in that ring but does not progress to the next ring. You can check the **Expiration** date for a deployment in the Managing ring deployments on page 359 section of the Deployment Details page.
Minimum deployment time	The minimum total time that an action requires to deploy through all the rings is the cumulative total across all the rings in the deployment plan. Therefore, do not use rings for deployments in which the total deployment time might exceed the 90-day maximum. For example, 90 days might not suffice if you have a Tanium Deploy maintenance window that allows deployments for only a few hours on one day of each month.
Action runtime (platform deployments only)	When a platform action starts deploying to endpoints in a ring, the runtime is the period during which the action remains open. When the action expires, endpoints can no longer run the associated package command. The runtime is the sum of the Command Timeout and Download Timeout on page 448 in the package.

© 2026 Tanium Inc. All Rights Reserved

Deployment timing factors and maintenance windows (continued)

Time factors	Description
Progression criteria	The following ring progression criteria affect the timing of ring progression: • Wait on page 293: This is the amount of time that a deployment waits in the ring before the Tanium Server evaluates the other criteria. • Minimum Endpoints on page 294: The action cannot progress to the next ring unless the specified minimum number of endpoints have time to attempt the action. • Execution Success Rate on page 294: The action cannot progress to the next ring unless the specified minimum percentage of endpoints have time to successfully complete the action.
Method of evaluation (Deploy deployments only)	You can specify whether the Tanium Server evaluates progression criteria periodically or only once to determine whether a Deploy (software) deployment can proceed to the next ring. For more information, see Default Criteria for Progression on page 388.

EXAMPLE: PLATFORM ACTION TIMING

For platform actions, the total time that is required for endpoints in a ring to pass the progression criteria is the action runtime plus the **Wait** value. For example, consider an action deployment with the following settings:

- Package settings:
  - **Command Timeout** = 2 minutes
  - **Download Timeout** = 10 minutes
- Ring 1 (deployment plan) settings:
  - **Wait** = 60 minutes
  - **Execution Success Rate** = 90%
  - **Assigned Endpoints** = 1,000

In this case, 900 endpoints in Ring 1 (90%) must successfully complete the action within 72 minutes for the deployment to progress to Ring 2 because the total time for endpoints to pass the progression criteria is: 2 + 10 + 60 = 72 minutes.

EXAMPLE: DEPLOY (SOFTWARE) DEPLOYMENT TIMING

For Deploy deployments, the **Wait** interval for a ring starts as soon as deployment starts in that ring. The **Wait** interval must be small enough that the minimum number of endpoints can attempt and/or complete the action within any maintenance windows that are configured.

© 2026 Tanium Inc. All Rights Reserved



The Tanium Server does not include maintenance windows when it evaluates the **Wait** interval. The Tanium Client on each endpoint evaluates the maintenance window if it is set on the endpoint and does not alter that window based on the **Wait**.

For example, consider a Deploy action deployment with the following settings:

- Ring 1 (deployment plan) settings:
  - **Wait** = 4 hours
  - **Execution Success Rate** = 90%
  - **Minimum Endpoints** = 800
  - **Assigned Endpoints** = filter group A (600 endpoints) + filter group B (400 endpoints) = 1,000 endpoints
  - **Method of Evaluation** = **Evaluate once**
- Deployment **Start Time** = 9 AM
- Maintenance window settings:
  - **Start Time** = 10 PM
  - **Targeting** = filter group B (400 endpoints)

In this case, the **Wait** ends at 1 PM (9AM + 4 hours). By that time, only the 600 endpoints in filter group A completed the deployment because the 400 endpoints in filter group B have a maintenance window that does not start until 10 PM. Consequently, only 60% of endpoints return an action status of `Completed`, while 40% return the status `Pending` (waiting for a maintenance window). The Tanium Server evaluates progression criteria only once for any ring. In this example, the Server evaluates the criteria status to `Failed` for Ring 1 because the **Execution Success Rate** is 90% and therefore the deployment enters a `Failed` state.



The Tanium Server counts `Pending` status as an action attempt for the **Minimum Endpoints** criterion. Therefore, if more than 800 endpoints across the two filter groups attempt the action by 1 PM, the Server evaluates that criterion to `Passed` even if fewer than 800 endpoints completed the action by that time. However, all progression criteria must pass for deployment to progress to the next ring. In this example, the progression criteria status is `Failed` for Ring 1 even if the **Minimum Endpoints** passed because the **Execution Success Rate** failed.

When the maintenance window starts at 10 PM, the 400 remaining endpoints can then run the action and return an updated action status of `Completed`. However, the Server does not re-evaluate progression criteria status based on updates to action status that occur after the **Wait** interval ends. Therefore, this example deployment remains in a `Failed` state even if more than 90% of endpoints have completed the action a few minutes after 10 PM. To promote the deployment to Ring 2, a user must manually progress the deployment, as described in Manually progress deployments through rings on page 377. The Server then marks Ring 1 as `Manually Progressed` without changing its progression criteria status, and starts deploying to Ring 2.

© 2026 Tanium Inc. All Rights Reserved

Deferred endpoints

When an action progresses to a ring, it deploys by default to all the endpoints that you assign to the ring in a deployment plan. However, you can specify filter groups of deferred endpoints to which the action does not deploy until the last ring of the plan. The action defers the endpoints regardless of assignments in earlier rings. The last ring is typically the safest because all the earlier rings enable you to assess the action impact across a range of progression criteria and endpoints. Consequently, deferral is useful for endpoints that you consider sensitive from a security viewpoint or that serve critical functions in your environment.

For example, if you want to deploy an action to Windows endpoints in the second ring but all your servers perform critical functions, you can assign the **All Windows** filter group to that ring and defer the **All Servers** filter group. When an action progresses to the second ring, it skips endpoints that are Windows Servers and deploys to them only in the last ring.

© 2026 Tanium Inc. All Rights Reserved

Actions overview

The following sections provide an overview of Tanium platform actions that you deploy from Tanium Console or Tanium Interact. For information about deployments that you manage through other Tanium solutions, see Deployment types on page 277.

What is an action?

A Tanium action is a configuration object that you deploy to endpoints to manage a change on those endpoints. In the action configuration, you specify the package that performs the change, endpoint targeting criteria such as an action group, and deployment conditions such as scheduling. You can schedule the action to run immediately or in the future and as a one-time deployment or at recurring intervals. An *adaptive action* deploys in progressive phases called rings that you define in a deployment plan. A *simple action* deploys to all targeted endpoints in one phase.



For more information about the end-to-end action deployment workflow, see Action deployment overview on page 307.

Example: Action deployment use case

Consider a case where you are responsible for ensuring that the Tanium Client continues running on all endpoints that support it. You might start by issuing an Interact question to check if any endpoints provide users the permissions to uninstall the Client: `Get Tanium Client Directory Permissions from all machines with Tanium Client Directory Permissions equals Not Restricted`. Then you can deploy an action to run a package that allows only the SYSTEM account to uninstall applications in that directory: **Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory**. If new endpoints with unrestricted permissions for the Client directory might join your network in the future, you can schedule recurring deployments to automatically restrict the permissions on those endpoints.

RBAC for actions

Actions can affect the security and health of endpoints. Therefore, when you configure role-based access control (RBAC) for deploying actions, consider which users need to manage changes on endpoints, which changes the users might apply, and on which endpoints the users have authority to make changes. Assign the following RBAC components to users, user groups, and personas to control action deployment:

- Computer Groups

  For example, some users in your Security Operations Center might be responsible for deploying vulnerability remediations to workstations, while a smaller set of users might be responsible for remediating servers. In this case, you can assign the **All Workstations** computer group to the first set of users and the **All Servers** computer groups to the second set.

- Roles

© 2026 Tanium Inc. All Rights Reserved

For example, assigning a role with the **Interact Execute action** permission enables users to deploy actions that use packages in the **Core Content** set. That content set includes packages for many use cases, such as managing registry keys on Windows endpoints. If you plan to assign that role to users who also need the ability to quarantine endpoints, you can add **Package read** permission to the **Threat Response** content set, which contains packages for quarantining endpoints.

For more information, see Action management permissions on page 89 and Configure RBAC for action users on page 310.

Action status and logs

When an action starts, the Client on each target endpoint runs the associated package and returns action status updates to the Tanium Server. The Client also generates action-related logs that you can use to troubleshoot deployment issues. You can view the action status and logs in Tanium Console. For more information, see Monitor actions on page 316.

Action packages

A Tanium package comprises a command, a script, and any related files that are required to run an action on endpoints managed through Tanium Client. You select the package when you configure an action. For example, consider a case where you are troubleshooting issues related to Domain Name Server (DNS) updates on Windows endpoints. If you decide to restart the **DHCP Client** service on those endpoints, you can configure an action with the predefined **Restart Service** package and specify `DHCP Client` as the service to restart. For more information, see Managing packages for platform actions on page 442.

When you deploy an action, Tanium Clients download the associated package files and distribute the files among peers in the Client linear chains. Each Client stores package files for an action in the *<Tanium_Client_installation_directory>*`/Downloads/Action_`*<ID>* folder, where *<ID>* is the action identifier. For more information, see Tanium Client Management User Guide: File distribution.

Action groups

An action group specifies the computer groups that an action targets. Each computer group specifies a collection of endpoints based on a question with sensors or based on a manual list. You must select an action group for each action to target only the endpoints that require the action and avoid unnecessary processing for other endpoints.

Each action group specifies the computer groups based on Boolean AND/OR logic. For example, to deploy an action that resets a registry key on Windows endpoints where the key is missing or incorrect, you might create an action group named `Registry Key` that joins the following computer groups with a Boolean OR.

Example: Computer group membership for action group

Computer group name	Membership definition
Registry Key Not Found	Registry Key Exists[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Tanium\Anykey] contains False
Registry Value Not Correct	(Registry Key Exists[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Tanium\Anykey] contains True and all Registry Value Data[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Tanium\Anykey,Value] not matches 1)

For more information, see Targeting actions through action groups on page 400.

© 2026 Tanium Inc. All Rights Reserved

Action locks

Action locks prevent actions from running on an endpoint. You might want to deploy action locks if, for example, you encounter unexpected behavior on certain endpoints and want to suspend actions on them during debugging. For more information, see Locking down actions on endpoints on page 407.

Scheduled actions

Scheduled actions are actions that the Tanium Server deploys at a future time or at intervals based on the values that you set for the following action settings:

- **Start At**: Specify the date and time when the Server first deploys the action.
- **Re-issue Every**: Optionally, you can specify the frequency at which the Server redeploys the action.
- **End At**: Optionally, you can specify the date and time when the Server stops redeploying the action regardless of the reissue interval.



For more information, see Configure action settings.

Scheduled recurring actions address the following use cases:

- The action is used to enforce policy or ensure good cyber hygiene in an environment. For example, the content-only solution Tanium™ Default Content contains several scheduled actions that periodically update tooling on endpoints, verify configuration settings are in place, and maintain the overall health of Tanium Clients in your deployment. Redeploying these actions at intervals ensures that any new endpoints that join your environment are protected and ready for Tanium operations.
- You want to apply changes, such as software or configuration updates, to endpoints that might not be online during the initial deployment but that you expect to be online at some point between the **Start At** and **End At** dates.
- Action approval on page 301 is required and you are not certain that an approver will approve the action before its initial deployment expires.

You can also schedule one-time-only actions to deploy at a future **Start At** date to accommodate other events in your network. For example, you might schedule actions to start during a maintenance window on endpoints.

For more information, see Managing scheduled actions and action history on page 341.

Action approval

Some organizations have policies that require an approval process for deploying actions. Action approval ensures two-person integrity for managing changes on endpoints. When action approval is enabled, the signed-in user who deploys the scheduled action cannot also approve it. The action is on hold (pending) until another user approves it. The approving user must be assigned a role with **Approve Action** and **Sensor read** permissions.

© 2026 Tanium Inc. All Rights Reserved

For recurring (scheduled) actions, approval is a manual process only for the first deployment interval and is automatic for subsequent intervals. The approval remains in force until the **End At** date that is set in the action configuration or until another user modifies the configuration.

For more information, see Managing action approval on page 411.

Adaptive actions and simple actions

An *adaptive (ring-based) action* is assigned a deployment plan that defines the target endpoints and progression criteria for each ring that an action must progress through to complete successfully. Adaptive actions are useful for controlling action impacts, mitigating action-related disruptions, and protecting sensitive endpoints. For example, if an action reboots endpoints, you can stagger the deployment one ring at a time to minimize the overall disruption to your environment. For more information, see Ring-based deployment on page 276.

A *simple (non-ring-based) action* deploys in a single phase and therefore does not require a deployment plan. For example, you might decide that adding a custom tag to a subnet of endpoints constitutes a low-impact change that you can apply to the entire subnet in one deployment.

Policy actions

A policy action is a scheduled, recurring action that uses a saved question instead of a dynamic question and uses a `from` clause that ensures the action deploys only to endpoints that match the question condition. Policy actions are useful for ensuring that endpoints comply with policies, and are more efficient than other recurring actions at conserving network bandwidth and endpoint resources. For example, if your organization requires all Windows endpoints to have restricted permissions on the Tanium Client installation directory, you can schedule an action to restrict permissions based on the following saved question.

`Get Tanium Client Directory Permissions equals Not Restricted from all machines with ( Tanium Client Directory Permissions equals Not Restricted and Is Windows equals True )`.

In this example, only Windows endpoints with open permissions on the Tanium Client installation directory match the condition, and therefore only those endpoints download the required package **Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory** and run the action to restrict permissions. By contrast, a scheduled action that is not a policy action runs on all the targeted endpoints at every scheduled interval, which unnecessarily consumes more network bandwidth and endpoint resources.



The Tanium Server does not deploy a policy action to endpoints that were offline when it issued the saved question and that then come online while the action is in progress.

If you delete a saved question, the Tanium Server continues reissuing it for any actions that use the question and continues recording the question in the Question History log, which you can view on the **Administration > Content > Question History** page.

The Tanium Server performs the following steps at each scheduled interval for a policy action:

© 2026 Tanium Inc. All Rights Reserved

1. Evaluate whether the question results exceed the question expiration period (10 minutes). If no, the Server uses the results that it cached the last time it issued the question. If yes, it reissues the question to collect new results.
2. Evaluate the question results to determine whether any endpoints match the question condition and belong to computer management groups that are assigned to the question owner:
    - **Yes**: The Server deploys the action to the targeted action group. Within the group, only endpoints that match the question condition run the action.
    - **No**: The action does not deploy.

Action best practices

Minimize the impact of actions on network and endpoint resources by following best practices for the questions that define action targeting and computer group management rights.

Optimize questions for action targeting

The action deployment workflow starts with a question that you issue to identify the endpoints that require the action. Understanding how the question affects the targeting can help you optimize actions through the Best practices for action questions on page 306. The Tanium Server deploys each action through a message that it sends to endpoints. The message contains all the action settings that you see on the **Action Deployment** page (see Configure action settings on page 395), including the **Target Question** that each Tanium Client uses to determine whether it must run the action. When you select rows on the **Question Results** page and click **Deploy Action**, Interact adds a sensor-based filter for each selected row to the `from all machines with` clause of the **Target Question**. Selecting more rows produces a longer **Target Question** and therefore a larger action message that requires more network bandwidth and endpoint resources to process.

Tanium Console limits the impact of any action on networking and endpoint resources by disabling the **Deploy Action** button if you select more than 100 rows on the **Question Results** page. You can avoid exceeding that limit, and further reduce resource consumption, by basing an action on a question that returns fewer result rows from the endpoints that require the action. You can also reduce resource consumption by constructing more efficient filters in the question syntax. The following examples illustrate how to achieve these efficiencies.

EXAMPLE: OPTIMIZING THE "GET" CLAUSE

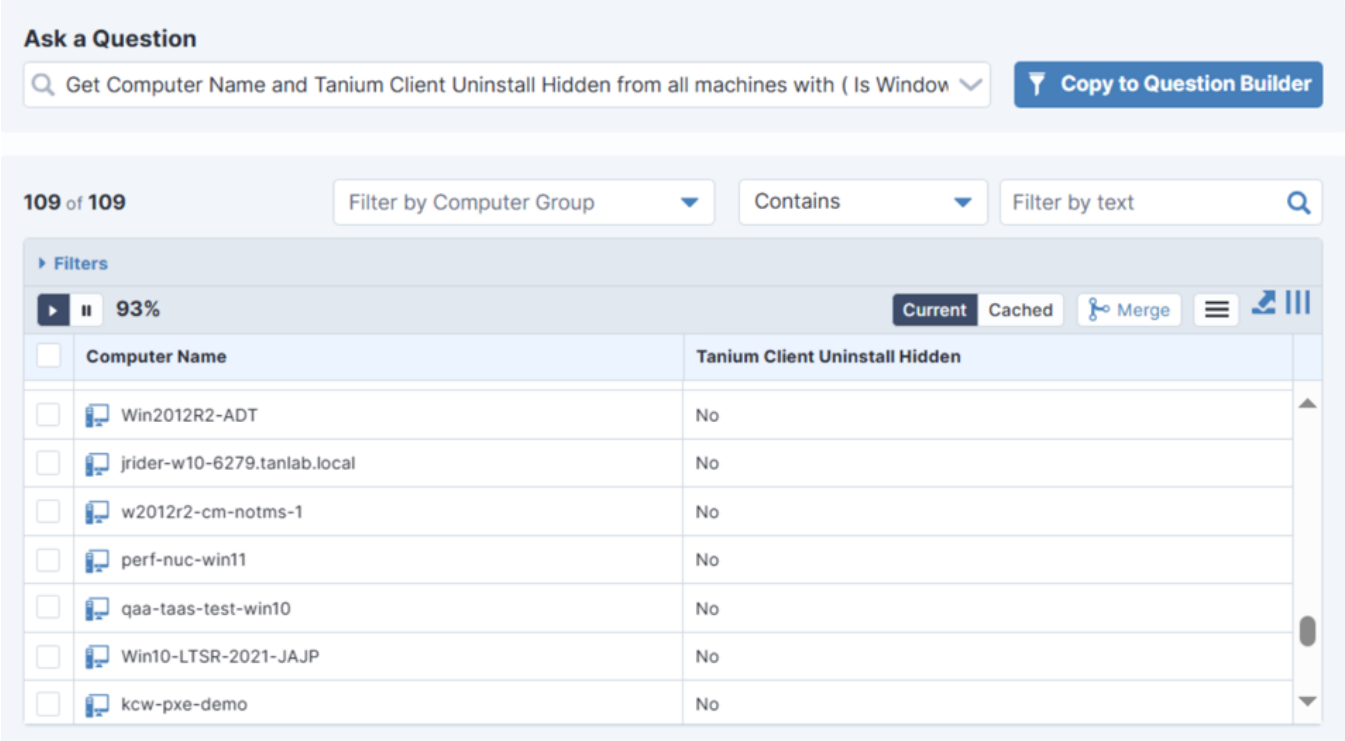
Consider a case where you issue the following question to identify Windows endpoints where the Tanium Client is listed among applications that endpoint users are allowed to remove:

```
Get Computer Name and Tanium Client Uninstall Hidden from all machines with Is Windows equals true and Tanium Client Uninstall Hidden equals no
```

That question returns a result row for each endpoint, which is useful if you want to know the computer names of the affected endpoints:

© 2026 Tanium Inc. All Rights Reserved

A question that returns a result row for each endpoint



However, that question might return too many rows to be useful for deploying an action that prevents endpoint users from removing the Client. The **Target Question** in the action would have a very long `from` clause if 100 endpoints required the action and you selected all 100 result rows for them. The following example shows how long the **Target Question** is even with just 5 endpoint results selected:

```
Get Computer Name and IP Address from all machines with ( All Computers and ( Is Windows equals true and Tanium Client Uninstall Hidden equals no ) and ( ( Computer Name equals Win2012R2-ADT and Tanium Client Uninstall Hidden equals No ) or ( Computer Name equals jrider-w10-6279.tanlab.local and Tanium Client Uninstall Hidden equals No ) or ( Computer Name equals w2012r2-cm-notms-1 and Tanium Client Uninstall Hidden equals No ) or ( Computer Name equals perf-nuc-win11 and Tanium Client Uninstall Hidden equals No ) or ( Computer Name equals qaa-taas-test-win10 and Tanium Client Uninstall Hidden equals No ) ) )
```

For every action, the `Get` clause in the **Target Question** is always `Get Computer Name and IP Address` regardless of the Interact question that you issued. The action uses the **Computer Name** and **IP Address** sensors to uniquely identify each target endpoint . The `from` clause of the **Target Question** always uses the sensors from both the `Get` and `from` clauses of the Interact question. Consequently, **Computer Name** is repeated in both the `Get` clause and `from` clause of the **Target Question** for this example.

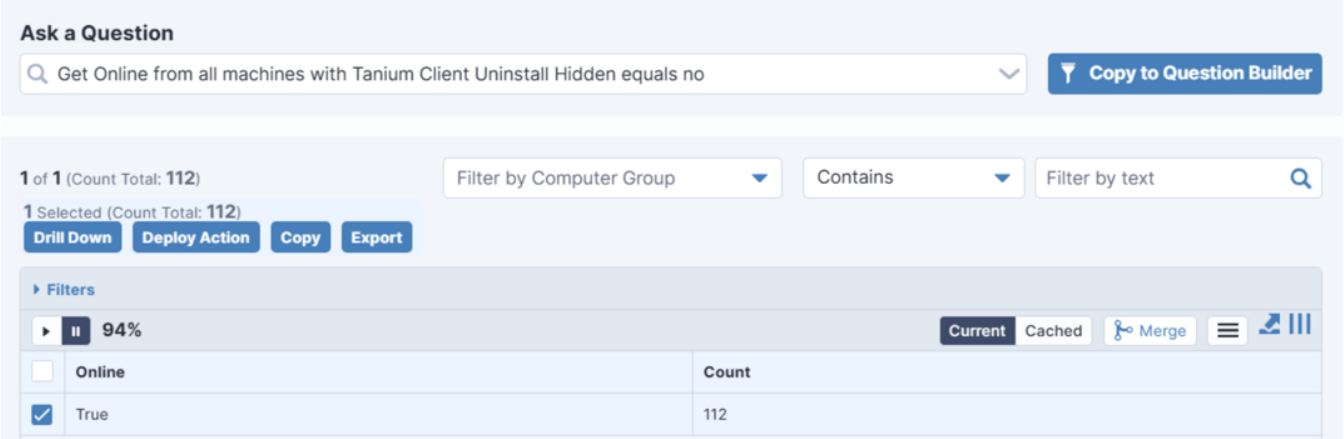
To deploy an action in this case, you can issue a more elegant Interact question that replaces **Computer Name** with the **Online** sensor in the `Get` clause and omits the **Is Windows** sensor in the `from` clause:

```
Get Online from all machines with Tanium Client Uninstall Hidden equals no
```

When **Online** is the only sensor in the `Get` clause, the Interact question always returns a single result row with the value `True` regardless of how many filters you add to the `from` clause:

© 2026 Tanium Inc. All Rights Reserved

A question that returns one result row for all endpoints



When you select the result row for this Interact question and click **Deploy Action**, Interact creates a much simpler **Target Question** than the example where you selected multiple rows:

```
Get Computer Name and IP Address from all machines with ( All Computers and Tanium Client Uninstall Hidden equals no and Online equals True )
```

> NOTE
>
> In the preceding examples, the **Target Question** specifies `All Computers` in the `from` clause because the default action group is **Default - All Computers**. However, you can specify a different action group and other filters in the action settings. For more information, see Configure action settings on page 395.

EXAMPLE: OPTIMIZING THE "FROM" CLAUSE

The following example is another question that might be useful for analyzing information but is not optimized for actions. In this case, you want to deploy an action to all endpoints that do not have a high enough Google Chrome version installed, but first you want to see what versions are distributed across all the endpoints in your network:

```
Get Installed Application Version[Chrome] from all machines
```

If multiple endpoints have the same Chrome version, the **Question Results** page would aggregate the results by version instead of showing a row for each endpoint. However, if endpoints across your network have a broad range of versions, the page might still list too many result rows (potentially more than the 100 limit) to be suitable for action deployment. Even if you select only five rows and click **Deploy Action**, the **Target Question** will have a long `from` clause:

```
Get Computer Name and IP Address from all machines with ( All Computers and ( Installed Application Version[Chrome] equals 99.0.4844.74 or Installed Application Version[Chrome] equals 109.0.5414.168 or Installed Application Version[Chrome] equals 94.0.4606.81 or Installed Application Version[Chrome] equals 123.0.6422.78 or Installed Application Version [Chrome] equals 123.0.6312.123 ) )
```

To optimize the question for actions, you can again use the **Online** sensor in the `Get` clause and move the **Installed Application Version[Chrome]** sensor to the `from` clause as a filter:

```
Get Online from all machines with Installed Application Version[Chrome] < 124.0.6367.91
```

© 2026 Tanium Inc. All Rights Reserved

When you select the single result row (`True`) and click **Deploy Action**, Interact applies that version filter to a much simpler **Target Question**:

```
Get Computer Name and IP Address from all machines with ( All Computers and Installed Application Version[Chrome] < 124.0.6367.91 and Online equals True )
```

The following Interact question is the same as the previous example but has multiple sensor filters in the `from` clause:

```
Get Online from all machines with ( Installed Application Version[Chrome] > 124.0.6367.91 and Operating System contains Windows 10 and Tanium Client Subnet contains 192.168.0.0/24 )
```

The preceding Interact question still returns only one result row, which you can select to deploy an action with the following **Target Question**:

```
Get Computer Name and IP Address from all machines with ( All Computers and ( Installed Application Version[Chrome] < 124.0.6367.91 and Operating System contains Windows 10 and Tanium Client Subnet contains 192.168.0.0/24 ) and Online equals True )
```

The preceding **Target Question** remains simpler, and requires less processing on endpoints, then the **Target Question** that is based on multiple result row selections and only one filter.

BEST PRACTICES FOR ACTION QUESTIONS

The following best practices enable you to construct Interact questions that minimize the complexity of the **Target Question** in an action:

- **Minimize result rows**

  Use a `Get` clause that returns only a few result rows, ideally just one, from all the endpoints that require the action. The preceding examples use the **Online** sensor, but you can use any other sensor that returns a few results that you can select from all the target endpoints. Avoid using sensors that return one result row per endpoint, particularly the **Computer Name** and **IP Address** sensors that produce duplicate filters in the **Target Question**.

- **Filter using the `from` clause**

  Add sensor filters to the `from` clause instead of the `Get` clause to specify endpoint targeting.



Tanium strongly recommends that you do not lower the default **Max Sensor Age** or **Maximum Data Age** for any sensor in the `Get` or `from` clause of a dynamic question or saved question that you use for deploying actions. For more information, see Best practices for saved questions on page 456.

Optimize action groups and computer groups for targeting

The complexity of an action group and its assigned computer groups affect the size of the action message that the Tanium Server sends to endpoints, and the message size affects the networking and endpoint resources that an action consumes. Resource consumption increases as you add more computer groups to an action group and as the targeting of those computer groups becomes more complex. Increasing the number and complexity of computer groups assigned to the user account that you use to deploy an action also increases the action message size and therefore resource usage. To optimize computer groups for action targeting, see Computer groups on page 557.

© 2026 Tanium Inc. All Rights Reserved

Conserving resources through action distribution

The Tanium Server distributes actions to endpoints in batches. When you Configure action settings, you can use the **Distribute Over** option to randomize the distribution over the specified period to prevent spikes in network traffic or other resource consumption. For example, an action that depends on a sensor that queries Active Directory (AD) might cause a flood of traffic to the AD server unless the action is distributed over time. Similarly, an action that targets endpoints in a virtual machine farm might exhaust the shared CPU or memory resources if all endpoints simultaneously run a resource-intensive program.

When the Tanium Client receives an action from the Tanium Server, the Client evaluates the action targeting criteria to verify that its endpoint is a target before calculating a **Distribute Over** delay to the action start time. Each Client sets a delay interval that ranges from zero to the **Distribute Over** value, which represents the maximum. After the delay, the Client starts running the action without re-evaluating the targeting criteria. The longer the delay between the targeting evaluation and action start, the higher the risk of the Client running an action for which the endpoint no longer qualifies. For example, an action might target endpoints with low disk space to run a package that removes data to clear space. An endpoint that has low disk space when the Client evaluates the targeting might no longer meet the low space threshold by the time the action starts.

The Client uses the **Distribute Over** delay to calculate the action expiration period. Therefore, the **Distribute Over** value affects the action status that the Client reports to the Tanium Server. For more information, see Action states on page 353.



You can set a **Distribute Over** value only for simple actions, not adaptive actions.

Action deployment overview

Configure platform settings, content, and role-based access control (RBAC) to optimize action deployment before users start configuring actions. Monitoring action status and history is also important to ensure that actions are having the expected effect and to troubleshoot otherwise. The three stages of action deployment are:

1. Administrative setup for actions on page 307
2. Configure and deploy actions on page 313
3. Monitor actions on page 316

Administrative setup for actions

Typically, you perform the following tasks once as part of the initial setup of a Tanium deployment. However, you might repeat some tasks if your environment changes. For example, you might update RBAC configurations to reflect changes to roles and personnel.

- Review and edit global settings for actions on page 308
- Review and customize action content on page 309
- Configure RBAC for action users on page 310
- Configure downloads authentication on page 313

© 2026 Tanium Inc. All Rights Reserved

TIP

Tanium provides several predefined scheduled actions, such as **Distribute Hardware Tools**. You can review these actions on the **Administration > Actions > Scheduled Actions** page. The Tanium Server automatically imports several predefined actions with the content-only solutions Default Content and Core Content and imports other actions when you import certain modules or shared services. You can manually import content-only solutions that contain additional predefined actions. For more information, see Part 4: Managing Tanium solutions on page 108.

Actions in the Default Content and Core Content solutions might initially target the predefined action groups **Default – All Computers** or **Default**, which specifies the **No Computers** computer group.

REVIEW AND EDIT GLOBAL SETTINGS FOR ACTIONS

Review and, if necessary, edit global settings that affect action deployment.

1. From the Main menu, go to **Administration > Configuration > Settings > Platform Settings** to assess whether the default values of the following global settings suffice for your Tanium deployment. Update any settings that require custom values.

   TIP

   On the **Platform Settings** page, Expand  a setting to see its full description.

Global settings for actions

Setting	Description
Require Action Approval Bulk Approval	Enable action approval if your organization implements two-person integrity. These settings are disabled by default. For more information, see Enable or disable action approval on page 412.
Action Target Estimate Minimum	After you issue a question to identify endpoints that require an action, you cannot deploy the action until the percentage of responding endpoints reaches the estimated percentage. The default is 20%. For more information, see Configure and deploy actions on page 313.
Prompt Estimate Threshold	When you deploy an action and the number of affected endpoints exceeds the threshold, Tanium Console prompts you to confirm the deployment before proceeding. The default is 100. Changing the value to 0 causes Console to prompt users whenever they deploy actions regardless of the number of affected endpoints.
Run Commands in Process Group	Enables you to control whether package commands run in a process group. This setting is disabled by default. For more information, see Launch this package in a process group on page 448.
Restricted Targeting	Sets the **No Computers** computer group as the action group target during initial configuration of Tanium solutions. This setting is disabled by default. For more information, see Tools deployment and restricted targeting on page 121.

© 2026 Tanium Inc. All Rights Reserved

2. Review the following advanced global settings to assess whether their default values suffice for your Tanium deployment. These settings control the maximum size of the cache that the Tanium Client uses to store file chunks for packages and Client API downloads. For more information, see Tanium Client Management User Guide: Chunk caching. Update any settings that require custom values.

Global settings for Tanium Client chunk cache

Setting	Description
ClientCacheLimitInMB	Controls the absolute amount of disk space that a Client can use for caching chunks. The value is in megabytes (MB) and the default is 2048.
ClientCachePercentageCapTimes100	Controls the maximum percentage of free disk space that a Client can use for caching chunks. Multiply the target percentage by 100 to determine the value. For example, the default value 1000 specifies that the cache limit is 10% of free disk space. If you change the value, the Client checks the free disk space and adjusts the cache size only when you restart the Client or wait for the next Client reset interval, which is a random interval typically in the range of 2 to 6 hours.

Tanium Console does not show these Client cache settings unless a user adds them. Adding the settings is necessary only if non-default values are required. In an environment where actions deploy large files, such as for software installations or operating system (OS) patches, you might have to increase the cache limit and percentage. If each setting applies a different cache limit on a Client, the Client enforces whichever setting specifies a lower limit. For more information, see Manage advanced settings on page 164.

These are global settings and therefore apply to all Tanium Clients. However you can override the settings for specific Clients. For example, you might have critical assets that need more resources for running non-Tanium processes or assets with very limited resources such as virtual desktop infrastructure (VDI) endpoints. To override the global settings for cache size, configure the settings locally on specific Clients. For more information, see Tanium Client Management User Guide: Tanium Client CLI and Client settings.

REVIEW AND CUSTOMIZE ACTION CONTENT

Review the content that is required for action deployment. If the predefined content does not suffice for the actions that you expect users to deploy, create customize content.

Content types required for actions

Content type	Description
Content sets	Content sets contain the content that you create. When you configure user roles for action deployment, you assign permissions to content sets to control which content users can access. For example, if you create a package that updates files on data center servers, you can assign it to a content set for which access is restricted to users who have a role that allows data center file management. For more information, see Managing access to content through content sets on page 561.

© 2026 Tanium Inc. All Rights Reserved

Content types required for actions (continued)

Content type	Description
Packages	A package configuration includes settings, a command, a script, and any other files that are needed to orchestrate an action on an endpoint. For example, you might create a package that updates a specific file to a specific version. For more information, see Managing packages for platform actions on page 442.
Sensors Saved questions	You use sensors and saved questions to identify the endpoints that require action. For example, you might create a saved question with the **File Version** sensor to identify which endpoints have a particular version of a file. For more information, see Managing sensors for collecting endpoint data on page 421 and Managing saved questions in Console and Interact on page 455.
Filter groups	You use filter groups to: • Filter the questions and question results on which actions are based. For example, you might create a filter group that contains only the endpoints in a data center. • Create action groups for targeting specific endpoints. For more information, see Targeting actions through action groups on page 400. • Define Endpoint targeting on page 278 and Deferred endpoints on page 298 in deployment plans for adaptive actions. For more information, see Managing filter groups for filtering questions and results on page 476.
Deployment plans	A deployment plan defines the ring set that an adaptive action must progress through to complete successfully, along with the target endpoints and progression criteria for each ring. For more information, see Managing deployment plans for ring deployments on page 384. Before you add plans, be sure to understand all the components and timing factors of ring-based actions, as described in Ring-based deployment on page 276. NOTE Simple actions do not use deployment plans.

BEST PRACTICE

Do not edit content that is provided through Tanium content-only solutions; create custom content instead. For more information, see Tip 4: Limit customizations to Tanium content on page 138.

Test custom content in a lab environment before using it in a production environment.

CONFIGURE RBAC FOR ACTION USERS

Review the predefined RBAC for deploying actions and customize the RBAC as necessary. RBAC includes roles, users, user groups, personas, computer management groups, filter groups, and action groups.

1. Configure roles for administering, deploying, and (optionally) approving actions. Figure Role permissions related to actions on page 312 shows the permissions that are related to these tasks. For the specific permissions that are required to deploy actions, see Deploy actions on page 90. For more information, see Managing access permissions through roles on page 569.

© 2026 Tanium Inc. All Rights Reserved

NOTE

Users cannot approve their own actions. However, you can assign the **Bypass Action Approval** permission to a role to enable certain users to deploy actions without requiring approval. You must create a custom role if you want any users to have the bypass ability because no predefined role has that permission.

Deployment Plan, **Progression Criteria Set**, and **Ring Set** permissions apply only to adaptive actions, not simple actions.

The following permissions control access to the Tanium Console and Interact pages from which users deploy actions.

- **Interact solution permissions**: Controls access to Interact module pages from which users issue dynamic or saved questions and deploy actions based on the results. The **Ask Dynamic Questions** permission also controls access to the **Ask a Question** field on the Tanium **Home** page. For more information, see Interact permissions on page 81.
- **Package read permission**: Controls access to the **Packages** page, from which users can select a package to deploy through an action.
- **Client Status read permission**: Controls access to the **Client Status** page, where users can select endpoints to target for actions. Users typically use this page to troubleshoot connectivity issues for Tanium Clients.

NOTE

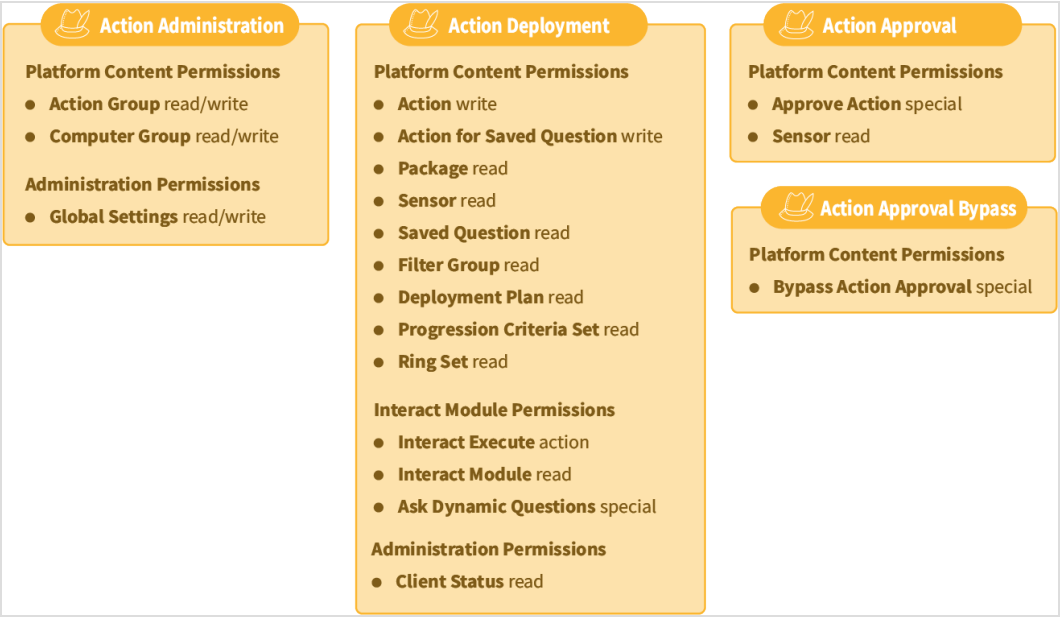
You can also deploy actions from the workbenches of other Tanium solutions, such as Reporting. For the permissions to access those workbenches, see the associated user guides in the Tanium Resource Center.

The following predefined roles provide action-related permissions but also other permissions. If you want action users to have a more limited range of permissions than what these roles provide, create custom roles.

- **Interact Power User**: This Interact role has all the permissions to deploy simple actions but not to approve actions or bypass action approval. For more information, see Interact permissions on page 81. This role does not have the permissions to assign a deployment plan, which is required for adaptive actions.
- **Deployment Plan User**: This Tanium Automate role has the permissions to assign deployment plans to adaptive actions. The **Deployment Plan Editor** role has the permissions to assign, create, edit, and delete deployment plans. For more information, see Tanium Automate User Guide: User role requirements.
- **Administrator**: This reserved role has all the action administration and deployment permissions but does not have permissions to approve actions or bypass action approval. For more information, see Administrator reserved role on page 582.

© 2026 Tanium Inc. All Rights Reserved

Role permissions related to actions



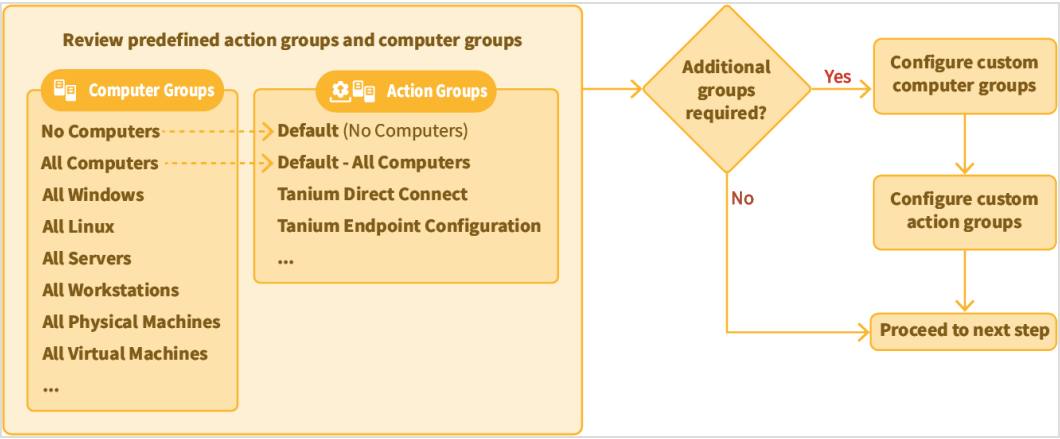
NOTE

After you deploy an action, you can view the contents of action logs to investigate issues related to the action. To view the logs, you require **Sensor read** permission on the **Client Management** content set. For more information, see View action status and settings on page 316.

2. Review the predefined action groups (**Administration > Actions > Action Groups**) and computer groups (**Administration > Permissions > Computer Groups**) to assess whether they suffice for action targeting in your environment. Configure custom groups if necessary.

   Action groups control which endpoints users can target for actions. Computer management groups and filter groups are the building blocks of action groups. For more information, see Controlling endpoint management rights through computer groups on page 610 and Targeting actions through action groups on page 400.

Computer groups and action groups

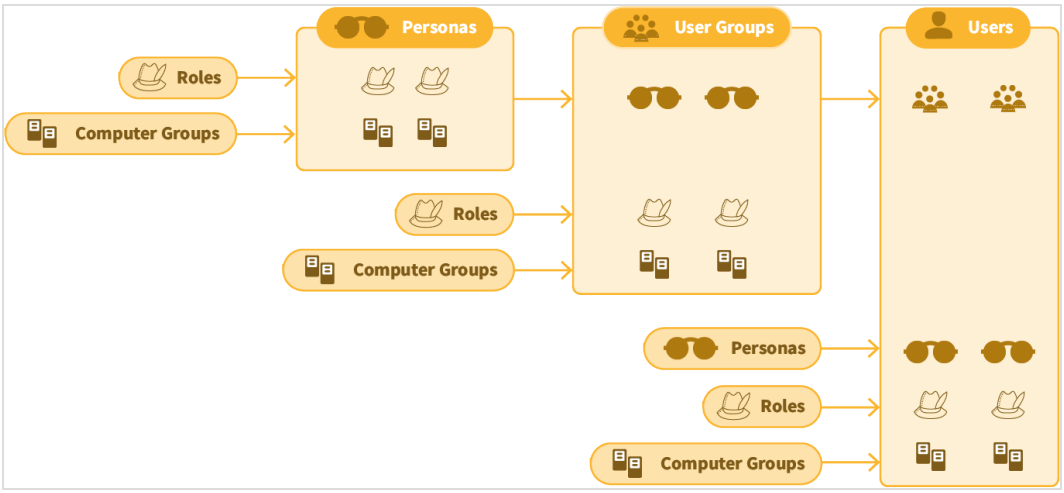


© 2026 Tanium Inc. All Rights Reserved

3. Assign the roles and computer groups to the user groups, user accounts, or personas of users who will deploy, approve, or administer actions. For more information, see:

   - Managing role and computer group permissions through personas on page 655
   - Managing user groups on page 643
   - Managing users on page 625

   Personas, user groups, and users



CONFIGURE DOWNLOADS AUTHENTICATION

Configure downloads authentication if the Tanium Server must establish trust with remote sources from which it downloads package files for actions. For example, Tanium™ Patch downloads patches from repositories such as the Red Hat Content Delivery Network to deploy to Linux endpoints. For more information, see Enabling authentication between platform servers and remote systems on page 173.

Configure and deploy actions

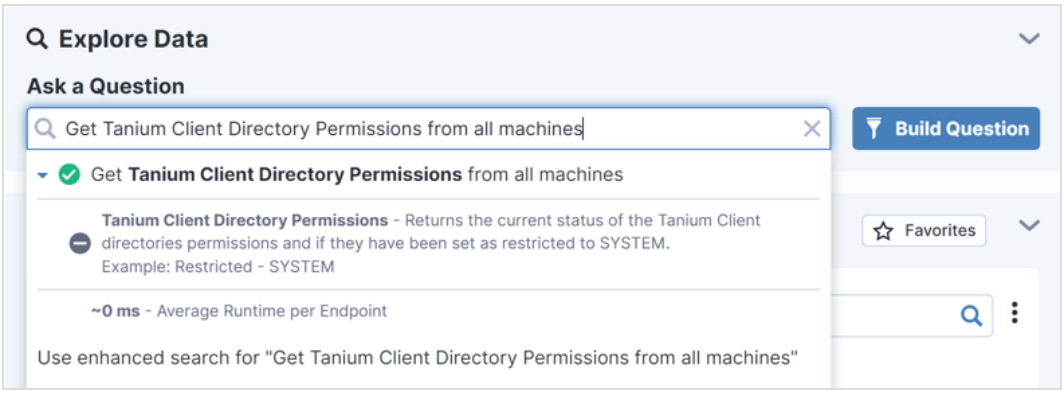
Perform the following steps for each new action:

1. Identify which endpoints require the action based on a dynamic or saved question. For more information about the questions and other methods that you use to initiate an action, see Select an action or playbook initiation method on page 391. To initiate the action in this example, you go to the Tanium **Home** page and enter `Get Tanium Client Directory Permissions from all machines` in the **Ask a Question** field.

   The purpose of this example action is to restrict permissions for the Tanium Client installation directory on Windows endpoints such that only the SYSTEM account can view or edit files in that directory. Because this action is based on question results, it deploys only to endpoints that have unrestricted permissions on the directory. Avoiding deployment to endpoints that do not need an action reduces its impact on network and endpoint resources.

© 2026 Tanium Inc. All Rights Reserved

Dynamic question issued through Ask a Question field



2. Select the results from endpoints that require the action and click **Deploy Action** to configure the action settings.

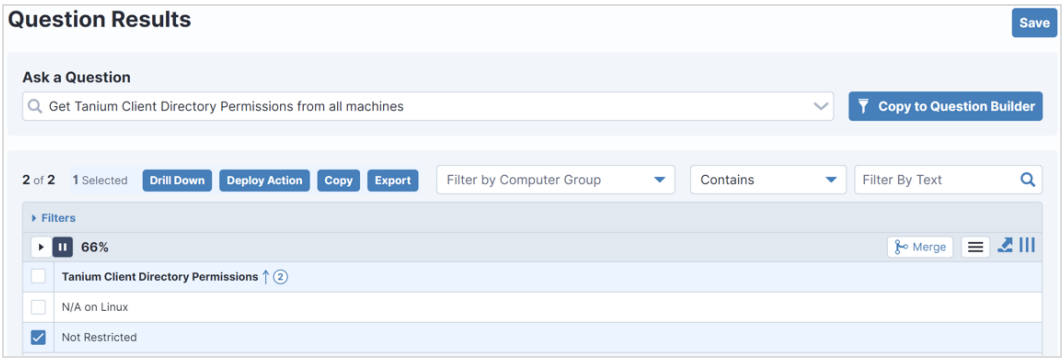
NOTE

You cannot deploy an action until the estimated percentage of endpoints that answer the question reaches the threshold that is specified in the **Action Target Estimate Minimum** platform setting.

TIP

You can refine the results before deploying an action. For example, you can issue drill-down questions, merge questions, or filter the results until you identify more precisely the endpoints that require the action. For more information, see Part 7: Analyzing question results in Console and Interact on page 255.

Question results



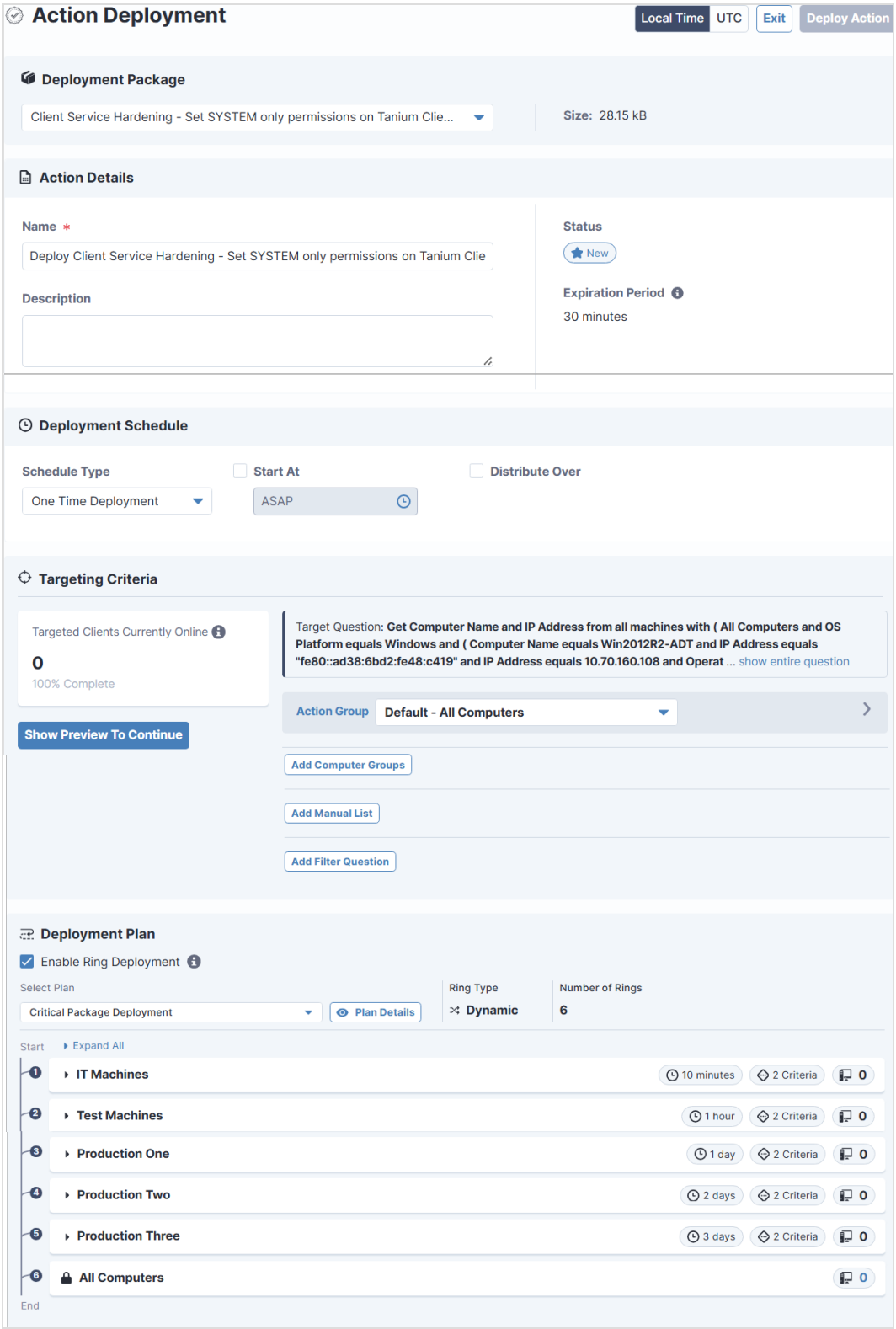
3. Configure the action settings.

TIP

When the action first deploys, some endpoints might be offline. To ensure that the action deploys to endpoints that come online after the initial deployment, set the **Schedule Type** to **Recurring Deployment** and set the interval (**Re-issue every**) and time period (between the **Start At** and **End At** dates) to appropriate values. For example, you can configure the action to deploy once per day for a month to ensure that all endpoints have a chance to come online.

© 2026 Tanium Inc. All Rights Reserved

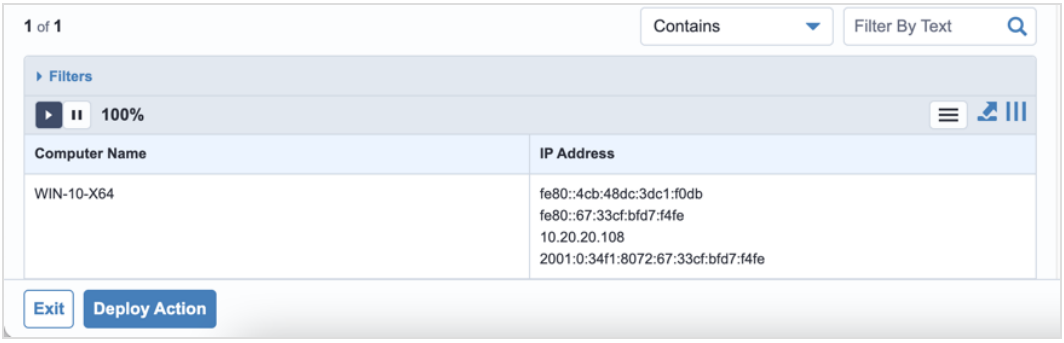
Action settings



© 2026 Tanium Inc. All Rights Reserved

4. Click **Show preview to continue**, review the affected endpoints, and click **Deploy Action**.

Preview and initiate deployment



NOTE

If the number of affected Tanium Clients exceeds the threshold that is specified in the **Prompt Estimate Threshold** platform setting, Tanium Console prompts you to confirm the deployment before proceeding.

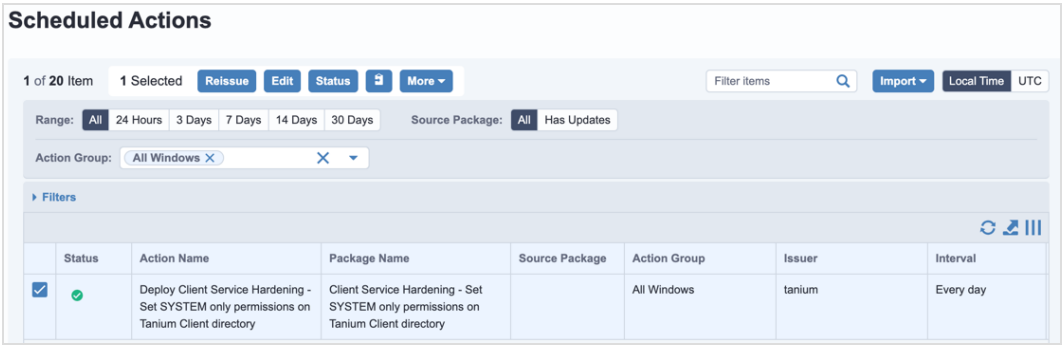
If the action deploys immediately, a page opens automatically to show the action status. If the action requires approval or has a future start date/time, you can view its status after deployment starts in the **Action History** page or Deployment Details page. For more information, see Monitor actions on page 316.

Monitor actions

Track the status of actions to ensure that they are configured correctly and deploy as expected, and to Troubleshoot actions on page 318 if necessary.

VIEW ACTION STATUS AND SETTINGS

1. If the action does not require approval and deployment starts immediately, skip to the next step. Otherwise, go to **Administration > Actions > Scheduled Actions** and confirm the action is listed.



Perform the next step after:

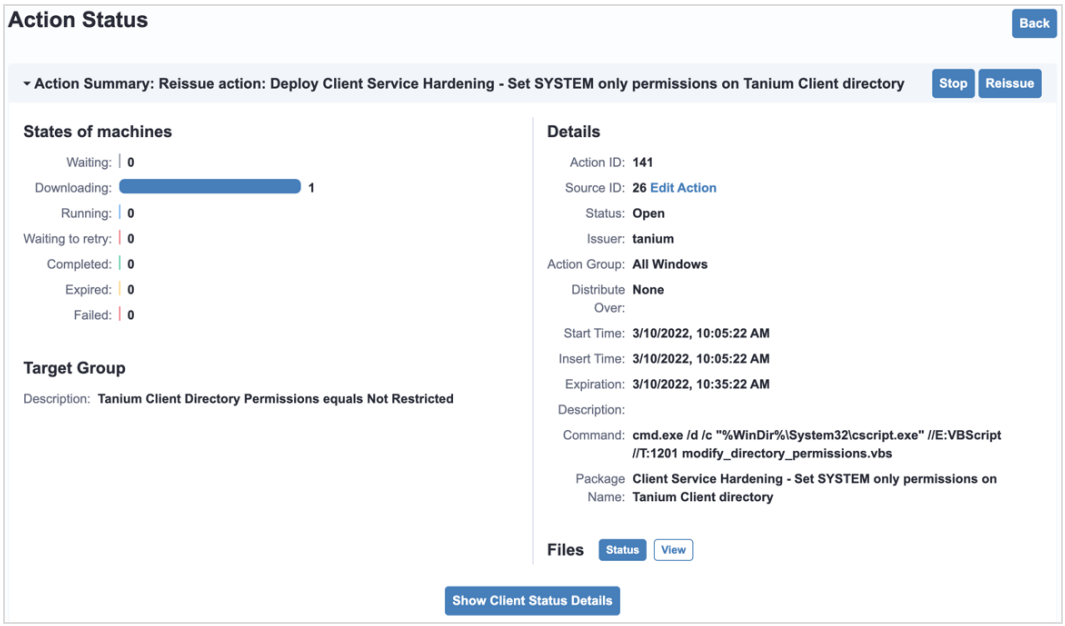
a. A user approves the action, if approval is required. For more information, see Approve pending actions on page 413.

b. Deployment starts, if it is scheduled for a future date/time.

© 2026 Tanium Inc. All Rights Reserved

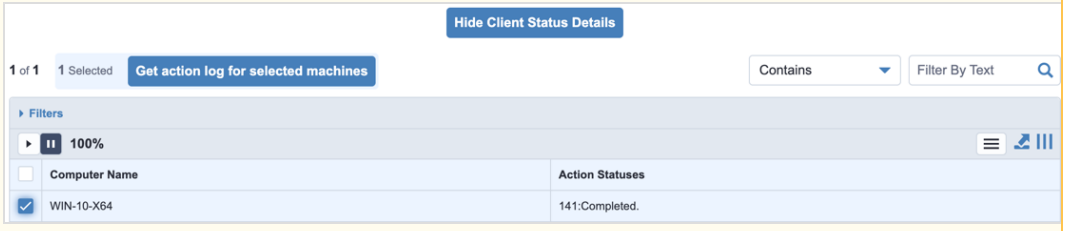
2. Perform one of the following steps based on the type of action:

   - **Adaptive action**: The Deployment Details page opens automatically. For more information, see Analyze and manage a single deployment on page 362.
   - **Simple action**: If the action did not require approval and deployment started immediately, the **Action Status** page opens automatically. After the first (or only) deployment interval, you can also open the **Action Status** page from the **Action History** page, as described in Manage actions that are completed or in progress on page 349. For more information, seeView status for simple actions on page 352.



TIP

The Tanium Client generates action logs to record the command-line interface (CLI) output that is associated with action commands. If you have **Sensor read** permission on the **Client Management** content set, you can display the log records to investigate issues related to an action. To display the records, on the **Action Status** page click **Show Client Status Details**, select up to 50 endpoints in the preview list, and click **Get action log for selected machines**. For more information, see Investigate action-related issues through logs on page 355.



© 2026 Tanium Inc. All Rights Reserved

TROUBLESHOOT ACTIONS

If issues occur during action deployment, the following tasks can help you to troubleshoot. Record the action IDs of the actions that you want to troubleshoot before reviewing logs. The **Action History**, **Scheduled Actions**, and **Action Status** pages all show action IDs. For more information, see Track action IDs on page 355.

For issues on Tanium Clients, investigate:

- **Log messages**:
    - View action logs for multiple endpoints through Tanium Console: see Investigate action-related issues through logs on page 355.
    - View action logs for a specific endpoint: see Tanium Client Management User Guide: Review action logs and associated files to troubleshoot actions and packages.
    - Troubleshoot actions, audit actions, or review action history logs: see Tanium Client Management User Guide: Review action history logs to troubleshoot or audit actions.
- **Action locks**: Verify whether action locks are turned on by issuing the saved question **Clients That Cannot Take Actions - Action Lock On**. For more information, see Issue a saved question on page 466 and Locking down actions on endpoints on page 407.
- **Sensor quarantines**: Verify whether the actions use sensors that are quarantined on the Clients and, if appropriate, remove those sensors from quarantine. For more information, see Manage sensor quarantines on page 433.

For issues on the Tanium Server, investigate:

- **Action deployment issues**: Review action scheduler logs:
    - Tanium Appliance User Guide: Action scheduler log
    - Tanium Core Platform User Guide for Windows Deployments: Action scheduler log
- **Download and caching issues**: Review the following logs:
    - Tanium Appliance User Guide: Tanium Downloader log
    - Tanium Core Platform User Guide for Windows Deployments: Tanium Downloader log
    - Tanium Appliance User Guide: Package download log
    - Tanium Core Platform User Guide for Windows Deployments: Package download log
    - Tanium Appliance User Guide: Package cache cleaner log
    - Tanium Core Platform User Guide for Windows Deployments: Package cache cleaner log

For more information about accessing and reviewing logs, see:

- Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform
- Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform

If the logs indicate package download issues, investigate:

© 2026 Tanium Inc. All Rights Reserved

- **Package files**: Review details about package files associated with the action and, if necessary, re-download the files if they are outdated. For more information, see Re-download package files on page 445.
- **Certificates**: Verify the validity of the certificates that the Tanium Server uses when downloading packages from remote sources. Update the certificates if necessary. For more information, see Enabling authentication between platform servers and remote systems on page 173.

If the logs indicate package caching issues, you can Manage the package file repository on page 711.

© 2026 Tanium Inc. All Rights Reserved

Actions overview

The following sections provide an overview of Tanium platform actions that you deploy from Tanium Console or Tanium Interact. For information about deployments that you manage through other Tanium solutions, see Deployment types on page 277.

What is an action?

A Tanium action is a configuration object that you deploy to endpoints to manage a change on those endpoints. In the action configuration, you specify the package that performs the change, endpoint targeting criteria such as an action group, and deployment conditions such as scheduling. You can schedule the action to run immediately or in the future and as a one-time deployment or at recurring intervals. An *adaptive action* deploys in progressive phases called rings that you define in a deployment plan. A *simple action* deploys to all targeted endpoints in one phase.



For more information about the end-to-end action deployment workflow, see Action deployment overview on page 328.

Example: Action deployment use case

Consider a case where you are responsible for ensuring that the Tanium Client continues running on all endpoints that support it. You might start by issuing an Interact question to check if any endpoints provide users the permissions to uninstall the Client: `Get Tanium Client Directory Permissions from all machines with Tanium Client Directory Permissions equals Not Restricted`. Then you can deploy an action to run a package that allows only the SYSTEM account to uninstall applications in that directory: **Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory**. If new endpoints with unrestricted permissions for the Client directory might join your network in the future, you can schedule recurring deployments to automatically restrict the permissions on those endpoints.

RBAC for actions

Actions can affect the security and health of endpoints. Therefore, when you configure role-based access control (RBAC) for deploying actions, consider which users need to manage changes on endpoints, which changes the users might apply, and on which endpoints the users have authority to make changes. Assign the following RBAC components to users, user groups, and personas to control action deployment:

- Computer Groups

  For example, some users in your Security Operations Center might be responsible for deploying vulnerability remediations to workstations, while a smaller set of users might be responsible for remediating servers. In this case, you can assign the **All Workstations** computer group to the first set of users and the **All Servers** computer groups to the second set.

- Roles

© 2026 Tanium Inc. All Rights Reserved

For example, assigning a role with the **Interact Execute action** permission enables users to deploy actions that use packages in the **Core Content** set. That content set includes packages for many use cases, such as managing registry keys on Windows endpoints. If you plan to assign that role to users who also need the ability to quarantine endpoints, you can add **Package read** permission to the **Threat Response** content set, which contains packages for quarantining endpoints.

For more information, see Action management permissions on page 89 and Configure RBAC for action users on page 331.

Action status and logs

When an action starts, the Client on each target endpoint runs the associated package and returns action status updates to the Tanium Server. The Client also generates action-related logs that you can use to troubleshoot deployment issues. You can view the action status and logs in Tanium Console. For more information, see Monitor actions on page 337.

Action packages

A Tanium package comprises a command, a script, and any related files that are required to run an action on endpoints managed through Tanium Client. You select the package when you configure an action. For example, consider a case where you are troubleshooting issues related to Domain Name Server (DNS) updates on Windows endpoints. If you decide to restart the **DHCP Client** service on those endpoints, you can configure an action with the predefined **Restart Service** package and specify `DHCP Client` as the service to restart. For more information, see Managing packages for platform actions on page 442.

When you deploy an action, Tanium Clients download the associated package files and distribute the files among peers in the Client linear chains. Each Client stores package files for an action in the *<Tanium_Client_installation_directory>*`/Downloads/Action_`*<ID>* folder, where *<ID>* is the action identifier. For more information, see Tanium Client Management User Guide: File distribution.

Action groups

An action group specifies the computer groups that an action targets. Each computer group specifies a collection of endpoints based on a question with sensors or based on a manual list. You must select an action group for each action to target only the endpoints that require the action and avoid unnecessary processing for other endpoints.

Each action group specifies the computer groups based on Boolean AND/OR logic. For example, to deploy an action that resets a registry key on Windows endpoints where the key is missing or incorrect, you might create an action group named `Registry Key` that joins the following computer groups with a Boolean OR.

Example: Computer group membership for action group

Computer group name	Membership definition
Registry Key Not Found	Registry Key Exists[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Tanium\Anykey] contains False
Registry Value Not Correct	(Registry Key Exists[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Tanium\Anykey] contains True and all Registry Value Data[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Tanium\Anykey,Value] not matches 1)

For more information, see Targeting actions through action groups on page 400.

© 2026 Tanium Inc. All Rights Reserved

Action locks

Action locks prevent actions from running on an endpoint. You might want to deploy action locks if, for example, you encounter unexpected behavior on certain endpoints and want to suspend actions on them during debugging. For more information, see Locking down actions on endpoints on page 407.

Scheduled actions

Scheduled actions are actions that the Tanium Server deploys at a future time or at intervals based on the values that you set for the following action settings:

- **Start At**: Specify the date and time when the Server first deploys the action.
- **Re-issue Every**: Optionally, you can specify the frequency at which the Server redeploys the action.
- **End At**: Optionally, you can specify the date and time when the Server stops redeploying the action regardless of the reissue interval.



For more information, see Configure action settings.

Scheduled recurring actions address the following use cases:

- The action is used to enforce policy or ensure good cyber hygiene in an environment. For example, the content-only solution Tanium™ Default Content contains several scheduled actions that periodically update tooling on endpoints, verify configuration settings are in place, and maintain the overall health of Tanium Clients in your deployment. Redeploying these actions at intervals ensures that any new endpoints that join your environment are protected and ready for Tanium operations.
- You want to apply changes, such as software or configuration updates, to endpoints that might not be online during the initial deployment but that you expect to be online at some point between the **Start At** and **End At** dates.
- Action approval on page 322 is required and you are not certain that an approver will approve the action before its initial deployment expires.

You can also schedule one-time-only actions to deploy at a future **Start At** date to accommodate other events in your network. For example, you might schedule actions to start during a maintenance window on endpoints.

For more information, see Managing scheduled actions and action history on page 341.

Action approval

Some organizations have policies that require an approval process for deploying actions. Action approval ensures two-person integrity for managing changes on endpoints. When action approval is enabled, the signed-in user who deploys the scheduled action cannot also approve it. The action is on hold (pending) until another user approves it. The approving user must be assigned a role with **Approve Action** and **Sensor read** permissions.

© 2026 Tanium Inc. All Rights Reserved

For recurring (scheduled) actions, approval is a manual process only for the first deployment interval and is automatic for subsequent intervals. The approval remains in force until the **End At** date that is set in the action configuration or until another user modifies the configuration.

For more information, see Managing action approval on page 411.

Adaptive actions and simple actions

An *adaptive (ring-based) action* is assigned a deployment plan that defines the target endpoints and progression criteria for each ring that an action must progress through to complete successfully. Adaptive actions are useful for controlling action impacts, mitigating action-related disruptions, and protecting sensitive endpoints. For example, if an action reboots endpoints, you can stagger the deployment one ring at a time to minimize the overall disruption to your environment. For more information, see Ring-based deployment on page 276.

A *simple (non-ring-based) action* deploys in a single phase and therefore does not require a deployment plan. For example, you might decide that adding a custom tag to a subnet of endpoints constitutes a low-impact change that you can apply to the entire subnet in one deployment.

Policy actions

A policy action is a scheduled, recurring action that uses a saved question instead of a dynamic question and uses a `from` clause that ensures the action deploys only to endpoints that match the question condition. Policy actions are useful for ensuring that endpoints comply with policies, and are more efficient than other recurring actions at conserving network bandwidth and endpoint resources. For example, if your organization requires all Windows endpoints to have restricted permissions on the Tanium Client installation directory, you can schedule an action to restrict permissions based on the following saved question.

`Get Tanium Client Directory Permissions equals Not Restricted from all machines with ( Tanium Client Directory Permissions equals Not Restricted and Is Windows equals True )`.

In this example, only Windows endpoints with open permissions on the Tanium Client installation directory match the condition, and therefore only those endpoints download the required package **Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory** and run the action to restrict permissions. By contrast, a scheduled action that is not a policy action runs on all the targeted endpoints at every scheduled interval, which unnecessarily consumes more network bandwidth and endpoint resources.



The Tanium Server does not deploy a policy action to endpoints that were offline when it issued the saved question and that then come online while the action is in progress.

If you delete a saved question, the Tanium Server continues reissuing it for any actions that use the question and continues recording the question in the Question History log, which you can view on the **Administration > Content > Question History** page.

The Tanium Server performs the following steps at each scheduled interval for a policy action:

© 2026 Tanium Inc. All Rights Reserved

1. Evaluate whether the question results exceed the question expiration period (10 minutes). If no, the Server uses the results that it cached the last time it issued the question. If yes, it reissues the question to collect new results.
2. Evaluate the question results to determine whether any endpoints match the question condition and belong to computer management groups that are assigned to the question owner:
    - **Yes**: The Server deploys the action to the targeted action group. Within the group, only endpoints that match the question condition run the action.
    - **No**: The action does not deploy.

Action best practices

Minimize the impact of actions on network and endpoint resources by following best practices for the questions that define action targeting and computer group management rights.

Optimize questions for action targeting

The action deployment workflow starts with a question that you issue to identify the endpoints that require the action. Understanding how the question affects the targeting can help you optimize actions through the Best practices for action questions on page 327. The Tanium Server deploys each action through a message that it sends to endpoints. The message contains all the action settings that you see on the **Action Deployment** page (see Configure action settings on page 395), including the **Target Question** that each Tanium Client uses to determine whether it must run the action. When you select rows on the **Question Results** page and click **Deploy Action**, Interact adds a sensor-based filter for each selected row to the `from all machines with` clause of the **Target Question**. Selecting more rows produces a longer **Target Question** and therefore a larger action message that requires more network bandwidth and endpoint resources to process.

Tanium Console limits the impact of any action on networking and endpoint resources by disabling the **Deploy Action** button if you select more than 100 rows on the **Question Results** page. You can avoid exceeding that limit, and further reduce resource consumption, by basing an action on a question that returns fewer result rows from the endpoints that require the action. You can also reduce resource consumption by constructing more efficient filters in the question syntax. The following examples illustrate how to achieve these efficiencies.

EXAMPLE: OPTIMIZING THE "GET" CLAUSE

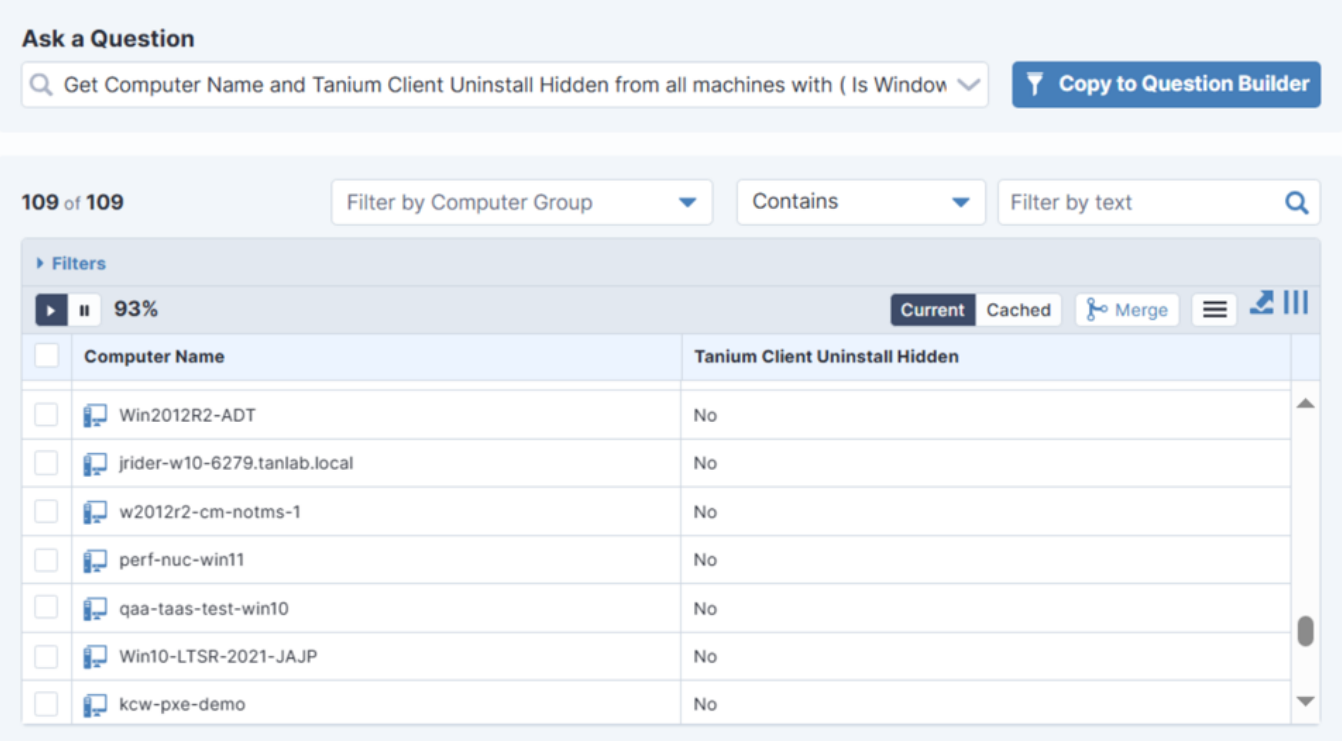
Consider a case where you issue the following question to identify Windows endpoints where the Tanium Client is listed among applications that endpoint users are allowed to remove:

```
Get Computer Name and Tanium Client Uninstall Hidden from all machines with Is Windows equals true and Tanium Client Uninstall Hidden equals no
```

That question returns a result row for each endpoint, which is useful if you want to know the computer names of the affected endpoints:

© 2026 Tanium Inc. All Rights Reserved

A question that returns a result row for each endpoint



However, that question might return too many rows to be useful for deploying an action that prevents endpoint users from removing the Client. The **Target Question** in the action would have a very long `from` clause if 100 endpoints required the action and you selected all 100 result rows for them. The following example shows how long the **Target Question** is even with just 5 endpoint results selected:

```
Get Computer Name and IP Address from all machines with ( All Computers and ( Is Windows equals true and Tanium Client Uninstall Hidden equals no ) and ( ( Computer Name equals Win2012R2-ADT and Tanium Client Uninstall Hidden equals No ) or ( Computer Name equals jrider-w10-6279.tanlab.local and Tanium Client Uninstall Hidden equals No ) or ( Computer Name equals w2012r2-cm-notms-1 and Tanium Client Uninstall Hidden equals No ) or ( Computer Name equals perf-nuc-win11 and Tanium Client Uninstall Hidden equals No ) or ( Computer Name equals qaa-taas-test-win10 and Tanium Client Uninstall Hidden equals No ) ) )
```

For every action, the `Get` clause in the **Target Question** is always `Get Computer Name and IP Address` regardless of the Interact question that you issued. The action uses the **Computer Name** and **IP Address** sensors to uniquely identify each target endpoint . The `from` clause of the **Target Question** always uses the sensors from both the `Get` and `from` clauses of the Interact question. Consequently, **Computer Name** is repeated in both the `Get` clause and `from` clause of the **Target Question** for this example.

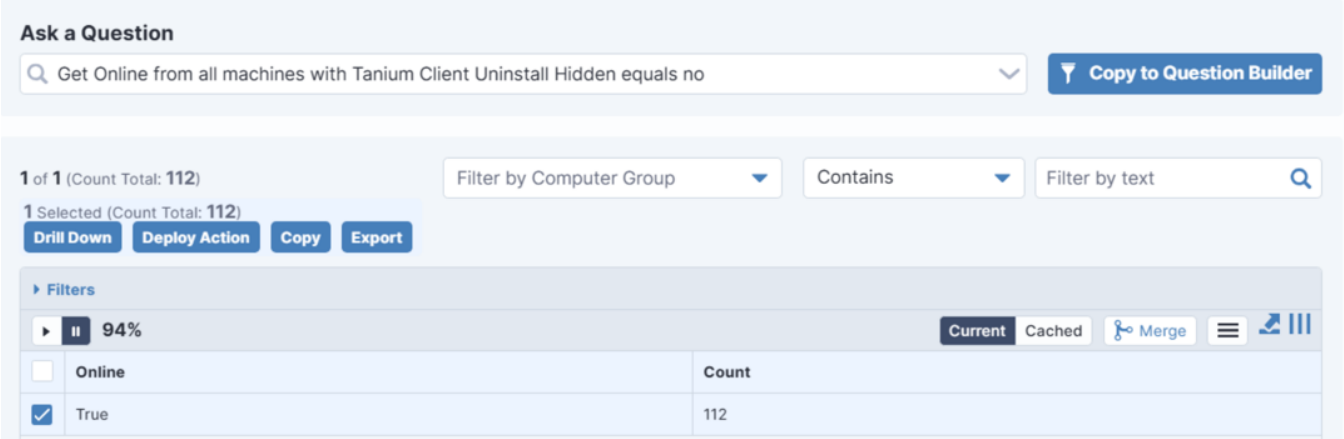
To deploy an action in this case, you can issue a more elegant Interact question that replaces **Computer Name** with the **Online** sensor in the `Get` clause and omits the **Is Windows** sensor in the `from` clause:

```
Get Online from all machines with Tanium Client Uninstall Hidden equals no
```

When **Online** is the only sensor in the `Get` clause, the Interact question always returns a single result row with the value `True` regardless of how many filters you add to the `from` clause:

© 2026 Tanium Inc. All Rights Reserved

A question that returns one result row for all endpoints



When you select the result row for this Interact question and click **Deploy Action**, Interact creates a much simpler **Target Question** than the example where you selected multiple rows:

```
Get Computer Name and IP Address from all machines with ( All Computers and Tanium Client Uninstall Hidden equals no and Online equals True )
```

> NOTE
>
> In the preceding examples, the **Target Question** specifies `All Computers` in the `from` clause because the default action group is **Default - All Computers**. However, you can specify a different action group and other filters in the action settings. For more information, see Configure action settings on page 395.

EXAMPLE: OPTIMIZING THE "FROM" CLAUSE

The following example is another question that might be useful for analyzing information but is not optimized for actions. In this case, you want to deploy an action to all endpoints that do not have a high enough Google Chrome version installed, but first you want to see what versions are distributed across all the endpoints in your network:

```
Get Installed Application Version[Chrome] from all machines
```

If multiple endpoints have the same Chrome version, the **Question Results** page would aggregate the results by version instead of showing a row for each endpoint. However, if endpoints across your network have a broad range of versions, the page might still list too many result rows (potentially more than the 100 limit) to be suitable for action deployment. Even if you select only five rows and click **Deploy Action**, the **Target Question** will have a long `from` clause:

```
Get Computer Name and IP Address from all machines with ( All Computers and ( Installed Application Version[Chrome] equals 99.0.4844.74 or Installed Application Version[Chrome] equals 109.0.5414.168 or Installed Application Version[Chrome] equals 94.0.4606.81 or Installed Application Version[Chrome] equals 123.0.6422.78 or Installed Application Version [Chrome] equals 123.0.6312.123 ) )
```

To optimize the question for actions, you can again use the **Online** sensor in the `Get` clause and move the **Installed Application Version[Chrome]** sensor to the `from` clause as a filter:

```
Get Online from all machines with Installed Application Version[Chrome] < 124.0.6367.91
```

© 2026 Tanium Inc. All Rights Reserved

When you select the single result row (`True`) and click **Deploy Action**, Interact applies that version filter to a much simpler **Target Question**:

```
Get Computer Name and IP Address from all machines with ( All Computers and Installed Application Version[Chrome] < 124.0.6367.91 and Online equals True )
```

The following Interact question is the same as the previous example but has multiple sensor filters in the `from` clause:

```
Get Online from all machines with ( Installed Application Version[Chrome] > 124.0.6367.91 and Operating System contains Windows 10 and Tanium Client Subnet contains 192.168.0.0/24 )
```

The preceding Interact question still returns only one result row, which you can select to deploy an action with the following **Target Question**:

```
Get Computer Name and IP Address from all machines with ( All Computers and ( Installed Application Version[Chrome] < 124.0.6367.91 and Operating System contains Windows 10 and Tanium Client Subnet contains 192.168.0.0/24 ) and Online equals True )
```

The preceding **Target Question** remains simpler, and requires less processing on endpoints, then the **Target Question** that is based on multiple result row selections and only one filter.

BEST PRACTICES FOR ACTION QUESTIONS

The following best practices enable you to construct Interact questions that minimize the complexity of the **Target Question** in an action:

- **Minimize result rows**

  Use a `Get` clause that returns only a few result rows, ideally just one, from all the endpoints that require the action. The preceding examples use the **Online** sensor, but you can use any other sensor that returns a few results that you can select from all the target endpoints. Avoid using sensors that return one result row per endpoint, particularly the **Computer Name** and **IP Address** sensors that produce duplicate filters in the **Target Question**.

- **Filter using the `from` clause**

  Add sensor filters to the `from` clause instead of the `Get` clause to specify endpoint targeting.



Tanium strongly recommends that you do not lower the default **Max Sensor Age** or **Maximum Data Age** for any sensor in the `Get` or `from` clause of a dynamic question or saved question that you use for deploying actions. For more information, see Best practices for saved questions on page 456.

Optimize action groups and computer groups for targeting

The complexity of an action group and its assigned computer groups affect the size of the action message that the Tanium Server sends to endpoints, and the message size affects the networking and endpoint resources that an action consumes. Resource consumption increases as you add more computer groups to an action group and as the targeting of those computer groups becomes more complex. Increasing the number and complexity of computer groups assigned to the user account that you use to deploy an action also increases the action message size and therefore resource usage. To optimize computer groups for action targeting, see Computer groups on page 557.

© 2026 Tanium Inc. All Rights Reserved

Conserving resources through action distribution

The Tanium Server distributes actions to endpoints in batches. When you Configure action settings, you can use the **Distribute Over** option to randomize the distribution over the specified period to prevent spikes in network traffic or other resource consumption. For example, an action that depends on a sensor that queries Active Directory (AD) might cause a flood of traffic to the AD server unless the action is distributed over time. Similarly, an action that targets endpoints in a virtual machine farm might exhaust the shared CPU or memory resources if all endpoints simultaneously run a resource-intensive program.

When the Tanium Client receives an action from the Tanium Server, the Client evaluates the action targeting criteria to verify that its endpoint is a target before calculating a **Distribute Over** delay to the action start time. Each Client sets a delay interval that ranges from zero to the **Distribute Over** value, which represents the maximum. After the delay, the Client starts running the action without re-evaluating the targeting criteria. The longer the delay between the targeting evaluation and action start, the higher the risk of the Client running an action for which the endpoint no longer qualifies. For example, an action might target endpoints with low disk space to run a package that removes data to clear space. An endpoint that has low disk space when the Client evaluates the targeting might no longer meet the low space threshold by the time the action starts.

The Client uses the **Distribute Over** delay to calculate the action expiration period. Therefore, the **Distribute Over** value affects the action status that the Client reports to the Tanium Server. For more information, see Action states on page 353.



You can set a **Distribute Over** value only for simple actions, not adaptive actions.

Action deployment overview

Configure platform settings, content, and role-based access control (RBAC) to optimize action deployment before users start configuring actions. Monitoring action status and history is also important to ensure that actions are having the expected effect and to troubleshoot otherwise. The three stages of action deployment are:

1. Administrative setup for actions on page 328
2. Configure and deploy actions on page 334
3. Monitor actions on page 337

Administrative setup for actions

Typically, you perform the following tasks once as part of the initial setup of a Tanium deployment. However, you might repeat some tasks if your environment changes. For example, you might update RBAC configurations to reflect changes to roles and personnel.

- Review and edit global settings for actions on page 329
- Review and customize action content on page 330
- Configure RBAC for action users on page 331
- Configure downloads authentication on page 334

© 2026 Tanium Inc. All Rights Reserved

TIP

Tanium provides several predefined scheduled actions, such as **Distribute Hardware Tools**. You can review these actions on the **Administration > Actions > Scheduled Actions** page. The Tanium Server automatically imports several predefined actions with the content-only solutions Default Content and Core Content and imports other actions when you import certain modules or shared services. You can manually import content-only solutions that contain additional predefined actions. For more information, see Part 4: Managing Tanium solutions on page 108.

Actions in the Default Content and Core Content solutions might initially target the predefined action groups **Default – All Computers** or **Default**, which specifies the **No Computers** computer group.

REVIEW AND EDIT GLOBAL SETTINGS FOR ACTIONS

Review and, if necessary, edit global settings that affect action deployment.

1. From the Main menu, go to **Administration > Configuration > Settings > Platform Settings** to assess whether the default values of the following global settings suffice for your Tanium deployment. Update any settings that require custom values.

   TIP

   On the **Platform Settings** page, Expand a setting to see its full description.

   Global settings for actions

Setting	Description
Require Action Approval Bulk Approval	Enable action approval if your organization implements two-person integrity. These settings are disabled by default. For more information, see Enable or disable action approval on page 412.
Action Target Estimate Minimum	After you issue a question to identify endpoints that require an action, you cannot deploy the action until the percentage of responding endpoints reaches the estimated percentage. The default is 20%. For more information, see Configure and deploy actions on page 334.
Prompt Estimate Threshold	When you deploy an action and the number of affected endpoints exceeds the threshold, Tanium Console prompts you to confirm the deployment before proceeding. The default is 100. Changing the value to 0 causes Console to prompt users whenever they deploy actions regardless of the number of affected endpoints.
Run Commands in Process Group	Enables you to control whether package commands run in a process group. This setting is disabled by default. For more information, see Launch this package in a process group on page 448.
Restricted Targeting	Sets the **No Computers** computer group as the action group target during initial configuration of Tanium solutions. This setting is disabled by default. For more information, see Tools deployment and restricted targeting on page 121.

© 2026 Tanium Inc. All Rights Reserved

2. Review the following advanced global settings to assess whether their default values suffice for your Tanium deployment. These settings control the maximum size of the cache that the Tanium Client uses to store file chunks for packages and Client API downloads. For more information, see Tanium Client Management User Guide: Chunk caching. Update any settings that require custom values.

Global settings for Tanium Client chunk cache

Setting	Description
ClientCacheLimitInMB	Controls the absolute amount of disk space that a Client can use for caching chunks. The value is in megabytes (MB) and the default is 2048.
ClientCachePercentageCapTimes100	Controls the maximum percentage of free disk space that a Client can use for caching chunks. Multiply the target percentage by 100 to determine the value. For example, the default value 1000 specifies that the cache limit is 10% of free disk space. If you change the value, the Client checks the free disk space and adjusts the cache size only when you restart the Client or wait for the next Client reset interval, which is a random interval typically in the range of 2 to 6 hours.

Tanium Console does not show these Client cache settings unless a user adds them. Adding the settings is necessary only if non-default values are required. In an environment where actions deploy large files, such as for software installations or operating system (OS) patches, you might have to increase the cache limit and percentage. If each setting applies a different cache limit on a Client, the Client enforces whichever setting specifies a lower limit. For more information, see Manage advanced settings on page 164.

These are global settings and therefore apply to all Tanium Clients. However you can override the settings for specific Clients. For example, you might have critical assets that need more resources for running non-Tanium processes or assets with very limited resources such as virtual desktop infrastructure (VDI) endpoints. To override the global settings for cache size, configure the settings locally on specific Clients. For more information, see Tanium Client Management User Guide: Tanium Client CLI and Client settings.

REVIEW AND CUSTOMIZE ACTION CONTENT

Review the content that is required for action deployment. If the predefined content does not suffice for the actions that you expect users to deploy, create customize content.

Content types required for actions

Content type	Description
Content sets	Content sets contain the content that you create. When you configure user roles for action deployment, you assign permissions to content sets to control which content users can access. For example, if you create a package that updates files on data center servers, you can assign it to a content set for which access is restricted to users who have a role that allows data center file management. For more information, see Managing access to content through content sets on page 561.

© 2026 Tanium Inc. All Rights Reserved

Content types required for actions (continued)

Content type	Description
Packages	A package configuration includes settings, a command, a script, and any other files that are needed to orchestrate an action on an endpoint. For example, you might create a package that updates a specific file to a specific version. For more information, see Managing packages for platform actions on page 442.
Sensors Saved questions	You use sensors and saved questions to identify the endpoints that require action. For example, you might create a saved question with the **File Version** sensor to identify which endpoints have a particular version of a file. For more information, see Managing sensors for collecting endpoint data on page 421 and Managing saved questions in Console and Interact on page 455.
Filter groups	You use filter groups to: • Filter the questions and question results on which actions are based. For example, you might create a filter group that contains only the endpoints in a data center. • Create action groups for targeting specific endpoints. For more information, see Targeting actions through action groups on page 400. • Define Endpoint targeting on page 278 and Deferred endpoints on page 298 in deployment plans for adaptive actions. For more information, see Managing filter groups for filtering questions and results on page 476.
Deployment plans	A deployment plan defines the ring set that an adaptive action must progress through to complete successfully, along with the target endpoints and progression criteria for each ring. For more information, see Managing deployment plans for ring deployments on page 384. Before you add plans, be sure to understand all the components and timing factors of ring-based actions, as described in Ring-based deployment on page 276. NOTE Simple actions do not use deployment plans.

BEST PRACTICE

Do not edit content that is provided through Tanium content-only solutions; create custom content instead. For more information, see Tip 4: Limit customizations to Tanium content on page 138.

Test custom content in a lab environment before using it in a production environment.

CONFIGURE RBAC FOR ACTION USERS

Review the predefined RBAC for deploying actions and customize the RBAC as necessary. RBAC includes roles, users, user groups, personas, computer management groups, filter groups, and action groups.

1. Configure roles for administering, deploying, and (optionally) approving actions. Figure Role permissions related to actions on page 333 shows the permissions that are related to these tasks. For the specific permissions that are required to deploy actions, see Deploy actions on page 90. For more information, see Managing access permissions through roles on page 569.

© 2026 Tanium Inc. All Rights Reserved

NOTE

Users cannot approve their own actions. However, you can assign the **Bypass Action Approval** permission to a role to enable certain users to deploy actions without requiring approval. You must create a custom role if you want any users to have the bypass ability because no predefined role has that permission.

Deployment Plan, **Progression Criteria Set**, and **Ring Set** permissions apply only to adaptive actions, not simple actions.

The following permissions control access to the Tanium Console and Interact pages from which users deploy actions.

- **Interact solution permissions**: Controls access to Interact module pages from which users issue dynamic or saved questions and deploy actions based on the results. The **Ask Dynamic Questions** permission also controls access to the **Ask a Question** field on the Tanium **Home** page. For more information, see Interact permissions on page 81.
- **Package read permission**: Controls access to the **Packages** page, from which users can select a package to deploy through an action.
- **Client Status read permission**: Controls access to the **Client Status** page, where users can select endpoints to target for actions. Users typically use this page to troubleshoot connectivity issues for Tanium Clients.

NOTE

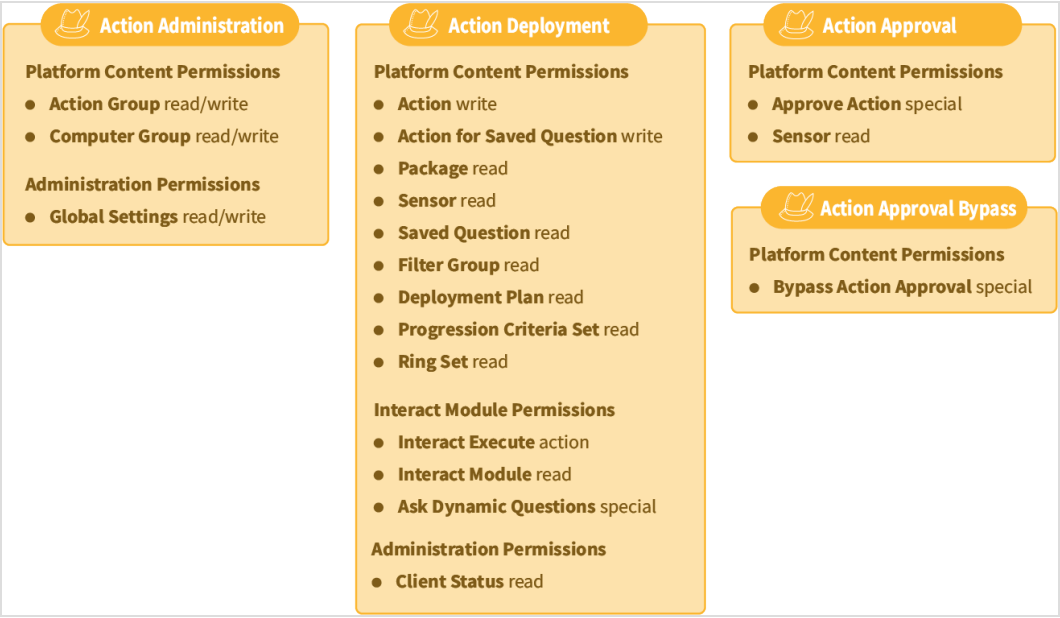
You can also deploy actions from the workbenches of other Tanium solutions, such as Reporting. For the permissions to access those workbenches, see the associated user guides in the Tanium Resource Center.

The following predefined roles provide action-related permissions but also other permissions. If you want action users to have a more limited range of permissions than what these roles provide, create custom roles.

- **Interact Power User**: This Interact role has all the permissions to deploy simple actions but not to approve actions or bypass action approval. For more information, see Interact permissions on page 81. This role does not have the permissions to assign a deployment plan, which is required for adaptive actions.
- **Deployment Plan User**: This Tanium Automate role has the permissions to assign deployment plans to adaptive actions. The **Deployment Plan Editor** role has the permissions to assign, create, edit, and delete deployment plans. For more information, see Tanium Automate User Guide: User role requirements.
- **Administrator**: This reserved role has all the action administration and deployment permissions but does not have permissions to approve actions or bypass action approval. For more information, see Administrator reserved role on page 582.

© 2026 Tanium Inc. All Rights Reserved

Role permissions related to actions



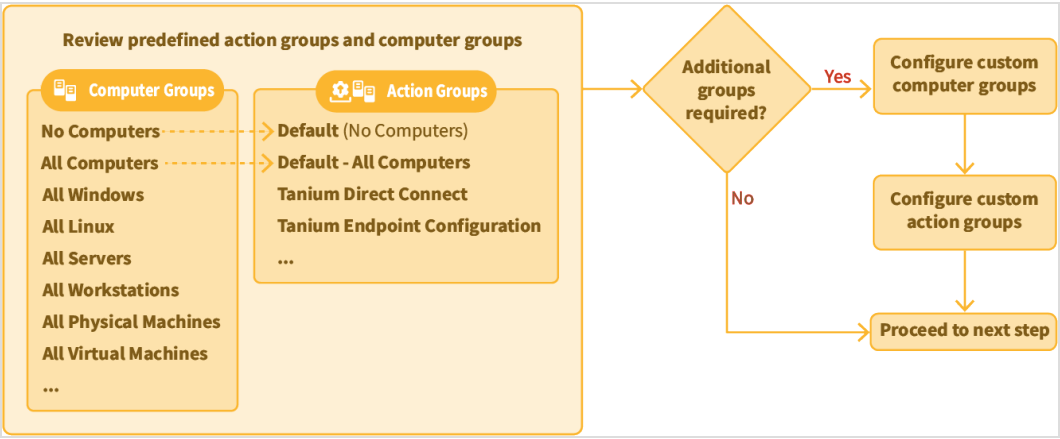
NOTE

After you deploy an action, you can view the contents of action logs to investigate issues related to the action. To view the logs, you require **Sensor read** permission on the **Client Management** content set. For more information, see View action status and settings on page 337.

2. Review the predefined action groups (**Administration > Actions > Action Groups**) and computer groups (**Administration > Permissions > Computer Groups**) to assess whether they suffice for action targeting in your environment. Configure custom groups if necessary.

   Action groups control which endpoints users can target for actions. Computer management groups and filter groups are the building blocks of action groups. For more information, see Controlling endpoint management rights through computer groups on page 610 and Targeting actions through action groups on page 400.

Computer groups and action groups

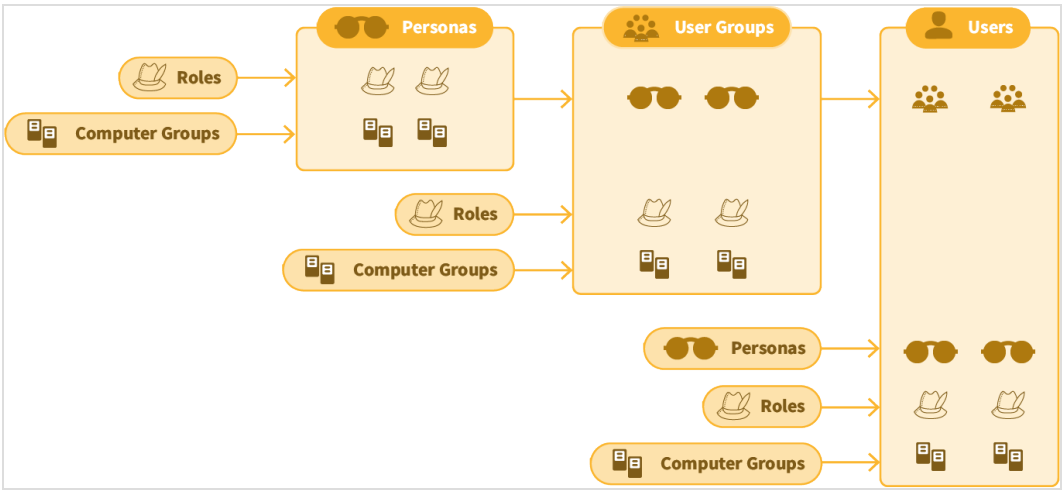


© 2026 Tanium Inc. All Rights Reserved

3. Assign the roles and computer groups to the user groups, user accounts, or personas of users who will deploy, approve, or administer actions. For more information, see:

   - Managing role and computer group permissions through personas on page 655
   - Managing user groups on page 643
   - Managing users on page 625

   Personas, user groups, and users



CONFIGURE DOWNLOADS AUTHENTICATION

Configure downloads authentication if the Tanium Server must establish trust with remote sources from which it downloads package files for actions. For example, Tanium™ Patch downloads patches from repositories such as the Red Hat Content Delivery Network to deploy to Linux endpoints. For more information, see Enabling authentication between platform servers and remote systems on page 173.

Configure and deploy actions

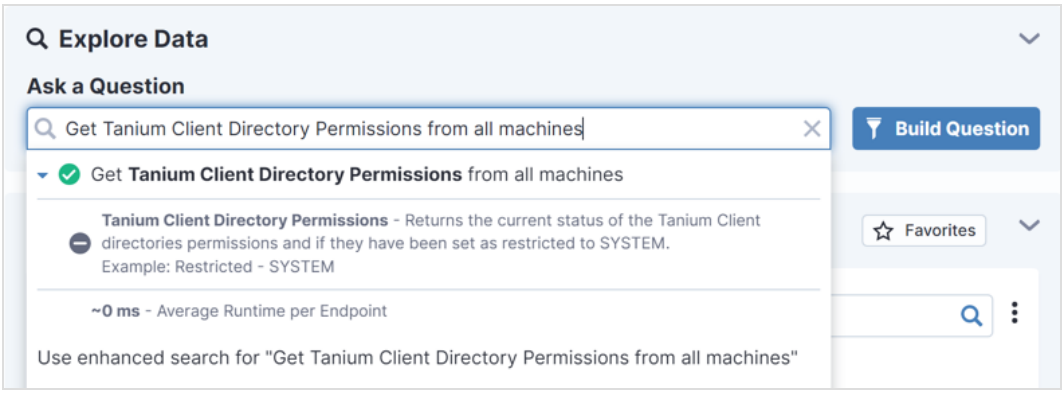
Perform the following steps for each new action:

1. Identify which endpoints require the action based on a dynamic or saved question. For more information about the questions and other methods that you use to initiate an action, see Select an action or playbook initiation method on page 391. To initiate the action in this example, you go to the Tanium **Home** page and enter `Get Tanium Client Directory Permissions from all machines` in the **Ask a Question** field.

   The purpose of this example action is to restrict permissions for the Tanium Client installation directory on Windows endpoints such that only the SYSTEM account can view or edit files in that directory. Because this action is based on question results, it deploys only to endpoints that have unrestricted permissions on the directory. Avoiding deployment to endpoints that do not need an action reduces its impact on network and endpoint resources.

© 2026 Tanium Inc. All Rights Reserved

Dynamic question issued through Ask a Question field



2. Select the results from endpoints that require the action and click **Deploy Action** to configure the action settings.

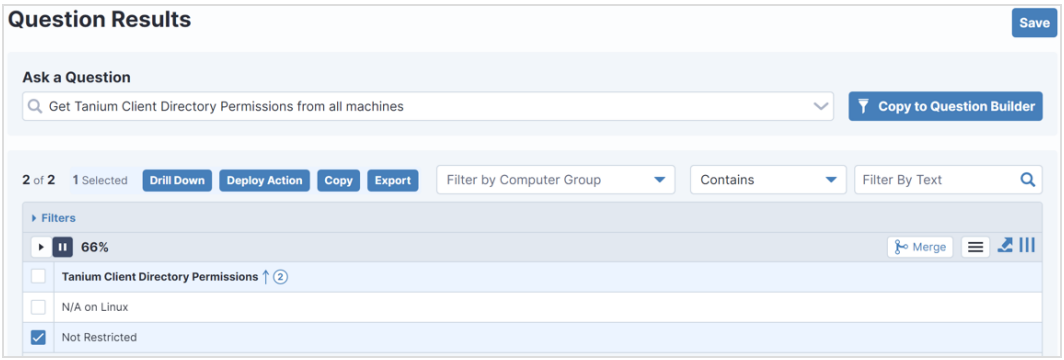
NOTE

You cannot deploy an action until the estimated percentage of endpoints that answer the question reaches the threshold that is specified in the **Action Target Estimate Minimum** platform setting.

TIP

You can refine the results before deploying an action. For example, you can issue drill-down questions, merge questions, or filter the results until you identify more precisely the endpoints that require the action. For more information, see Part 7: Analyzing question results in Console and Interact on page 255.

Question results



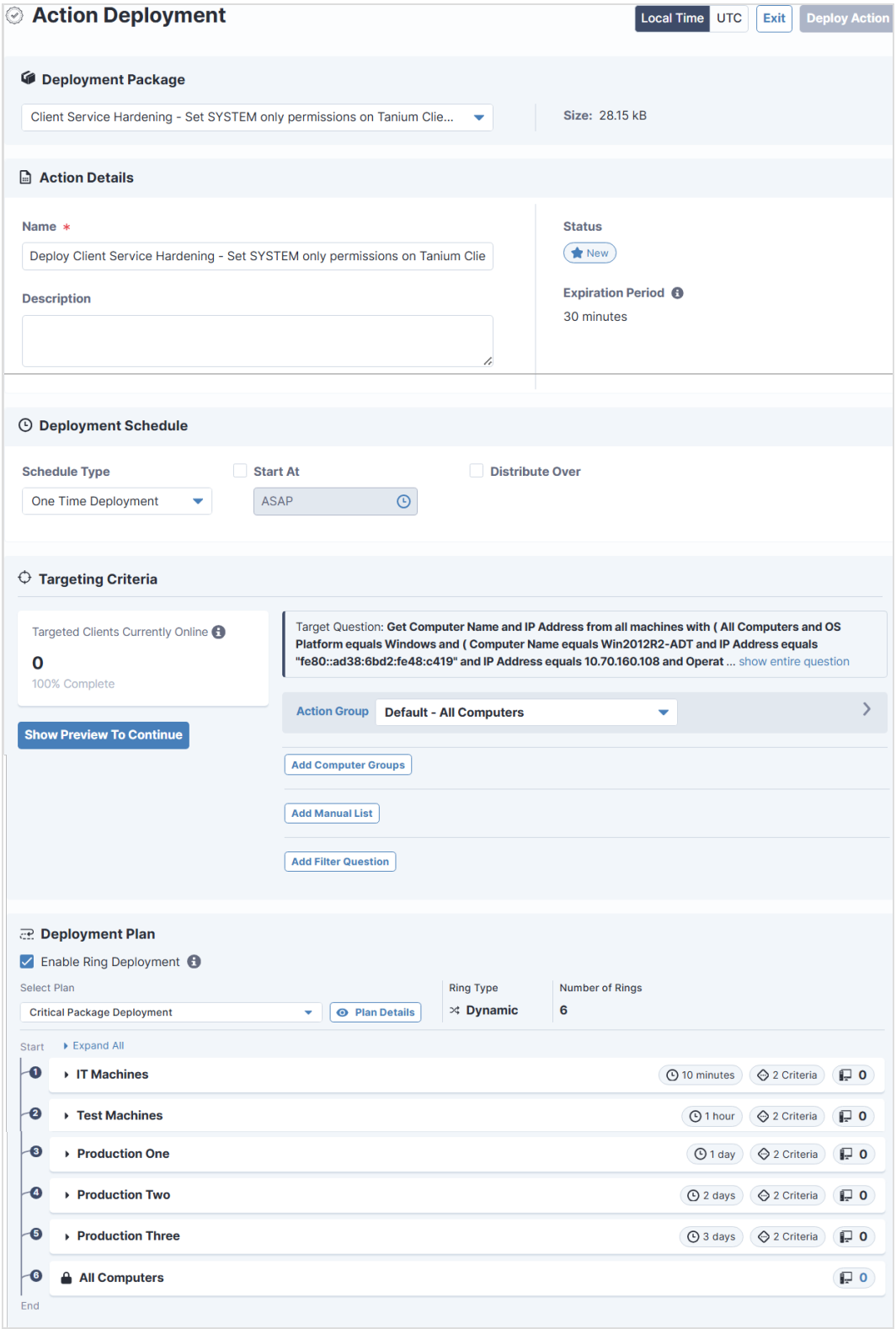
3. Configure the action settings.

TIP

When the action first deploys, some endpoints might be offline. To ensure that the action deploys to endpoints that come online after the initial deployment, set the **Schedule Type** to **Recurring Deployment** and set the interval (**Re-issue every**) and time period (between the **Start At** and **End At** dates) to appropriate values. For example, you can configure the action to deploy once per day for a month to ensure that all endpoints have a chance to come online.

© 2026 Tanium Inc. All Rights Reserved

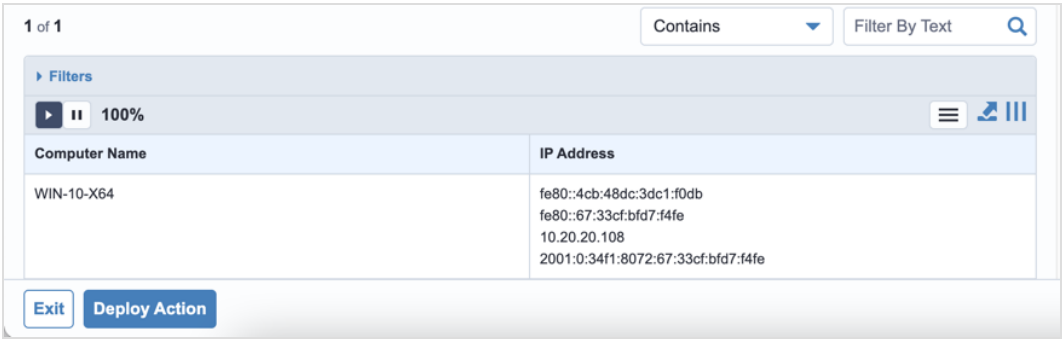
Action settings



© 2026 Tanium Inc. All Rights Reserved

4. Click **Show preview to continue**, review the affected endpoints, and click **Deploy Action**.

   Preview and initiate deployment



> NOTE
>
> If the number of affected Tanium Clients exceeds the threshold that is specified in the **Prompt Estimate Threshold** platform setting, Tanium Console prompts you to confirm the deployment before proceeding.

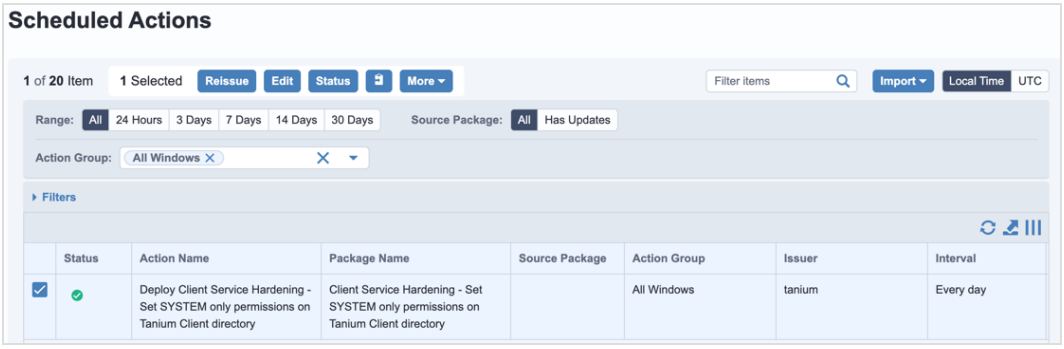
   If the action deploys immediately, a page opens automatically to show the action status. If the action requires approval or has a future start date/time, you can view its status after deployment starts in the **Action History** page or Deployment Details page. For more information, see Monitor actions on page 337.

Monitor actions

Track the status of actions to ensure that they are configured correctly and deploy as expected, and to Troubleshoot actions on page 339 if necessary.

VIEW ACTION STATUS AND SETTINGS

1. If the action does not require approval and deployment starts immediately, skip to the next step. Otherwise, go to **Administration > Actions > Scheduled Actions** and confirm the action is listed.



   Perform the next step after:

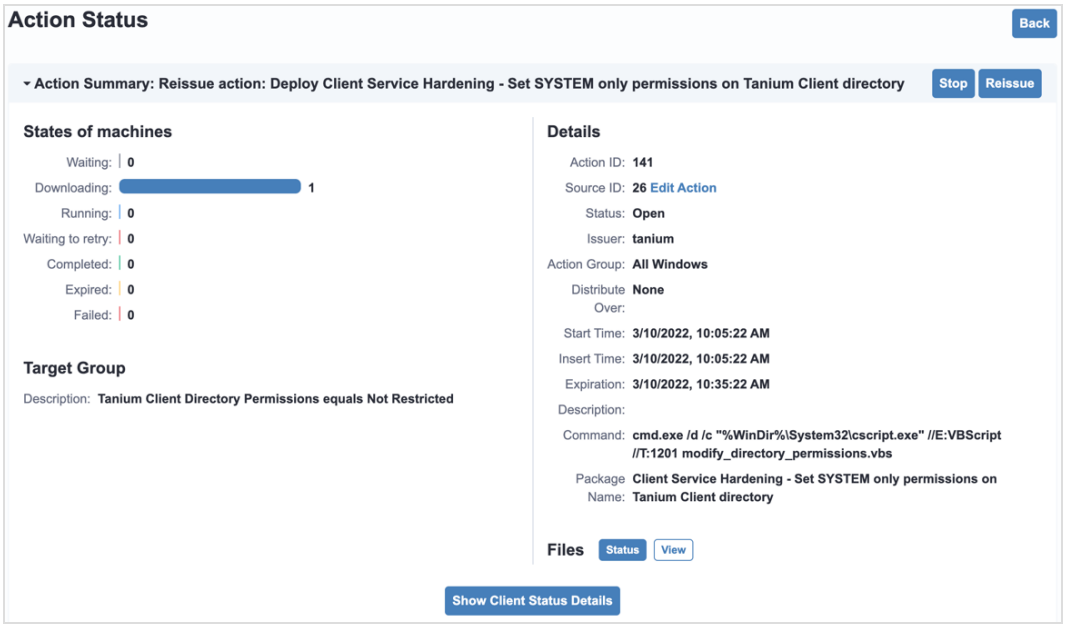
   a. A user approves the action, if approval is required. For more information, see Approve pending actions on page 413.

   b. Deployment starts, if it is scheduled for a future date/time.

© 2026 Tanium Inc. All Rights Reserved

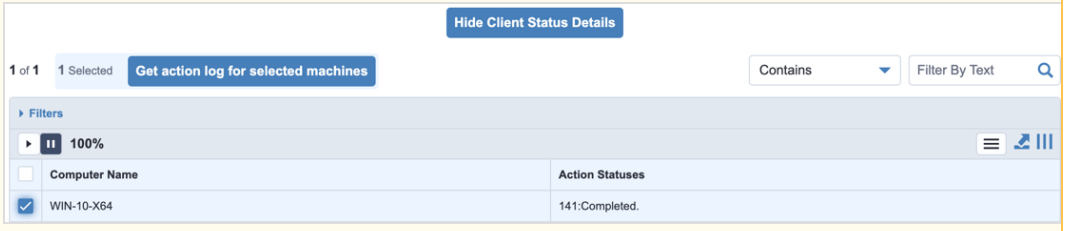
2. Perform one of the following steps based on the type of action:

   - **Adaptive action**: The Deployment Details page opens automatically. For more information, see Analyze and manage a single deployment on page 362.
   - **Simple action**: If the action did not require approval and deployment started immediately, the **Action Status** page opens automatically. After the first (or only) deployment interval, you can also open the **Action Status** page from the **Action History** page, as described in Manage actions that are completed or in progress on page 349. For more information, seeView status for simple actions on page 352.



TIP

The Tanium Client generates action logs to record the command-line interface (CLI) output that is associated with action commands. If you have **Sensor read** permission on the **Client Management** content set, you can display the log records to investigate issues related to an action. To display the records, on the **Action Status** page click **Show Client Status Details**, select up to 50 endpoints in the preview list, and click **Get action log for selected machines**. For more information, see Investigate action-related issues through logs on page 355.



© 2026 Tanium Inc. All Rights Reserved

TROUBLESHOOT ACTIONS

If issues occur during action deployment, the following tasks can help you to troubleshoot. Record the action IDs of the actions that you want to troubleshoot before reviewing logs. The **Action History**, **Scheduled Actions**, and **Action Status** pages all show action IDs. For more information, see Track action IDs on page 355.

For issues on Tanium Clients, investigate:

- **Log messages**:
    - View action logs for multiple endpoints through Tanium Console: see Investigate action-related issues through logs on page 355.
    - View action logs for a specific endpoint: see Tanium Client Management User Guide: Review action logs and associated files to troubleshoot actions and packages.
    - Troubleshoot actions, audit actions, or review action history logs: see Tanium Client Management User Guide: Review action history logs to troubleshoot or audit actions.
- **Action locks**: Verify whether action locks are turned on by issuing the saved question **Clients That Cannot Take Actions - Action Lock On**. For more information, see Issue a saved question on page 466 and Locking down actions on endpoints on page 407.
- **Sensor quarantines**: Verify whether the actions use sensors that are quarantined on the Clients and, if appropriate, remove those sensors from quarantine. For more information, see Manage sensor quarantines on page 433.

For issues on the Tanium Server, investigate:

- **Action deployment issues**: Review action scheduler logs:
    - Tanium Appliance User Guide: Action scheduler log
    - Tanium Core Platform User Guide for Windows Deployments: Action scheduler log
- **Download and caching issues**: Review the following logs:
    - Tanium Appliance User Guide: Tanium Downloader log
    - Tanium Core Platform User Guide for Windows Deployments: Tanium Downloader log
    - Tanium Appliance User Guide: Package download log
    - Tanium Core Platform User Guide for Windows Deployments: Package download log
    - Tanium Appliance User Guide: Package cache cleaner log
    - Tanium Core Platform User Guide for Windows Deployments: Package cache cleaner log

For more information about accessing and reviewing logs, see:

- Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform
- Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform

If the logs indicate package download issues, investigate:

© 2026 Tanium Inc. All Rights Reserved

- **Package files**: Review details about package files associated with the action and, if necessary, re-download the files if they are outdated. For more information, see Re-download package files on page 445.
- **Certificates**: Verify the validity of the certificates that the Tanium Server uses when downloading packages from remote sources. Update the certificates if necessary. For more information, see Enabling authentication between platform servers and remote systems on page 173.

If the logs indicate package caching issues, you can Manage the package file repository on page 711.

© 2026 Tanium Inc. All Rights Reserved

Managing scheduled actions and action history

You can use the **Scheduled Actions** page to view details about actions that are scheduled and use the **Action History** page to view details about actions that are completed or in progress. Both pages enable you to perform administrative tasks for actions, such as redeploying or editing them.



For the user role permissions that are required to manage actions and view action history, see Action management permissions on page 89.

Scheduled actions overview

The Tanium Server creates a scheduled action when you deploy an action from the **Question Results** page and specify a **Start At** date (instead of deploying immediately) or set the **Schedule Type** to **Recurring Deployment**. A scheduled action configuration has the following components:

- Package. For information, see Managing packages for platform actions on page 442.
- Schedule settings, which include start times, end times, reissue intervals, and distribution periods. For information, see Configure action settings on page 395.
- Deploying actions and playbooks in Console and Interact on page 391 that specify which endpoints run the action.

Only simple (non-ring-based) actions can have future start dates or reissue intervals, and only simple actions appear on the **Scheduled Actions** page. To view and manage adaptive (ring-based) actions, see Managing ring deployments on page 359.

The **Action History** page lists scheduled or unscheduled (one-time deployment) actions after they deploy for the first time.

Predefined scheduled actions

Certain Tanium solutions provide scheduled actions that target the **Default** action group, which includes only the **No Computers** computer group. You must assign other action groups to those actions before they can deploy to endpoints. For more information, see Reconfigure action groups that target No Computers on page 405. For information about the action groups for particular solutions, see the user guides for those solutions at https://help.tanium.com.

Scheduled actions with parameterized packages

A parameterized package requires input (parameters) from users before the package can run on endpoints. For more information about parameterized packages, see:

- Example: Parameterized packages on page 508
- Example: Sensor-sourced packages on page 522

For more information about the impact on scheduled actions when a parameterized package configuration is updated, see Scheduled action with parameterized package on page 443.

© 2026 Tanium Inc. All Rights Reserved

Manage scheduled actions

Perform the following steps to manage simple actions that have a future start date or that recur at intervals. To create a new scheduled action, see Deploying actions and playbooks in Console and Interact on page 391.

NOTE

Adaptive actions cannot have future start dates or reissue intervals, and therefore the **Scheduled Actions** page does not list them. If you use the **Action History** page to reissue an adaptive action, the reissued action becomes a simple action, even though its name on the **Scheduled Actions** page is `Ring Deployment (ID: <deployment ID>, Ring Index: <ring index>)`.

BEST PRACTICE

To reduce resource use on the Tanium Server and Tanium Clients, review scheduled actions on a quarterly basis and delete any that are no longer useful or that duplicate other actions. For more information, see Tanium Maintenance User Guide: Review and update scheduled actions.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Actions > Scheduled Actions**.
2. (Optional) To find specific actions, configure any of the following filters.

Filtering options for scheduled actions

Filter by	Description
Text string	Filter the grid by any value text in any column by entering a text string in the **Filter items** field.
Date Range	Filter the grid to display only actions for which the **Next Issue Time** is within a specific future date range, such as the next **24 Hours**. The default **All** means no date range filter is applied.
Source Package	The default **All** specifies that the grid shows all actions regardless if the settings in their associated packages changed after the actions were last issued or saved. To show only actions that have changed package settings, click **Has Updates**. In the **Source Package** column, clicking Update Source Package opens the **Edit Action** page, where you can update the package that is associated with the action. For more information, see Update action packages on page 347.
Action group	Add one or more action groups as a filter by selecting one at a time in the **Select Action Group** drop-down.
Attribute (column)	Expand the **Filters** section, select an action attribute (such as **Issuer**), select an operator (such as **is equal to**), enter an attribute value (such as `Administrator`), and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters. NOTE: The **Status** attribute indicates whether the action is enabled or disabled. For the action status that Tanium Clients report after running an action (such as `Completed` or `Failed`), see View status for simple actions on page 352.

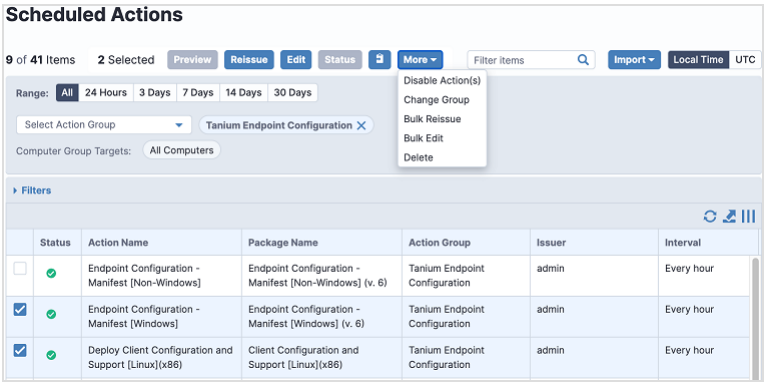
3. Select the actions that you want to manage.

TIP: To export all actions, you can skip this step.

Action buttons for administrative tasks appear above the grid and in the **Source Package** column. The available buttons depend on the row you select. For example, the **Status** column displays a green check mark to indicate enabled actions and a red minus to indicate disabled actions. When you open the **More** dropdown list for an enabled action, the options include **Disable Action**, but not **Enable Action**. If the status column indicated a disabled action, the **More** list would include **Enable Action** but not **Disable Action**.

© 2026 Tanium Inc. All Rights Reserved

Scheduled Actions page



4. Click a button or menu to perform one of the following tasks.

> **NOTE** To stop deploying a scheduled action, you must use the **More** menu to disable or delete it instead of clearing the **Start At** and **Re-issue every** values.

Administrative tasks for scheduled actions

Button / Task	Guideline
Reissue	Opens the **Reissue Action** page, where you can change the name, schedule, and the action group to target before re-issuing the action. For information about these settings, see Deploying actions and playbooks in Console and Interact on page 391. If you selected multiple actions, use the ❮ and ❯ widgets to navigate among the pages for each action. **TIP** To use the same start time and distribution period for multiple actions in a one-time deployment, select **More > Bulk Reissue** instead.
Edit	Opens the **Edit Action** page. The only action settings that you can edit are the time standard (**Local Time**/**UTC**), **Deployment Schedule** settings, and **Action Group** (see Configure action settings on page 395). If you selected multiple actions, use the ❮ and ❯ widgets to navigate among the pages for each action. **TIP** To set the same scheduling values for multiple actions, select **More > Bulk Edit** instead.
Status (Re-download files)	Displays details about any files associated with the action package. You can use this dialog to re-download package files if you encountered issues with outdated files. For more information, see Re-download package files on page 445.

© 2026 Tanium Inc. All Rights Reserved

Administrative tasks for scheduled actions (continued)

Button / Task	Guideline
Copy	Copies information from the selected rows to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the copy. TIP To copy information from an individual cell, hover over the cell, click Options, and click Copy.
More > Enable/Disable Action(s)	Prompts you to enable or disable the action. You can click the name of an action to review its configuration in the **Edit Action** page before clicking **Confirm** to enable or disable it.
More > Change Group	Prompts you to select a new action group for the scheduled action.
More > Copy Action	Prompts you to copy the scheduled action to a new action group. You can copy only one action at a time.
More > Bulk Reissue	For a one-time deployment only, select this option to configure multiple actions with the same values for the following settings, and then re-issue the actions: • **Local Time / UTC** (time standard) • **Start At** date/time • **Distribute Over** period For a description of these settings, see Deploying actions and playbooks in Console and Interact on page 391. NOTE If you bulk reissue multiple recurring actions, the Tanium Server creates copies of the actions with their **Schedule Type** set to **One Time Deployment**. TIP To use a different start time or distribution period for each action, click **Reissue** instead.

© 2026 Tanium Inc. All Rights Reserved

Administrative tasks for scheduled actions (continued)

Button / Task	Guideline
More > Bulk Edit	Select this option to configure multiple actions with the same values for one or more of the following settings. The bulk edit applies only to the settings that you change. • **Local Time / UTC** (time standard) • **Schedule Type** (**One Time Deployment** or **Recurring Deployment**) • **Re-issue every** interval (for recurring deployments) • **Start At** date/time • **End At** date/time • **Distribute Over** period For a description of these settings, see Deploying actions and playbooks in Console and Interact on page 391. TIP To use different values for each action, click **Edit** instead.
More > Delete	Prompts you to delete the selected actions. IMPORTANT Do not delete the predefined scheduled actions that Tanium solutions provide. When you import solution updates, the update process restores any predefined actions that users deleted.
Import	Import actions on page 348.
Local Time / **UTC**	Specify the time standard that the **Scheduled Actions** grid uses to display settings that have date/time values: • **Local Time** (default), which is local to the system that you use to access Tanium Console • **UTC** (Coordinated Universal Time)
Refresh	Manually refresh the **Scheduled Actions** grid.
Export	Export actions on page 347 as a file.
Customize Columns	Select hidden columns to show them in the grid or deselect columns to hide them. Some columns are hidden by default, such as **ID** and **Issue Count**.
Update Source Package	This icon appears in the **Source Package** column only for actions that use a package that was updated after the action was initially created. Clicking the icon opens the action in edit mode to enable updating the package parameters. For more information, see Update action packages on page 347.

© 2026 Tanium Inc. All Rights Reserved

Update action packages

When you update Tanium modules, shared services, or content-only solutions, the Tanium Server imports any packages that are associated with those solutions. After updating solutions, perform the following steps to verify whether any scheduled actions use updated packages and then update the actions.

1. From the Main menu, go to **Administration > Actions > Scheduled Actions** and set the **Source Package** filter to **Has Updates**.
   The grid lists only the actions that have updated packages. Perform the remaining steps for each of those actions.
2. In the **Source Package** column, click Update Source Package  to edit the action.
3. Perform one of the following sub-steps in the **Deployment Package** section:
   - If Tanium Console shows the original parameters, click **Update Source Package** and enter the new values.
   - If Tanium Console shows the message, `Original package parameters cannot be displayed`, you must leave the **Edit action** page to review the original parameters:
     a. Go to **Administration > Actions > Action History**, select an instance of the action that deployed before the package update, click **Status**, and review the package **Command**. The **Command** value shows the original parameters.
     b. Repeat the previous steps to edit the action, click **Click here to continue to use updated package parameters**, and enter the new values.
4. Update other action settings, click **Show Preview to Continue**, and click **Save Action**. For more information, see Configure action settings.

Export actions

Export actions as a file in the format required for your workflow:

- **CSV**
  You can use any application that supports CSV format to display the same action attributes (columns) as the Console **Scheduled Actions** or **Action History** grids show and then customize the display. For example, you can use Microsoft Excel to create charts based on action attributes.
- **JSON**
  You can export multiple action configurations as a JSON file. Exporting configurations is useful if you want to import them into another Tanium environment. For example, you might test actions in a lab environment to ensure that they work as intended before importing the actions into your production environment. You must be assigned a role with the **Export Content** permission to export a JSON file. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.

  The export file excludes non-recurring actions that are in progress or expired.

Perform the following steps to export actions:

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Actions** and select **Scheduled Actions** or **Action History**.
2. (Optional, CSV exports only) To add or remove attributes (columns) for the CSV file, click Customize Columns in the grid and select the attributes.
3. Select rows in the grid to export only specific actions. If you want to export all actions, skip this step.
4. Click Export.
5. (Optional) Edit the default export **File Name**.

   NOTE

   The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.
6. Select an **Export Data** option: **All** actions in the grid or just the **Selected** actions.
7. Set the file **Format** to JSON (**Administrator** reserved role only) or CSV.
8. Click **Export**.
   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

Import actions

Importing is useful if you want to copy action configurations from another Tanium environment. For example, you might test custom actions in a lab environment to ensure that they work as intended. You can then export the actions from the lab environment and import them into your production environment. You can import actions and other content as a JSON or XML file.

You must be assigned a role with **Import Signed Content** permission to import content files.

1. (Non-Tanium-provided content only) Digitally sign the content file and ensure a public key is in place to validate the signature. For more information, see Authenticating content files on page 482.

   NOTE

   You do not have to generate keys or signatures for Tanium-provided solutions. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process.

   If you plan to import a file that another user signed, you can first perform an integrity check on the file. For more information, see Verify content file signatures on page 487.
2. From the Main menu, go to any of the following **Administration** pages:
   - **Configuration > Solutions**
   - **Permissions > Filter Groups**
   - Under **Content**, select **Sensors**, **Packages**, or **Saved Questions**
   - Under **Actions**, select **Scheduled Actions**, **All Pending Approvals**, or **Actions I Can Approve**

© 2026 Tanium Inc. All Rights Reserved

3. Select an **Import** option based on the source of the content:
    - **Import > Import Files**: Perform one of the following steps to select one or more files:
        - Drag and drop files from your file explorer.
        - Click **Browse for File**, select the files, and click **Open**.
    - **Import > Import URL**: Enter the URL in the **Import URL** field, and click **Import**.
4. For each file, expand  the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts on page 135.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, **Include content set overwrite** is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Install**.

Manage actions that are completed or in progress

The **Action History** page provides a chronology of actions that are in progress or completed. The page shows only actions that have been approved (if approval is required) and have deployed at least once in the last 30 days. You can use the page to show action details (such as status and issuer), display action log data, stop actions that are in progress, and reissue actions.

1. From the Main menu, go to **Administration > Actions > Action History**.
   The page displays the **Status** of each action:
    - `Open`: The time window for the action has not expired. For more information about how the expiration is determined, see Deploying actions and playbooks in Console and Interact on page 391.
    - `Closed`: The time window has expired. If an action is reissued, the grid displays a new row based on the new start time.
    - `Stopped`: A user stopped the action.



For the action status that Tanium Clients report after running an action (such as `Completed` or `Failed`), see View status for simple actions on page 352.

For each action, the **Computer Groups** column displays the number of computer groups in the targeted action group and whether they use Boolean AND or OR combination logic. For more information about the combination logic, see Targeting actions through action groups on page 400. To display a tooltip that lists the computer group names, hover over the entry in that column.

© 2026 Tanium Inc. All Rights Reserved

2. (Optional) To find specific actions, configure any of the following filters:

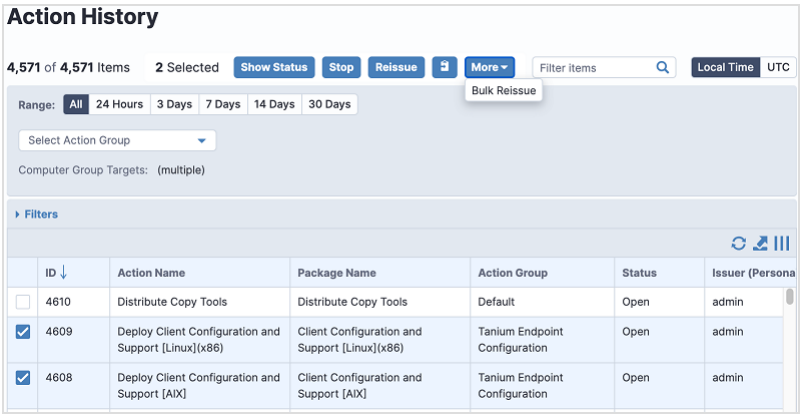
Filtering options for actions that are completed or in progress

Filter by	Description
Text string	Filter the grid by any value text in any column by entering a text string in the **Filter items** field. The filter also applies to the names of computer groups in the targeted action group. TIP You can filter the grid to show only adaptive actions by entering a string that reflects their naming convention: `Ring Deployment (ID: <deployment ID>, Ring Index: <ring index>)`. To see additional details and perform additional management tasks for an adaptive action, append its `ID` value to the URL of the **Ring Deployment Status** page, as described in Analyze and manage a single deployment on page 362.
Date Range	Filter the grid to display only actions for which the **Start Time** is within a specific past date range, such as the last **24 Hours**. The default **All** means no date filter is applied.
Action group	Add one or more action groups as a filter by selecting one at a time in the **Select Action Group** drop-down.
Attribute (column)	Expand the **Filters** section, select an action attribute (such as **Issuer**), select an operator (such as **is equal to**), enter an attribute value (such as `Administrator`), and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.

3. Select the actions that you want to manage.

TIP
To export all actions, you can skip this step.

Action History page



© 2026 Tanium Inc. All Rights Reserved

4. Click a button to perform one of the following tasks.

Administrative tasks for action history

Button / Task	Guideline
Show Status	Display the **Action Status** page to see additional status details, view information from action logs, or edit the package that is associated with the action. For more information, see View status for simple actions on page 352.
Stop	Stop the action if its **Status** is `Open`.
Reissue	Displays the **Reissue Action** page, where you can change the name, schedule, and the action group to target before reissuing the action. For more information about these settings, see Configure action settings on page 395. If you selected multiple actions, use the and widgets to navigate among the pages for each action. TIP To set the same start time and distribution period for multiple action in a one-time deployment, select **More > Bulk Reissue** instead.
Copy 	Copies information from the selected rows to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the copy. TIP To copy information from an individual cell, hover over the cell, click Options , and click Copy .
More > Bulk Reissue	For a one-time deployment only, select this option to configure multiple actions with the same values for the following settings, and then re-issue the actions: • **Local Time / UTC** (time standard) • **Start At** date-time • **Distribute Over** period For a description of these settings, see Configure action settings on page 395. NOTE If you bulk reissue multiple recurring actions, the Tanium Server creates copies of the actions with their **Schedule Type** set to **One Time Deployment**. TIP To use a different start time or distribution period for each action, click **Reissue** instead.

© 2026 Tanium Inc. All Rights Reserved

Administrative tasks for action history (continued)

Button / Task	Guideline
Local Time / **UTC**	Specify the time standard that the **Action History** grid uses to display settings that have date-time values: • **Local Time** (default), which is local to the system that you use to access Tanium Console • **UTC** (Coordinated Universal Time)
Export 	The steps to export actions from the **Action History** page are the same as from the **Scheduled Actions** page except that your user account requires the **Administrator** reserved role to export the actions as a JSON file. For more information, see Export actions on page 347.

View status for simple actions

The **Action Status** page displays details about simple actions that are completed or in progress, and enables you to:

- Edit action settings: Click **Edit Action** beside the **Source ID**. For more information, see Configure action settings on page 395.
- Re-download package files on page 445 associated with an action: Click **Status** beside **Files**.
- View the Managing packages for platform actions on page 442 of the package that is associated with the action: Click **View** beside **Files**.
- Investigate action-related issues through logs on page 355: Click **Show Client Status Details**, select up to 50 endpoints in the preview list, and click **Get action log for selected machines**.



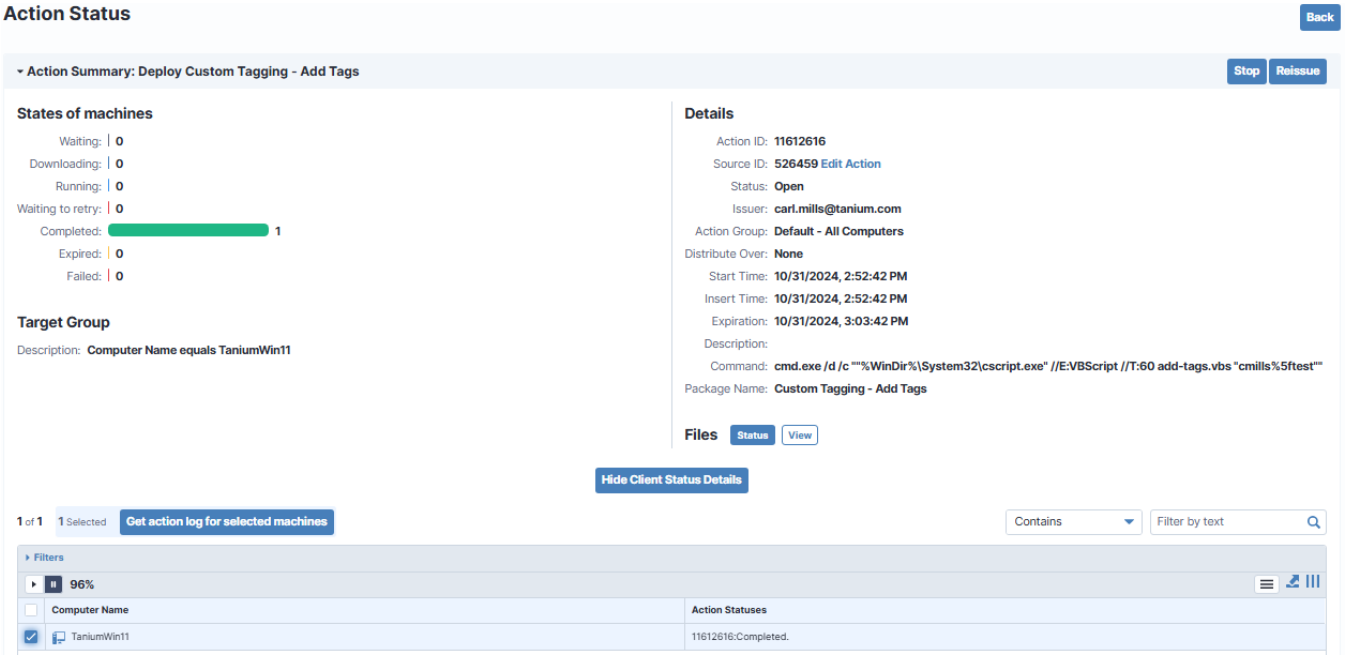
The **Action Status** page uses the same naming convention for adaptive actions as the **Action History** page, as described in Before you begin on page 362. Use the **Ring Deployment Status** page to view the status of adaptive actions, as described in Analyze and manage a single deployment on page 362.

The **Action Status** page shows accurate values for the **States of machines** (action status on endpoints) only for actions that deployed in the last 7 days. The state counts all show as `0` for actions that deployed before that timeframe.

The **Action Status** page opens automatically when you deploy an action immediately instead of setting a **Start At** date-time in the action configuration. For any scheduled action that has deployed at least once, you can also open the page from the **Administration > Actions > Action History** page by selecting an action and clicking **Show Status**. If you select multiple actions, the **Action Status** page displays a separate **Action Summary** for each action.

© 2026 Tanium Inc. All Rights Reserved

Action Status page



Action states

The Tanium Client reports the following states when it receives a simple action that targets the Client. You can monitor the progression of an action through these states in the **Action Status** page.

> NOTE
>
> The *action timeout* controls several action states. The Tanium Server calculates the timeout relative to the moment when you deploy the action or, if approval is required, a user approves the action. the Server calculates the timeout by adding the expiration period to the time when the action starts. All targeted Clients then receive the same calculated timestamp from the Server. For more information about the expiration period, see Configure action settings.

Action states for simple actions

Action State	Description
Waiting	This is the initial state of an action that has a non-zero Distribute Over on page 396 value. If **Distribute over** is zero, the action skips the **Waiting** state. An action in the **Waiting** state waits for a random amount of time up to the **Distribute over** value before proceeding to the next state.
Downloading	The Client is downloading package files if the action requires them. Otherwise, the Client skips the **Downloading** state and enters the **Running** state. An action in the **Downloading** state proceeds to the next state when one of the following events occurs: • The Client finishes downloading the files before the action timeout: The next state is **Running**. • The Client reaches the action timeout before finishing the download: The next state is **Expired**.

© 2026 Tanium Inc. All Rights Reserved

Action states for simple actions (continued)

Action State	Description
Running	The Client is running the Command on page 448 that is configured in the associated package. The action proceeds to the next state when one of the following events occurs: • The command finishes executing before the action timeout: The next state is **Completed**. • The command reaches the action timeout before finishing execution: The command terminates and the next state is **Expired**. • The command runtime reaches the **Command Timeout** before the action timeout and before the command finishes execution: The command terminates and the next state is **Failed**. • The command execution fails before any timeout (for example, the Client might fail to spawn a new process to run the command): The next state is **Failed**.
Completed	The command finishes executing. This state applies regardless of whether the command produced the expected results. For example, a command might finish executing but generate errors. If the package specifies Verification Exit Codes on page 444 or a Verification Query on page 444 (to verify the results), the next state is **Pending Verification**. Otherwise, **Completed** is the final state.
Expired	This is the final state if the Client reaches the action timeout before finishing one of the following processes: • Command execution • Package file downloads
Failed	The action enters this state if one of the following events occurs: • The command execution fails before the action timeout or command timeout • The command reaches the **Command Timeout** before the action timeout and before completing execution • The command completes execution but the Client does not report **Verification Query** results before the query timeout **Failed** is a final state.
Pending Verification	The action proceeds from the **Completed** state to the **Pending Verification** state if the associated package specifies Verification Exit Codes or a Verification Query. The Client then performs the verification to determine whether the package ran successfully: • **Yes**: The next state is **Verified**. • **No**: The next state is **Failed Verification**.
Verified	The action proceeds from the **Completed** state to the final **Verified** state if the associated package specifies Verification Exit Codes on page 444 or a Verification Query on page 444 and the verification indicates success.
Failed Verification	The action proceeds from the **Completed** state to the final **Failed Verification** state if the associated package specifies Verification Exit Codes on page 444 or a Verification Query on page 444 and the verification does not indicate success.

© 2026 Tanium Inc. All Rights Reserved

Investigate action-related issues through logs

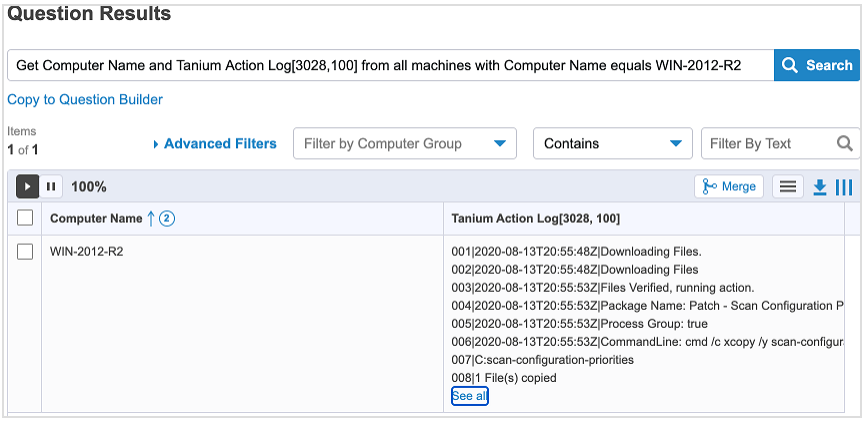
The Tanium Client generates action logs to record the CLI output associated with action commands. You can display the log records to investigate issues related to an action. To display the records, you require the **Sensor read** permission on the **Client Management** content set. Perform the following steps to display the log records for an action.

For additional troubleshooting tasks related to actions, see Troubleshoot actions on page 339.

1. From the Main menu, go to **Administration > Actions > Action History**, select an action, and click **Show Status** to open the **Action Status** page.
2. Click **Show Client Status Details**, select up to 50 endpoints in the preview list, and click **Get action log for selected machines**.

   The Tanium Server then issues the question `Get Computer Name and Tanium Action Log[<action_ID>, 100] from all machines with (Computer Name equals <computer_name>)` through the Interact **Ask a Question** field. Clients that ran the action respond with the first 100 lines of the corresponding action log. Clients that did not run the action respond with `Error: Cannot read Action_<ID>.log`.

   Question results for action log



Track action IDs

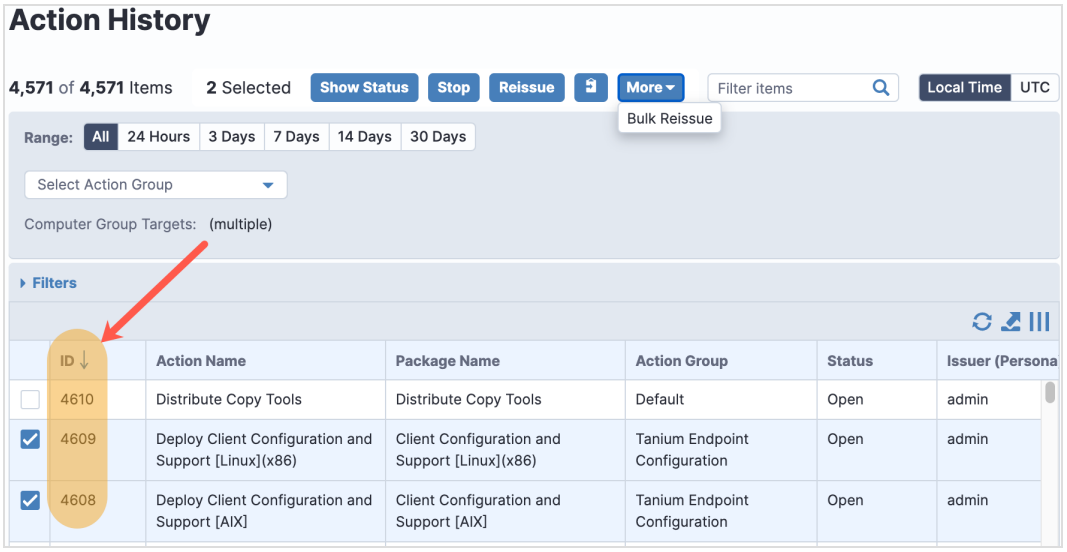
The Tanium Server assigns an action ID to each action that you deploy. Knowing the ID is useful when you want to see details about an action. For example, to investigate unexpected outcomes related to actions (such as package scripts that failed to run), you can use action IDs to find and review actions logs and action history log entries. Tanium Console displays action IDs in multiple places.

© 2026 Tanium Inc. All Rights Reserved

View action IDs on Tanium Console

- **Action History page**: For actions that have deployed at least once, go to **Administration > Actions > Action History** and view the action **ID** column.

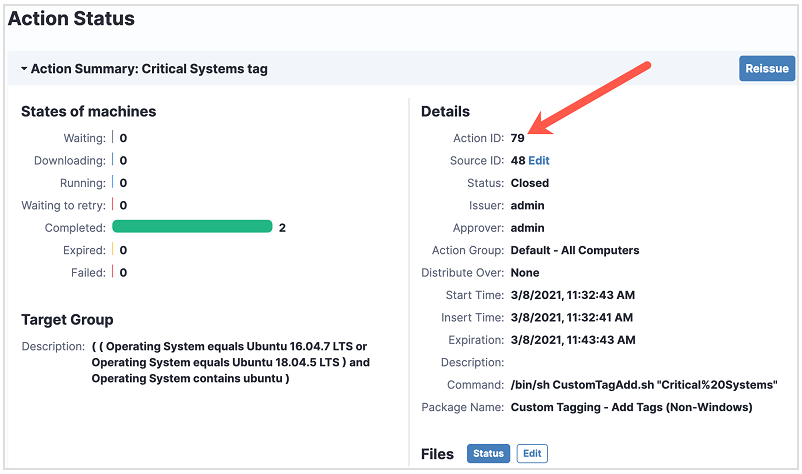
  Action ID on the Action History page



- **Scheduled Actions page**: For actions that are recurring or have a future start date, go to **Administration > Actions > Scheduled Actions** and view the **ID** column, which is hidden by default. To show the column, click Customize Columns and select **ID**.

- **Action Status page**: The **Action Status** page displays the **Action ID** in the **Details** section. For more information, see View status for simple actions on page 352.

  Action ID on the Action Status page



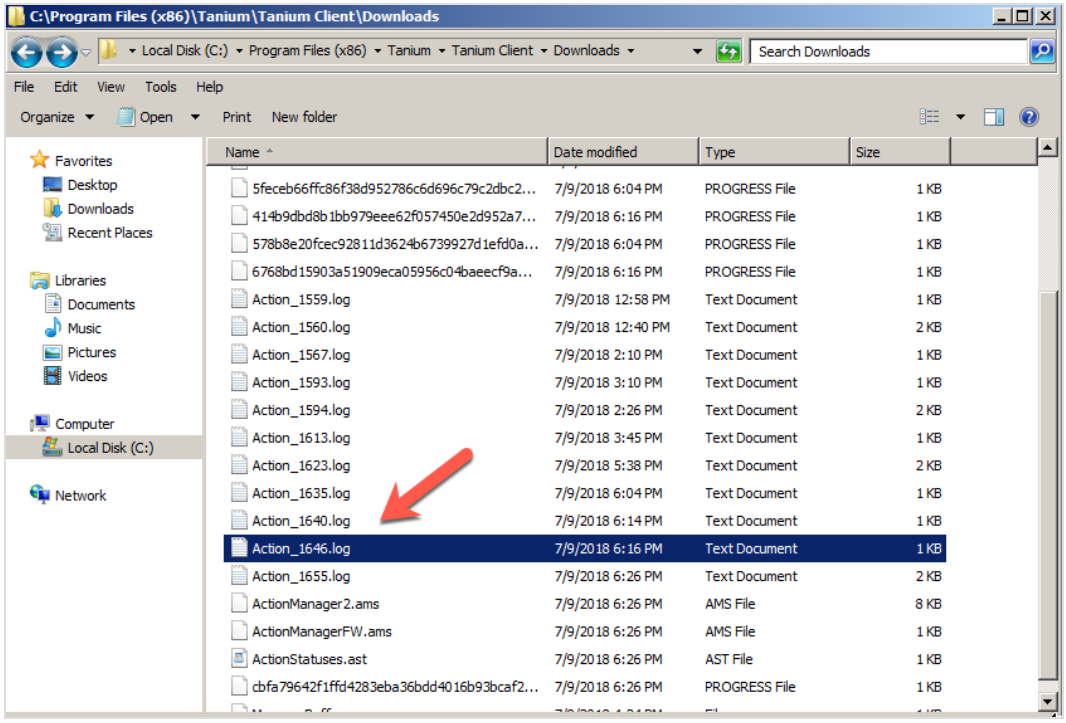
© 2026 Tanium Inc. All Rights Reserved

Navigate Tanium Client logs by action IDs

On managed endpoints, the Tanium Client displays action IDs in log files. In the following file paths, *<Tanium Client>* represents the Tanium Client installation directory.

- **Action logs**: In the `<Tanium Client>\Downloads` folder, each action log contains the associated action ID in its file name. For more information, see Tanium Client Management User Guide: Review action logs and associated files to troubleshoot actions and packages.

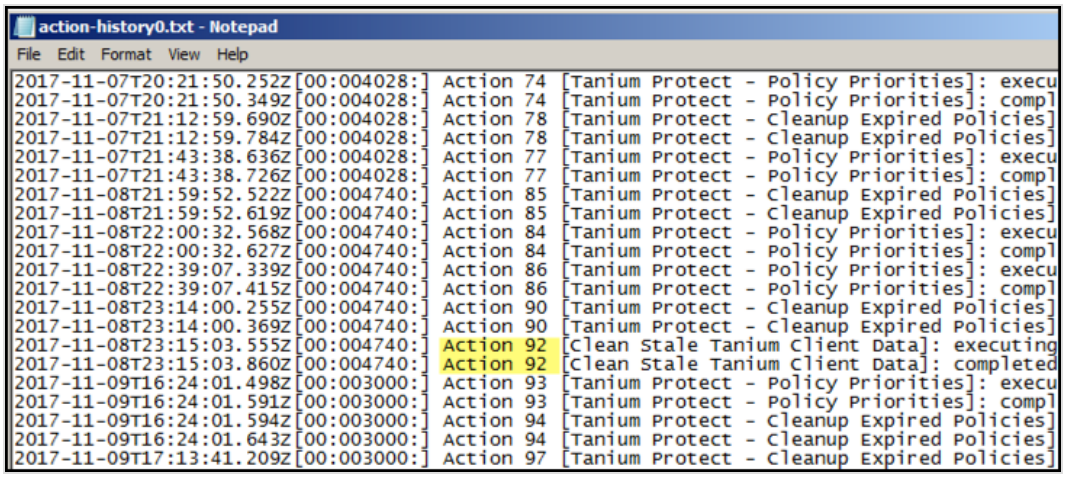
  Action ID in action log file name



- **Action history logs**: In the `<Tanium Client>\Logs` folder, action history logs identify actions by their IDs in the log contents. For more information, see Tanium Client Management User Guide: Review action history logs to troubleshoot or audit actions.

© 2026 Tanium Inc. All Rights Reserved

Action ID in action history log



© 2026 Tanium Inc. All Rights Reserved

Managing ring deployments

The **Ring Deployment Status** page shows action status and other deployment details that you can use to monitor and troubleshoot adaptive (ring-based) actions. The page also provides management options that you might use while monitoring or troubleshooting. For example, you can pause a deployment that is producing unexpected results or investigate the results by issuing questions through Tanium Interact. The page provides these details and options only for adaptive actions that meet the following conditions:

- A deployment plan is assigned to the action. For more information, see Managing deployment plans for ring deployments on page 384.
- The action is currently deploying or has completed in the last 30 days.
- The user account or persona that you use for the current Tanium session has Role permissions for managing deployments on page 359.

The page includes actions for all the Deployment types on page 277 that users deployed manually or that Tanium solutions deployed automatically. For an overview of adaptive action deployments, see Ring-based deployment on page 276.



To view and manage simple (non-ring-based) actions, see Managing scheduled actions and action history on page 341.

Role permissions for managing deployments

The **Ring Deployment Status** page shows data only from endpoints in computer groups that are assigned to the user account or persona of your current Tanium session.

To view and manage adaptive actions, you require the user role permissions for viewing and managing the deployment plans that are assigned to the actions, as described in Manage deployment plans on page 91. You require additional permissions for the following deployment types. For all types, read permission enables viewing the deployments and write permission enables performing management tasks on them, such as pausing or stopping.

- Tanium platform and Tanium Guardian deployments

  The platform content permission **Action read/write** is required on the content sets of the deployments. For more information, see Interact permissions on page 81.
- Tanium Deploy (software) deployments

  The solution permission **Deploy Deployment read/write** is required on the content sets of the deployments. For more information, see Tanium Deploy User Guide: User role requirements.

Analyze multiple deployments

The **Ring Deployment Status** page shows basic information about all ring-based deployments. Use the page to track the status of deployments, verify that they run on endpoints as expected, and troubleshoot any issues. For example, you can investigate why certain deployments are in a **Failed** state. From the **Ring Deployment Status** page, you can open the Deployment Details page

© 2026 Tanium Inc. All Rights Reserved

for any single deployment to view comprehensive details and to perform management or investigation tasks.

1. From the Main menu, go to **Administration > Actions > Ring Deployment Status**.
   The page lists deployment details in a grid. For more information, see Deployment details on the Ring Deployment Status page on page 360.
2. (Optional) Use the display options to find deployments that match filter criteria and to show or hide grid columns. For more information, see Use display options on the Ring Deployment Status page on page 361.
3. (Optional) Click the **Name** of a specific deployment to view its full details and to access management and investigation options. For more information, see Analyze and manage a single deployment on page 362.

Deployment details on the Ring Deployment Status page

The **Ring Deployment Status** page shows the following basic details about all the listed deployments. View the details to determine if a deployment needs investigation or troubleshooting.

Ring Deployment Status page: basic details for all deployments

Information	Description
Deployment details	The following columns show details about the latest deployment for each action: • **Deployment Status**: For details on each status, see Deployment status on page 381. • **Ring Progress**. This column shows how far the action has progressed in the ring set. For example, the value `3 of 5` indicates that the ring set has 5 rings and that the action is deploying to ring 3 or is stuck in ring 3. An action might be stuck in a ring due to any of the causes described in Ring status on page 382. • **Endpoints Completed**: This is the number of endpoints that finished running the action (regardless of success or failure) in the current ring (for deployments in progress) or the last ring (for completed deployments). • **Start Time**: This is the date and time when the deployment started in the first ring. • **End Time** (hidden by default): This is the date and time when the deployment ended in the last ring.
Action settings	The following columns show basic settings for all the listed deployments. • **Name**: Click the name of an action to view all the details for its current or last deployment. For more information, see Analyze and manage a single deployment on page 362. • **Type**: Shows the type of deployment, as described in Deployment types on page 277. You can sort the grid by type. • **Content Set** (hidden by default): Shows the content set to which the deployment is assigned. When you configure a deployment, it defaults to the content set of the content that the action deploys, such as a Tanium platform package or Tanium Deploy software package.

© 2026 Tanium Inc. All Rights Reserved

Ring Deployment Status page: basic details for all deployments (continued)

Information	Description
Audit details	The following columns show details that are useful for auditing actions. • **Issuer**: This is the user who initiated the current or last deployment, either through the default persona (user account) or an alternative persona. The value is **Tanium** for Tanium-managed actions that Tanium solutions deploy automatically. • **Creation Time** (hidden by default): This is the date and time when a user created the action.

Use display options on the Ring Deployment Status page

Use the following options to control the display of actions on the **Ring Deployment Status** page. For example, you can use filters to find specific deployments.

> NOTE
>
> Tanium Console preserves your filter selections for the current Tanium session if you navigate to a different Console page and then return to the **Ring Deployment Status** page.

Display options on the Ring Deployment Status page

Filter option	Description
Failed	The page shows a banner with the count of failed deployments if any exist. Click the count to set the **Deployment Status** filter to **Failed**.
Deployment Status	Select one or more deployment states. For descriptions of the states, see Deployment status on page 381.
Issued by Me	Select this checkbox to show only deployments that you issued through the user account of your current Tanium session. This filter includes deployments that you issued through a persona that is assigned to your account, even if you have not selected that persona for the current session.
Advanced Filters	Expand the **Filters** section and select options in one or more of the following dropdown lists to filter the grid based on the selected attribute values: • **Type**: Select the Deployment types on page 277 of the actions. • **Issuer**: Select the users who deployed the actions. If a user deployed actions through an alternative persona, this filter includes those deployments. This filter appears only to users who have the **User read** role permission. • **Content Set**: Select the content sets to which the actions are assigned.
Filter by Name	Enter a text string that contains part or all of an action name to filter the grid by that string.
Columns	Click Customize Columns and select or clear the checkboxes of the columns (deployment attributes) that you want to show or hide. You can also change the order of columns by dragging them. Some columns are hidden by default, such as the **End Time**.

© 2026 Tanium Inc. All Rights Reserved

Analyze and manage a single deployment

The Deployment Details page shows all the information about a single deployment and enables you to perform management tasks, such as pausing a deployment or investigating action status through Interact.

Before you begin

ACCESS THE DEPLOYMENT AS THE CREATOR

For all deployment types, the Deployment Details page shows the counts of targeted endpoints across all rings and in specific rings. However, if a Tanium platform deployment has not started in one or more rings, the counts for those rings are visible only if your current Tanium session matches the user account (default persona) or alternative persona that created the deployment. To see endpoint counts for all rings regardless of the state of a platform deployment, perform the following steps to determine which user or persona created the deployment and then switch to that user or persona before opening the Deployment Details page.



In rings where a Tanium platform deployment has started or finished, endpoint counts are visible to any user account or persona that has RBAC permissions to view the deployment. In all rings of a Deploy (software) deployment, endpoint counts are visible to any user account or persona that has RBAC permissions to view the deployment regardless of the deployment state.

1. From the Main menu, go to **Administration > Actions > Ring Deployment Status**.

   To filter the grid to find a particular deployment, see Display options on the Ring Deployment Status page on page 361.

2. Check the **Issuer** (creator) column for the deployment.
3. Perform one of the following steps:
   - Sign in to Console on page 49 as the user who created the deployment, regardless of which persona that user used to create the deployment.
   - Switch to the persona that another user used to create the deployment, as described in Select a persona for your Console session on page 663.

DETERMINE THE DEPLOYMENT ID

You must know the action name or deployment ID for a deployment to find it on the **Ring Deployment Status** page and open the corresponding Deployment Details page. Perform the following steps only if you do not know the action name for a deployment because you found it on the **Action History** page. That page show a unique entry for each ring where the action finished deploying successfully. The **Action Name** column on the **Action History** page uses the following convention to identify adaptive actions instead of showing their actual names: `Ring Deployment (ID: <deployment ID>, Ring Index: <ring index>`. Each action deployment has a unique deployment `ID`, but the `ID` is the same for all the rings of a single deployment. The `Ring Index` value is the ring number.

© 2026 Tanium Inc. All Rights Reserved

NOTE

If you use the **Action History** page to reissue an adaptive action, the reissued action becomes a simple action, even though its name retains the convention of an adaptive action. You can view and manage simple actions only through the **Action History** or **Scheduled Actions** page, as described in Managing scheduled actions and action history on page 341.

1. From the Main menu, go to **Administration > Actions > Action History**. For the steps to find specific actions on this page, see Manage actions that are completed or in progress on page 349.
2. Copy or record the deployment `ID` value from the **Action Name** column. You need the `ID` to perform the steps in Analyze, investigate, or manage a single deployment on page 363.

Analyze, investigate, or manage a single deployment

Perform the following steps to view all the details about a single deployment , to manage it, or to explore its target endpoints.

1. From the Main menu, go to **Administration > Actions > Ring Deployment Status**.

   TIP

   To filter the grid to find a particular deployment, see Display options on the Ring Deployment Status page on page 361.

2. Click the action **Name** to open the Deployment Details page. If you do not know the action name but you know the deployment ID from the **Action History** page, append the ID to the URL of the **Ring Deployment Status** page. For example, if the **Action History** page identifies the deployment as `Ring Deployment (ID: 35a0555e-5bcd-4c26-85b0-9dcb6b2368ae, Ring Index: 3)`, enter the URL `https://<Tanium Server>/ui/console/ring-deployment-status/35a0555e-5bcd-4c26-85b0-9dcb6b2368ae` to open the Deployment Details page for that deployment.
   The title of the Deployment Details page is the action name.
3. (Optional) Perform any necessary management tasks if the deployment requires intervention or troubleshooting.

Deployment management tasks

Field/Widget	Description
View in Deploy	(Tanium Deploy deployments only) Click the link to open a new browser tab that shows the deployment details in the workbench of the Tanium solution that initiated the deployment. For example, clicking **View in Deploy** opens the deployment summary page of the Deploy workbench.
Stop Pause Resume	You can stop or pause an action if deployment has started, or resume the deployment if it is paused. For details, see Stop, pause, or resume deployments on page 375.
Reissue	This button appears only for Tanium platform deployments. Click the button to open the **Reissue Action** page, where you can optionally change several action settings and then start a new deployment. For more information, see Reissue deployments on page 376.

© 2026 Tanium Inc. All Rights Reserved

Deployment management tasks (continued)

Field/Widget	Description
Options	A banner shows the message `Needs Attention: Ring <number> Progression Criteria Not Met` if the target endpoints in the current ring did not meet the criteria for progressing to the next ring. The banner shows the minimum (**Target**) values that are required to progress and the actual values that endpoints reported. You can select one of the following **Options**: • **Retry Ring** (Tanium platform actions only): First resolve the progression criteria failures that occurred in the initial deployment attempt. Then click **Retry Ring** to reattempt the deployment in the current ring. For more information, see Retry a deployment in one ring on page 378. • **Start Next Ring**: Override the progression criteria and progress the deployment to the next ring. For more information, see Manually progress deployments through rings on page 377. • **View Failed Ring**: This option takes you to the Deployment Plan Status on page 366 section, which shows details about the ring where endpoints failed to meet the progression criteria.

4. Use the fields and widgets in the following sections of the Deployment Details page to review the deployment, explore the target endpoints, and perform additional management tasks.

   - Summary on page 364
   - Deployment Plan Status on page 366
   - Ring Progression Failures on page 370
   - Endpoint Details on page 370

Summary

On the Deployment Details page, the **Summary** section shows basic information about the deployment. For platform deployments, the section also provides buttons for viewing details about the package that the deployment runs on endpoints.

Deployment Details page: Summary section

Field/Button	Description
Status	Shows the Deployment status on page 381 up to the current or last completed ring.
Issued By	Identifies the user who initiated the deployment through the default persona (user account) or an alternative persona.

© 2026 Tanium Inc. All Rights Reserved

Deployment Details page: Summary section (continued)

Field/Button	Description
Endpoints Targeted	Shows the total count of targeted endpoints across all rings. For Tanium platform deployments, the count is visible only to the user account (default persona) or alternative persona that was used to create the deployment. For all deployment types, the deployment state determines which endpoints the count includes: • **Deployments in progress**: The count includes all endpoints that match the targeting criteria. • **Completed deployments**: The count includes only the endpoints that attempted the action, regardless of whether the action finished successfully. The count excludes endpoints that did not attempt the action even if they were assigned to rings. For example, the count excludes endpoints that were offline throughout the deployment. For a deployment in progress, you can click the count to issue an Interact question that lists the computer names of all the targeted endpoints. For a completed deployment, click the count to go to the Endpoint Details on page 370 section of the page. NOTE For details on how the Tanium Server evaluates endpoint targeting at the deployment level and ring level, see Endpoint targeting on page 278.
Deployment Plan	Shows the deployment plan that is assigned to the deployment. Click the plan name to open and optionally edit the plan configuration in a new browser tab. For details about plan configurations, see Deployment plan settings on page 386 and Rings and progression criteria on page 387.
Start	Shows the date and time when the deployment started.
End	If the **End** has a value, it indicates when one of the following events occurred: • Tanium platform deployments only: The deployment completed. • Tanium Deploy (software) deployments only: The deployment has progressed to the final **All Targeted Computers** ring. • Any deployment type: ◦ The deployment stopped due to errors. ◦ A user paused the deployment. A blank **End** indicates one of the following states: • Platform deployments only: The deployment is in progress. • Deploy (software) deployments only: The deployment has not progressed to the final **All Targeted Computers** ring.

© 2026 Tanium Inc. All Rights Reserved

Deployment Details page: Summary section (continued)

Field/Button	Description
Expiration	Shows the deployment expiration date and time, which is 90 days after the deployment starts. If the deployment expires after starting in a ring, it continues deploying to endpoints in that ring but does not progress to the next ring. NOTE The deployment expiration is distinct from the action **Expiration Period**, which determines the Action runtime on page 295.
Endpoint Status	This section shows the following metrics: • ***<Endpoint count> <status>***: This is the count of endpoints that returned each action status across the current ring and prior rings. Hover over the chart to see the percentage of endpoints that returned a particular status. For more information, see Action status on endpoints on page 380. • **Retried Rings: *<#>*** (Tanium platform actions only): This count indicates the number of rings for which users have retried the deployment because it failed progression criteria in the initial attempt. Hover over the count to see the number of attempts for each ring, including the initial attempt. For more information, see Retry a deployment in one ring on page 378.
View Package File Status	This button is available only for Tanium platform actions. Click it to view the status and other details for each package file, and re-download the files if necessary. For more information, see Re-download package files on page 445.
View Package Files	This button is available only for Tanium platform actions. Click it to view details about the files and other settings of the package that the action deploys, as described in Managing packages for platform actions on page 442. The **Preview Package** page shows the settings in a new browser tab.

Deployment Plan Status

On the Deployment Details page, the **Deployment Plan Status** section shows information about the rings through which the action progresses, as defined in the deployment plan.

The ring set pane lists the names of all the rings and numbers them according to the deployment sequence. The icon beside each ring name indicates the Ring status on page 382. If users retried a ring, you can hover over Ring Retries to view details about all the attempts to deploy in that ring. For more information, see Retry a deployment in one ring on page 378.

The following sections describes the information that the ***<ring name>*** pane shows when you select a ring in the ring set:

- Attempt (platform actions only) on page 367
- Endpoint count on page 367
- Message banner on page 367
- Ring Details on page 368

© 2026 Tanium Inc. All Rights Reserved

- Endpoint Execution Status on page 368
- Progression Criteria on page 369
- Includes Deferred Endpoints on page 370

If your browser window is too narrow to view all the contents of the ***<ring name>*** pane, you can expand it by collapsing the ring set pane to show only the ring numbers.

ATTEMPT (PLATFORM ACTIONS ONLY)

On the Deployment Details page, the **Deployment Plan Status** section shows an **Attempt** dropdown list only if users have retried the ring after the initial deployment attempt in that ring failed the progression criteria. Select an attempt to see the corresponding ring details or select **All** to see the current status details that resulted from all the attempts. For more information, see Retry a deployment in one ring on page 378.

ENDPOINT COUNT

On the Deployment Details page, the **Deployment Plan Status** section shows the total number of endpoints that are assigned to the ring, minus any Deferred endpoints on page 298. In rings where a Tanium platform deployment has not started, counts are visible only to the user account (default persona) or alternative persona that was used to create the deployment. This limitation does not apply to Deploy (software) deployments.

Click the count to see the Action status on endpoints on page 380 (only for the current or completed rings) and identifying information about the endpoints. The deployment type determines where the information appears:

- Tanium platform

  Click the count to see the information on the Interact **Question Results** page in a new browser tab. To show information for all endpoints that the deployment targets across all rings, select the **All Targeted Computers** ring and click the count.

- Tanium Deploy deployments

  For rings that are in progress or completed, click the count to go to the Endpoint Details on page 370 section of the Deployment Details page. Console automatically filters the section to show information only for endpoints in the ring where you clicked the count. To show information for all endpoints that the deployment targets across all rings, select the **All Targeted Computers** ring and click the count. For rings that have not yet started, clicking the count shows the information on the Interact **Question Results** page as it does for platform deployments.

MESSAGE BANNER

On the Deployment Details page, the **Deployment Plan Status** section shows a banner if one of the following events occurred:

- / `Progression Criteria Not Met`

  The target endpoints in the current ring did not meet the criteria for progressing to the next ring. The following options are available if this occurs:

© 2026 Tanium Inc. All Rights Reserved

    - **Retry Ring** (Tanium platform actions only): First resolve the progression criteria failures that occurred in the initial deployment attempt in the ring. Then click **Retry Ring** to reattempt the current ring. For more information, see Retry a deployment in one ring on page 378.
    - **Start Next Ring**: Click this button to override the progression criteria and progress the deployment to the next ring. After you manually progress the deployment, the Failed icon changes to Warning in the banner and changes to User Approved in the ring set pane.
- `The ring is waiting before starting the progression criteria evaluation.`

  This banner appears if the Wait on page 293 period is in progress. Optionally, click **Skip the Wait** to start the progression criteria evaluation immediately, as described in Skip the wait intervals during deployment on page 378.
- Stopped

  The banner indicates which user stopped the deployment and when.

RING DETAILS

On the Deployment Details page, the **Deployment Plan Status** section shows the following **Ring Details**:

- Ring status on page 382
- **Start Time**: This field shows the date and time when deployment started in the ring or, if users have retried the ring at least once for a Tanium platform action, the field shows when a user initiated the selected Attempt (platform actions only) on page 367. If you set the **Attempt** to **All**, this field shows the start time of the initial attempt.
- **End Time**: This field shows the date and time when deployment ended in the ring or, if users have retried the ring at least once for a Tanium platform action, the field shows when the selected **Attempt** ended. If you set the **Attempt** to **All**, this field shows the end time of the last attempt. This field does not appear in the final **All Targeted Computers** ring for Tanium Deploy (software) deployments because they do not have an action expiration period.
- **Ring Execution Time**: This field appears only in the final **All Targeted Computers** ring for Deploy (software) deployments and indicates when the deployment became eligible to run on endpoints in the ring.
- **Initiated By** (platform actions only): This field appears only if you select an **Attempt** that is not the initial deployment attempt. The field shows the name of the user who initiated the selected **Attempt**. If you set the **Attempt** to **All**, this field shows who initiated the last attempt.
- **Assigned Endpoints**: This field shows the endpoint assignments for the ring based on the type of associated deployment plan:
    - **Custom plan**: The field shows the assigned filter groups.
    - **Dynamic plan**: The field shows the percentage of endpoints that are targets.

ENDPOINT EXECUTION STATUS

On the Deployment Details page, the **Deployment Plan Status** section shows the **Endpoint Execution Status** chart only if deployment has started in the ring. The chart shows the same information as the Endpoint Status on page 366 chart except for platform actions that users have retried in the ring. For retried rings, the chart shows information about the state of all endpoints in the ring after the selected Attempt (platform actions only) on page 367 finished.

© 2026 Tanium Inc. All Rights Reserved

PROGRESSION CRITERIA

On the Deployment Details page, the **Deployment Plan Status** section shows the following fields to describe the progress of the deployment through the current ring:

- (Tanium platform actions only) **Progression Criteria - Attempts *<first>* through *<current>***

  The **Progression Criteria** section shows the cumulative results from the first attempt to the selected Attempt (platform actions only) on page 367, and the section title reflects that range.

- **View failed endpoints**

  If a deployment cannot progress because of failed progression criteria, you can click **View Failed Endpoints** to go to the Ring Progression Failures on page 370 section of the page, which shows details about the failures.

- **Execute Endpoint Action**

  This field appears only for Tanium platform deployments, and shows whether the action is still running or has ended or has failed to run. When the action ends, the **Wait** interval begins.

- **Initiate Endpoint Execution**

  This field appears only for Tanium Deploy deployments, and shows when the deployment becomes eligible to run on endpoints in the ring. The deployment runs on endpoints as soon as they enter a maintenance window. If no window is configured on endpoints, they run the deployment immediately. The **Wait** interval begins when the deployment becomes eligible to run.

- **Wait *<interval>***

  This field shows the duration of the Wait on page 293 interval and whether it is pending, is in progress, has stopped (because a user paused the deployment), or has ended. You have the option to Skip the wait intervals during deployment on page 378.

- **Evaluate Criteria**

  This section shows the **Status** (see Progression criteria status on page 294), **Threshold** (see Progression criteria descriptions on page 293), and **Result** of the criteria that determine if a deployment can progress to the next ring. For example, in a ring that includes the **Minimum Endpoints** criterion, the **Status** is Passed if the **Threshold** is `≥ 900` endpoints and the **Result** is that `1,000` endpoints attempted the action. The **Status** and **Result** do not appear in rings where criteria are not yet evaluated, a user has stopped the deployment, or the deployment is in an `Error` state.

  The **Evaluate Criteria** section also provides the following information:

  - **Not applicable criteria**

    Progression criteria are defined in the deployment plan. However, the **Evaluate Criteria** section excludes criteria that do not apply to the current deployment even if those criteria are defined in the plan. The Not Applicable icon indicates criteria that do not apply to the current deployment type. For details, see Ring progression criteria on page 292.

  - **Evaluated date**

    The **Evaluated** date is when the Tanium Server finished evaluating the criteria. The criteria results might differ from the values in the Endpoint Execution Status on page 368 and Endpoint Status on page 366 charts because the Server evaluates criteria only once (after the **Wait** interval) but Tanium Clients can continue returning action status

© 2026 Tanium Inc. All Rights Reserved

data after the evaluation ends. For example, the **Evaluate Criteria** section might show an **Execution Success Rate** of 75% while the **Endpoint Status** chart shows a `Completed` percentage of 80% if Clients that did not return their action status in time for the evaluation subsequently return `Completed` status.

- **Method of Evaluation**

  This field appears only for Deploy (software) deployments, and indicates whether the Tanium Server evaluates progression criteria periodically or only once to determine whether the deployment can proceed to the next ring. For more information, see Default Criteria for Progression on page 388.

INCLUDES DEFERRED ENDPOINTS

On the Deployment Details page, the **Deployment Plan Status** section shows the **Includes Deferred Endpoints** section only in the final **All Targeted Computers** ring and only if the assigned **Deployment Plan** specifies Deferred endpoints on page 298. The section lists the filter groups that contain the deferred endpoints.

Ring Progression Failures

On the Deployment Details page, the **Ring Progression Failures** section appears only if the action had progression criteria failures. The section lists the **Progression Criteria** that endpoints failed to meet and in which rings. The User Approved icon in a ring indicates that a user manually progressed the deployment to the next ring despite the failures. Hover over the icon to open a tooltip that shows who manually progressed the deployment and when. To troubleshoot progression failures, see Troubleshoot deployments on page 379.

Endpoint Details

On the Deployment Details page, the **Endpoint Details** section contains the following tabs, which show details about the endpoints that ran the deployment.

- Endpoint Status on page 370
- Evaluation Results on page 373

Endpoint Status

On the Deployment Details page, the **Endpoint Status** tab shows the following information:

Deployment Details page: Endpoint Status tab

Column	Description
Action Status	The Action status on endpoints on page 380 across all the rings.
Endpoint	The computer name for each target endpoint. To view comprehensive details about an endpoint and perform management tasks on the endpoint, click its **Endpoint** icon and click **View Details**. For the specific steps and additional information, see Explore and manage a single endpoint on page 374.
Ring	The ring where each endpoint ran the deployment.

© 2026 Tanium Inc. All Rights Reserved

Deployment Details page: Endpoint Status tab (continued)

Column	Description
Evaluation Results (Deploy deployments only)	The results for progression criteria that are specific to software deployments appear only if the deployment plan specifies such criteria.
Error Messages (Deploy deployments only)	Error that are specific to Deploy (software) deployments when they are in a `Failed` state.
Ring Deployment Attempt (Tanium platform actions only)	This column appears only if a user has retried any ring in the deployment after the initial attempt in that ring failed the progression criteria. The grid shows a row for each endpoint and identifies the last attempt that included the endpoint. Expand ▶ a row to view the action status that the endpoint returned for each attempt. The Ring Deployment Attempts on page 372 tab shows additional information about each attempt. To retry a ring, see Retry a deployment in one ring on page 378.
Action Status Log  (Tanium platform actions only)	This column appears only if a user has retried any ring in the deployment after the initial attempt in that ring failed the progression criteria. To investigate issues related to an action attempt on an endpoint, click the corresponding Action Status Log icon for the attempt. The **Action Status** page opens and shows a grid that lists the endpoints that ran the action. Select the endpoint in the grid and click **Get action log for selected machines** to issue an Interact question that returns the first 100 lines of the log. For more information, see Investigate action-related issues through logs on page 355.

The Tanium Server might take up to one hour to populate the status information. For a Tanium platform action, you can click **Reissue Question** to show the information immediately or to refresh the information if you think it might have changed. The reissued question retrieves fresh results for the **Action Statuses** sensor from all endpoints.

FILTER THE GRID

Use one of the following filters to show only certain endpoints in the **Endpoint Status** grid. For platform actions, only the **Filter by Endpoint** filter is available.

- **Filter by Endpoint**: Enter a string that contains all or part of a computer name, as it is shown in the **Endpoint** column.
- **Action Status**: Select one or more action states.
- **Ring**: Select one or more ring numbers.

© 2026 Tanium Inc. All Rights Reserved

- **Evaluation Results**: This filter applies only to Deploy (software) deployments. Select an option to filter the grid by the evaluation status that endpoints return for progression criteria:
  - **All** endpoints regardless of status
  - Only endpoints that **Passed** the criteria
  - Only endpoints that **Failed** the criteria

> NOTE
>
> Some endpoints might return progression criteria status after the Tanium Server finishes the criteria evaluation that determines whether the deployment proceeds to the next ring. For details, see Progression Criteria on page 369.

SORT THE GRID

You can sort the **Endpoint Status** grid by **Endpoint** (computer name) or **Ring** number.

> NOTE
>
> Sorting by **Ring** might not group all instances of `All Targeted Computers` until all the targeted endpoints have the latest versions of client extensions. However, all endpoints identified in the `All Targeted Computers` rings executed the deployment in the last ring.

VIEW ADDITIONAL INFORMATION

Perform any of the following steps on the **Endpoint Status** tab to see additional status information:

- (Tanium Deploy deployments only) Click **View in Deploy** to open a new browser tab that shows the deployment details in the deployment summary page of the Deploy workbench.
- To view question results in Interact that list action status and endpoint identifiers for each endpoint, click **View in Interact**.

Ring Deployment Attempts

On the Deployment Details page, the **Ring Deployment Attempts** tab appears only for Tanium platform actions and only if users retried at least one ring in the deployment after the initial attempt in the ring failed progression criteria. The tab shows the Ring status on page 382 and number of attempts (including the initial attempt) for each ring. Expand a ring to show additional information about the action attempts in that ring, including:

- Charts that show data about how many endpoints returned `Completed` or `Failed` status for each attempt
- A grid that shows additional data about each attempt, including action status on endpoints (**Completed**, **Failed**, or **Other**) and auditing information (attempt **Initiator**, **Start** time, and **End** time)

To retry a deployment, see Retry a deployment in one ring on page 378.

© 2026 Tanium Inc. All Rights Reserved

Evaluation Results

On the Deployment Details page, the **Evaluation Results** tab appears only for Deploy (software) deployments. The tab shows the count of endpoints for each Progression criteria status on page 294 (**Passed** or **Failed**) and status details for each endpoint.

FILTER THE GRID

You can filter the **Evaluation Results** grid to include only the entries that match:

- Criteria that match the text you enter in the **Filter by Criteria** field
- **Passed** or **Failed** criteria instead of **All** criteria
- A specific **Ring**

VIEW ADDITIONAL INFORMATION

Perform any of the following steps on the **Evaluation Results** tab to see additional information about criteria status:

- Expand a criterion to show details about the status that each endpoint returned. You can sort the grid by **Endpoint** (computer name) and **Ring** number.

  > **NOTE**
  >
  > Sorting by **Ring** might not group all instances of `All Targeted Computers` until all the targeted endpoints have the latest versions of client extensions. However, all endpoints identified in the `All Targeted Computers` rings executed the deployment in the last ring.

- Click the **Passed** or **Failed** count to view question results in Interact that list the endpoints that returned only that specific criteria status. The results include identifying information about each endpoint (such as computer name) and details about the deployment status.
- To view comprehensive details about an endpoint that returned criteria status, Expand a criterion, click the **Endpoint** icon, and click **View Details**. For the specific steps and additional information, see Explore and manage a single endpoint on page 374.

Explore deployment status and targeting

Explore multiple endpoints

From the Deployment Details page, you can investigate the endpoint status and targeting for each ring or for all rings by exploring question results in Interact. Exploring in Interact is useful for troubleshooting deployment issues or evaluating whether targeting is configured appropriately. Interact shows the results in the **Question Results** page within a new browser tab. From there, you can issue additional questions to explore details about the endpoints, as described in Part 7: Analyzing question results in Console and Interact on page 255. For example, you can issue a drill-down question with the **CPU Consumption** sensor to determine if CPU usage is interfering with action deployment on certain endpoints.

© 2026 Tanium Inc. All Rights Reserved

NOTE

The total number of endpoints on the **Question Results** page might differ from the endpoint count that you click to view the results. The **Ring Deployment Status** page and Deployment Details page show endpoint counts that reflect which endpoints were online when the Tanium Server last tallied the count. The **Question Results** page does not show results from endpoints that went offline since the last tally. For more information, see Endpoint targeting on page 278.

1. From the Main menu, go to **Administration > Actions > Ring Deployment Status** and click the action **Name**.
2. Go to one of the following sections of the Deployment Details page based on which endpoints you want to explore, and click the endpoint count or the **View in Interact** button:
   - Summary on page 364: The **Endpoints Targeted** count shows the total number of targeted endpoints across all rings. For Tanium platform deployments, the count is visible only to the user account (default persona) or alternative persona that was used to create the deployment. Click the count to view question results that list the computer names of all the targeted endpoints.
   -  Deployment Plan Status on page 366: Select the ring that targets the endpoints you want to explore. The endpoint count  **<#>** indicates the total number of endpoints that are assigned to the ring, minus any Deferred endpoints on page 298. In rings where a Tanium platform deployment has not started, counts are visible only to the user account (default persona) or alternative persona that was used to create the deployment. This limitation does not apply to Deploy (software) deployments. Click the count to view question results for the Action status on endpoints on page 380 and identifying information about the endpoints. To view results for all endpoints, including deferred endpoints, select the **All Targeted Computers** ring and click the count.
   - Endpoint Status on page 370: Click **View in Interact** to see action status and endpoint identifiers for endpoints across all rings.
   - Evaluation Results on page 373 (Deploy deployments only): Click **View in Interact** to see a list of the endpoints that returned each Progression criteria status on page 294 (`Passed` or `Failed`).

Explore and manage a single endpoint

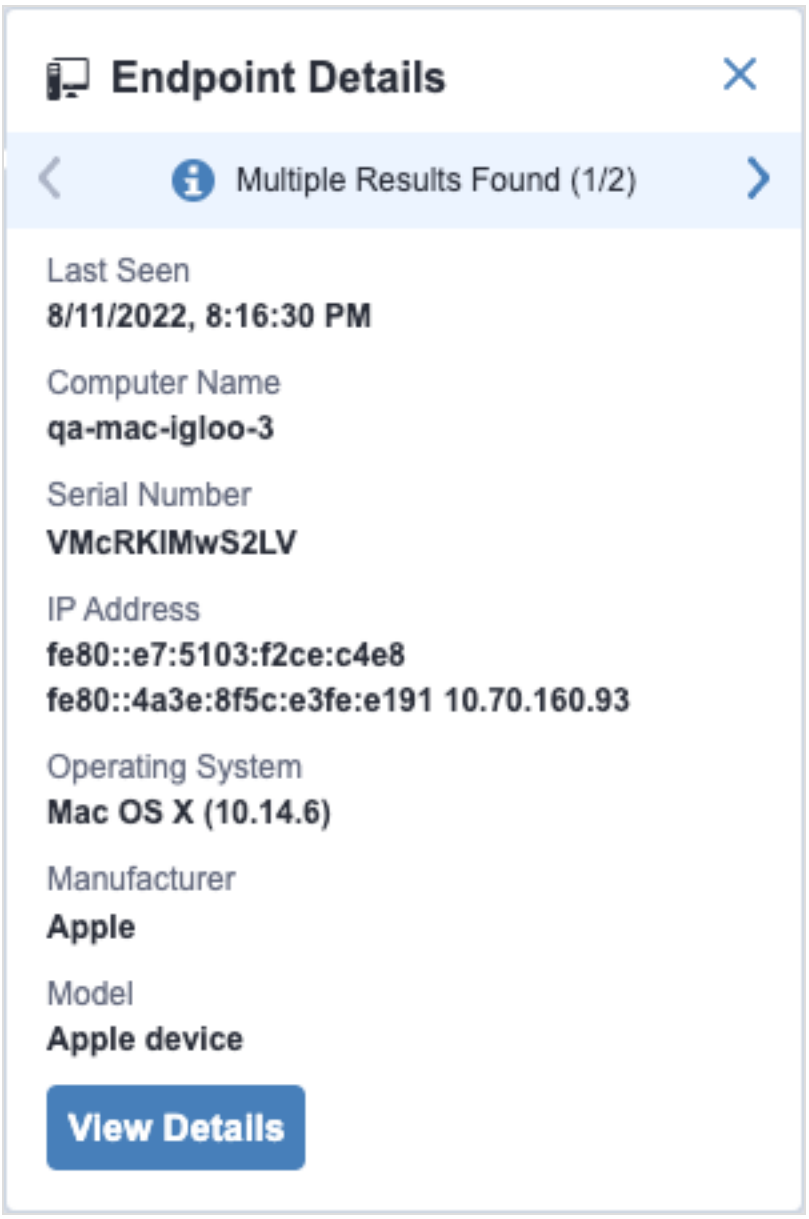
From the Deployment Details page, you can view comprehensive information about a single endpoint and perform management tasks on the endpoint by opening the Endpoint Details page. For example, you can use the Endpoint Details page to deploy software packages, investigate performance history, stop services, and review compliance findings. The Endpoint Details page opens in the Tanium Reporting workbench within a new browser tab. For more information about the page, see Tanium Reporting User Guide: Viewing and managing a single endpoint.

1. From the Main menu, go to **Administration > Actions > Ring Deployment Status** and click the action **Name**.
2. Go to one of the following sections of the Deployment Details page based on how you want to determine which endpoint to explore:
   - Endpoint Status on page 370: This tab shows details about Action status on endpoints on page 380 across all the rings.
   - Evaluation Results on page 373: Expand  a criterion to show details about the status that each endpoint returned.

© 2026 Tanium Inc. All Rights Reserved

3. Click the **Endpoint** icon for the endpoint that you want to explore.

   An **Endpoint Details** dialog opens with basic details for the endpoint. If multiple endpoints have the same **Computer Name**, click Previous or Next in the **Multiple Results Found** banner to find the details for a specific endpoint.



4. Click **View Details** to open the Endpoint Details page.

Stop, pause, or resume deployments

Stop, pause, or resume an action deployment that is in progress depending on what you want to achieve:

© 2026 Tanium Inc. All Rights Reserved

- **Stop**

  Stop an action to prevent the current deployment from continuing and to prevent any users from resuming the current deployment. Stopping does not prevent future deployments that are scheduled for the action. Stopping is useful if you observe action results on endpoints that are unexpected and undesirable. You can then update, disable, or delete the action as necessary. You cannot resume a deployment after stopping it but you can start a new deployment for the action.

- **Pause** or **Resume**

  If you pause an action while it is running on endpoints in a ring, the action runs to completion on any endpoints that the ring targets but the subsequent Wait on page 293 interval does not start until you resume the action. If you pause the action while the wait is in progress, the wait timer pauses until you resume the action. For example, if the wait is 12 hours, 9 hours of the wait time passes, and you pause the deployment for 4 hours before resuming it, the action waits for 3 hours (12 minus 9) before the Tanium Server evaluates progression criteria. Pausing is useful if you observe anomalies on endpoints that already ran the action and you need time to investigate before allowing the deployment to continue. Another case for pausing is when unexpected network events occur that might interfere with the deployment, in which case you can pause the action until the events conclude.

Deployment status on page 381 determines whether you can stop, pause, or resume a deployment.

Stop, pause, and resume operations based on deployment status

Deployment Status	Stop	Pause	Resume
Running	✓	✓	✗
Not Started	✓	✓	✗
Pending Approval	✓	✓	✗
Paused (not Pausing)	✓	✗	✓

To stop, pause, or resume an action:

1. From the Main menu, go to **Administration > Actions > Ring Deployment Status**.
2. Click the **Name** of the deployment and click **Stop**, **Pause**, or **Resume**.

   On the **Ring Deployment Status** page, a deployment initially has `Stopping`, `Pausing`, or `Resuming` status after you click the **Stop**, **Pause**, or **Resume** button. When the operation finishes, the status changes to `Stopped`, `Paused`, or `Running` (resumed) respectively.

Reissue deployments

You can reissue a Tanium platform deployment regardless of its current state. You can change any of the action settings for the reissued deployment except the following settings:

© 2026 Tanium Inc. All Rights Reserved

- **Deployment Package**.
- **Targeting Criteria** based on specific computer groups, a manual list of endpoints, or filter questions. You can still change targeting based on the **Action Group** and deployment plan.

For example, you might reissue a failed deployment after changing the settings that you think caused the failure. Alternatively, you might reissue a successful deployment to a different set of endpoints by changing the action group or deployment plan. The Tanium Server records a fresh history for the new deployment, which does not affect the action settings or results of the original deployment.

1. From the Main menu, go to **Administration > Actions > Ring Deployment Status**.

   TIP

   To filter the grid to find a particular deployment, see Display options on the Ring Deployment Status page on page 361.

2. Click the action **Name** and click **Reissue**.
3. Edit the action settings as necessary. For more information, see Configure action settings on page 395.
4. Click **Show Preview To Continue** and click **Reissue Action**.

Manually progress deployments through rings

You can manually progress a deployment from the current ring to the next ring in a ring set if the progression criteria status is `Failed` for reasons that you decide do not warrant revising and reissuing the deployment. For an example of such a case, see Example: Deploy (software) deployment timing on page 296.

NOTE

You cannot manually progress a deployment that has stalled because of errors other than progression criteria failures. For example, you cannot manually progress a deployment that failed during the **Execute Endpoint Action** phase.

To resume a deployment that a user paused in a ring, see Stop, pause, or resume deployments on page 375.

TIP

You might be able to avoid the need for manually progressing Deploy (software) deployments by selecting the deployment plan option to repeat criteria evaluations periodically. For more information, see Default Criteria for Progression on page 388.

1. From the Main menu, go to **Administration > Actions > Ring Deployment Status**.
2. Click the **Name** of the deployment.
   The Deployment Details page shows a message banner that indicates the ring where progression criteria failed: `Needs Attention: Ring <number> Progression Criteria Not Met.`

© 2026 Tanium Inc. All Rights Reserved

3. Click **Options > Start Next Ring** to progress the deployment to the next ring.
   The page shows two changes to indicate the manual progression event occurred:
   - In the ring details pane, the icon in the banner changes from Failed to Warning.
   - In the ring set pane, the icon changes from Failed to User Approved.

Retry a deployment in one ring

If a Tanium platform action fails the progression criteria in a particular ring, you can save time, network resources, and endpoint resources by retrying the deployment only in that ring instead of reissuing the deployment for all rings. If the retried deployment passes the progression criteria, it progresses to the next ring. You can retry a deployment in all rings except the last **All Targeted Computers** ring. After the initial deployment attempt in a ring, users can retry the deployment up to 9 more times in that ring.

When you retry a ring, the deployment targets only the endpoints that:

- Tried to run the action but returned `Failed` action status in the previous attempt. This condition includes endpoints that tried but failed to run the package script or failed to run it to completion in the previous attempt.
- Were online during the initial attempt. This condition does not apply to endpoints that go offline between subsequent reattempts. For example, consider the following case:
  - Initial attempt: Endpoint A is online but fails to complete the action.
  - Second attempt: Endpoint A goes offline and therefore is excluded from the retry.
  - Third attempt: Endpoint A comes back online and therefore is included in the retry.

> NOTE
> The last ring targets endpoints that were offline during the initial attempt.

Try to resolve the issues that caused the progression criteria failures before retrying the deployment. For more information, see Troubleshoot deployments on page 379.

Perform the following steps to retry the deployment in the ring where it failed progression criteria.

1. From the Main menu, go to **Administration > Actions > Ring Deployment Status**.
2. Click the **Name** of the deployment.
   The Deployment Details page shows a message banner that indicates the ring where the deployment failed to finish or progress.
3. Click **Retry Ring**.

Skip the wait intervals during deployment

In a deployment plan, the Wait interval is a required setting for each ring except the last ring. However, you can skip a wait interval that is pending or in progress in one or more rings during action deployment. Skipping the wait is useful if the action resolves an urgent incident for which haste is a higher priority than providing Tanium Clients more time to measure the action impacts. If you

© 2026 Tanium Inc. All Rights Reserved

skip the wait, the deployment type determines whether the Tanium Server starts evaluating the Ring progression criteria when the action starts (Tanium Deploy deployments) or when the action ends (Tanium platform deployments). You can revert to applying the wait for a ring as long as the progression criteria evaluation has not started.

1. From the Main menu, go to **Administration > Actions > Ring Deployment Status** and click the **Name** of the deployment.
2. Go to the **Deployment Plan Status** section, select the ring where you want to skip the wait, and perform one of the following sub-steps based on the **Wait *<interval>*** state:
    - (pending): Select **Skip** in the **Progression Status** section. As long as the wait is still pending, you can revert to applying the wait by clearing **Skip**.
    - (in progress): Click **Skip the Wait** in the message banner, review the information about the wait interval, and click **Skip the Wait** again.

For the sake of auditing, the **Wait *<interval>*** field on the Deployment Details page records the event with the message: `Skipped by <user name> on <date> at <time>`.

Troubleshoot deployments

Perform the following steps to check Deployment status on page 381, analyze action results on endpoints, and troubleshoot any unexpected results:

1. Review the current status of the deployment and its individual rings, and determine how many endpoints have run the action. You can see this information on the Deployment Details page when you Analyze and manage a single deployment on page 362.
2. Pause or stop the deployment if you want to prevent the action from deploying to any more rings until you investigate and resolve issues in the current ring. For more information, see Stop, pause, or resume deployments on page 375.
3. List the affected endpoints in Interact if the Deployment Details page shows anomalies in action status or targeting, as described in Explore multiple endpoints on page 373. You can then issue Interact questions to investigate the endpoints. For example, you can issue a question with the **CPU Consumption** sensor to determine if CPU usage is interfering with action deployment.
4. Review action logs and verify whether action locks are turned on, as described in Troubleshoot actions on page 339.
5. Update the action deployment settings if necessary to resolve issues. For more information, see Configure action settings on page 395.
6. Update the deployment plan settings if necessary to resolve issues. For more information, see Edit a deployment plan on page 390.
7. After you finish resolving issues, perform one of the following steps:
    - Resume the deployment if you paused it, as described in Stop, pause, or resume deployments on page 375.
    - Manually progress the deployment to the next ring if the deployment stalled because progression criteria failed and if circumstances warrant overriding the criteria. For more information, see Manually progress deployments through rings on page 377.

© 2026 Tanium Inc. All Rights Reserved

- Retry the deployment only in the ring where it failed to complete or failed to progress to the next ring. For more information, see Retry a deployment in one ring on page 378.
- Start a new deployment if you stopped the previous deployment. To start a deployment, see Deploying actions and playbooks in Console and Interact on page 391.

Action status on endpoints

Each Tanium Client reports one of the following states for an adaptive action that runs on the endpoint. The Summary on page 364 section of the Deployment Details page shows action status metrics in the **Endpoint Status** chart. To view additional details about action status, see Explore deployment status and targeting on page 373.

Action status on endpoints

State	Description
Completed	The command in the action package finished executing and the action achieved its intended outcome. The Client returns this state if it finds no deviations after evaluating the action success criteria. **Completed** is the final state.
Running	The Client is running the Command on page 448 that the associated package specifies. The action proceeds to the next state when one of the following events occurs: • The command finishes executing before the action timeout: The next state is **Completed**. • The command reaches the action timeout before finishing execution: The command terminates and the next state is **Failed**. • The command runtime reaches the **Command Timeout** before the action timeout and before the command finishes execution: The command terminates and the next state is **Failed**. • The command execution fails before any timeout (for example, the Client might fail to spawn a new process to run the command): The next state is **Failed**.
Pending	The Client staged the action and is waiting for a maintenance window to end before initiating the action. For more information, see: • Tanium Deploy User Guide: Managing maintenance windows
Downloading	The Client is downloading package Managing packages for platform actions on page 442 if the action requires them. Otherwise, the Client skips the **Downloading** state and enters the **Running** state. An action in the **Downloading** state proceeds to the next state when one of the following events occurs: • The Client finishes downloading the files before the action timeout: The next state is **Running**. • The Client reaches the action timeout before finishing the download: The next state is **Failed**.

© 2026 Tanium Inc. All Rights Reserved

Action status on endpoints (continued)

State	Description
Failed	The action did not achieve its intended outcome due to any of the following reasons: • **Failed verification**: The Client returns this state if it finds any deviations after evaluating the action success criteria that are defined in the package Verification Exit Codes on page 444 or Verification Query on page 444. • **Expiration**: The Client reaches the action timeout before finishing one of the following processes: ◦ Command execution ◦ Package file downloads

Deployment status

The **Ring Deployment Status** page shows one of the following states for each adaptive action deployment based on its progress through the ring set.

> NOTE
>
> The Deployment Details page shows the Ring status on page 382 of individual rings in a single deployment. To view details about action status on specific endpoints, see Explore deployment status and targeting on page 373.

Deployment status

State	Description
Deployed	The progression criteria have `Passed` status in all the rings that have criteria defined and the deployment has finished running successfully through all the rings.
Running	The deployment is running in one of the rings.
Pausing/Paused	A deployment has `Pausing` status if a user initiated the pause operation. When the operation finishes, the status changes to `Paused`. You can resume a deployment that a user paused, as described in Stop, pause, or resume deployments on page 375.
Resuming	A user resumed the deployment after it was paused. When the resume operation finishes, the deployment status changes to `Running`.
Stopping/Stopped	A deployment has `Stopping` status if a user initiated the stop operation, as described in Stop, pause, or resume deployments on page 375. When the operation finishes, the status changes to `Stopped`. You cannot resume a `Stopped` deployment, but you can start a new deployment for the same action, as described in Deploying actions and playbooks in Console and Interact on page 391.
Not Started	The deployment has not started running in any ring. This status does not apply if deployment has not started because approval is pending.

© 2026 Tanium Inc. All Rights Reserved

Deployment status (continued)

State	Description
Failed	The deployment failed due to errors. You cannot resume a `Failed` deployment. However, you can manually progress the deployment to the next ring if circumstances warrant it, as described in Manually progress deployments through rings on page 377.
Pending Approval	The deployment requires approval before the Tanium Client can run it. For more information, see Managing action approval on page 411.
Unknown	The Tanium Server cannot determine the status.

Ring status

On the Deployment Details page, the Deployment Plan Status on page 366 section shows one of the following states for each ring in the ring set.

Ring status

State	Description
Deployed	If progression criteria are configured in the ring, the criteria status is `Passed` and the deployment has finished running successfully in the ring. If progression criteria are not configured, the Wait on page 293 interval has passed and the deployment has finished running successfully in the ring.
Running or resuming	The deployment is running in the ring. The status remains `Running` even if a user paused or resumed the deployment in that ring.
Retrying	This status applies only to Tanium platform actions and indicates that the deployment is running in the ring because a user retried the ring after the first attempt failed the progression criteria. For more information, see Retry a deployment in one ring on page 378.
Stopped	A user stopped the deployment in the ring.
Not Started	The deployment has not started running in the ring.
Evaluating Criteria	This status applies only to Deploy (software) deployments, and indicates that the Tanium Server has started periodically evaluating the progression criteria, but has not yet evaluated to pass status and has not reached the end of the evaluation time limit. For details on the periodic evaluation option in deployment plans, see **Method of Evaluation** in Default Criteria for Progression on page 388.
Failed	If progression criteria are configured in the ring, the criteria status is `Failed`. If progression criteria are not configured, deployment failed in the ring due to other errors. For example, the deployment might fail to run during the **Execute Endpoint Action** phase. You can manually progress a deployment that failed progression criteria, as described in Manually progress deployments through rings on page 377.

© 2026 Tanium Inc. All Rights Reserved

Ring status (continued)

State	Description
 User Approved	This icon appears only in the ring set pane and only if a user manually progressed the deployment to the next ring even though the progression criteria status is `Failed`. For more information, see Manually progress deployments through rings on page 377.
 Unknown	The Tanium Server cannot determine the status.

© 2026 Tanium Inc. All Rights Reserved

Managing deployment plans for ring deployments

A deployment plan defines the sequence of rings (ring set) that an adaptive action must progress through to complete successfully, along with the target endpoints and progression criteria for each ring, as described in Ring-based deployment on page 276. You assign the plan when you configure an action deployment, such as for remediating an emerging issue. Use the **Deployment Plans** page to view the settings of existing plans, create or edit plans to suit your environment, and delete plans that are no longer used.

NOTE

For the role permissions that you require to view and manage deployment plans, see Manage deployment plans on page 91.

Deployment plan types

Choose a deployment plan type based on how you want to select the endpoints that an action targets. The plan type that you choose applies to all the rings in a plan; you cannot select different types for different rings in the same plan.

Custom deployment plans

In a custom deployment plan, each ring targets endpoints based on filter group assignments. Use this plan type if targeting endpoints with particular characteristics matters more than targeting a sample that is representative of all your endpoints. For example, the first ring might target only the endpoints that are members of a filter group that is designated for testing actions.

Dynamic deployment plans

In a dynamic deployment plan, each ring targets endpoints based on a percentage of all the endpoints that are targeted across all rings. Deployment ends for a ring when the specified percentage of endpoints finish running the action. The Tanium Server selects the target endpoints at random in each ring when the action starts deploying in that ring. The selection does not persist for a ring across multiple deployments of the same action. Each time you redeploy the action, the Server randomly selects a new set of endpoints for each ring.

Use a dynamic plan if, for each ring, targeting a representative sample of endpoints matters more than specific characteristics of the endpoints. For example, if your environment has 10,000 endpoints and the first ring targets 10%, the action deploys to a random selection of 1,000 endpoints regardless of whether they are servers or non-servers, physical or virtual, Windows or Linux. Targeting representative samples is useful for predicting how actions will affect larger populations of endpoints. The higher the percentage of endpoints that a ring targets, the more closely the ring represents your whole environment and the more accurately you can predict action outcomes for the environment.

BEST PRACTICE

When you configure progression criteria for a dynamic deployment plan, specify the Execution Success Rate on page 294 instead of the Minimum Endpoints on page 294. For more information, see Endpoint targeting on page 278.

© 2026 Tanium Inc. All Rights Reserved

View deployment plans

Viewing deployment plans can help you to determine if new plans are necessary and to manage or troubleshoot existing plans. For example, you might review the progression criteria of a plan to investigate why actions that use it are stalling in a particular ring.

1. From the Main menu, go to **Administration > Actions > Deployment Plans**.

   The **Deployment Plans** page lists all the plans that you have permissions to access. The page shows some settings for all the plans, such as the **Name** and **Content Set** assignment. The page also shows attributes that are useful for auditing, such as the name of the user (**Author**) who created the plan and the date/time when any user **Last Modified** the plan.

2. (Optional) Use any of the following filtering options to find specific plans if the grid is long.

   You can sort the grid by the plan **Name**, the plan **Type**, and the time when a user **Last Modified** the plan.

   - **Ring Type**: Select an option to see only **Custom** plans, only **Dynamic** plans, or **All** types of plans. For more information, see Deployment plan types on page 384.
   - **Filters** (attribute filters): Expand the **Filters** section and select one or more plan attributes: **Content Set** assignment, **Preferred For**, or **Created By** (user). For information about the **Preferred For** attribute, see Preferred for Deployment Type on page 386.
   - **Filter by Name**: Enter an alphanumeric string that contains all or part of a plan name.

3. (Optional) Click the **Name** of a plan to open it and view its **Rings and Progression Criteria** and deferred endpoints. For more information, see Configure rings, progression criteria, and deferred endpoints on page 387.

Create a deployment plan

Create a deployment plan for each set of action deployments that require the same rings, progression criteria, and deferred endpoints. You can create up to 150 plans.

Before you begin

Perform the following tasks before creating a deployment plan.

- **Review existing plans**

  Review existing deployment plans to determine if you need new plans for the actions that you expect to deploy. For more information, see View deployment plans on page 385. If you need a new plan that is similar to an existing plan, cloning a plan is easier than creating a plan from scratch. For more information, see Clone a deployment plan on page 389.

- **Review and create filter groups**

  Review existing filter groups to determine if they include all the endpoints that you plan to assign to specific rings or defer to the last ring in custom deployment plans. Create new filter groups if necessary. For more information, see Managing filter groups for filtering questions and results on page 476.

© 2026 Tanium Inc. All Rights Reserved

- **Assign role permissions**

  Ensure that users who select plans for deployments have the permissions **Deployment Plan read**, **Progression Criteria Set read**, and **Ring Set read** for the content sets that you will assign to deployment plans. To update user roles, see Configure role permissions on page 591.

Add a deployment plan

Perform the following tasks to create a deployment plan:

- Configure the deployment plan overview on page 386
- Configure rings, progression criteria, and deferred endpoints on page 387
- Preview and save the deployment plan on page 389

CONFIGURE THE DEPLOYMENT PLAN OVERVIEW

On the **Create/Edit Deployment Plan** page, define the basic attributes of the plan in the **Overview** section.

1. From the Main menu, go to **Administration > Actions > Deployment Plans**.
2. In the **Create Plan** dropdown list, select **Custom** or **Dynamic** as the plan type. For more information, see Deployment plan types on page 384.
3. Configure the following plan settings.

   Deployment plan settings

Setting	Description
Name	Enter a name to uniquely identify the deployment plan. For example, you might name the plan `emerging-issues` if you intend it for actions that remediate issues for which Tanium Guardian provides alerts.
Description	(Optional) Enter a description of the plan to help other users understand its purpose. For example, you might enter `Use this plan only for Guardian emerging issues` if you do not want users to select the plan for other deployment types.
Content Set	Select a content set that is accessible to users who select the plan for deployments. The users must be assigned a role with the permissions **Deployment Plan read**, **Progression Criteria Set read**, and **Ring Set read** applied to the content set.
Preferred for Deployment Type	Select the deployment types for which this plan is preferred. When users configure a deployment of any type, they can select any plan in the **Deployment Plan** dropdown list. The preferred plans for the deployment type appear at the top of the list for convenience. The list shows other plans in alphabetical order. For a description of the deployment types, see Deployment types on page 277.

4. Add rings and (optionally) deferred endpoints, as described in Configure rings, progression criteria, and deferred endpoints on page 387.

© 2026 Tanium Inc. All Rights Reserved

CONFIGURE RINGS, PROGRESSION CRITERIA, AND DEFERRED ENDPOINTS

On the **Create/Edit/Clone Deployment Plan** page, use the **Rings and Progression Criteria** section to add rings, configure target endpoints and progression criteria for each ring, and optionally defer a subset of the target endpoints to the last ring. Each plan requires 1 to 15 user-defined rings and the predefined last ring (**All Targeted Computers**). The ring set pane shows the rings that you add in **Start** to **End** order. The pane shows the optional **Deferred Endpoints** below all the rings. You can select a ring in the ring set pane to view or edit the settings of that ring in the **Definition** pane. You cannot view or edit the **All Targeted Computers** ring because it is non-editable and it has no progression criteria because it is always the last ring.

1. (Optional) Select **Custom** or **Dynamic** to change the plan type. For more information, see Deployment plan types on page 384.
2. For each ring in the deployment plan, click **Add Ring** and configure the following settings.

To add a ring that has many settings in common with an existing ring, select the existing ring in the ring set pane and click Duplicate in the **Definition** pane.

Rings and progression criteria

Setting	Description
Name	Enter a name to identify the ring. The name must be unique within the deployment plan but does not have to be unique among different plans.
Assigned Endpoints	Assign endpoints based on the plan type: • **Custom**: Click **Select Filter Groups**, select the filter groups that contain the endpoints for the ring, and click **Save**. To remove a filter group from your selections, click the **X**. • **Dynamic**: Specify the percentage of endpoints that the ring targets relative to the total number of endpoints that the action targets across all rings. For important considerations related to targeting endpoints, see Endpoint targeting on page 278.

© 2026 Tanium Inc. All Rights Reserved

Rings and progression criteria (continued)

Setting	Description
Default Criteria for Progression	• **Wait** Enter the time that a deployment must Wait on page 293 in the ring before the Tanium Server evaluates the other progression criteria. A **Wait** value is required, but you can enter `0` to specify no wait before the Server starts evaluating the criteria. NOTE Criteria evaluation is more likely to accurately represent endpoint states if the wait is longer. • **Evaluation Criteria** Deployments must match all the criteria that you specify to progress to the next ring. To add a criterion, select **Add > <*Criterion*>** and enter a value. Optionally, select **Ignore pending endpoints** for either or both of the **Execution Success Rate** and **Minimum Endpoints** criteria to evaluate results only from endpoints that have returned a `Completed` or `Failed` status for the action. For more information about specific criteria, important considerations when configuring criteria, and the **Ignore pending endpoints** option, see Ring progression criteria on page 292. • **Method of Evaluation** The following options are available only for Deploy (software) deployments. Progression criteria evaluations occur only once for Tanium platform and Guardian deployments. ◦ **Evaluate once**: The Tanium Server evaluates the criteria only once to determine whether the deployment can proceed to the next ring. Some Tanium Clients might return action status data after the evaluation ends but that post-evaluation data does not affect ring progression. ◦ **Evaluate periodically**: The Tanium Server evaluates the criteria every five minutes until the end of the **Reevaluation Duration** that you specify. If the **Reevaluation Duration** is shorter than five minutes, the criteria are evaluated only twice: at the start and at the end of the duration. The deployment progresses at whichever interval the evaluation first produces a pass status. Client results that return after that interval do not affect ring progression. The periodic option is useful in cases where the software deployment might take longer than expected on endpoints. In such cases, a one-time only evaluation might produce a result that does not accurately represent the probability of success for that deployment. NOTE Periodic evaluations do not affect endpoint resources more than a one-time evaluation because the Tanium Server queries Tanium Data Service (TDS) for the periodic criteria updates instead of issuing new questions to endpoints.
Start-to-End order	In the ring set pane, the predefined **All Targeted Computers** ring is always last. To change the order of the other rings, drag their icons. For important considerations related to the number and order of rings, see Ring-based deployment on page 276.

© 2026 Tanium Inc. All Rights Reserved

3. (Optional) Click **Defer Endpoints**, click **Select Filter Groups**, and select the filter groups that contain the endpoints you want to defer to the last ring. Click **X** on a filter group if you need to remove that group from your selections. For more information, see Deferred endpoints on page 298.
4. Go to Preview and save the deployment plan on page 389.

PREVIEW AND SAVE THE DEPLOYMENT PLAN

Perform the following steps to see a preview of the endpoint counts that each ring targets in a deployment plan and then save the plan if the counts are correct.



The **Preview Deployment Plan** section shows accurate counts only after you select a **Content Set** for the deployment plan and select **Assigned Endpoints** for each user-defined ring.

1. On the **Create/Edit/Clone Deployment Plan** page, go to the **Preview Deployment Plan** section and verify that the endpoint targeting is correct for each ring. The section shows the count of endpoints that are both targeted and online in each ring.

   In a custom deployment plan, you can list the endpoints in a ring by clicking the endpoint count. Interact then issues the question `Get Computer Name from all machines with <filter group expression> equals True`. The `<filter group expression>` comprises the membership expressions of the filter groups that are selected for the **Assigned Endpoints** in the ring. The `<filter group expression>` also specifies the deferred endpoints to exclude from the results. Interact opens the **Question Results** page in a new browser tab to show the results.

   Endpoint targeting during deployment might differ from the assigned endpoints in a deployment plan based on the targeting that is configured for the deployment. For more information, see Endpoint targeting on page 278.
2. Click **Save** to finish adding or updating the deployment plan if the targeting is accurate. Otherwise, edit the targeting as described in Configure rings, progression criteria, and deferred endpoints on page 387 and then repeat the preceding step to preview the plan.

Clone a deployment plan

Cloning a deployment plan is easier than creating a plan from scratch if you want a new plan that has many settings in common with an existing plan. To determine if any existing plan resembles the plan you want to create, see View deployment plans on page 385. If the clone will differ from the original plan in terms of target endpoints, deferred endpoints, or content set assignment, see Before you begin on page 385 before cloning. Perform the following steps to clone a deployment plan. You can clone only one plan at a time.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Actions > Deployment Plans**.
2. Perform one of the following steps based on if you want to review the plan settings before deciding whether to clone the plan:
    - **Review**: Click the plan **Name**, review the plan details, and click **Clone**.
    - **No review**: Select the plan and click **Clone**.
3. Edit the settings and click **Save**. For more information, see Deployment plan settings on page 386 and Configure rings, progression criteria, and deferred endpoints on page 387.

Edit a deployment plan

You can edit all the settings for user-defined deployment plans. For **Tanium Managed** plans, you can edit the **Content Set** and **Preferred for Deployment Types** selections only.

When you edit a deployment plan that is assigned to an action, the changes apply to future deployments of the action, not to deployments that are in progress.

If you want to edit the target endpoints, deferred endpoints, or content set assignment of a deployment plan, see Before you begin on page 385 before proceeding.

Perform the following steps to edit a deployment plan. You can edit only one plan at a time.

1. From the Main menu, go to **Administration > Actions > Deployment Plans**.
2. Select the plan and click Edit.
3. Edit the settings and click **Save**. For more information, see Deployment plan settings on page 386 and Configure rings, progression criteria, and deferred endpoints on page 387.

Delete a deployment plan

You can delete user-defined deployments but not **Tanium Managed** deployment plans. Deleting a deployment plan unassigns it from actions, but the change applies only to future deployments of those actions. Deployments that are in progress continue to use the plan that was assigned before you deleted the plan. You must assign a new plan to the actions that used the deleted plan to enable future deployments of those actions.

1. From the Main menu, go to **Administration > Actions > Deployment Plans**.
2. Perform one of the following steps based on if you want to review the plan settings before deciding whether to delete the plan:
    - **Review**: Click the plan **Name**, review the plan details, and click Delete.
    - **No review**: Select one or more plans and click **Delete**.

© 2026 Tanium Inc. All Rights Reserved

Deploying actions and playbooks in Console and Interact

After you issue a question, analyze the question results, and determine which endpoints require changes, you can deploy actions to those endpoints. For example, you can deploy an action that restricts access to certain directories on endpoints. You can also deploy a series of actions as steps in a Tanium Automate playbook. For example, if question results indicate that some endpoints have non-approved software installed, you can run a playbook that uninstalls the software and performs related cleanup activities. You can run a playbook multiple times to streamline and simplify your business processes.



Do not deploy an action unless you completely understand its scope, impact on individual endpoints, and impact on the environment given the number of targeted endpoints. Review the Action best practices on page 324 before deploying.

Be sure that your organization has authorized you to perform the action. Some organizations require a second administrator to review and approve actions. For more information, see Managing action approval on page 411.



For the user role permissions required to deploy actions, see Deploy actions on page 90. **Automate Playbook execute** permission is required to run playbooks. For more information, see Tanium Automate User Guide: User role requirements.

Tanium provides predefined roles, content (such as packages), computer groups, action groups, and deployment plans for deploying actions. If you need to customize your environment to optimize action deployment, see Action deployment overview on page 328.

For information about viewing, running, or creating a playbook, and the available playbook steps, see Tanium Automate User Guide.

Disable or delete a simple (non-ring-based) action to stop deploying it, as described in Manage scheduled actions on page 342. To stop or pause an adaptive (ring-based) action, see Stop, pause, or resume deployments on page 375.

Select an action or playbook initiation method

In Tanium Console or Interact, select a method to initiate action deployment based on whether the actions are new or existing.

To deploy an action with predefined settings through Tanium Reporting or Tanium Guide, see Deploy a predefined action on page 393.

To run an existing playbook through Console or Interact, see Initiate an existing playbook on page 393.

© 2026 Tanium Inc. All Rights Reserved

Initiate a new action

Initiate a new action based on:

- **Endpoint data** (question results): Issue a dynamic question (see Issue a free-form question on page 241) or a saved question (see Issue a saved question on page 466). From the **Question Results** page, select up to 100 rows for the endpoints that require the action, click **Deploy Action**, and go to Configure action settings on page 395.
- **Client connection status**: Go to **Administration > Configuration > Client Status**, select the Tanium Clients (up to 100) to which you want to deploy actions, click **Deploy Action**, and go to Configure action settings on page 395.
- **Specific packages**: Go to **Administration > Content > Packages**, select a package, click **Deploy Action**, and go to Configure action settings on page 395.

Initiate an existing action

Perform the following steps and then go to Configure action settings on page 395.

1. Go to the **Administration > Actions** page for the actions that you want to deploy:
   - To deploy scheduled or unscheduled actions that were previously deployed, go to **Administration > Actions > Action History**.
   - To immediately deploy scheduled actions that are configured with a future start date, go to **Administration > Actions > Scheduled Actions**.

   After an action is created or edited, a user might update the files or settings of the associated package. Before you redeploy an action, you can check the status of, and optionally update, package files. For more information, see Re-download package files on page 445. When you redeploy or edit an action, the workflow includes an option for updating the Deploying actions and playbooks in Console and Interact on page 391 to use its latest settings.

2. Select one or more actions and perform one of the following steps:
   - To redeploy a single action, or to re-issue multiple actions that each require a different start time or distribution period, click **Reissue** and skip to Configure action settings on page 395.
   - To redeploy multiple actions with the same start time and distribution period, select **More > Bulk Reissue**, specify the time standard (**Local Time / UTC**), **Start At**, and **Distribute Over** values (see Action schedule settings on page 396), click **Confirm**, and skip to Review action status on page 399. This option is for a one-time deployment only. If you select multiple recurring actions, the Tanium Server creates copies of the actions with their **Schedule Type** set to **One Time Deployment**.

© 2026 Tanium Inc. All Rights Reserved

Initiate an existing playbook

1. Issue a dynamic question (see Issue a free-form question) or a saved question (see Issue a saved question).
2. When the **Question Results** page shows the results, select up to 100 rows for the endpoints that require the playbook.
3. Click **Start a Playbook**. The **Select a Playbook** dialog provides the following options for finding specific playbooks and assessing whether they are appropriate for the target endpoints:
    - Enter a text string that matches all or part of a playbook name in the **Filter items** field to find a specific playbook.
    - Expand the **Limiting Group** to see the syntax of the targeting question. Click the endpoint count to issue the question and see the results in a new browser tab.
    - Expand a playbook to see its steps.
4. Click **Review Playbook** in the row for the playbook that you want, review the playbook settings to ensure they match your expectations, and click **Start**.

For information about viewing, running, or creating a playbook, see Tanium Automate User Guide.

Deploy a predefined action

In just a few steps, you can quickly deploy an adaptive (ring-based) action with predefined settings if you initiate the action from a report or a dashboard in Tanium Reporting. You can also deploy an action from an emerging-issue dashboard that Tanium Guardian provides through Tanium Guide. You perform the predefined action workflow through the Adaptive Action dialog, which has the following prerequisites:

- **Adaptive actions**: The predefined action workflow requires a deployment plan assignment, and therefore the workflow does not apply to simple (non-ring-based) actions.
- **Permissions**: You must sign in using a user account or persona with role permissions that enable access to at least one deployment plan. For more information, see Manage deployment plans on page 91.
- **Tanium Automate**: Automate must be installed. For more information, see Part 4: Managing Tanium solutions on page 108.
- **Package**: The Adaptive Action dialog is available only for actions with packages that are not parameterized.

If the preceding prerequisites are not met, the **Action Deployment** page appears instead of the Adaptive Action dialog and you must Configure action settings on page 395 as for a custom action.

Perform the following steps to deploy a predefined action:

1. Initiate action deployment from one of the following sources:
    - **Report**: The predefined action workflow is available only for recommended actions that are configured in a report. Otherwise, you must Configure action settings on page 395 before deployment. To initiate recommended actions from a report, see Tanium Reporting User Guide: Deploy an action.
    - **Dashboard**: To initiate an action from the action panel of a dashboard, see Tanium Reporting User Guide: Deploy

© 2026 Tanium Inc. All Rights Reserved

action.

- **Guardian notification**: To initiate an action from an emerging issue dashboard, see Tanium Guide User Guide: View notifications.

Dashboards show an action button with the icon for predefined actions and without any icon for custom actions.

2. Review the settings in the Adaptive Action dialog and select a deployment plan if none is selected or you need to change the default selection. The settings in the dialog match corresponding settings in the **Action Deployment** page (see Configure action settings on page 395), with the following exceptions.

Adaptive Action dialog settings

Setting	Description
Deployment Name	This field corresponds to the action **Name**, which defaults to the name of the **Deployment Package** .
Deployment Plan	A plan is selected automatically if the package matches the Preferred for Deployment Type on page 386 setting of only one deployment plan, but you can manually select a different plan. If the field displays `None Selected`, you must manually select a plan. You can select a plan or see the current selection in the **Select Plan** dropdown list. Only the **Preferred Plans** in the list (if any) are intended for the type of package that is associated with the current action.
Total Eligible Endpoints	This field shows a count of all the endpoints that are targeted for the action based on the **Targeting Criteria** in the action settings and the Assigned Endpoints on page 387 in the deployment plan. Click the count to view question results that list the endpoints by **Computer Name**. The Interact **Question Results** page shows the list in a new browser tab. For an explanation of all the factors that affect how the Tanium Server determines eligible endpoints, see Endpoint targeting on page 278.
Question Criteria	This field corresponds to the **Target Question** in the action **Targeting Criteria**.

3. If no setting edits are necessary, click **Deploy** and go to the next step. If edits are necessary, click **Edit** and Configure action settings on page 395 to deploy a custom action instead of a predefined action.

4. If the number of **Estimated clients affected** exceeds the configured threshold (the default is 100), enter the estimated number and click **Confirm**. The Tanium Server enforces this confirmation step to ensure that you understand the impact that an action will have on your network.

To change the threshold that controls whether Console prompts users for the **Estimated clients affected**, edit the **Prompt Estimate Threshold** setting as described in Review and edit global settings for actions on page 329.

5. (Optional) Monitor the progress of the action. For more information, see Review action status on page 399.

© 2026 Tanium Inc. All Rights Reserved

Configure action settings

After you open the **Action Deployment** dialog, configure the action settings. If you are deploying multiple actions, use the Previous and Next arrows to navigate the actions.

> **NOTE** If an existing action has **Start At** and **Re-issue every** values and you clear them instead of specifying new values, those settings revert to the values that existed before you cleared them.

1. Perform one of the following steps to open the **Action Deployment** dialog:
   - Initiate a new action on page 392
   - Initiate an existing action on page 392
2. Select a time standard for the action scheduling settings:
   - **Local Time** (default) is local to the system that you use to access Console.
   - **UTC** is Coordinated Universal Time.
3. Select a **Deployment Package**. You might have to configure additional settings based on your selection:
   - **Parameterized package**: Configure any package parameters. For more information, see Example: Parameterized packages on page 508.
   - **Updated package**: If you are re-issuing or editing an action and the package settings changed after the action was last issued or saved, see Update action packages on page 347.
4. Configure the basic **Action Details**.
   - **Name**: The name defaults to `Deploy <deployment package>` but you can overwrite the value with whatever name you want to use for identifying the action in Console and Interact pages.
   - **Description** (optional): Enter a description that helps other users understand the purpose of the action.

   The read-only **Expiration Period** appears if you are editing or reissuing the action. It indicates when the action expires, which means Tanium Clients can no longer run the associated package command. The expiration timer resets for each deployment of a recurring action but does not change the **Deployment Schedule**. The value is the larger result of the following calculations:
   - The sum of the command and download timeout values in the selected package. For more information, see Command Timeout and Download Timeout on page 448.
   - The sum of the package **Command** timeout and optional Distribute Over on page 396 action setting.

© 2026 Tanium Inc. All Rights Reserved

5. Configure the **Deployment Schedule**.

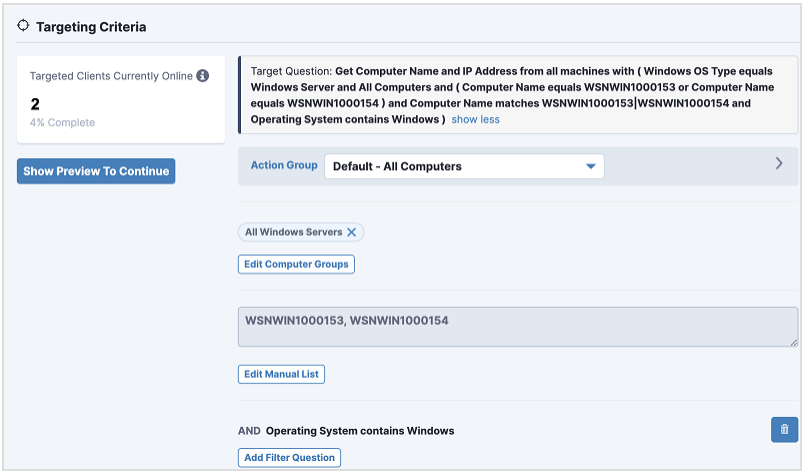
Action schedule settings

Setting	Description
Schedule Type	Select one of the following options: • **One Time Deployment**: Deploy the action only once. This option is required for adaptive actions and optional for simple actions. • **Recurring Deployment**: Schedule the action to deploy at intervals (**Re-issue every**) over a specified period (from the **Start At** to **End At** date-times). This option is required for policy actions and is available only for simple actions.
Re-issue every	This setting appears only if you set the **Schedule Type** to **Recurring Deployment**. Recurring deployments are available only for simple actions, not adaptive actions. Specify a number and unit: **Minutes**, **Hours**, **Days**. The **Re-issue every** interval must exceed the action **Expiration Period**. For more information about the use cases for recurring deployments, see Scheduled actions on page 322.
Start At	By default, actions that do not require approval deploy immediately after you click **Deploy Action** at the bottom of the **Action Deployment** page. To override the default behavior, set a **Start At** date/time. For example, you might want deployment to start during a maintenance window for the targeted endpoints. Future start dates are available only for simple actions, not adaptive actions. NOTE: If you set a Distribute Over on page 396 value, it delays the start time of the action beyond the **Start At** value. For information about how action approval affects the start time, see Approval impact on action timing on page 411.
End Time	This setting appears only if you set the **Schedule Type** to **Recurring Deployment**. Configure the setting if you do not want to re-deploy the action indefinitely. For example, you might want to stop deployment before the end of a maintenance window for the targeted endpoints. BEST PRACTICE: Specify an **End At** date-time unless you are sure that you want to re-deploy the action indefinitely. If you are not sure, configuring the schedule to end in six months is better than running indefinitely.
Distribute Over	The Tanium Server distributes actions to endpoints in batches. The **Distribute Over** option randomizes the distribution over the specified period to prevent spikes in network traffic or other resource consumption. For more information, see Conserving resources through action distribution on page 328. You can set a **Distribute Over** value only for simple actions, not adaptive actions.

© 2026 Tanium Inc. All Rights Reserved

6. Configure the **Targeting Criteria**, click **Show Preview to Continue**, and review the list of target endpoints.

   If you initiated action deployment from the **Question Results** page, the **Target Question** is based on the rows that you selected on that page. The action targets all endpoints that match the question. The question updates automatically when you change other **Targeting Criteria**. For a recurring action, only the endpoints that match the latest results of the **Target Question** perform the action.



> **NOTE**
>
> Interact applies Boolean AND logic if you add both a manual list of endpoints and computer groups.
>
> If you **Enable Ring Deployment**, the **Targeting Criteria** apply as a filter to the endpoint assignments in a deployment plan. For more information, see Endpoint targeting on page 278.

Action targeting settings

Setting	Description
Action Group	Select the action group that you want to target. For more information, see Targeting actions through action groups on page 400.
Add Computer Groups (optional)	Select one or more computer groups and click **Save**. For more information, see Controlling endpoint management rights through computer groups on page 610.
Add Manual List (optional)	Enter the computer names (case insensitive) or IP addresses of up to 100 managed endpoints and click **Save**. Use a new line or comma to separate each endpoint.
Add Filter Question (optional)	Add a filter to the `from` clause of the **Target Question** and click **Save**. For more information, see Filters in from clause.

© 2026 Tanium Inc. All Rights Reserved

7. (Adaptive actions only) Select **Enable Ring Deployment** and select a **Deployment Plan**. This option is available only for an adaptive action that meets the following conditions:

   - The action is new.
   - The **Schedule Type** is **One Time Deployment**.
   - The action is scheduled to deploy immediately, not with a future **Start At** date.
   - The action does not have a **Distribute Over** value.

   NOTE

   For more information about adaptive actions, see Ring-based deployment on page 276.

   Perform the following tasks to select and (optionally) review a deployment plan:

   - **Select a plan**

     Select the deployment plan in the **Select Plan** dropdown list. If only one deployment plan specifies a **Preferred for Deployment Type** that matches the action deployment type, that plan is the default selection. For more information, see Deployment types on page 277. You can select a different plan than the default. The dropdown list shows the Tanium icon for Tanium-managed plans.

   - **Review ring details**

     By default, each ring section is collapsed and shows only the wait time, number of progression **Criteria**, and target endpoint count. You can Expand a ring or **Expand All** rings to show additional ring settings, such as assigned endpoints and progression criteria. The Not Applicable icon indicates criteria that do not apply to the current deployment type.

     TIP

     For each ring, you can click the count of target endpoints to view a list of the endpoints. The Interact **Question Results** page shows the list in a new browser tab.

   - **Review deferred endpoints**

     If the deployment plan specifies Deferred endpoints on page 298, you also can Expand the **Deferred Endpoints** section to see the filter groups that are deferred to the last ring.

   TIP

   To view the entire deployment plan configuration in a new browser tab, click **Plan Details**. Optionally, you can then edit the plan settings. For more information, see:

   - Configure the deployment plan overview on page 386
   - Configure rings, progression criteria, and deferred endpoints on page 387

8. Click **Deploy Action** to deploy a new action or reissue an action. Click **Save Action** if you are editing an action.

© 2026 Tanium Inc. All Rights Reserved

9. If the number of **Estimated clients affected** exceeds the configured threshold (the default is 100), enter the estimated number and click **Confirm**. The Tanium Server enforces this confirmation step to ensure that you understand the impact that an action will have on your network.

   To change the threshold that controls whether Console prompts users for the **Estimated clients affected**, edit the **Prompt Estimate Threshold** setting as described in Review and edit global settings for actions on page 329.

If the action deploys immediately, a page opens automatically to show the action status. If the action requires approval or has a future start date/time, you can view its status after deployment starts in the **Action History** page or Deployment Details page. For more information, see Review action status on page 399.

Review action status

1. If the action does not require approval and deployment starts immediately, skip to the next step. Otherwise, go to **Administration > Actions > Scheduled Actions** and confirm the action is listed.

   Perform the next step after:

   a. A user approves the action, if approval is required. For more information, see Approve pending actions on page 413.

   b. Deployment starts, if it is scheduled for a future date/time.

2. Perform one of the following steps based on the type of action:

   - **Adaptive action**: The Deployment Details page opens automatically. For more information, see Analyze and manage a single deployment on page 362.
   - **Simple action**: If the action did not require approval and deployment started immediately, the **Action Status** page opens automatically. Otherwise, you can manually open the **Action Status** page from the **Action History** page after the action is approved and starts deploying. For more information, see View status for simple actions on page 352.



To troubleshoot action deployment issues, see Monitor actions.

© 2026 Tanium Inc. All Rights Reserved

Targeting actions through action groups

Action groups define which endpoints managed using Tanium Client are the targets for actions. You configure the targets by assigning computer groups to the action groups. For example, to deploy certain actions only to Active Directory domain controllers, you can create an action group with the **All Windows Domain Controllers** computer group. Use the **Action Groups** page to view the attributes of existing action groups, create or edit groups to suit your environment, and delete groups that are no longer used.

The Tanium Server automatically creates several predefined action groups and their associated computer groups as part of the initial content that is available to all deployments. For more information about the predefined groups, see Action groups and computer groups on page 48.

BEST PRACTICE

Understand the best practices for action groups and computer groups before you create or edit custom groups. For more information, see Computer groups on page 557.

NOTE

Action Group read permission is required to view action groups in the **Administration > Actions > Action Groups** page. **Action Group write** permission is required to create, edit, and delete action groups. The **Administrator** reserved role has these permissions.

View action groups

Viewing action groups can help you to determine if new groups are necessary and to manage or troubleshoot existing groups. For example, you might check which computer groups are members of an action group and check the boolean AND/OR setting to investigate why actions are not targeting all the expected endpoints.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
   For each action group, the page displays the following attributes:
   - Action group **ID** and **Name**
   - Number of assigned computer groups and whether they use Boolean AND or OR combination logic. To display a tooltip that lists the computer group names, hover over the entry in the **Computer Groups** column for the action group. The count excludes the **No Computers** computer group if it is assigned.
   - User (persona) who last modified the group and when
2. (Optional) Display action group attributes (columns) that are hidden by default, such as which users (personas) created action groups and when, by clicking Customize Columns and selecting the attributes.

© 2026 Tanium Inc. All Rights Reserved

3. (Optional) Use the filters to find specific action groups:
    - **Filter by text**: Enter a text string in the **Filter items** field to filter the grid by an alphanumeric string that matches an action group **ID**, action group **Name**, or computer group name.
    - **Filter by attribute**: Expand the **Filters** section, select an action group attribute (such as **Name**), select an operator (such as **contains**), enter an attribute value (such as `Default Content`), and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.
4. (Optional) To see the RBAC visibility setting, assigned computer groups, and associated actions of an action group, click the action group **Name**.

Create an action group

Computer management groups and filter groups are the building blocks of action groups. Therefore, you must create the necessary computer groups before performing the following steps.

NOTE

To view or create computer groups, see Controlling endpoint management rights through computer groups on page 610.

BEST PRACTICE

Understand the best practices for action groups and computer groups before you create or edit custom groups. For more information, see Computer groups on page 557 and Best practices for action groups on page 405.

1. From the Main menu, go to **Administration > Actions > Action Groups** and click **New Group**.
2. Enter a **Name** of up to 255 characters to identify the action group.
3. Select a **Visibility** option:
    - **Only administrators can see this group**: Only users with the **Administrator** or **Content Administrator** reserved role can see this action group.
    - **All users can see this action group**
    - **Limit visibility to specific user groups**: Select the **User Groups** that can see the action group.

    NOTE

    Action Group read permission overrides the **Visibility** setting. A user who has **Action Group read** and action deployment permissions can select any action group when deploying an action. A user who has **Action Group read** and **Approve Action** permissions can approve actions that target any action group. However, the computer groups that are assigned to a user still control which endpoints run an action that the user deploys to the selected action group.

© 2026 Tanium Inc. All Rights Reserved

4. Select **Computer Groups** and select the type of Boolean matching to apply:

    - **AND**: Endpoints run an action only if they are in all the computer groups that are assigned to the action group. For example, a macOS endpoint runs an action that targets an action group containing the **All Computers** and **All Mac** computer groups, but does not run an action that targets an action group containing the **All Windows** and **All Mac** computer groups.
    - **OR**: Endpoints run an action if they are in any of the computer groups that are assigned to the action group. For example, a macOS endpoint runs an action that targets an action group containing the **All Windows** and **All Mac** computer groups.

    If you select the **All Computers** or **No Computers** group, Console automatically clears any other selection because targeting for those groups works only in isolation from all other groups.

5. Click **Save**.

Edit an action group

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Click the action group **Name**.
3. Edit the settings that are listed in Create an action group on page 401.

    By default, the **Computer Groups** list is filtered to show only the **Selected** (assigned) groups. To show all the assigned and unassigned groups, click **All**.

4. Review the **Actions associated to this Group** to assess the impact of your changes and then click **Save**.

Edit action group assignments for scheduled actions

Reassign actions to a different action group as follows:

1. From the Main menu, go to **Administration > Actions > Scheduled Actions**.
2. Select the actions that you want to reassign.
3. Select **More > Change Group**.
4. Select the action group and click **Confirm**.

Export and import action groups

Export action groups

Export action groups as a file in the format required for your workflow:

© 2026 Tanium Inc. All Rights Reserved

- **CSV**

  You can use any application that supports CSV format to display the same action group attributes (columns) as the Console **Action Groups** grid shows and then customize the display. For example, you can use Microsoft Excel to create charts based on action group attributes.

- **JSON**

  You can export multiple action group configurations as a JSON file. Exporting configurations is useful if you want to import them into another Tanium environment. For example, you might test custom action groups in a lab environment to ensure that they work as intended before importing the groups into your production environment. You must be assigned a role with the **Export Content** permission to export a JSON file. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.

Perform the following steps to export action groups:

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. (Optional, CSV exports only) To add action groups IDs as a column in the CSV file, click Customize Columns in the grid and select **ID**. If you skip this step, the file show only action group names.
3. Select rows in the grid to export only specific action groups. If you want to export all action groups, skip this step.
4. Click Export.
5. (Optional) Edit the default export **File Name**.

   NOTE

   The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.

6. Select an **Export Data** option: **All** action groups in the grid or just the **Selected** action groups.
7. Select the file **Format**:
   - **List of Action Groups - CSV**
   - **Action Group Definitions - JSON** (**Administrator** reserved role only)
8. Click **Export**.

   The Tanium Server exports the file to the downloads folder on the system that you use to access Tanium Console.

Import action groups

Importing is useful if you want to copy action group configurations from another Tanium environment. For example, you might test custom action groups in a lab environment to ensure that they work as intended. You can then export the groups from the lab environment and import them into your production environment. You can import action groups and other content as a JSON or XML file.

You must be assigned a role with **Import Signed Content** permission to import content files through the following steps.

© 2026 Tanium Inc. All Rights Reserved

1. (Non-Tanium-provided content only) Digitally sign the content file and ensure a public key is in place to validate the signature. For more information, see Authenticating content files on page 482.

   NOTE

   You do not have to generate keys or signatures for Tanium-provided solutions. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process.

   If you plan to import a file that another user signed, you can first perform an integrity check on the file. For more information, see Verify content file signatures on page 487.

2. From the Main menu, go to any of the following **Administration** pages:
   - **Configuration > Solutions**
   - **Permissions > Filter Groups**
   - Under **Content**, select **Sensors**, **Packages**, or **Saved Questions**
   - Under **Actions**, select **Scheduled Actions**, **All Pending Approvals**, or **Actions I Can Approve**
3. Select an **Import** option based on the source of the content:
   - **Import > Import Files**: Perform one of the following steps to select one or more files:
     - Drag and drop files from your file explorer.
     - Click **Browse for File**, select the files, and click **Open**.
   - **Import > Import URL**: Enter the URL in the **Import URL** field, and click **Import**.
4. For each file, expand the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, **Include content set overwrite** is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Install**.

Copy action group configuration details

Copy information from the **Action Groups** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the content that you copy.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy.
   - **Copy cell information**: Hover over the cell, click Options, and click Copy.

© 2026 Tanium Inc. All Rights Reserved

Delete an action group



Do not delete the predefined action groups that Tanium solutions provide. When you import solution updates, the update process restores any predefined action groups that users have deleted.

You can delete any action group except **Default** and **Default - All Computers**. If any scheduled actions target the action group that you will delete, you can transfer those actions to another action group during the deletion workflow.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Select the action group and click **Migrate and Delete**.
3. Go to the **Actions associated to this Group** grid and perform one of the following steps based on whether any actions currently target the action group:
    - No associated actions: Go to the bottom of the dialog and click **Delete Action Group**.
    - Actions are associated:
        a. Review the **Computer Groups** that are assigned to the current action group to understand the impact of migrating the actions to a new action group.
        b. Select a new action group in the **Migrate existing scheduled actions to selected action group** dropdown list.
        c. Click **Show Preview to Continue** and review the affected computer groups and endpoints in the new action group.
        d. Click **Transfer Actions and Delete Action Group**.

Best practices for action groups

Reconfigure action groups that target No Computers

Certain action groups that you import with Initial content on page 48 include only the **No Computers** computer group. Therefore, actions that target these action groups do not deploy to endpoints until you perform one of the following tasks:

- Reconfigure the action groups to target other computer groups. For more information, see Tanium Endpoint Configuration User Guide: Configure action groups for content-only solutions.
- Reassign other action groups for the actions. For more information, see Edit action group assignments for scheduled actions on page 402.

For actions that target the **Default** action group (which includes only **No Computers**), the best practice is to change the action group assignments instead of reconfiguring **Default**.

As a best practice for weekly maintenance, review any actions that target the **Default** action group and, if appropriate, assign different action groups. For more information, see Tanium Maintenance User Guide: Review and update actions that target No Computers.

© 2026 Tanium Inc. All Rights Reserved

Define a specific use for each action group

Action groups comprise one or more computer management groups. You can create an action group for a particular event and add computer groups over time: first a test group, then groups that are based on operating system or region.

Limit access to edit action groups

Coordinate changes you make to the action groups configuration with all affected administrators. An administrator might have configured scheduled actions that target the set of computers that belong to the action group as it existed when the scheduled action was last configured.

Minimize action group complexity

When the Tanium Server issues a recurring action, action groups with long and complex targeting conditions use more resources and network traffic than groups with short and simple conditions. To reduce resource usage and traffic, minimize the number of computer groups associated with each action group and keep the definitions of those computer groups as simple as possible. For more information, see Computer groups on page 557.

© 2026 Tanium Inc. All Rights Reserved

Locking down actions on endpoints

To prevent the Tanium Client from running Tanium package scripts on certain endpoints, you can deploy an *action lock*. For example, you might prevent actions while troubleshooting endpoint issues or to protect sensitive endpoints. An action lock prevents all actions from running unless you configure overrides for the associated packages or for specific Tanium solution operations. For more information, see Override action locks on page 410 and Solution-specific impacts and overrides for action locks on page 407.

All Tanium deployments provide the content-only solution Default Content, which includes packages for turning action locks on or off for Windows and non-Windows endpoints. This solution also includes a sensor named **Action Lock Status** and saved questions that use this sensor, which enable you to track Tanium Clients that have the action lock turned on.



You must deploy an action to turn on, turn off, or test action locks. The associated packages are in the **Client Management** content set. For the user role permissions that are required to deploy actions with those packages, see Deploy actions on page 90. The saved questions and sensor that you use to track and test action locks are in the **Base** content set. For the user role permissions that are required to issue the questions, see Use Interact Saved Questions on page 83.

Solution-specific impacts and overrides for action locks

Most Tanium solutions use Endpoint Configuration for deploying tools and configuration changes to endpoints. If action locks are turned on, you must enable the **Manifest Package Ignore Action Lock** and **Deploy Client Configuration and Support Package Ignore Action Lock** settings in Endpoint Configuration. For more information, see Tanium Endpoint Configuration User Guide: Integration with other Tanium products and Tanium Endpoint Configuration User Guide: Global Endpoint Configuration settings.

You can also configure the following Tanium solutions to ignore action locks for certain operations:

- **Deploy**: Specify whether to ignore action locks for applicability scanning and deployments. For more information, see Tanium Deploy User Guide: Configure module settings.
- **Direct Connect**: Specify whether to ignore action locks for new connections and configuration changes. For more information, see Tanium Direct Connect User Guide: Configure Endpoint Connection settings.
- **Enforce**: Specify whether to ignore action locks for anti-malware enforcements. For more information, see Tanium Enforce User Guide: Action Lock Override.

For more information about how action locks affect other Tanium solutions, see the associated user guides:

- Asset
- Client Management:
    - Access detailed client health and troubleshooting information on an endpoint
    - Upgrade Tanium Clients using Client Management

© 2026 Tanium Inc. All Rights Reserved

- Comply
- Discover
- Patch

Turn on action locks

Windows and non-Windows endpoints require separate packages for turning on action locks. Therefore, perform the following steps for each type of endpoints:

1. List the endpoints where action locks are turned off by issuing a question such as:
   `Get Is Windows and Action Lock Status from all machines with Action Lock Status contains Action Lock Off`
   Perform the remaining steps for Windows endpoints and then again for non-Windows endpoints.
2. Select the endpoints that require the action lock turned on, and click **Deploy Action**.
3. Select the **Deployment Package** that matches the target endpoints:
   - Windows endpoints: **Tanium Client - Set Action Lock On**
   - Non-windows endpoints: **Tanium Client (Non-Windows) - Set Action Lock On**
4. Configure the remaining action settings and deploy the action. For more information, see Configure action settings on page 395.
5. Monitor the action status. For more information, see View status for simple actions on page 352.
   If you want to Test action locks on page 408, record the **Action ID** and wait for the action to complete.

Test action locks

1. Issue the saved question **Clients That Cannot Take Actions - Action Lock On**. For more information, see Issue a saved question on page 466.
2. Check the **ActionLockFlag** setting on an endpoint that is included in the question results. Turning on action locks creates the setting on endpoints and sets its value to 1.
   a. Sign in to the endpoint and open a **Command Prompt**.

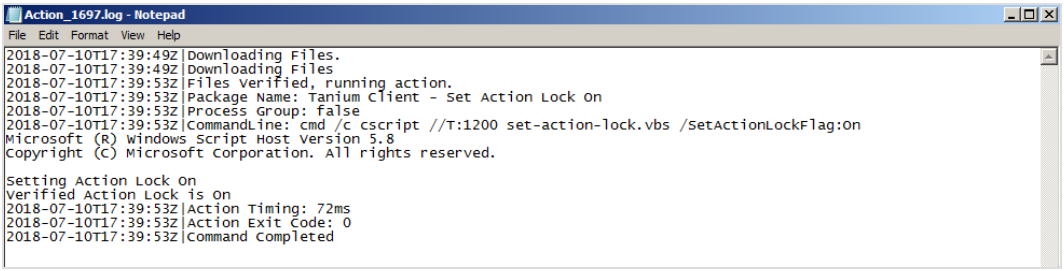
   For more information about the Tanium Client CLI, see Tanium Client Management User Guide: Tanium Client command line interface (CLI).

   b. Navigate to the Tanium Client installation directory:
   ```
   cd <installation directory>
   ```
   c. Verify that the **ActionLockFlag** value is 1:
   `TaniumClient config get ActionLockFlag`

© 2026 Tanium Inc. All Rights Reserved

```
1
```

3. On the endpoint, open the associated action log and look for a message that indicates the action lock is on. Action logs are in the `<Tanium_Client_installation_directory>/Downloads` folder. You can identify the log for a specific action by the log file name (`Action_<ID>.txt`), which contains the **Action ID**. For more information, see Track action IDs on page 355.



4. Deploying actions and playbooks in Console and Interact on page 391 to the endpoint. After the **Action Status** page opens, the action eventually times out and its status changes to **Expired**. The **Administration > Actions > Action History** page shows the **Status** as `Closed` after the action expires.

Turn off action locks

Windows and non-Windows endpoints require separate packages for turning off action locks. Therefore, perform the following steps for each type of endpoint:

1. Issue the saved question **Clients That Cannot Take Actions - Action Lock On**. For more information, see Issue a saved question on page 466.
   Perform the remaining steps for Windows endpoints and then again for non-Windows endpoints.
2. Select the endpoints that require the action lock turned off, and click **Deploy Action**.
3. Select the **Deployment Package** that matches the target endpoints:
   - Windows endpoints: **Tanium Client - Set Action Lock Off**
   - Non-windows endpoints: **Tanium Client (Non-Windows) - Set Action Lock Off**
4. Configure the remaining action settings and deploy the action. For more information, see Configure action settings on page 395.
5. Monitor the action status and wait for the action to complete: see View status for simple actions on page 352.
   Perform the remaining steps to verify that the action lock is off.
6. Re-issue the saved question **Clients That Cannot Take Actions - Action Lock On** and verify that the results do not include the endpoints for which you turned off the action lock.

© 2026 Tanium Inc. All Rights Reserved

7. Review the Tanium Client settings on an endpoint that is not included in the question results. Turning off the action lock removes the **ActionLockFlag** setting on endpoints.

   a. Sign in to the endpoint and open a **Command Prompt**.

   > NOTE
   >
   > For more information about the Tanium Client CLI, see Tanium Client Management User Guide: Tanium Client command line interface (CLI).

   b. Navigate to the Tanium Client installation directory:

   ```
   cd <installation directory>
   ```

   c. Verify that the list of settings does not include **ActionLockFlag**:

   ```
   TaniumClient config list
   ```

8. On the endpoint, open the associated action log and look for a message that indicates the action lock is off. Action logs are in the `<Tanium_Client_installation_directory>/Downloads` folder. You can identify the log for a specific action by the log file name (`Action_<ID>.txt`), which contains the **Action ID**. For more information, see Track action IDs on page 355.

Override action locks

To override action locks for certain operations that Tanium solutions perform, see Solution-specific impacts and overrides for action locks on page 407.

To override action locks for a specific action, perform the following steps to edit the associated package before deploying the action.

> BEST PRACTICE
>
> If a package is Tanium-defined content, clone it and edit the clone instead of editing the original package. For more information, see Tip 4: Limit customizations to Tanium content on page 138. You require **Package write** permission on the content set of a package to edit it.

1. Consult whoever turned on action locks to verify that it is safe to run the action on the target endpoints.
2. From the Main menu, go to **Administration > Content > Packages** and click the package **Display Name**.
3. Click **Edit Mode** , select **Ignore Action Lock**, and click **Save**.

© 2026 Tanium Inc. All Rights Reserved

Managing action approval

Action approval overview

Actions can have a significant impact on your environment. To mitigate the risk of unexpected impacts, some organizations require two-person integrity, which means that actions a user initiates cannot deploy to endpoints until another user approves those actions. To implement two-person integrity in a Tanium environment, you enable action approval and configure the RBAC for approving pending actions. A *pending action* is one that is initiated but not yet approved.

RBAC for action approval

Action approvers can be users with the **Administrator** reserved role or a role that grants **Approve Action** and **Sensor read** permissions. If your organization allows exceptions to approval requirements, you can configure a role that grants **Bypass Action Approval** permission.

Tanium Endpoint Configuration 1.6 or later automatically bypasses approval at the Tanium Core Platform level when deploying actions that distribute Tanium Client configuration and manifest packages. To require approval for these actions, configure Endpoint Configuration approvals. For more information, see Tanium Endpoint Configuration User Guide: Managing approvals.



For more information about the role permissions for managing action approval, see Manage action approval on page 97.

Approval impact on action timing

Approval affects action timing based on whether a **Start At** time is configured in the Action schedule settings on page 396:

- **Start At** time omitted: The action deploys immediately after it is approved, provided other action conditions do not preclude the Tanium Server from deploying it.
- **Start At** time specified: The action deploys at the next start time following approval. For example, if you set the action to deploy daily at 1:00 am and a user approves it at 2:00 am, the action deploys the next day at 1:00 am.

Create an action approver role

Users who have a role that grants **Approve Action** permission can approve pending actions that are associated with packages in the specified content sets.

1. From the Main menu, go to **Administration > Permissions > Roles**.
2. Configure a custom role on page 586 that grants **Approve Action** and **Sensor read** permissions on the content sets that you specify, and click **Save**.

© 2026 Tanium Inc. All Rights Reserved

Create a bypass action approval role

Users who have a role that grants **Bypass Action Approval** permission are not subject to approval requirements when they deploy actions that are associated with packages in the specified content sets.

1. From the Main menu, go to **Administration > Permissions > Roles**.
2. Configure a custom role on page 586 that grants **Bypass Action Approval** permission on the content sets that you specify, and click **Save**.

Assign the action approval and bypass roles

You can assign the action approval and bypass roles to personas, users, and user groups:

- Manage role assignments for a persona on page 658
- Manage role assignments for a user on page 631
- Managing user groups on page 643

Enable or disable action approval

1. From the Main menu, go to **Administration > Configuration > Settings > Platform Settings**.
2. Set **Require Action Approval** to **ON** (enable) or **OFF** (disable), and click **Save All**.
3. (Optional) Give users the option to approve multiple actions without being prompted to review the action configurations: set **Bulk Approval** to **ON** (enable) or **OFF** (disable), and click **Save All**.
   This setting enables the **More > Bulk Approval** option in the **Actions I can Approve** page.



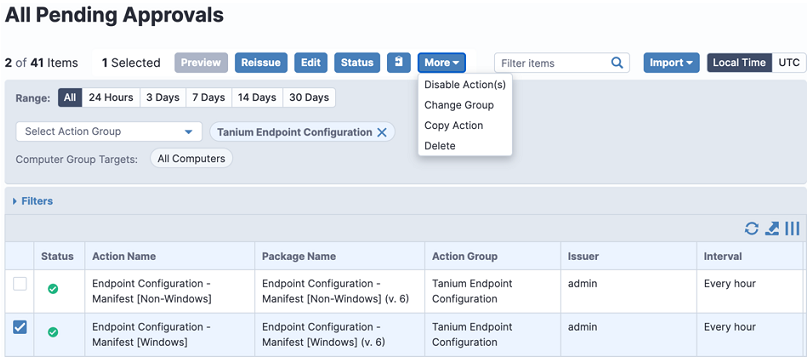
If any pending actions exist when you disable action approval, those actions can never deploy. To avoid this, ask your approver to delete the pending actions before disabling the feature. Alternatively, after disabling the feature, go to **Administration > Actions > Scheduled Actions**, review the pending actions, and reissue any that are still needed.

Review and manage pending actions

When action approval is enabled, users with the **Administrator** reserved role can display the **Administration > Actions > All Pending Approvals** page. The page has the same fields and action buttons as the **Administration > Actions > Scheduled Actions** page, but displays only the actions that are waiting for approval. For information about the fields and buttons, see Manage scheduled actions on page 342.

© 2026 Tanium Inc. All Rights Reserved

All Pending Approvals page



Approve pending actions

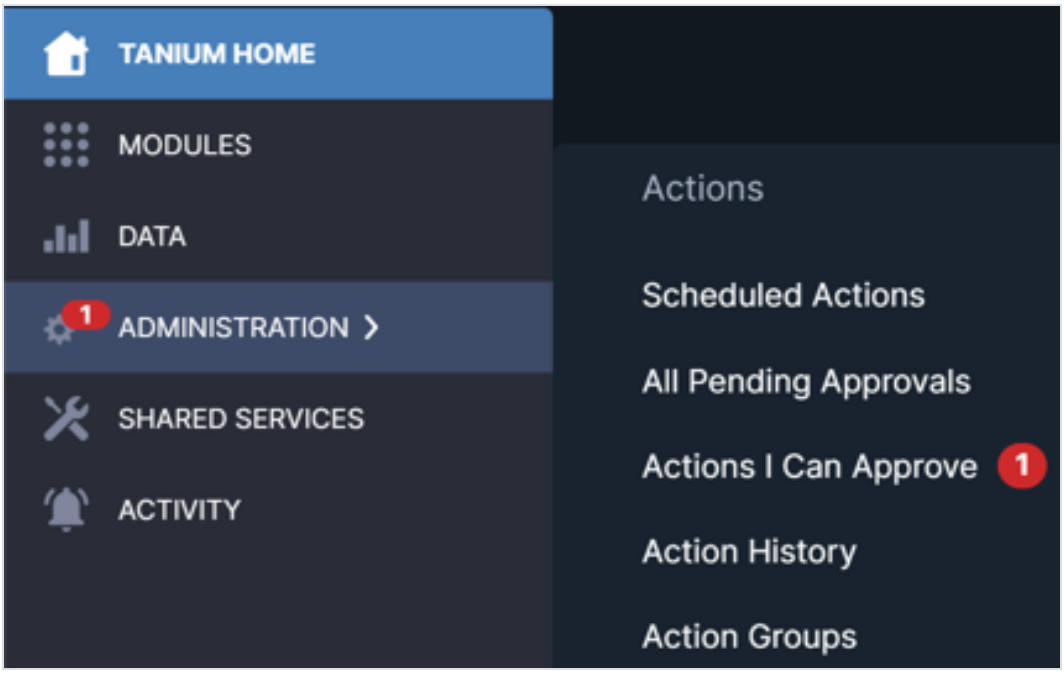
You can approve one-time only or recurring (scheduled) actions that other users create. For recurring actions, approval is a manual process only for the first deployment interval and is automatic for subsequent intervals. The approval remains in force until the **End At** date-time that is set in the action configuration or until another user modifies the configuration.

NOTE

Even if you are assigned a role that grants **Approve Action** permission, you cannot approve an action that you modified. If you modify an action, only other users who have **Approve Action** permission can approve it.

1. Sign in as a user who is assigned a role with **Approve Action** permission.

   The **Administration** menu and its **Actions > Actions I Can Approve** sub-menu show the number of actions that you can approve.



© 2026 Tanium Inc. All Rights Reserved

2. From the Main menu, go to **Administration > Actions > Actions I Can Approve**.
3. (Optional) To find specific actions, configure the filters described in Filtering options for scheduled actions on page 343.
4. Select the actions that you want to approve and perform one of the following steps:
   - To approve actions without reviewing their configurations, select **More > Bulk Approval** and click **Confirm**. You can skip the remaining steps. This option is available only if the **Bulk Approval** setting is enabled. For more information, see Enable or disable action approval on page 412.
   - To review action configurations before approving them, click **Preview** and perform the remaining steps.
5. Review the action configuration and click **Approve**. If you selected multiple actions, use the Previous and Next widgets to navigate among the pages for each action.
   Tanium Console indicates the estimated number of endpoints that the action will affect, as entered by the user who created the action. Note that the Tanium Server does not recalculate this estimate during the approval workflow; the displayed number is the same as when the action creator configured the action, regardless of how the actual endpoint count might have changed since then.
6. If the number of **Estimated clients affected** exceeds the configured threshold (default is 100), enter the estimated number and click **Confirm**.
   The Tanium Server enforces this confirmation step to ensure that you understand the impact that the action will have on your network.

   TIP

   To change the threshold that controls whether Tanium Console prompts approvers for the **Estimated clients affected**, go to **Administration > Configuration > Settings > Platform Settings** and edit the **Prompt Estimate Threshold** setting. Note that changing the value to 0 causes Tanium Console to prompt approvers regardless of the number of affected endpoints.

© 2026 Tanium Inc. All Rights Reserved

Solution content overview

What is content?

In a Tanium deployment, *content* refers to configuration objects such as sensors, packages, saved questions, dashboards, filter groups, and scheduled actions. You use content in various operations for managing, monitoring, and protecting your environment. For example, you can use the **Running Applications** saved question to determine which applications are running on endpoints and use the **All Windows** filter group to show results only from Windows endpoints. You might then deploy an action that runs the **Kill Application** package to stop a specific application on those endpoints.

Tanium provides predefined content through solutions that you manually import or that the Tanium Server imports automatically. For example, Tanium Comply provides predefined reports for vulnerability findings. For more information, see Part 4: Managing Tanium solutions on page 108.

You can create custom content to extend Tanium solutions for particular environments or objectives. For example, if users start using a new application in your environment, a content developer can write a sensor script that maintains data about the application and write a package script that starts or stops the application.

Custom content development

Content developers require the following knowledge and experience:

- Understanding of the Tanium Core Platform
- Expert knowledge of endpoint operating systems (OSs)
- Experience writing and testing scripts that are written in shell script (non-Windows endpoints) or Python



When you choose a scripting engine for custom sensors or packages, note that Microsoft has announced the deprecation of VBScript. For more information, see Tanium Community article: VBScript Retirement in a future Windows Release (sign in required).

Your team might include content developers who create saved questions that you can reissue at scheduled intervals or that you can associate with packages for deploying actions. These content developers do not necessarily write scripts, but they must be aware of the systems and processes running on endpoints, understand the impact that scheduled questions and actions might have on endpoints, and make any necessary adjustments. For more information, see Best practices for saved questions on page 456 and Action best practices on page 324.

As much as possible, most customers leverage the content that Tanium solutions provide, and work with Tanium Support on customizations and new scenarios. For more information, see Contact Tanium Support on page 724.

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

When developing custom content for the Tanium Core Platform, examine Tanium-defined content for examples of code and settings that were tested for best results. Use the tested sensors and packages as models for your custom content.

Create custom content instead of editing content that is provided through Tanium solutions. For more information, see Tip 4: Limit customizations to Tanium content on page 138.

Develop and test custom content in your lab environment before distributing the content to the Tanium Servers in your production environment. You can use Tanium Console to export and import content between Tanium Servers. For more information, see Part 4: Managing Tanium solutions on page 108.

TIP

If you need new content that is similar to existing content except for a few settings, cloning existing content is often easier than creating new content from scratch.

Managing content

To view, clone, create, edit, or delete core content that you use in Tanium Console and Interact, see:

- Managing sensors for collecting endpoint data on page 421
- Managing packages for platform actions on page 442
- Managing filter groups for filtering questions and results on page 476
- Managing saved questions in Console and Interact on page 455
- Manage categories and dashboards on page 469

You can also manage content that is specific to a Tanium solution. For example, Tanium Reporting provides predefined reports and dashboards, and you can create your own. To manage content for a specific solution, go to the Tanium Resource Center and view the user guide for that solution.

Content sets

All content is assigned to content sets. The roles that you assign to users control access to the content sets. For more information, see Managing access to content through content sets on page 561.

Content-only solutions

Some Tanium solutions provide only content and do not have a workbench or service. For more information, see Content-only solutions on page 120.

To see documentation for content-only solutions, see Tanium Core Content Documentation.

© 2026 Tanium Inc. All Rights Reserved

Content ownership

By default, the user account or persona that a user selects for a Tanium Console or API session is the owner of any content that the user creates during the session. However, you can transfer ownership if you plan to delete a user account or persona or you plan to change its assigned roles or computer groups. For more information, see Delete content or transfer ownership on page 637.

Content exports and imports

You can export content as a file in CSV or JSON format. You can import a JSON file into another Tanium environment. For example, you can export sensor configurations as a JSON file from one Tanium environment and import the file into another environment. For more information, see:

- Export content files on page 133
- Import content files on page 134

© 2026 Tanium Inc. All Rights Reserved

Solution content overview

What is content?

In a Tanium deployment, *content* refers to configuration objects such as sensors, packages, saved questions, dashboards, filter groups, and scheduled actions. You use content in various operations for managing, monitoring, and protecting your environment. For example, you can use the **Running Applications** saved question to determine which applications are running on endpoints and use the **All Windows** filter group to show results only from Windows endpoints. You might then deploy an action that runs the **Kill Application** package to stop a specific application on those endpoints.

Tanium provides predefined content through solutions that you manually import or that the Tanium Server imports automatically. For example, Tanium Comply provides predefined reports for vulnerability findings. For more information, see Part 4: Managing Tanium solutions on page 108.

You can create custom content to extend Tanium solutions for particular environments or objectives. For example, if users start using a new application in your environment, a content developer can write a sensor script that maintains data about the application and write a package script that starts or stops the application.

Custom content development

Content developers require the following knowledge and experience:

- Understanding of the Tanium Core Platform
- Expert knowledge of endpoint operating systems (OSs)
- Experience writing and testing scripts that are written in shell script (non-Windows endpoints) or Python



When you choose a scripting engine for custom sensors or packages, note that Microsoft has announced the deprecation of VBScript. For more information, see Tanium Community article: VBScript Retirement in a future Windows Release (sign in required).

Your team might include content developers who create saved questions that you can reissue at scheduled intervals or that you can associate with packages for deploying actions. These content developers do not necessarily write scripts, but they must be aware of the systems and processes running on endpoints, understand the impact that scheduled questions and actions might have on endpoints, and make any necessary adjustments. For more information, see Best practices for saved questions on page 456 and Action best practices on page 324.

As much as possible, most customers leverage the content that Tanium solutions provide, and work with Tanium Support on customizations and new scenarios. For more information, see Contact Tanium Support on page 724.

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

When developing custom content for the Tanium Core Platform, examine Tanium-defined content for examples of code and settings that were tested for best results. Use the tested sensors and packages as models for your custom content.

Create custom content instead of editing content that is provided through Tanium solutions. For more information, see Tip 4: Limit customizations to Tanium content on page 138.

Develop and test custom content in your lab environment before distributing the content to the Tanium Servers in your production environment. You can use Tanium Console to export and import content between Tanium Servers. For more information, see Part 4: Managing Tanium solutions on page 108.

TIP

If you need new content that is similar to existing content except for a few settings, cloning existing content is often easier than creating new content from scratch.

Managing content

To view, clone, create, edit, or delete core content that you use in Tanium Console and Interact, see:

- Managing sensors for collecting endpoint data on page 421
- Managing packages for platform actions on page 442
- Managing filter groups for filtering questions and results on page 476
- Managing saved questions in Console and Interact on page 455
- Manage categories and dashboards on page 469

You can also manage content that is specific to a Tanium solution. For example, Tanium Reporting provides predefined reports and dashboards, and you can create your own. To manage content for a specific solution, go to the Tanium Resource Center and view the user guide for that solution.

Content sets

All content is assigned to content sets. The roles that you assign to users control access to the content sets. For more information, see Managing access to content through content sets on page 561.

Content-only solutions

Some Tanium solutions provide only content and do not have a workbench or service. For more information, see Content-only solutions on page 120.

To see documentation for content-only solutions, see Tanium Core Content Documentation.

© 2026 Tanium Inc. All Rights Reserved

Content ownership

By default, the user account or persona that a user selects for a Tanium Console or API session is the owner of any content that the user creates during the session. However, you can transfer ownership if you plan to delete a user account or persona or you plan to change its assigned roles or computer groups. For more information, see Delete content or transfer ownership on page 637.

Content exports and imports

You can export content as a file in CSV or JSON format. You can import a JSON file into another Tanium environment. For example, you can export sensor configurations as a JSON file from one Tanium environment and import the file into another environment. For more information, see:

- Export content files on page 133
- Import content files on page 134

© 2026 Tanium Inc. All Rights Reserved

Managing sensors for collecting endpoint data

Sensors overview

When you issue a question to retrieve information from endpoints, each sensor in the question includes a script that runs on the endpoints to compute the information. Tanium Clients return the information to the Tanium Server, which shows the information on the Interact **Question Results** page. For example, you can issue a question with the **Running Applications** sensor to view the name and version of each application that is running on endpoints.

NOTE

For more information about how Interact shows sensor results, see What is a sensor? on page 232.

You can also use sensors to define Dynamic membership on page 614 of the endpoints in the following types of computer groups:

- Computer management groups, which control user access to endpoints when issuing questions or deploying actions.
- Filter groups, which you can use as filters in questions and question results.

The Tanium Server automatically imports Initial content on page 48 that includes sensors for a wide range of common questions. Other Tanium solutions that you import might provide more sensors. If you cannot find a sensor that you need within Tanium-provided content, you can create custom sensors.

NOTE

For the role permissions required to manage sensors, see Manage sensors on page 98.

Sensor scripts

A sensor configuration includes settings, script content, and script parameters. Sensors use industry-standard scripting languages rather than proprietary coding syntax. When you create custom sensors, the best practice is to use the scripting engine that is available on the largest number of managed endpoints. On macOS and Linux endpoints, shell script generally provides the most comprehensive out-of-the-box coverage. You can develop sensors using any other scripting language that the operating system (OS) supports (such as PowerShell on Windows) if the associated scripting engine exists on endpoints. You can deploy and configure the engine on any endpoints where the engine is not present.

IMPORTANT

Windows endpoints require certain configurations to enable some Tanium sensors and packages that rely on Windows Management Instrumentation (WMI) queries, VBScript, and PowerShell. For more information, see Tanium Client Management User Guide: Prepare for deployment to Windows endpoints.

When you choose a scripting engine for custom packages, note that Microsoft has announced the deprecation of VBScript. For more information, see Tanium Community article: VBScript Retirement in a future Windows Release (sign in required).

© 2026 Tanium Inc. All Rights Reserved

Parameterized sensors

A parameterized sensor requires input (parameter values) from users before the sensor can collect results from endpoints. When you issue a question or configure a computer group that uses a parameterized sensor, the Tanium Server creates an object called a *temporary sensor*, which contains the substituted parameter values and a link to the actual sensor. For more information, see:

- Questions with parameterized sensors on page 238
- Dynamic membership on page 614 (for computer groups)
- Example: Parameterized sensors on page 495

Virtual sensors

Tanium solutions use virtual sensors to provide data for endpoints without running scripts on those endpoints. Virtual sensors are useful for exploring data that Tanium Clients cannot provide directly. You use reports in Tanium Reporting or other Tanium solutions to view virtual sensor data because the Interact **Question Results** page shows data only for non-virtual sensors. For example, Tanium Benchmark provides a report that uses the virtual sensor **Tanium Risk Score** to show risk metrics for endpoints. Benchmark derives the sensor data from multiple sources that do not exist on the endpoints.

Solutions might also generate virtual sensor data based on data from multiple non-virtual sensors. For example, Tanium Data Service (TDS) uses three non-virtual sensors to generate data for the virtual sensor **Endpoint ID**. **Endpoint ID** is a useful identifier for endpoints because its value is more likely to be unique and stable for each endpoint than the individual values of the three non-virtual sensors. For more information, see Tanium Interact User Guide: Endpoint identification sensors.

VIRTUAL SENSOR CREATION AND REGISTRATION

Tanium solutions automatically create virtual sensors and register them with TDS. For example, Tanium Asset creates a corresponding virtual sensor when you add a custom entity, such as **Custom Asset: Boot Time**. A solution might also provide virtual sensors along with other content when you import the solution. For example, Tanium™ Criticality provides the **Endpoint Criticality with Level** sensor, which you can add to a report to view endpoint criticality levels and rules.

VIRTUAL SENSOR LIMITATIONS

Virtual sensors have the following limitations:

Limitations of virtual sensors

Limitation	Description
Sensor management	All virtual sensors are predefined and you cannot perform the following management tasks on them: • Create, edit, delete, or view the configurations of virtual sensors. In Tanium Console, the **Sensors** page does not show virtual sensors. • Quarantine virtual sensors. In Console, the **Quarantined Sensors** page does not show virtual sensors. • Unregister virtual sensors or purge their results in TDS. In Interact, the **Registration and Collection** page does not list virtual sensors because they are not included in the questions that TDS periodically issues to collect updated sensor results from Tanium Clients. For more information, see Tanium Interact User Guide: Managing Tanium Data Service (TDS).

© 2026 Tanium Inc. All Rights Reserved

Limitations of virtual sensors (continued)

Limitation	Description
Questions	You cannot use Tanium Interact to issue questions with virtual sensors. This limitation also applies to the filtering questions that you configure in the targeting criteria of actions.
Computer groups	You cannot use virtual sensors to define endpoint membership in computer management groups and filter groups.

Solution-generated sensor attributes

Each sensor result provides one or more attributes (columns) of data that you can see on the **Question Results** page in Tanium Interact or in reports that Tanium Reporting and other solutions provide. In most cases, Tanium Clients run the sensor script to provide all the attribute data when you issue a question that uses the sensor. However, for certain sensors, Tanium solutions add attributes with data that Clients do not provide. These solution-generated attributes are useful for exploring data that is not available on endpoints.

You use reports in Tanium Reporting or other Tanium solutions to view sensors with solution-generated attributes. The Interact **Question Results** page shows data only for sensors with exclusively Client-provided attributes.

EXAMPLE: SENSOR WITH COMPLY-GENERATED ATTRIBUTES

Tanium Data Service (TDS) periodically collects data from Tanium Clients for the **Comply - Compliance Status** sensor because Tanium Comply automatically registers that sensor with TDS. The Clients return values for all the sensor attributes, including the Check ID, which identifies compliance rules. Comply uses the Check ID values to find attributes related to compliance standards, benchmark profiles, and benchmark rules. The data for these additional attributes comes from compliance standards that are imported into Comply rather than from data that exists on Clients. Comply adds the attributes to a sensor named **Comply - Compliance Findings Details**, which is available for reports but not for Interact questions.

LIMITATIONS FOR SENSORS WITH SOLUTION-GENERATED ATTRIBUTES

Sensors with solution-generated attributes have the same limitations as virtual sensors. For more information, see Limitations of virtual sensors on page 422.

Sensor results caching and refreshing

Tanium Clients re-run sensors at a configurable frequency to update results. The frequency affects the accuracy of results and affects resource consumption on endpoints.

In a sensor configuration, the **Max Sensor Age** setting specifies the maximum time for which the Tanium Client can use a cached result for the sensor, instead of re-executing it for a fresh result, when answering questions. For example, the maximum age for the **File Size** sensor is 15 minutes by default. When a Client receives a question that executes the **File Size** sensor, it caches the result. Within the next 15 minutes, if the Client receives another question with the **File Size** sensor, it returns the cached result. After 15 minutes, if the Client receives a question with the **File Size** sensor, it re-executes the sensor script to return a fresh result.

To improve the accuracy of results, use shorter ages for sensors with values that change frequently, such as status and utilization sensors. To reduce unnecessary CPU usage on endpoints, use longer ages for sensors with values that typically do not change frequently, such as the chassis type or Active Directory domain membership.

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

A lower **Max Sensor Age** increases CPU usage on endpoints. Therefore, lower ages are more appropriate for sensors that you use in dynamic questions than for sensors in saved questions that periodically reissue or in the endpoint membership questions of computer management groups and filter groups.

NOTE

By default, the **Max Sensor Age** applies to all questions that use the sensor. To set a different age for the sensor in a specific question, see Maximum Data Age.

Client restarts do not cause a re-evaluation of the elapsed time for the **Max Sensor Age**.

Sensor data types

A sensor configuration specifies the data type for the values that the sensor returns. Choosing the correct type is required for the Tanium Server to properly evaluate results and sort them in results grids. For example, if you issue the question `Get Uptime > "10 days"`, the Server evaluates the greater than (`>`) operation based on the **Time Duration** type of the **Uptime** sensor. This ensures that the Server returns results only for endpoints that rebooted more than 10 days ago. If that sensor used the **Text** result type instead, the Server would evaluate the operation alphabetically and return results such as `2 days`.

NOTE

For a multi-column sensor, set the **Result Type** to **Text** and then select a specific result type for each column. For example, the **Tanium Client Dump Files** sensor returns both **Date/Time (WMI)** and **Integer** result types.

Different sensors can return values in different units even if the sensors use the same result type. For example, the **Tanium Client CPU** sensor returns a percentage value while the **CPU Speed Mhz** sensor returns a megahertz value, even though both sensors use the **Numeric** result type.

The following table describes the sensor result types.

Sensor result types

Type	Description
Text	An alphanumeric text string. For example, the **Computer Name** sensor returns a string such as `workstation-1.company.com`.
File Size	The size of the result, including both the number and units. For example, the **Page File Details** sensor returns size values for the page files on a Windows endpoint, such as `11264 MB` for the **Size On Disk**. TIP To return size values without the associated units, select **Integer** as the result type. For instance, a sensor that returns file sizes and uses **Integer** as the result type displays only the number of bytes: `1048576` instead of `1 MB`, as an example.

© 2026 Tanium Inc. All Rights Reserved

Sensor result types (continued)

Type	Description
IP Address	One or more IPv4 and/or IPv6 addresses. For example, the **Tanium Client IP Address** sensor returns the IP address (such as `192.168.1.1`) that a Tanium Client is using to communicate with the Tanium Server or Tanium Zone Server.
Version	The version of an operating system, file, application, or other component on an endpoint. For example, the **NET Version** sensor returns the full version numbers of all .NET installations, such as version `4.5.51641`.
Numeric	A number that can have decimals and a positive or negative value. For example, the **Tanium Client CPU** sensor returns the percentage of CPU usage that the Tanium Client process currently uses on an endpoint, such as `1.4`. TIP For sensors that return unsigned whole numbers, select the **Integer** result type instead.
Date/Time (RFC822)	A date-time string in RFC-822 format. For example, the **OS Boot Time** sensor returns the date and time when an endpoint operating system last booted.
Date/Time (WMI)	A date-time string in Windows Management Instrumentation (WMI) format. For example, the **Tanium Client Dump Files** sensor returns the date and time when a Tanium Client dump file was created on an endpoint, such as `2017-09-13T18:29:22.412Z`.
Time Duration	A time range. For example, the **Uptime** sensor returns the number of days since the last reboot of an endpoint, such as `48 days` or `Less than 1 day`. Results can include units other than days (such as `42 minutes` or `8 hours`) and can include multiple units (such as `2 years, 3 months, 18 days, 4 hours, 22 minutes and 3.67 seconds`).
Integer	An unsigned whole number, which excludes decimal values and negative values. For example, the **RAM Slots Unused** sensor returns the number of empty, unused RAM slots, such as `2`.

View sensor details

Viewing sensor attributes and runtime metrics can help you to determine if new sensors are necessary and to manage or troubleshoot existing sensors. For example, viewing the script that a sensor runs on endpoints can help you troubleshoot unexpected question results. A high runtime indicates the sensor consumes more endpoint resources than most sensors typically do.

1. From the Main menu, go to **Administration > Content > Sensors**.
   The **Sensors** grid displays columns for most of the sensor attributes that are described in Create a sensor on page 427.
2. (Optional) To display attributes that the grid hides by default, click Customize Columns and select the attributes.
3. (Optional) For the **Runtime** option, click **Show** to display sensor runtime metrics or **Hide** (default) to conceal them.
   For each sensor, the **Runtime** column displays an icon that indicates whether the sensor has exceeded a runtime threshold. You can hover over the icon to display a tooltip with the runtime average in milliseconds. For more information, see Assessing question impacts on endpoints through sensor runtime indicators on page 438.

© 2026 Tanium Inc. All Rights Reserved

> TIP
>
> Set the **Show Hidden** option to **Yes** to display hidden sensors and a **Hidden State** column, which indicates which sensors are configured as **Visible** or **Hidden**. For more information, see Hide this sensor from sensor lists and parse results on page 428.

4. (Optional) Use the filters to find specific sensors:
   - **Filter by text**: Enter a text string in the **Filter items** field to filter the grid by sensor **Name**, **Category**, or **Description**.
   - **Filter by attribute**: Expand the **Filters** section, select a sensor attribute (such as **Content Set** assignment), select an operator (such as **contains**), enter a text string that contains all or part of the attribute value, and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.
5. (Optional) To see all the attributes that are described in Create a sensor on page 427, click a sensor **Name**.

Clone a sensor

Cloning is useful when you need to:

- Create a modified version of a predefined sensor from a Tanium content-only solution.

  > BEST PRACTICE
  >
  > Do not modify a predefined sensor.

- Create a new sensor with settings that differ only slightly from an existing sensor. This is often easier than creating a new sensor from scratch.

Review Custom content development on page 418 and Sensor scripts on page 421 before you clone a sensor.

> NOTE
>
> You cannot clone sensors that are configured for endpoints managed using Part 1: Tanium Console and Interact overview on page 42.

Perform the following steps to clone a sensor:

1. From the Main menu, go to **Administration > Content > Sensors**.
2. Use the search and column sorting features to find the sensor that you want to clone.
3. Select the sensor and click **Clone**.
4. Configure the settings as described in Create a sensor on page 427 and click **Save**.

© 2026 Tanium Inc. All Rights Reserved

Create a sensor

Create a custom sensor for endpoint data collection scenarios that Tanium-defined sensors do not address. For example, you might create a sensor to collect information about a specific application installed on endpoints. As another example, you might create a sensor that is similar to an existing sensor except for the content set assignment to ensure that only certain users can use the sensor in questions.

Instead of creating a new sensor from scratch, cloning is usually easier if the sensor settings differ only slightly from an existing sensor. For more information, see Clone a sensor on page 426.

Review Custom content development on page 418 and Sensor scripts on page 421 before you perform the following steps to create a custom sensor.

1. From the Main menu, go to **Administration > Content > Sensors** and click **New Sensor**.
2. Configure the sensor **Details**.

Sensor details

Detail	Description
Name	Enter a name of up to 255 characters to identify the sensor wherever Tanium Console displays sensor lists. The name cannot have certain special characters and the best practice is to avoid reserved words. However, certain Tanium-defined sensors use reserved words in their names. For more information, see Use reserved words or characters on page 735.  If you change the sensor name, reconfigure content that references it. For example, update the sensor name in any saved questions that are configured with the previous name.
Description	Enter a description to help other users understand the purpose of the sensor. It might help to include examples of formatted results. The description appears in the **Sensors** page and in the **Browse Sensors** dialog of the **Question Builder**.
Content Set	Assign the sensor to a content set. The list is populated with all content sets for which you have **Sensor write** permission.

3. Configure the sensor **Settings**.

Sensor settings

Detail	Description
Category	Select the sensor category, which you can use to filter the list of sensors on the **Sensors** page and in the **Browse Sensors** dialog of the **Question Builder**.

© 2026 Tanium Inc. All Rights Reserved

Sensor settings (continued)

Detail	Description
Result Type	Select the data type for the values that the sensor returns. Choosing the correct type is required for the Tanium Server to properly evaluate results and sort them in results grids. For more information, see Sensor data types on page 424.
Max Sensor Age	Enter the maximum time for which the Tanium Client can use a cached result for this sensor, instead of re-executing it for a fresh result, when answering questions. For more information, see Sensor results caching and refreshing on page 423.
Max String Age	To adjust the impact that results for the sensor have on Tanium Server disk space, select **Enable** and specify the maximum age that answer strings for the sensor can reach before the Server removes them. For more information, see Maximum string age on page 758.
Max Strings	To reduce the impact that question results have on Tanium Server disk space, select **Enable** and enter the maximum number of answer strings that the Server stores for this sensor before removing the oldest strings. For more information, see Maximum strings per sensor on page 758.  BEST PRACTICE When limiting string growth, set the **Max Strings Age** instead of the **Max Strings**. For more information, see Reference: Manage sensor string growth on page 758. Contact Tanium Support on page 724 before setting the **Max Strings** in extreme cases that might require a string count limit for individual sensors.
Ignore case in result values	Group and count result values regardless of differences in upper-case and lower-case characters.  NOTE By default, this setting applies to all questions that use the sensor. To control case sensitivity for the sensor in a specific question, see Case Sensitivity.
Hide this sensor from sensor lists and parse results	Select this option if you want sensor lists throughout Tanium Console to exclude the sensor.
Split into multiple columns	(Multi-column sensors only) If the sensor returns multiple results from each endpoint, display the results in multiple columns on the **Question Results** grid. For more information, see Configure settings for multi-column sensors on page 493.  IMPORTANT When creating questions that filter multi-column sensors, single-column filtering works only if the sensor definition specifies column delimiters with a single character (such as `|`), not multiple characters (such as `|:`).

4. Configure the **Parameters** if this is a parameterized sensor. For more information, see Example: Parameterized sensors on page 495.

© 2026 Tanium Inc. All Rights Reserved

5. Configure the **Scripts** by performing the following steps for each target operating system (OS):
    a. Select the OS type and select **Enable sensor for <*OS*> platform**.
    b. Set the **Query Type** to the desired scripting engine.
    c. Enter the script text.

    > NOTE
    > For a parameterized sensor, see Script for a parameterized sensor on page 497.

6. Run a **Sensor Results Preview**. Previewing sensor results on a small number of non-critical endpoints enables you to test the sensor before making it available for user questions or for automatic sensor results collection through TDS. Previewing is a useful precaution in case the sensor script has flaws that might adversely affect endpoints.
    a. Click **Select Groups to Preview.**
    b. Select an existing computer group or click **Create Ad Hoc Group**. An ad-hoc group exists only for the sensor preview and does not appear elsewhere in Tanium Console. Use one of the following methods to define the ad-hoc group and then click **Create Group**.
        - **Filter Bar**: Define a filter using the same syntax as in the `from` clause of the Interact **Ask a Question** field. For more information, see Issue a free-form question on page 241.
        - **Filter Builder**: Define a filter using the same **from computers with** fields as in the Interact **Question Builder**. For more information, see Issue a question through the Question Builder on page 245.
        - **Manual Group**: Enter a list of computer names or IP addresses. Computer names must match the results that the **Computer Name** sensor returns. Short forms or alternative names do not work.
    c. Click **Preview Sensor Results** and review the results.
7. Click **Save** to save the configuration.

Edit a sensor

Limitations and best practices for editing sensors

You can edit all the settings of all sensors except:

- Tanium *reserved sensors*, which are core system sensors that include **Computer Name**, **Action Statuses**, **Computer ID**, and **Download Statuses**. For reserved sensors, edits are restricted to the **Max String Age** and **Max Strings** settings to prevent users from inadvertently compromising critical Tanium operations, such as action deployment, that depend on the sensors.
- Sensors that are configured for endpoints managed using Part 1: Tanium Console and Interact overview on page 42. You cannot edit any attributes for these sensors.

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

As a best practice, do not edit predefined sensors that are provided through content-only solutions imported from Tanium. For more information, see Tip 4: Limit customizations to Tanium content on page 138.Contact Tanium Support on page 724 if editing the Tanium-provided sensors is necessary. Alternatively, you can Clone a sensor on page 426 that Tanium provided and edit the copy. You can also edit custom sensors that you created from scratch.

Edit the sensor configuration

Review Custom content development on page 418 and Sensor scripts on page 421 before you edit a sensor. Before you edit a parameterized sensor, see Parameterized sensors on page 422 for information about the impact on saved questions and computer groups that use the sensor.

TIP

To change the content set assignment in bulk for multiple sensors that must belong to the same set, see Move sensors between content sets on page 430.

1. From the Main menu, go to **Administration > Content > Sensors**.
2. (Optional) Use the search and column sorting features to find the sensor that you want to edit.
3. Click the sensor **Name**.
4. Click **Edit Mode**, configure the settings described in Create a sensor on page 427, and click **Save**.

Move sensors between content sets

You can move sensors in bulk between content sets to accommodate RBAC changes in your organization. For example, you might want to move certain sensors to a content set that only highly privileged users can access.

1. From the Main menu, go to **Administration > Content > Sensors**.
2. Select the sensors and click **Move to Content Set**.
3. Select a content set and click **Confirm**.

Export or import sensors

Export sensors

Export sensors as a file in the format required for your workflow:

- **CSV**
  You can use any application that supports CSV format to display the same sensor attributes (columns) as the Console **Sensors** grid shows and then customize the display. For example, you can use Microsoft Excel to create charts based on sensor attributes.

© 2026 Tanium Inc. All Rights Reserved

- **JSON**

  You can export multiple sensor configurations as a JSON file. Exporting configurations is useful if you want to import them into another Tanium environment. For example, you might test custom sensors in a lab environment to ensure that they work as intended before importing the sensors into your production environment. You must be assigned a role with the **Export Content** permission to export a JSON file. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.

Perform the following steps to export sensors:

1. From the Main menu, go to **Administration > Content > Sensors**.
2. (Optional, CSV exports only) To add or remove attributes (columns) for the CSV file, click Customize Columns  in the grid and select the attributes.
3. Select rows in the grid to export only specific sensors. If you want to export all sensors, skip this step.
4. Click Export .
5. (Optional) Edit the default export **File Name**.

   The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.
6. Select an **Export Data** option: **All** sensors in the grid or just the **Selected** sensors.
7. Select the file **Format**:
   - **List of Sensors - CSV**
   - **Sensor Definitions - JSON** (requires **Export Content** permission)
8. Click **Export**.

   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

Import sensors

Importing is useful if you want to copy sensor configurations from another Tanium environment. For example, you might test custom sensors in a lab environment to ensure that they work as intended. You can then export the sensors from the lab environment and import them into your production environment. You can import sensors and other content as a JSON or XML file.

You must be assigned a role with **Import Signed Content** permission to import content files.

1. (Non-Tanium-provided content only) Digitally sign the content file and ensure a public key is in place to validate the signature. For more information, see Authenticating content files on page 482.

   You do not have to generate keys or signatures for Tanium-provided solutions. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process.

© 2026 Tanium Inc. All Rights Reserved

> **NOTE** If you plan to import a file that another user signed, you can first perform an integrity check on the file. For more information, see Verify content file signatures on page 487.

2. From the Main menu, go to any of the following **Administration** pages:
   - **Configuration > Solutions**
   - **Permissions > Filter Groups**
   - Under **Content**, select **Sensors**, **Packages**, or **Saved Questions**
   - Under **Actions**, select **Scheduled Actions**, **All Pending Approvals**, or **Actions I Can Approve**
3. Select an **Import** option based on the source of the content:
   - **Import > Import Files**: Perform one of the following steps to select one or more files:
     - Drag and drop files from your file explorer.
     - Click **Browse for File**, select the files, and click **Open**.
   - **Import > Import URL**: Enter the URL in the **Import URL** field, and click **Import**.
4. For each file, expand the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts on page 135.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, **Include content set overwrite** is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Install**.

Copy sensor configuration details

Copy information from the **Sensors** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the content that you copy.

1. From the Main menu, go to **Administration > Content > Sensors**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy.
   - **Copy cell information**: Hover over the cell, click Options, and click Copy.

© 2026 Tanium Inc. All Rights Reserved

Delete sensors

IMPORTANT

Do not delete the predefined sensors that Tanium solutions provide. When you import solution updates, the update process restores any deleted predefined sensors.

BEST PRACTICE

Instead of deleting custom sensors, instruct users not to use them.

Deleting a custom sensor might be warranted in certain scenarios. For example, Tanium users and solutions might not need the sensor anymore, the sensor might not behave as expected on endpoints, or another sensor might use fewer endpoint resources to collect the same data.

Perform the following steps before you delete a sensor:

1. Determine if any content uses the sensor and assess the impact of removing or replacing the sensor. For example, a saved question or a report might use the sensor to collect data from endpoints.
2. Decide which sensor is a suitable replacement or create a replacement if necessary. This step is required only if you must recreate or reconfigure the content that uses the sensor you plan to delete. For more information, see View sensor details on page 425 and Create a sensor on page 427.
3. Reconfigure or recreate scheduled content to remove dependencies on the sensor and replace it if necessary.

Perform the following steps to delete a sensor:

1. From the Main menu, go to **Administration > Content > Sensors**.
2. Select the sensor and click Delete .

Manage sensor quarantines

IMPORTANT

Do not enable the enforcement of sensor quarantines without consulting Tanium Support. For more information, see Contact Tanium Support on page 724.

Overview of sensor quarantines

Enforcing *sensor quarantines* prevents sensors from running on an endpoint for the current question or action if those sensors exceeded the runtime timeout during a previous question or action. Quarantines are useful for limiting the impact on endpoint resources, such as CPU utilization, when questions and actions use excessively long-running sensors. The non-configurable timeout is set to one minute.

By default, quarantines are not enforced: after a sensor exceeds the one-minute timeout, the Tanium Client stops the sensor from running any longer and assigns it quarantined status but the sensor still runs for future questions or actions until it finishes or times out again. When quarantines are not enforced, the Client uses quarantined status just to record that the sensor timed out. After the

© 2026 Tanium Inc. All Rights Reserved

Client assigns quarantine status, the status does not automatically revert to unquarantined if the sensor later finishes running for another question or action. You must manually Remove sensors from quarantine on page 435 to change their status. Otherwise, the **Quarantined Sensors** page shows the cumulative results for any sensor that ever timed out on an endpoint since the initial Tanium Client installation.

The Tanium Client stops any sensor at the moment it exceeds the timeout regardless of whether you enable enforcement. Each Client quarantines sensors and enforces the quarantines independently. Consequently, a sensor might be quarantined on some endpoints and not on others. When a Client quarantines a sensor, Interact shows the following message in the **Question Results** grid: `TSE-Error: Sensor evaluation timed out`.



The message `TSE-Error: Sensor evaluation timed out` means only that the Client could not finish executing the sensor within the one-minute timeout. If some Clients return this message while other do not for the same sensor, the cause is usually an issue on the endpoints where the quarantine occurs. For example, Clients might not finish running the sensor within the timeout if their host endpoints have insufficient resources or if interactions with anti-virus software on the endpoints cause unexpected delays.

When you issue a question that uses a sensor that is already quarantined and enforcement is enabled, the **Question Results** grid displays `TSE-Error: The sensor is quarantined`. The Tanium Client adds entries to the Client logs and sensor history logs when it quarantines a sensor or prevents an already quarantined sensor from running.

If temporary sensors exceed the one-minute timeout, the Tanium Client quarantines the original sensor as well as all current and future temporary sensors that are based on the original sensor. The Tanium Server creates a temporary sensor for questions that use parameterized sensors. For more information, see Questions with parameterized sensors on page 238.



When enforcement is enabled, quarantined sensors do not run when you use them for targeting endpoints, even if the sensors are members of computer groups. However, quarantined sensors might skew the targeting of a question that has a vague *from* clause, such as `from all machines with Is Windows not equals true`. In this case, Windows endpoints on which the Is Windows sensor is quarantined would match the condition `not equals true` because their response would be `TSE-Error: The sensor is quarantined` rather than `true`. To avoid such outcomes, make the target clause as specific as possible and do not use negative matching conditions such as `not equals true`.

View quarantined sensors

To see the attributes of quarantined sensors:

1. From the Main menu, go to **Administration > Content > Quarantined Sensors**.
   The **Quarantined Sensors** grid displays many of the sensor attributes that are described in Create a sensor on page 427.
2. (Optional) To display attributes that the grid hides by default, click Customize Columns and select the attributes.

© 2026 Tanium Inc. All Rights Reserved

3. (Optional) Use the filters to find specific sensors:
    - **Filter by text**: To filter the grid by sensor **Name** or **Description**, enter a text string in the **Filter by text** field.
    - **Filter by attribute**: Filter the grid by one or more attributes, such as the **Content Set** assignment. Expand the **Filters** section, click **Row** or **Grouping** (to group by Boolean operators), click **Add**, select an attribute and operator, enter a text string that contains all or part of the attribute value, and click **Apply**. After you finish specifying attributes, click **Apply All** to filter the grid.
4. (Optional) To view all the attributes that are described in Create a sensor on page 427, click a sensor **Name**.

Remove sensors from quarantine

You can use Tanium Console to unquarantine a sensor on some or all endpoints. After you unquarantine a sensor, the Tanium Client allows it to run for subsequent questions and actions, but will stop and quarantine the sensor again if it exceeds the timeout.

NOTE

If you modify a sensor, Tanium Clients that receive its new definition will automatically unquarantine that sensor.

The Tanium Server cannot unquarantine sensors on endpoints that are offline. If you know that some endpoints might come online only at a later time, consider scheduling an action that uses the **Un-Quarantine Sensor** or **Un-Quarantine Sensor (Non-Windows)** package. For more information, see Deploying actions and playbooks in Console and Interact on page 391.

1. From the Main menu, go to **Administration > Content > Quarantined Sensors**.
2. Select the sensors and click **Unquarantine**.
3. Select the **Action Group** that includes the endpoints where you want to unquarantine the sensors.
4. Preview the affected endpoints and then click **Unquarantine**.

Enable or disable enforcement of quarantined sensors

After you enable quarantine enforcement, Tanium Clients do not answer questions that use quarantined sensors and those sensors do not run for actions. After you disable enforcement, Clients still quarantine sensors and log quarantine events, but do not prevent those sensors from running.

NOTE

Your user account must have a role with the **Global Settings** write permission to enable or disable quarantine enforcement. Users with the **Administrator** reserved role have this permission.

The first time you enable enforcement, you must add the **EnableSensorQuarantine** setting to the platform settings on the Tanium Server as follows. By default, enforcement is disabled and the setting does not appear in Tanium Console. After you add the setting, the Tanium Server applies it to all Tanium Clients.

© 2026 Tanium Inc. All Rights Reserved

1. Access Tanium Console.
2. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**, and click **Add Setting**.
3. Enter the following values and click **Save**.
    - **Setting Type** = **Server**
    - **Platform Setting Name** = `EnableSensorQuarantine`
    - **Value Type** = `Numeric`
    - **Value** = `1`

Perform the following steps if you want to change the enforcement setting after adding it to the platform settings:

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.
2. In the **Name** column, click **EnableSensorQuarantine**, set the value to `1` to enable enforcement or `0` to disable enforcement, and click **Save**.

If you want to change the enforcement setting in specific Tanium Clients instead of all Clients, add or edit the **EnableSensorQuarantine** setting in the local configuration of those Clients. For more information, see Tanium Client Management User Guide: Tanium Client CLI and Client settings.

Export quarantined sensor details

You can export quarantined sensor details as a CSV file. When you open the file in an application that supports CSV format, it lists the sensors with the same attributes (columns) as the Console **Quarantined Sensors** grid displays. Displaying the grid in a CSV application is useful when you want to customize the display. For example, you can use Microsoft Excel to create charts based on sensor attributes.



You can export the details of specific quarantined sensors if you are assigned a role with **Sensor write** permission on the content sets for those sensors. Users with the **Administrator** or **Content Administrator** reserved role can export the details of all quarantined sensors.

1. From the Main menu, go to **Administration > Content > Quarantined Sensors**.
2. (Optional) To add or remove attributes (columns) for the CSV file, click Customize Columns in the grid and select the attributes.
3. Select rows in the grid to export only specific sensors. If you want to export all sensors, skip this step.
4. Click Export.
5. (Optional) Edit the default export **File Name**.

© 2026 Tanium Inc. All Rights Reserved

6. To include grid column headers in the CSV file, select **Include headers in export**.
   Skip the **Flatten rows** option. It does not apply to quarantined sensors.
7. Click **Export**.
   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

Copy quarantined sensor details

Copy information from the **Quarantined Sensors** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the copy.

1. From the Main menu, go to **Administration > Content > Quarantined Sensors**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy .
   - **Copy cell information**: Hover over the cell, click Options , and click Copy .

Manage sensor results collection

With Tanium Data Service (TDS), you can see the cached results that endpoints return for *registered* sensors. The Tanium Server automatically collects results from registered sensors by issuing questions to all managed endpoints. TDS and Tanium solutions automatically register certain sensors and you can manually register other sensors. By default, TDS caches the results from each endpoint for 30 days after the last successful collection. You can view the cached results for both online and offline endpoints in Interact, Tanium Reporting, and any solution that provides Reporting dashboards.

For more information, see Tanium Interact User Guide: Managing Tanium Data Service.

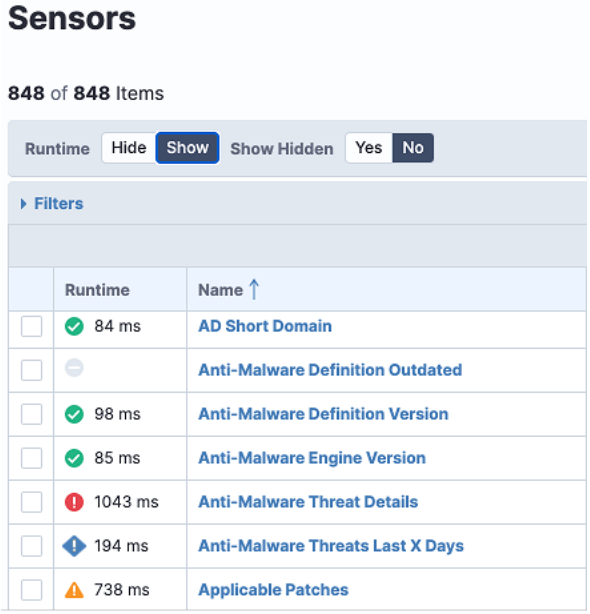
© 2026 Tanium Inc. All Rights Reserved

Assessing question impacts on endpoints through sensor runtime indicators

Sensor runtime thresholds overview

The time that a Tanium Client takes to run a question varies widely, based on which sensors, and how many, the question invokes. To help you assess the impact that running Tanium questions has on endpoint resources, you can customize sensor runtime thresholds that trigger indicator icons in Tanium Console. The following figure shows how the indicator icons appear.

Sensor runtime indicators



NOTE

Your user account requires the **Administrator** reserved role to see and use the **Administration > Content > Sensor Thresholds** page.

Sensor runtime calculations

The Tanium Client tracks the runtime for each sensor when a question runs it, calculates the average of all the past runtimes for that sensor, and sends the updated runtime information to the Tanium Server every three hours. The Server calculates the average runtime based on the latest updates from all the endpoints that reported runtimes for the sensor.

Sensor runtime icons and defaults

The following table describes the threshold icons and their default values.

© 2026 Tanium Inc. All Rights Reserved

Sensor runtime threshold icons

Threshold icon	Description
Not Run	The Tanium Server has not yet received runtime information from any endpoints for this sensor. This icon also displays for built-in sensors regardless of their runtimes. The Server does not record runtime statistics for built-in sensors, and does not account for those sensors when calculating runtimes for questions that use them. The built-in sensors are: • Action Statuses • Download Statuses • Computer Name • Computer ID • Manual Group Membership • IP Address
Below any threshold	The runtime average for a sensor does not exceed any threshold.
Low	The runtime average exceeds the Low threshold but does not exceed the Medium threshold. By default, the Low threshold is 100 ms. You can customize the threshold and the label.
Medium	The runtime average exceeds the Medium threshold but does not exceed the High threshold. By default, the Medium threshold is 500 ms. You can customize the threshold and the label.
High	The runtime average exceeds the High threshold, which by default is 1,000 ms. You can customize the threshold and the label.

Sensor runtime caveats and exceptions

When viewing threshold indicators, note the following caveats:

- The Tanium Server does not use cached responses to questions when calculating runtime averages.
- Sensors that require data sampling are more likely to exceed runtime thresholds. However, the longer runtimes required for sampling do not necessarily indicate high resource usage when endpoints run these sensors. Contact Tanium Support on page 724 for more information. The affected sensors include:
    - CPU by Process
    - CPU Consumption
    - Disk IOPS
    - High CPU Consumption
    - High CPU Processes

© 2026 Tanium Inc. All Rights Reserved

- Network Throughput Inbound
- Network Throughput Outbound
- SQL Server CPU Consumption
- Tanium Client CPU

Configure sensor thresholds

Work with Tanium Support (see Contact Tanium Support on page 724) to determine the runtime thresholds that you expect to influence administrator decisions about whether to run a question, how often to run it, and which sensors to include in the question. The goal is to plan questions in a way that does not interfere with other, more critical tasks that endpoints perform.



Set thresholds that reflect decisions Tanium users must make, based on the endpoint management policies of your organization. For example, policies might dictate that users must never run a question that exceeds 10 seconds during peak traffic times on endpoints that perform tasks with a higher priority than responding to questions.

1. From the Main menu, go to **Administration > Content > Sensor Thresholds**.
2. Select whether you want Tanium Console to **Display thresholds to** only those Tanium users with predefined administrative roles (**Admin**) or to all users who are allowed to see questions and sensors (**Admin and Users**).
3. Set the average runtime (in milliseconds) for each threshold (**High**, **Medium**, and **Low**) or accept the defaults, and then click **Save**.

Verify sensor thresholds

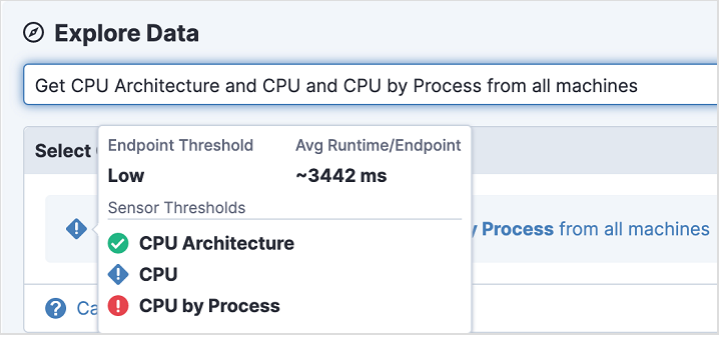
Threshold indicator icons appear wherever you view and select sensors in Tanium Console. After modifying threshold values, verify that the Tanium Server applied your changes.

The **Administration > Content > Sensors** page displays runtime statistics for all sensors.

1. Go to the Console header, select the Question option  if it is not already selected, and type (without pressing **Enter**) a question with a sensor that you expect to have a short runtime, such as **Computer Name**, and a sensor that you expect to have a long runtime, such as **Running Processes of User**. For example, type: `Get Computer Name and Applicable Patches from all machines`.
2. Verify that the list of suggested questions displays the expected threshold icons. If you see unexpected indicators, review the icon descriptions and caveats described in Sensor runtime thresholds overview on page 438.

© 2026 Tanium Inc. All Rights Reserved

3. Hover over the icon for the suggested question that you want, and verify that the popup displays the expected runtime (in milliseconds) and the expected threshold icons for each sensor.



© 2026 Tanium Inc. All Rights Reserved

Managing packages for platform actions

Packages overview

A platform *package* configuration includes a command, a script, and any related files that are needed to orchestrate a platform action on an endpoint managed using Tanium Client. For example, the **Restart Service** package includes a Windows command-line command that executes a script to restart a service on Windows endpoints. You deploy packages through the action deployment workflow to apply changes on endpoints. Tanium provides predefined packages to address numerous endpoint change scenarios and you can create custom packages for additional scenarios.

For more information, see Deploying actions and playbooks in Console and Interact on page 391.

IMPORTANT

Windows endpoints require certain configurations to enable some Tanium sensors and packages that rely on Windows Management Instrumentation (WMI) queries, VBScript, and PowerShell. For more information, see Tanium Client Management User Guide: Prepare for deployment to Windows endpoints.

When you choose a scripting engine for custom packages, note that Microsoft has announced the deprecation of VBScript. For more information, see Tanium Community article: VBScript Retirement in a future Windows Release (sign in required).

An endpoint requires free disk space that is twice the size of the package that the Tanium Client is downloading for the download to succeed. To check the package size, see View package details on page 445.

NOTE

For the role permissions that are required to manage package configurations, see Manage packages on page 98.

To troubleshoot issues relating to package downloads, see Troubleshoot actions on page 339.

Manage client applications through packages

The Tanium Client service can perform almost any command line instruction available to an Administrator user who is signed in to the endpoint because the service runs with the permissions of the LocalSystem account (Windows) or root account (non-Windows). Consequently, even if signed-in users do not have administrative rights, a Tanium Console user can deploy actions to the endpoint that install, update, or remove client applications as long as those applications meet the following conditions:

- The applications are installed from a command line using the permissions of the LocalSystem account or root.
- The applications are configured to suppress any interaction with an end user who is signed in to a target endpoint at installation time.
- The applications can be dynamically customized at installation if necessary through options, switches, or input files passed to the application installer.

© 2026 Tanium Inc. All Rights Reserved

If the required executables, scripts, and configuration files do not natively have these characteristics, you might be able to use a commercial software packaging tool such as InstallShield or an open-sourced application like Nullsoft Scriptable Install System to create a new version of the installer.

You can use the Tanium Core Platform to track the count of installed applications, as well as whether those applications are running on endpoints. Therefore, before installing new software or upgrading versions of existing software, verify that your organization owns the required number of licenses or meets the Acceptable-Use criteria to centrally distribute and install the commercial or open-sourced software to endpoints within your organization.

Package files

A package might include files that are required to run an action, such as a script file. The files might be bundled with the package or reside on an internet location, such as `content.tanium.com` or other remote sources. The Tanium Server downloads remote files to a sub-directory of its installation directory. For more information about downloading from remote sources, see Enabling authentication between platform servers and remote systems on page 173. Tanium Clients then download the package files from the Server. For more information, see Throttling bandwidth and connections to Tanium Clients on page 187.

Tanium might deliver package files from third-party providers. For more information on each package, see the `README.txt` file that is referenced with the package.

For examples of package files, see Example: Package files on page 490.

Scheduled action with parameterized package

A scheduled action is an action that is configured to deploy in the future or at recurring intervals (see Managing scheduled actions and action history on page 341). A parameterized package requires input (parameters) from users before the package can run on endpoints (see Example: Parameterized packages on page 508). When you configure a scheduled action to use a parameterized package, the Tanium Server saves the package definition, including the user-entered parameter values, in an object called a *temporary package* without altering the configuration of the original package. On the endpoint, the Tanium Client runs the temporary package when it has a directive to run the scheduled action that uses the package. A scheduled action continues to use the temporary package even if the original package configuration is updated. Therefore, if a package configuration is updated and you want the scheduled action to use the updated package, you must re-issue or edit the scheduled action and click the **Update Source Package** option for the **Deployment Package** setting. For more information, see Update action packages on page 347. Alternatively, you can re-create the scheduled action to use the updated version of the package. For more information, see Deploying actions and playbooks in Console and Interact on page 391.

Running a package command within a process group

In a package configuration, the **Launch this package in a process group** setting controls whether the package command runs within a process group. If the setting is enabled, the process group and any remaining descendant processes are killed when the command completes or times out.

By default, you cannot change this setting and its default state depends on how the package was added:

- You created the package through Tanium Console: The checkbox is selected by default.

© 2026 Tanium Inc. All Rights Reserved

- You manually imported the package or the Tanium Server automatically imported the package: When you view the configurations of Tanium-defined packages, the checkbox is selected for most packages but deselected for those that must run processes outside of a process group. When you manually import a package file, the checkbox is deselected unless you set the `<process_group_flag>` to `1` in the file before importing.

For most packages that you create or manually import, running processes within a process group is the best practice. Some exceptions are:

- Packages that initiate an installation process that must be able to run beyond the command completion or timeout.
- A process that must run constantly. For example, some Tanium modules have predefined packages that initiate long-running indexing processes.

To change the **Launch this package in a process group** setting after you import a package, or while you are creating or editing the package, first make the setting editable as follows:

1. From the Main menu, go to **Administration > Configuration > Settings > Platform Settings**.
2. Set **Run Commands in Process Group** to **ON** and click **Save All**.

Package verification

You can add verification exit codes or a verification query to a package to confirm whether it ran successfully during action deployment. For the steps to add the verification, see Create a package on page 447.



You can use Tanium Console to configure verification exit codes or a verification query, but not both.

VERIFICATION EXIT CODES

An exit code is a number that indicates the outcome of a package script or command. Specifying exit codes enables Tanium Clients to return Action states on page 353 that confirm success status, not just completion status:

- `Verified` status indicates that the package finished running and returned an exit code for success.
- `Failed Verification` status indicates that the package finished running but returned an exit code that does not mean success.

VERIFICATION QUERY

A verification query is a preview question that indicates whether an action that used the package produced the expected results on endpoints. For example, if the package is intended to restrict permissions for the Tanium Client installation directory on Windows endpoints, you can specify the query `Tanium Client Directory Permissions contains "restricted"`. After the action runs, the **Action Status** page shows the verification states (see Action states on page 353) and the **Client Status Details** section shows the endpoints for which the action is verified. You require the **Sensor read** permission on the **Reserved** content set to issue the **Verification Query**.

© 2026 Tanium Inc. All Rights Reserved

NOTE

The Client executes all the sensors in the **Verification Query** instead of reading from the sensor cache, regardless of the **Max Sensor Age** setting for those sensors.

View package details

Viewing package attributes can help you to determine if new packages are necessary and to manage or troubleshoot existing packages. For example, you might check the **Command** and script files of a package to diagnose unexpected results for actions that deploy the package.

1. From the Main menu, go to **Administration > Content > Packages**.
   The **Packages** grid displays most of the attributes that are described in Create a package on page 447.

   NOTE

   The **Size** column indicates the total size of all the files that are associated with the package. The value `Not available` indicates that the package has no associated files. The value `Pending` indicates that the Tanium Server has not finished downloading and caching the files. To see the size of individual files in a package, select the package and click **Status**.

2. (Optional) To display attributes that the grid hides by default, click Customize Columns and select the attributes.
3. (Optional) Use the filters to find specific packages:
   - **Filter by text**: Enter a text string in the **Filter items** field to filter the grid by package **Name**, **Display Name**, or **Command**.
   - **Filter by attribute**: Expand the **Filters** section, select a package attribute (such as **Content Set** assignment), select an operator (such as **contains**), enter a text string that contains all or part of the attribute value, and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.
4. To view the download status of package files, select the package and click **Status**. You can Re-download package files on page 445 if necessary.
5. To see all the attributes of a particular package, click the package **Display Name**. For information about the attributes, see Create a package on page 447.

Re-download package files

The Tanium Server caches package files. If updated file versions are available, or re-downloading the current file versions is necessary for troubleshooting, you can manually re-download to the Server. Re-downloading ensures that the package deploys the correct files to endpoints.

© 2026 Tanium Inc. All Rights Reserved

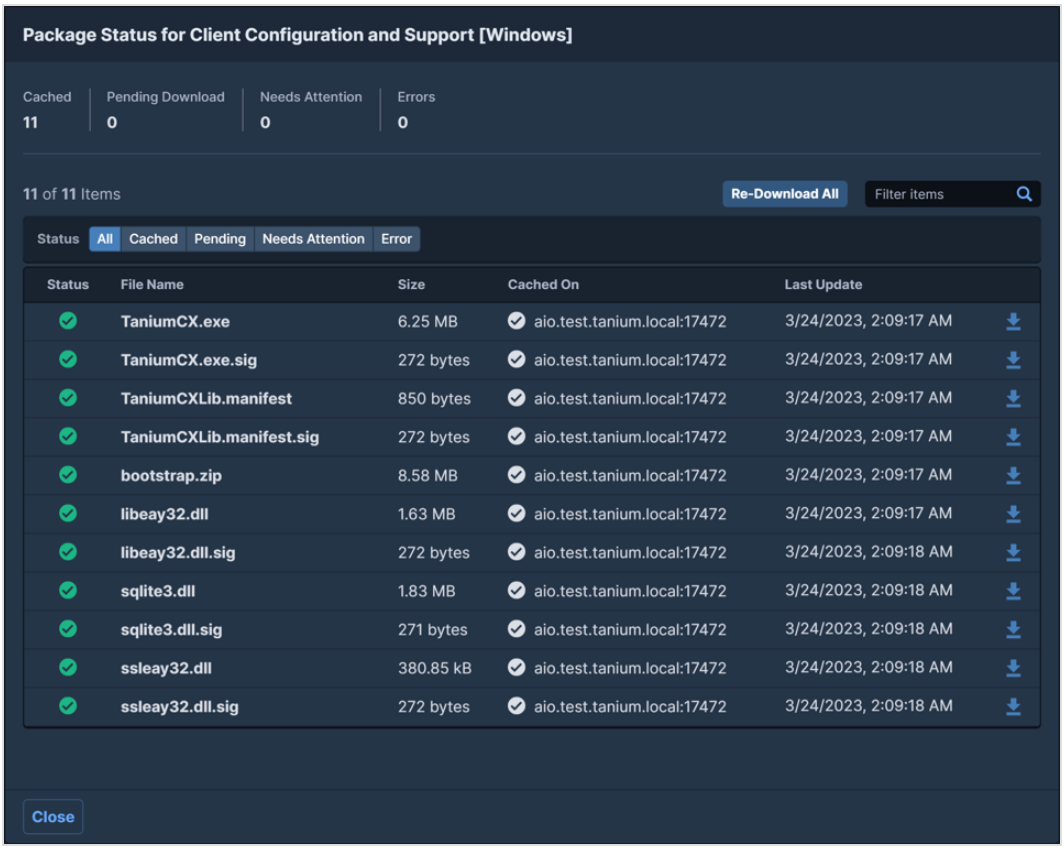
NOTE

The Tanium Server automatically retries downloading every few minutes if the initial download failed for a package.

TIP

To download the package files that are associated with a specific action, go to **Administration > Actions > Scheduled Actions**, select the action, and click **Show Status**.

1. From the Main menu, go to **Administration > Content > Packages**.
2. Select the package for which you want to download files and click **Status**.



3. (Optional) Filter by **Status** (such as **Needs Attention** or **Error**) if the list is long.
4. Re-download an individual file or click **Re-Download All** to re-download all the files.

TIP

If you want the Tanium Server to automatically check for, and download, updated versions of remote package , set a **Check for update** interval in the package configuration. For more information, see Create a package on page 447.

© 2026 Tanium Inc. All Rights Reserved

Clone a package

Cloning is useful when you need to:

- Create a modified version of a predefined package from a Tanium content-only solution such as Default Content.

  Do not modify a predefined package.

- Create a new package with settings that differ only slightly from an existing package. This is often easier than creating a new package from scratch.

Perform the following steps to clone a package:

1. From the Main menu, go to **Administration > Content > Packages**.
2. Use the search and column sorting features to find the package that you want to clone.
3. Select the package and click **Clone**.
4. Configure the settings as described in Managing packages for platform actions on page 442 and click **Save**.

Create a package

Create a custom package for endpoint change scenarios that Tanium-defined packages do not address. For example, you might create a package to activate the key for a product that is specific to your organization. As another example, you might create a package that is similar to an existing package except for the content set assignment to ensure that only certain users can deploy the package through actions.

Instead of creating a new package from scratch, cloning is usually easier if the package settings differ only slightly from an existing package. For more information, see Clone a package on page 447.

Review Custom content development on page 418 before you perform the following steps to create a custom package.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Content > Packages** and click **New Package**.
2. Configure the package **Details**.

Package details

Detail	Description
Name	Enter a name of up to 255 characters to identify the package. For sensor-sourced packages, you have the option to use a sensor variable in the package name. For more information, see Configure settings for a sensor-sourced package on page 523.
Display Name	(Optional) Specify a name to display for the package in the **Packages** page and **Action Deployment** page. If you do not enter a value, the **Package Name** is the default **Display Name**.
Description	Enter a description to help other users understand the purpose of the package, what it does, and any special requirements. For example, you can note the parameters for a sensor-sourced package. You can also enter text that helps users to distinguish the package from other packages with similar names.
Content Set	Assign the package to a content set. The list displays all content sets for which you have **Package write** permission. If you do not select a content set, the **Default** set is assigned.
Command	Specify the command to run on the endpoint. The syntax must include all the appropriate command-line switches to ensure silent execution when that is required. For example, you can enter `setup.exe /S`, `msiexec.exe /i installme.msi /qn`, `installme.exe /S /D=DIR`, or `ipconfig /flushdns`. For more information about commands and examples of their usage, see: • Example: Package files on page 490 • Example: Parameterized packages on page 508 • Example: Sensor-sourced packages on page 522
Command Timeout and Download Timeout	These timeouts affect the state (**Completed**, **Expired**, or **Failed**) of an action that uses the package. The **Download Timeout** is the amount of time available to download packages files. The **Command Timeout** is the amount of time available for the command to run. For more information, see View status for simple actions on page 352.
Ignore action lock	Enable endpoints to execute actions that include this package regardless of whether action locks are on for those endpoints. Use this option in packages that are critical for the health and security of a network. For more information, see Locking down actions on endpoints on page 407.
Launch this package in a process group	Run the package command within a process group. When the command completes or times out, the process group and any remaining descendant processes are killed. For more information, see Running a package command within a process group on page 443.

© 2026 Tanium Inc. All Rights Reserved

3. Specify the **Files** that are required to run the package, such as a script file. You do not have to specify files that are already present on endpoints. Each package can have up to 100 files. To select files, select an option in the **Add** dropdown list:

   - **Local Files**: Upload one or more files from your local host computer by drag-and-dropping them or by clicking **Browse for Files**. When you upload it, the Tanium Server generates a SHA-256 hash.
   - **Remote File**: Specify the following settings:
     - **File Address**: Enter the file address, including the protocol. The supported protocols are HTTPS, HTTP, FTPS, and FTP. Universal Naming Convention (UNC) paths without hidden shares are also supported. For example, enter:
       `https://content.tanium.com/files/published/emerging-issues-content/2023-10-16_17-46-22_1.2.31.0000/cve-2023-36884_mitigation/cve-2023-36884-Mitigation.bat`

       NOTE

       You can specify a folder address if that folder contains only the files that the package requires. For example, you might store package files on a Server Message Block (SMB) file share. Tanium™ Downloader compresses the folder when downloading it from the remote source. Therefore, include a script in the package to extract the folder on endpoints when an action deploys the package.
     - **Name**: For example, enter `cve-2023-36884-Mitigation.bat`.
     - **Check for update**: Select the interval at which the Tanium Server checks for an updated version of the file.
     - **SHA-256**: Enter the SHA-256 hash of the file.

   To view or edit file settings for an existing package, select the file name in the list. You can filter the list by entering a search string in the **Filter by File Name** field.
   For more information about script files and examples of their usage, see:

   - Example: Parameterized packages on page 508
   - Example: Sensor-sourced packages on page 522

   All the files related to packages are stored in a sub-directory of the Tanium Server installation directory. The Server downloads remote files to that sub-directory.

4. Configure the **Parameters** if this is a parameterized package. For more information, see Configure parameter inputs for a package on page 516.

5. (Optional) Add a **Verfication** query that indicates whether an action that used the package produced the expected results on endpoints. For more information, see Verification Query on page 444.

   NOTE

   You can use Tanium Console to configure a verification query or verification exit codes, but not both.

© 2026 Tanium Inc. All Rights Reserved

a. Click **Add**, use the **Filter Bar**, **Filter Builder**, or **Manual Group** tab to build the filter part of the question, and then click **Confirm**.

b. Specify a verification failure timeout. The clock begins when the action finishes, which is when verification starts. The Tanium Client periodically reissues the verification question throughout the timeout period. If the Client does not return a `Verified` state within that period, the Client returns `Failed Verification` as the action state.

6. (Optional) Add **Verfication** exit codes to enable Tanium Clients to return Action states on page 353 that confirm success status, not just completion status. For more information, see Verification Exit Codes on page 444.

   a. Click **Add Exit Codes** and enter a code or range of codes that indicates the package ran successfully. For example, the value `-1 - 5` specifies that any exit code from -1 to 5 indicates success.

   b. For each additional exit code, click **+ Add Code** and enter the code.

7. Click **Save** to save the configuration.

Edit a package



For more information about the impact on scheduled actions when a parameterized package configuration is edited, see Scheduled action with parameterized package on page 443.



As a best practice, do not edit a predefined package that is provided through a Tanium solution. For more information, see Tip 4: Limit customizations to Tanium content on page 138.Contact Tanium Support on page 724 if editing a Tanium-provided package is necessary. Alternatively, you can Clone a package on page 447 that is predefined and edit the copy. You can also edit custom packages that you created from scratch.

To change the content set assignment in bulk for multiple packages that must belong to the same set, see Move packages between content sets on page 450.

1. From the Main menu, go to **Administration > Content > Packages**.
2. (Optional) Use the search and column sorting features to find the package you want to edit.
3. Click the package **Display Name**.
4. Click **Edit Mode**, configure the settings described in Managing packages for platform actions on page 442, and click **Save**.

Move packages between content sets

You can move packages in bulk between content sets to accommodate RBAC changes in your organization. For example, you might want to move certain packages to a content set that only highly privileged users can access.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Content > Packages**.
2. Select the packages and click **Move to Content Set**.
3. Select a content set and click **Confirm**.

Export or import packages

Export packages

Export packages as a file in one of the following formats based on your objective:

- **CSV**
  You can use any application that supports CSV format to display the same package attributes (columns) as the Console **Packages** grid shows and then customize the display. For example, you can use Microsoft Excel to create charts based on package attributes.
- **JSON**
  You can export multiple package configurations as a JSON file. Exporting configurations is useful if you want to import them into another Tanium environment. For example, you might test custom packages in a lab environment to ensure that they work as intended before importing the packages into your production environment. You must be assigned a role with the **Export Content** permission to export a JSON file. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.

Perform the following steps to export packages:

1. From the Main menu, go to **Administration > Content > Packages**.
2. (Optional, CSV exports only) To add or remove attributes (columns) for the CSV file, click Customize Columns in the grid and select the attributes.
3. Select rows in the grid to export only specific packages. If you want to export all packages, skip this step.
4. Click Export.
5. (Optional) Edit the default export **File Name**.

   NOTE

   The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.
6. Select an **Export Data** option: **All** packages in the grid or just the **Selected** packages.
7. Select the file **Format**:
   - **List of Packages - CSV**
   - **Package Definitions - JSON** (requires **Export Content** permission)
8. Click **Export**.
   The Tanium Server exports the file to the downloads folder on the system that you use to access Tanium Console.

© 2026 Tanium Inc. All Rights Reserved

Import packages

Importing is useful if you want to copy package configurations from another Tanium environment. For example, you might test custom packages in a lab environment to ensure that they work as intended. You can then export the packages from the lab environment and import them into your production environment. You can import packages and other content as a JSON or XML file.

You must be assigned a role with **Import Signed Content** permission to import content files through the following steps:

1. (Non-Tanium-provided content only) Digitally sign the content file and ensure a public key is in place to validate the signature. For more information, see Authenticating content files on page 482.

   NOTE

   You do not have to generate keys or signatures for Tanium-provided solutions. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process.

   If you plan to import a file that another user signed, you can first perform an integrity check on the file. For more information, see Verify content file signatures on page 487.

2. From the Main menu, go to any of the following **Administration** pages:
   - **Configuration > Solutions**
   - **Permissions > Filter Groups**
   - Under **Content**, select **Sensors**, **Packages**, or **Saved Questions**
   - Under **Actions**, select **Scheduled Actions**, **All Pending Approvals**, or **Actions I Can Approve**
3. Select an **Import** option based on the source of the content:
   - **Import > Import Files**: Perform one of the following steps to select one or more files:
     - Drag and drop files from your file explorer.
     - Click **Browse for File**, select the files, and click **Open**.
   - **Import > Import URL**: Enter the URL in the **Import URL** field, and click **Import**.
4. For each file, expand the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts on page 135.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, **Include content set overwrite** is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Install**.

   Perform the next step only for imported packages that reference other files. You must manually download these files on the Tanium Server because the file that you imported contains only the package configurations, not associated files.

© 2026 Tanium Inc. All Rights Reserved

7. For each package that you imported, select the package, click **Status**, and click **Re-Download All** to download the referenced files.

   If the Tanium Server cannot access a file location, move the file to an accessible location, change the **File Address** in the package configuration (see Edit a package on page 450), and repeat this step.

Copy package configuration details

Copy information from the **Packages** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the copy.

1. From the Main menu, go to **Administration > Content > Packages**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy .
   - **Copy cell information**: Hover over the cell, click Options , and click Copy .

Deploy actions from the Packages page

You can configure an action to deploy any package from the **Packages** page except for sensor-sourced packages. You can deploy actions for sensor-sourced packages only from the **Question Results** page. For more information, see Example: Sensor-sourced packages on page 522 and Deploying actions and playbooks in Console and Interact on page 391.



For the role permissions that you require to deploy actions, see Deploy an action on page 84.

1. From the Main menu, go to **Administration > Content > Packages**.
2. Select a package, click **Deploy Action**, and complete the action deployment workflow as described in Configure action settings.

Delete packages



Do not delete the predefined packages that Tanium solutions provide. When you import solution updates, the update process restores any deleted predefined packages.



Instead of deleting custom packages, instruct users not to use them.

Deleting a custom package might be warranted in certain scenarios. For example, the package might not be needed for actions anymore, the package might not run successfully on endpoints, or another package might use fewer endpoint resources to perform the same change.

© 2026 Tanium Inc. All Rights Reserved

Perform the following steps before you delete a package:

1. Determine if any scheduled actions use the package and assess the impact of deleting the action. You cannot change the package for an action after you save the action configuration. For more information, see Manage scheduled actions on page 342.
2. Decide which package is a suitable replacement or create a replacement if necessary. This step is required only if you must recreate the actions that use the package you plan to delete. For more information, see View package details on page 445 and Create a package on page 447.
3. (Optional) Recreate the action with the replacement package. For more information, see Deploying actions and playbooks in Console and Interact on page 391.

Perform the following steps to delete a package:

1. From the Main menu, go to **Administration > Content > Packages**.
2. Select the package and click Delete .

© 2026 Tanium Inc. All Rights Reserved

Managing saved questions in Console and Interact

Saved questions overview

Saved questions are questions that you store on the Tanium Server as configuration objects that include settings such as reissue intervals and access permissions. Saved questions expedite collecting information from endpoints because you can reissue the questions without reconstructing them in the Interact **Ask a Question** field or **Question Builder**. You can configure settings that facilitate merge and drill-down operations when you analyze question results. You can also associate each question with specific packages to facilitate action deployment.

NOTE

To control which saved questions appear as favorites on the Tanium **Home** page, see Work with favorite Interact categories, dashboards, and saved questions on page 71.

For information about the user roles and permissions required to manage saved questions, see Manage saved questions on page 99. For information about how RBAC assignments control who can issue saved questions and view the results, see RBAC for saved questions, dashboards, and categories on page 458.

Scheduled saved questions

You can reissue saved questions manually or based on a schedule through Tanium solutions or custom applications that use the Tanium XML API. For example, you can use Tanium™ Connect to periodically issue a saved question and send the results to an external server. If you schedule reissue intervals, saved questions can collect results in the future from endpoints that are not yet online. For example, employee laptops that are offline at the moment you save the saved question configuration might be online at least once during an eight-hour reissue interval.

You can set a periodic reissue interval when you create a saved question: select **Reissue this question every** and specify a number and unit for the reissue interval: **Minutes**, **Hours**, **Days**. The Tanium Server first issues the saved question immediately after you save the configuration and Tanium Clients that are online at that time return their answers.

If you configure reissuing, the Tanium Server reissues the saved question in the background at the specified interval. For example, if you save the saved question configuration at 9:00 a.m. local time and specify a reissue interval of every eight hours, the the Server reissues the saved question at 5:00 p.m., 1:00 a.m., 9:00 a.m., and so on.

By default, the Tanium Server stores responses for seven days. The Interact **Question Results** page shows the responses as **Recent** results for endpoints that are offline when the the Server issues the question. For more information, see Display results for online and offline endpoints on page 258.

You can use the question history to verify that the Tanium Server issues the saved questions based on the specified reissue interval. For more information, see Question history on page 253.

© 2026 Tanium Inc. All Rights Reserved

NOTE

If you specify an eight-hour reissue interval, the Tanium Server reissues the question exactly every eight hours, regardless of time changes due to daylight savings time.

Which users can see the reissue interval for a saved question depends on the computer groups assigned to those users. For more information, see Reference: User-specific saved questions.

Predefined and custom saved questions

Tanium solutions that you import provide predefined saved questions. To list the questions and view their details, see View saved question details on page 459. On the **Administration > Content > Saved Questions** page, the `User Name` column shows Tanium solutions as the owners of predefined questions.

You can also create a saved question by issuing a dynamic question through the **Ask a Question** field or **Question Builder** and then saving the question. For more information, see Create a saved question on page 463.

Best practices for saved questions

The following are best practices for creating, editing, and issuing saved questions.

Configuring the refresh frequency of sensor results

A lower value for the **Max Sensor Age** or **Maximum Data Age** setting increases CPU usage on endpoints. Do not lower the default values for sensors in saved questions that periodically reissue, or in questions that you use to deploy actions, or in questions that define membership in computer management groups and filter groups. Both settings control the maximum time for which Tanium Clients can use a cached result for a sensor, instead of re-executing it for a fresh result, when answering questions that use the sensor. You define the **Max Sensor Age** in a sensor configuration and the setting applies to all questions that use the sensor. You set the **Maximum Data Age** for a sensor when you issue a question and the setting applies only to that question. For more information, see Max Sensor Age on page 428 and Maximum Data Age on page 749.

Use Reporting to view the results of questions with registered sensors

If a question uses sensors that are registered with Tanium Data Service (TDS), Tanium Reporting has advantages over Interact for viewing the results. For more information, see Viewing the results of saved questions in Interact or Reporting on page 457.

Do not edit Tanium-defined questions

Do not edit the predefined saved questions that Tanium solutions provide. For more information, see Tip 4: Limit customizations to Tanium content on page 138. Contact Tanium Support on page 724 and review User-specific settings and results for saved questions on page 459 if editing Tanium-defined questions is necessary. Alternatively, you can Clone a saved question on page 463 that Tanium provides and edit the clone. You can also edit custom saved questions that you created from scratch.

© 2026 Tanium Inc. All Rights Reserved

Viewing the results of saved questions in Interact or Reporting

Interact provides a **Saved Question Results** page and dashboard results page for viewing the results of saved questions and dashboards of saved questions (see Question results overview on page 255). However, if you want to review results from sensors that are registered with TDS, Tanium Reporting provides the following advantages over Interact:

- **Fresh results**

  For online endpoints, results that you see in Reporting are never stale because TDS reissues questions every 30 minutes and the questions remain open for that entire interval. By contrast, results that you collect through Interact saved questions become stale if the associated values on endpoints change after the 10-minute question expiration interval but before the next reissue interval. For more information, see Question expiration on page 252.

- **Offline endpoint data**

  For offline endpoints, you can see results in Reporting for up to 30 days (the storage duration for registered sensors), whereas the Tanium Server stores the results of Interact saved questions for only 7 days. For more information, see Display results for online and offline endpoints on page 258.

Reporting shows results in reports and on the **Explore Data** page. For more information, see Tanium Reporting User Guide: Working with reports.

You must register sensors with TDS before their results appear in Reporting. For more information, see Tanium Interact User Guide: Register or unregister sensors for collection.

Interact dashboards and categories

Interact uses dashboards and categories to organize saved questions.

- Dashboard

  A *dashboard* is a group of saved questions that are related with respect to the information that they retrieve from endpoints. For example, the predefined **Hardware Inventory** dashboard contains questions that retrieve CPU, disk, memory, and BIOS information. You can issue all the questions in a dashboard simultaneously. For more information, see Issue a dashboard of saved questions on page 467.

  Interact dashboards differ from Tanium Reporting dashboards. For more information, see Tanium Reporting User Guide: Dashboards.

- Category

  A *category* is a group of related dashboards. It serves as an umbrella term for questions that you use for a particular purpose. For example, the **Security** category includes multiple dashboards that contain security-related questions.

Interact provides predefined dashboards and categories, and you can create your own. To create, edit, reassign, export, or delete dashboards and categories, see Manage categories and dashboards on page 469.

© 2026 Tanium Inc. All Rights Reserved

RBAC for saved questions, dashboards, and categories

Content set permissions and dependencies

By default, users can see a saved question, dashboard, or category only if you assign those users a role with the associated read permission for the content set of that content. For example, users require **Saved Question read** permission on a content set to issue saved questions in that set. Users require **Saved Question read** and **Dashboard read** permissions to issue a dashboard of questions. Users require **Dashboard Group read** permission to see a category.



You can override the default RBAC controls and allow access only to content owners and administrators through the **Visibility** setting of a question, dashboard, or category. For more information, see Visibility options on page 458.

Any single saved question, dashboard, or category can belong to only one content set. Assigning questions to dashboards or assigning dashboards to categories does not automatically realign the content set permissions of that content to account for dependencies. For example, consider a case where you configure the following RBAC assignments:

- **Content set assignments**: You assign two saved questions and a dashboard to content sets named **Base** and **Core Content**:

Content set name	Content name
Base	Dashboard 1 Saved Question A
Core Content	Saved Question B

- **Dashboard assignments**: You assign Saved Question A and Saved Question B to Dashboard 1.
- **Role configuration**: You assign **Saved Question read** and **Dashboard read** permissions only to the **Base** content set in Role X. The role does not provide permissions to the **Core Content** set.

After you assign Role X to users, they can see Dashboard 1 and Saved Question A but not Saved Question B.

For more details about content permissions and content sets, see:

- Content management permissions on page 97: Describes the roles and permissions required to manage saved questions, dashboards, and categories
- Managing access to content through content sets on page 561: Describes how to view, create, edit, and reassign content sets

Visibility options

In the configuration of each saved question, dashboard, or category, you can select one of the following **Visibility** options to control user access to that content:

© 2026 Tanium Inc. All Rights Reserved

- **According to RBAC**

  Role permissions on content sets control access to the content, as described in Content set permissions and dependencies on page 458.

- **Only the Owner and Admins can see this object**

  Only the content owner and users with the **Administrator** reserved role can see the saved question, dashboard, or category. Other users cannot see the content even if they have the necessary content set permissions.

  By default, the user who creates a question, dashboard, or category is its owner but you can transfer ownership to another user. For more information, see Delete content or transfer ownership on page 637.

To change the **Visibility** option for a saved question, see Edit a saved question on page 465. To change the option for a dashboard or category, see Edit category or dashboard settings on page 471.

The computer management groups that you assign to a user determine from which endpoints the question results are visible to the user. To change computer group assignments, see Assign computer groups on page 618. For more information about how computer group assignments affect the visibility of recent results, see Recent results and computer group assignments on page 756.

User-specific settings and results for saved questions

If you configure RBAC permissions that enable multiple users to work with the same saved question, the following factors control which question settings and results those users can see:

- **User-specific configuration changes**

  When a user saves changes to the question configuration, the Tanium Server saves a copy of the question. Anytime that user subsequently views the question, only the copy with the user-specific changes is visible instead of the original question.

- **Computer group management rights**

  The computer groups that you assign to users determine the **Reissue** value that they see in the question configuration and which recent results the users see for that question.

For more information, see Reference: User-specific saved questions on page 750.

View saved question details

Viewing saved question attributes can help you manage the questions, assess their impact on endpoints, and troubleshoot unexpected question results. For example, the **Question Text** attribute shows the sensors that the question includes, which can help you assess the question runtime on endpoints. Use the following pages to view saved questions:

© 2026 Tanium Inc. All Rights Reserved

- **Administration > Content > Saved Questions** page: Use this page to view all question settings and other information, such as when a question was last modified. For more information, see View saved question settings on page 460.
- **Modules > Interact > Overview** page: Use this page to see the list of questions and to issue them. The page provides several options for finding specific questions in a long list:
  - Filter by categories and dashboards on page 460
  - Filter by text strings on page 461
  - Filter by favorites on page 462

View saved question settings

1. From the Main menu, go to **Administration > Content > Saved Questions**.
   The **Saved Questions** grid displays many of the attributes that are described under Create a saved question on page 463.
2. (Optional) To view the entire **Question Text** when that column cannot show it all on one line, click **Show More** in the cell for that question.
3. (Optional) To display attributes that the grid hides by default, click Customize Columns and select the attributes.
4. (Optional) Use the filters to find specific saved questions. For more information, see Filter by question attributes on page 462.
5. To see all the attributes for a particular question, click the question **Name**. For information about the attributes, see Create a saved question on page 463.

Filter by categories and dashboards

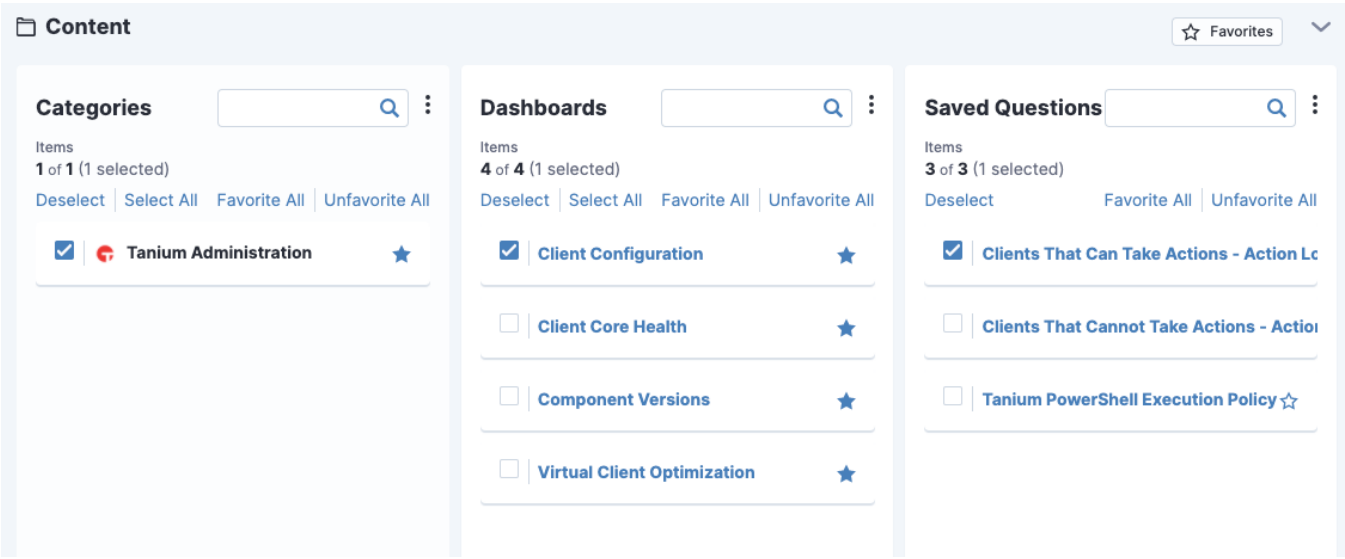
1. From the Main menu, go to **Modules > Interact > Overview**.
2. Select checkboxes in the panels so that only items belonging to the selected categories or dashboards appear. You can apply multiple filters.

   TIP

   Click **Deselect** in a panel header to clear all the panel filters.

© 2026 Tanium Inc. All Rights Reserved

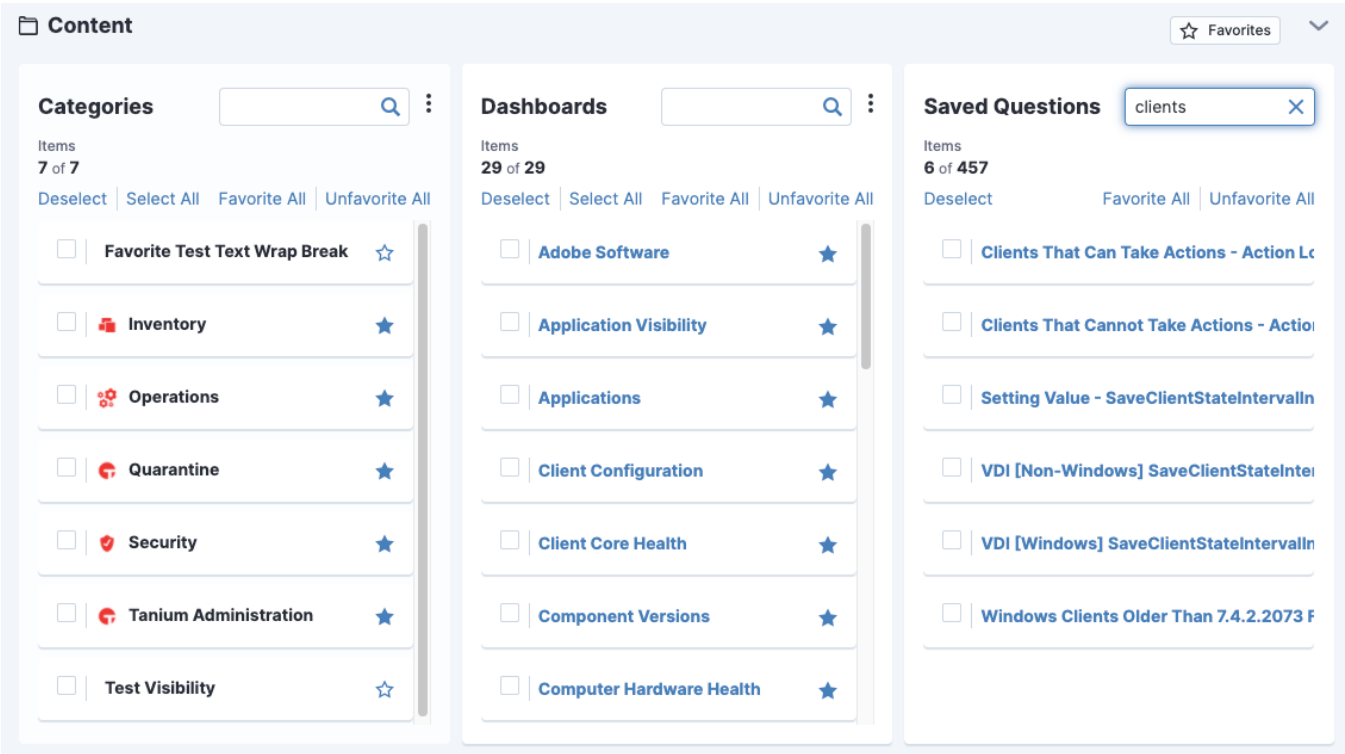
Filter Interact content by category and dashboard



Filter by text strings

1. From the Main menu, go to **Modules > Interact > Overview**.
2. Use the text filters in the panels to find items that match a specified string. Click the **x** in the text search box to clear the filter.

Filter Interact content by text



© 2026 Tanium Inc. All Rights Reserved

Filter by favorites

A *favorite* is a category, dashboard, or saved question that you want to use as an optional filter on the Interact **Overview** page. The Tanium Server saves favorites as a user-specific setting; your favorites selections do not apply to other users.

> **NOTE** Favorites also appear on the Tanium **Home** page. For more information, see Work with favorite Interact categories, dashboards, and saved questions on page 71.

To configure the display of favorite content, perform the following steps:

1. From the Main menu, go to **Modules > Interact > Overview**.
2. Click the Favorites icon next to the name of a category, dashboard, or saved question to select or deselect that item as a favorite.

   > **TIP** To reduce clicks, click **Favorite All** or **Unfavorite All** in a panel header and then toggle on or off individual items in that panel.

3. To view only favorite categories, dashboards, and saved questions, click **Favorites** in the upper right of the **Content** section. The button changes to a dark background to indicate that the panels display only favorites. Click **Favorites** again to toggle off the filter.

   > **TIP** After you find and select your favorite **Categories** or **Dashboards**, you might want to toggle off the **Favorites** filter so that the **Saved Questions** panel displays both favorite and non-favorite questions.

Filter by question attributes

1. From the Main menu, go to **Administration > Content > Saved Questions**.
2. Use the following filters to find specific saved questions based on their attributes:
   - **Filter by text**: Enter a text string in the **Filter items** field to filter the grid by question **Name** or **Question Text**.
   - **Filter by attribute**: Expand the **Filters** section, select a question attribute (such as **Content Set** assignment), select an operator (such as **contains**), enter a text string that contains all or part of the attribute value, and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.

     > **TIP** You can filter by the tags attribute only for questions that have tags configured. To add tags to a question, see Tags on page 464. To show the **Tags** column on the **Saved Questions** page, click Customize Columns and select **Tags**.

© 2026 Tanium Inc. All Rights Reserved

Clone a saved question

Cloning is useful when you need to:

- Create a modified version of a predefined saved question from a Tanium content-only solution.

  BEST PRACTICE

  Do not modify a predefined saved question.

- Create a new saved question with settings that differ only slightly from an existing question. This is often easier than creating a new question from scratch.

BEST PRACTICE

Review Best practices for saved questions on page 456 before cloning saved questions.

Perform the following steps to clone a saved question:

1. From the Main menu, go to **Modules > Interact > Overview**.
2. In the **Saved Questions** panel, mouse over the question, click Options, and select an option to issue the question:
   - **Copy to Question Bar**: Go to the **Ask a Question** field, optionally modify the question, and press `Enter`. For more information, see Issue a free-form question on page 241.
   - **Copy to Question Builder**: Optionally modify the question and then click **Ask Question**. For more information, see Issue a question through the Question Builder on page 245.
3. Click **Save**, configure the settings (see Create a saved question on page 463), and click **Save**.

Create a saved question

Creating saved questions expedites data collection from endpoints because you can reissue the questions without reconstructing them in the Interact **Ask a Question** field or **Question Builder**.

IMPORTANT

If you create a saved question that has a parameterized sensor, review Questions with parameterized sensors on page 238 to understand the impact on results that Tanium Clients return if the sensor definition changes.

TIP

Instead of creating a new saved question from scratch, cloning is usually easier if the question settings differ only slightly from an existing question. For more information, see Clone a saved question on page 463.

BEST PRACTICE

Review Best practices for saved questions on page 456 before creating saved questions.

© 2026 Tanium Inc. All Rights Reserved

1. Issue a dynamic question as described in Issue a free-form question on page 241 or Issue a question through the Question Builder on page 245.

   The **Question Results** page shows the results.

2. Click **Save** and configure the question **Details**.

   Saved question details

Details	Guidelines
Name	Enter a name of up to 255 characters to identify the saved question in lists that appear in Tanium Console workflows.
Content Set	Assign the question to a content set. The list is populated with all content sets for which you have **Saved Question write** permission.
Tags	To filter by tags on the **Saved Questions** page, you must first add the tags to questions. Click **Add tags**, enter a **Name** to identify the tag, and enter the tag **Value**. Add a **Name**-**Value** pair for each additional tag. For more information about filtering by attributes such as tags, see Filter by question attributes on page 462.

3. Configure the question **Preferences**.

   Saved question settings

Settings	Guidelines
Visibility	• **According to RBAC**. Users must have the **Saved Question read** permission for the content set to which the saved question belongs to see the saved question. • **Only the Owner and Admins can see this object**. Only the question owner and users with the **Administrator** reserved role can see the saved question. NOTE By default, the user who creates the question is the owner but you can transfer ownership to another user. For more information, see Delete content or transfer ownership on page 637.
Reissue	If you want to periodically reissue the question, select **Reissue this question every** and specify a number and unit for the reissue interval: **Minutes**, **Hours**, **Days**. For more information, see Scheduled saved questions on page 455.
Display this question in the list of questions that are available for drilling down	Enable this option to include the question in the list that users see when selecting a question for a drill-down operation on question results. For more information, see Drill down into results on page 267.

© 2026 Tanium Inc. All Rights Reserved

Saved question settings (continued)

Settings	Guidelines
Display this question in the list of questions that are available to merge	Enable this option to include the question in the list that users see when selecting a question for a merge operation on question results. Only non-counting questions provide this option. For more information, see Merge questions on page 264. NOTE You cannot change this setting after you save a new saved question configuration. Enabling this option automatically enables the **Yes, turn into non-counting question** option.
Do not turn into non-counting question Yes, turn into non-counting question	The option to convert the question to a non-counting question is available only if the question has one sensor in the `get` clause. A single-sensor question is a counting question by default. Converting to a non-counting question is required for users to include the question in merge operations. However, converting has other ramifications to consider before you select that option. For more information, see Counting and non-counting questions on page 235. NOTE You cannot change this setting after you save a new saved question configuration.
Save these settings for myself and other users with no prior settings saved Save these settings for my view only	Select whether the **User Settings** values that you configured are visible to other users who might view the saved question configuration. This visibility option is useful when you want a question to initially have the same **User Settings** values for everyone until individual users specify their own values. For more information, see User-specific saved questions.

4. (Optional) Select one or more **Associated Packages** to appear at the top of the **Deployment Package** dropdown list in the **Action Deployment** page when users deploy an action based on the question. By default, the **Deployment Package** selection is set to the first package that you add to the **Associated Packages**. As an example, for a question that returns the logging level of Tanium Clients on Windows endpoints, you might want to add the package **Set Windows Tanium Client Logging Level**. For more information, see Configure action settings on page 395 and Example: Saved questions with associated packages on page 525.
5. Expand the **Preview** section to preview the results of the saved question, and then click **Save**.

The question appears in the **Administration > Content > Saved Questions** page and Interact **Overview** page.

Edit a saved question

You can edit all the attributes of a saved question except the actual query (**Question Text**).

© 2026 Tanium Inc. All Rights Reserved

NOTE

To edit the query, create a new question. For more information, see Create a saved question on page 463.

BEST PRACTICE

Review Best practices for saved questions on page 456 before editing questions.

TIP

To change the content set assignment for multiple saved questions that must belong to the same set, see Move saved questions between content sets on page 466.

1. Use one of the following methods to open the **Edit Saved Question** page:
   - From the Main menu, go to **Administration > Content > Saved Questions** and click the question **Name**.
   - From the Main menu, go to **Modules > Interact > Overview**, find the question in the **Saved Questions** panel, mouse over the question, click Options ..., and select **Edit Properties**.
2. Configure the settings and click **Save**. For information about the settings, see Create a saved question on page 463.

Move saved questions between content sets

You can move saved questions in bulk between content sets to accommodate RBAC changes in your organization. For example, you might want to move certain saved questions to a content set that only highly privileged users can access.

1. From the Main menu, go to **Administration > Content > Saved Questions**.
2. Select the saved questions and click **Move to Content Set**.
3. Select a content set and click **Confirm**.

Issue a saved question

After you save a question, use one of the following methods to issue the question to endpoints:

- **Interact Overview page**
  From the Main menu, go to **Modules > Interact > Overview**, go to the **Saved Questions** panel, and click the question name.
- **Tanium Home page**
  Go to the Tanium **Home** page and, if the question has favorite status, go to the **Favorite Interact Questions** section and click the question name. If the **Favorite Interact Questions** section is not visible, see Work with favorite Interact categories, dashboards, and saved questions on page 71.
- **Saved Questions page**
  From the Main menu, go to **Administration > Content > Saved Questions**, select a question, and click **Load**.

© 2026 Tanium Inc. All Rights Reserved

- **Question configuration**

  To automatically reissue a saved question at intervals, edit the question configuration and set the **Reissue** interval. For more information, see Edit a saved question on page 465.

Tanium Console shows the results in the saved question results page. To filter or otherwise manipulate the results, see Part 7: Analyzing question results in Console and Interact on page 255.

BEST PRACTICE

Use Tanium Reporting instead of Interact saved questions if you want to review results from sensors that are registered with Tanium Data Service (TDS). For more information, see Viewing the results of saved questions in Interact or Reporting on page 457.

Issue a dashboard of saved questions

In some cases, it is useful to issue several saved questions that are related based on the kind of information they retrieve from endpoints. In such cases, you can group the questions in a single dashboard and issue them simultaneously. For example, the predefined **Hardware Inventory** dashboard contains questions that retrieve chassis type, operating system, monitor, CPU, disk, memory, and BIOS information. For more information, see Interact dashboards and categories on page 457.

BEST PRACTICE

Use Tanium Reporting instead of Interact dashboards if you want to review results from sensors that are registered with Tanium Data Service (TDS). For more information, see Part 7: Analyzing question results in Console and Interact on page 255.

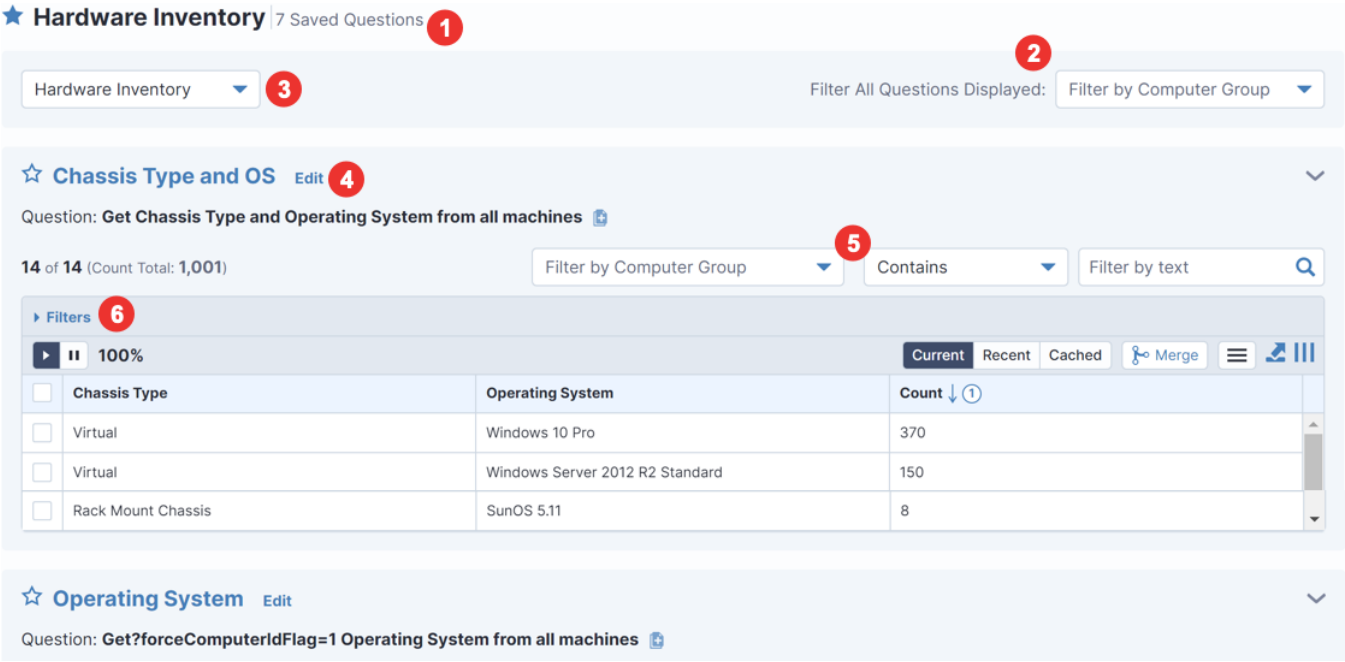
To issue all the questions in a dashboard:

1. From the Main menu, go to **Modules > Interact > Overview**.
2. In the **Dashboards** panel, click the dashboard name.

   The dashboard results page appears, which shows a results grid for each saved question in the dashboard.

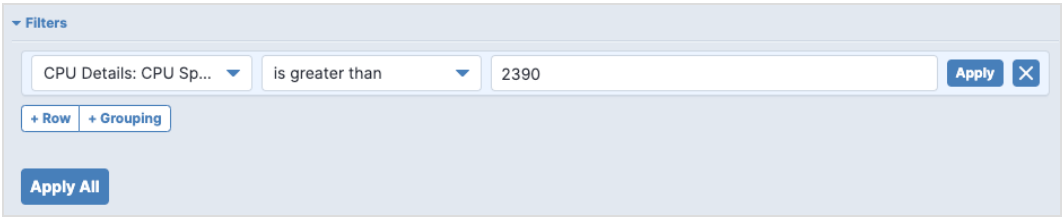
© 2026 Tanium Inc. All Rights Reserved

Dashboard results page



For each question, the dashboard results page provides all the features that are available in the saved question results page, such as viewing **Current**, **Recent**, or **Cached** results. For more information, see Part 7: Analyzing question results in Console and Interact on page 255. The dashboard results page also has the following features (matching the numbers in the figure Dashboard results page on page 468):

1. The page shows the dashboard name, favorite status (★ for favorite, ☆ for non-favorite), and number of saved questions in the dashboard. Click the favorite icon ★/☆ to toggle the favorite status of the dashboard.
2. Use the **Filter All Questions Displayed** drop-down to filter all the results grids by computer group.
3. Use the dashboards dropdown list to issue a different dashboard.
4. For each results grid, the page shows the question name and favorite status. Click the favorite icon ★/☆ to toggle the favorite status of the question. Click the question name to reissue the question. Click **Edit** to change the question settings. For more information, see Edit a saved question on page 465.
5. Filter by computer group or text string.
6. Apply additional filters to a specific results grid.



© 2026 Tanium Inc. All Rights Reserved

Manage categories and dashboards

Interact provides predefined dashboards and categories for organizing saved questions. For example, the **Inventory** category contains all the dashboards related to your hardware, software, and virtual inventory. The **Applications** dashboard contains saved questions that collect information about installed and running applications. You can manage both predefined and custom dashboards and categories to suit the needs of your organization. For example, you might create a custom dashboard to contain custom saved questions that do not relate to any existing dashboard.

The following tasks describe how to create, edit, reassign, export, or delete dashboards and categories.

> NOTE
>
> For more conceptual information, see Interact dashboards and categories on page 457.

View and filter categories or dashboards

You can filter the categories and dashboards on the Interact **Overview** page if the lists are too long to scan quickly.

- Filter by categories and dashboards on page 460
- Filter by text strings on page 461
- Filter by favorites on page 462

To view the settings of a category or dashboard, open it in edit mode. For more information, see Edit category or dashboard settings on page 471.

Create a category

1. From the Main menu, go to **Modules > Interact > Overview**.
2. In the **Categories** panel heading, click Options and select **New Category**.
3. Configure the following settings and click **Save**:

Category settings

Setting	Description
Name	Enter a name to identify the category.
Content Set	Assign a content set to control user access to the category. NOTE: If you set the **Visibility** option to **Only the Owner and Admins can see this object**, other users cannot see the category even if they have the necessary content set permissions.
Change Icon	(Optional) Click **Choose File** and select the file of an icon to add as a visual identifier for the category.
Visibility	Select one of the options described in Visibility options on page 458 to control user access to the category.

© 2026 Tanium Inc. All Rights Reserved

Create a dashboard

1. From the Main menu, go to **Modules > Interact > Overview**.
2. In the **Dashboards** panel heading, click Options and select **New Dashboard**.
3. Configure the following settings and click **Save**:

Dashboard settings

Setting	Description
Name	Enter a name to identify the dashboard.
Content Set	Assign a content set to control user access to the dashboard. NOTE If you set the **Visibility** option to **Only the Owner and Admins can see this object**, other users cannot see the category even if they have the necessary content set permissions.
Change Icon	(Optional) Click **Choose File** and select the file of an icon to add as a visual identifier for the dashboard.
Visibility	Select one of the options described in Visibility options on page 458 to control user access to the dashboard.

Assign dashboards to a category

1. From the Main menu, go to **Modules > Interact > Overview**.
2. In the **Categories** panel, mouse over the category, click Options, and select **Add/Remove Dashboards**.
3. In the **Dashboards** panel, select the dashboards to include in this category and click **Apply**.

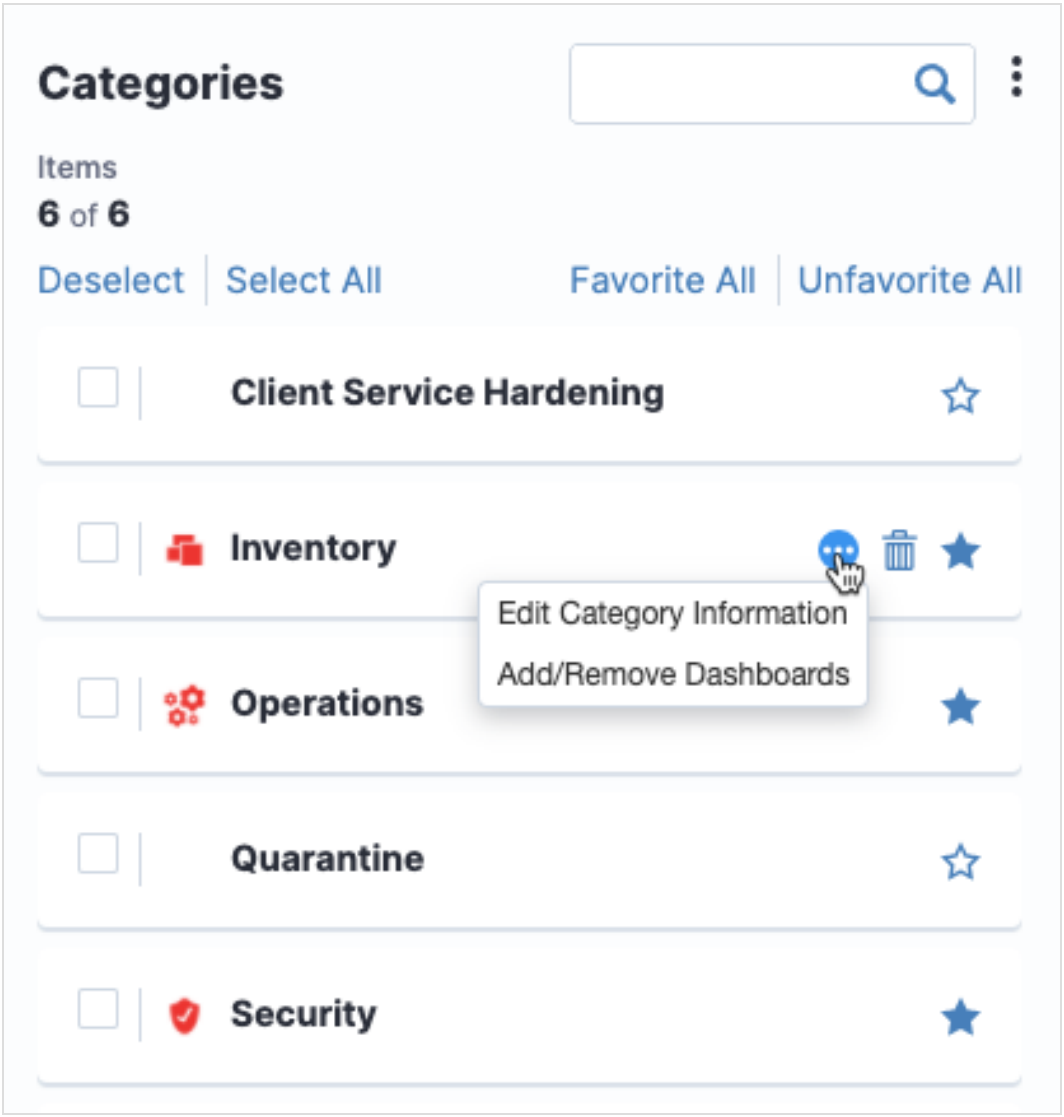
Assign saved questions to a dashboard

1. From the Main menu, go to **Modules > Interact > Overview**.
2. In the **Dashboards** panel, mouse over the category, click Options, and select **Add/Remove Saved Questions**.
3. In the **Saved Questions** panel, select the saved questions to include in this dashboard and click **Apply**.

© 2026 Tanium Inc. All Rights Reserved

Edit category or dashboard settings

1. From the Main menu, go to **Modules > Interact > Overview**.
2. In the **Categories** or **Dashboards** panel, mouse over the category or dashboard, click Options ..., and select **Edit Category Information** or **Edit Dashboard Information**.



3. Edit the settings and save the configuration. For more information, see Category settings on page 469 or Dashboard settings on page 470.

TIP To edit saved questions settings, see Edit a saved question on page 465.

Export categories, dashboards, or questions

© 2026 Tanium Inc. All Rights Reserved

You can export multiple category, dashboard, or saved question configurations as a JSON file from the Interact **Overview** page. Exporting configurations is useful if you want to import them into another Tanium environment. For example, you might test saved questions in a lab environment to ensure they work as intended before importing the questions into your production environment.

You must be assigned a role with the **Export Content** permission to export configurations. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.

You can also export saved questions in CSV or JSON format from the **Administration > Content > Saved Questions** page. For more information, see Export saved questions on page 472.

1. From the Main menu, go to **Modules > Interact > Overview**.
2. In the panel header for **Categories**, **Dashboards**, or **Saved Questions**, click Options and select the export option.
3. Select items to export or **Select all**.
4. Click **Export**, optionally modify the **File Name**, and click **Export** again.

The JSON file is saved to the downloads folder on the computer that you use to access Tanium Console. To import the file into another environment, see Import content files on page 134.

Delete a category or dashboard configuration

When you delete a category, the Tanium Server does not assign its dashboards to any other category. When you delete a dashboard, the Server does not assign its saved questions to any other dashboard.

1. From the Main menu, go to **Modules > Interact > Overview**.
2. In the **Categories** or **Dashboards** panel, mouse over the category or dashboard and click Delete .
3. Confirm that you want to delete the configuration.



You cannot delete a saved question configuration from the Interact **Overview** page, only from the **Administration > Content > Saved Questions** page.

Export or import saved questions

Export saved questions

Export saved questions as a file in the format required for your workflow:

© 2026 Tanium Inc. All Rights Reserved

- **CSV**

  You can use any application that supports CSV format to display the same saved question attributes (columns) as the Console **Saved Questions** grid shows and then customize the display. For example, you can use Microsoft Excel to create charts based on saved question attributes.

- **JSON**

  You can export multiple saved question configurations as a JSON file. Exporting configurations is useful if you want to import them into another Tanium environment. For example, you might test saved questions in a lab environment to ensure that they work as intended before importing the questions into your production environment. You must be assigned a role with the **Export Content** permission to export a JSON file. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.

Perform the following steps to export saved questions:

1. From the Main menu, go to **Administration > Content > Saved Questions**.
2. (Optional, CSV exports only) To add or remove attributes (columns) for the CSV file, click Customize Columns  in the grid and select the attributes.
3. Select rows in the grid to export only specific saved questions. If you want to export all saved questions, skip this step.
4. Click Export .
5. (Optional) Edit the default export **File Name**.

   The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.
6. Select an **Export Data** option: **All** saved questions in the grid or just the **Selected** saved questions.
7. Select the file **Format**:
   - **List of Saved Questions - CSV**
   - **Saved Question Definitions - JSON** (requires **Export Content** permission)
8. Click **Export**.

   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

Import saved questions

Importing is useful if you want to copy saved question configurations from another Tanium environment. For example, you might test saved questions in a lab environment to ensure that they work as intended. You can then export the questions from the lab environment and import them into your production environment. You can import saved questions and other content as a JSON or XML file.

You must be assigned a role with **Import Signed Content** permission to import content files.

© 2026 Tanium Inc. All Rights Reserved

1. (Non-Tanium-provided content only) Digitally sign the content file and ensure a public key is in place to validate the signature. For more information, see Authenticating content files on page 482.

   NOTE

   You do not have to generate keys or signatures for Tanium-provided solutions. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process.

   If you plan to import a file that another user signed, you can first perform an integrity check on the file. For more information, see Verify content file signatures on page 487.

2. From the Main menu, go to any of the following **Administration** pages:
   - **Configuration > Solutions**
   - **Permissions > Filter Groups**
   - Under **Content**, select **Sensors**, **Packages**, or **Saved Questions**
   - Under **Actions**, select **Scheduled Actions**, **All Pending Approvals**, or **Actions I Can Approve**
3. Select an **Import** option based on the source of the content:
   - **Import > Import Files**: Perform one of the following steps to select one or more files:
     - Drag and drop files from your file explorer.
     - Click **Browse for File**, select the files, and click **Open**.
   - **Import > Import URL**: Enter the URL in the **Import URL** field, and click **Import**.
4. For each file, expand the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts on page 135.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, **Include content set overwrite** is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Install**.

Copy saved question configuration details

Copy information from the **Saved Questions** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the content that you copy.

1. From the Main menu, go to **Administration > Content > Saved Questions**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy.
   - **Copy cell information**: Hover over the cell, click Options, and click Copy.

© 2026 Tanium Inc. All Rights Reserved

Delete saved questions

IMPORTANT

Do not delete the predefined saved questions that Tanium solutions provide. When you import solution updates, the update process restores any predefined saved questions that users have deleted.

BEST PRACTICE

Instead of deleting custom saved questions, instruct users not to use them.

Deleting a custom saved question might be warranted in certain scenarios. For example, the question might not be needed anymore, the question might not collect the expected data from endpoints, or another question might use fewer endpoint resources to collect the same data.

Perform the following steps before you delete a saved question:

1. Determine if any scheduled content uses the saved question and assess the impact of removing or replacing the question. For example, a Tanium Connect connection might use the question as a source. To preserve the connection, you must find a replacement source.
2. Decide which saved question is a suitable replacement or create a replacement if necessary. This step is required only if you must recreate or reconfigure the content that uses the question you plan to delete. For more information, see View saved question details on page 459 and Create a saved question on page 463.
3. Reconfigure or recreate scheduled content to remove dependencies on the question and replace it if necessary.

Perform the following steps to delete a saved question:

1. From the Main menu, go to **Administration > Content > Saved Questions**.
2. Select the question and click Delete.

© 2026 Tanium Inc. All Rights Reserved

Managing filter groups for filtering questions and results

Filter groups overview

Filter groups are a type of computer group that you use as filters in questions (see Use filter groups) and question results (see Filter question results on page 259). For example, you can use the **All Windows** filter group to show results only from Windows endpoints. When you first sign in to Tanium Console after a fresh installation of the Tanium Server, the Server automatically imports Default computer groups on page 615 that include filter groups. You can add custom filter groups to address filtering scenarios that are specific to your environment.

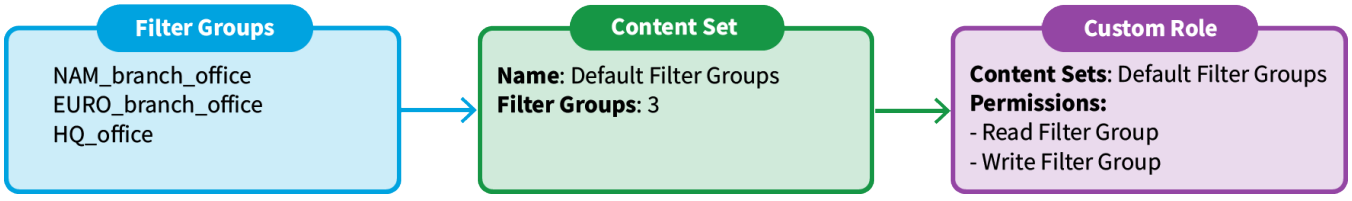
To manage computer groups that function as both filter groups and computer management groups, use the **Computer Groups** page, as described in Controlling endpoint management rights through computer groups on page 610. The reserved computer groups **All Computers** and **No Computers** function as both types. These reserved groups are in the **Reserved** content set, and you cannot edit them.

> NOTE
>
> For the role permissions required to manage filter groups, see Manage filter groups on page 101.

Filter group permissions

Users acquire permissions for a filter group when you assign it to a content set that is associated with a custom role and assign the role to personas, users, and user groups. The following figure shows an example of a custom role that grants **Filter Group read** and **write** permissions to the **Default Filter Groups** content set:

Filter group assignment



> NOTE
>
> Users cannot receive question results from endpoints in a filter group unless those endpoints also belong to a computer management group that is assigned to the persona that the user used to issue the question. For more information about the interaction between computer management groups and filter groups, and how best to use them, see Computer groups overview on page 610.

© 2026 Tanium Inc. All Rights Reserved

View filter group details

Viewing filter group attributes can help you to determine if new groups are necessary and to manage or troubleshoot existing groups. For example, you might check the **Expression** attribute of a group to diagnose unexpected filtering results.

1. From the Main menu, go to **Administration > Permissions > Filter Groups**.
   The **Filter Groups** grid displays the following attributes for each filter group:
   - **Name**: The name that identifies the filter group.
   - **Type**: Indicates whether group membership is sensor-based (`Standard`) or manually defined (`Manual`). For more information, see Computer group membership on page 614.
   - **Content Set**: The content set to which the group is assigned.
   - **Expression**: For standard filter groups, the expression is a sensor-based filter that defines group membership. For manual filter groups, the value is `[Manual List]`.
   - **Modified By (Persona)**: The name of the user who last modified the filter group. If the user used an alternative persona during the modification, the persona appears in parentheses.
   - **Last Modification**: The date and time when a user last modified the filter group.
2. (Optional) Use the filters to find specific filter groups:
   - **Filter by text**: Enter a text string in the **Filter items** field to filter the grid by filter group **Name** or membership **Expression**.
   - **Filter by attribute**: Expand the **Filters** section, select a group attribute (such as **Content Set** assignment), select an operator (such as **contains**), enter a text string that contains all or part of the attribute value, and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.
3. To see the members of a particular filter group, click the group **Name** and go to the **Members** section.

Configure a filter group

Create custom filter groups if the Tanium-defined groups do not address all the scenarios for filtering questions and question results in your environment. For example, you might want to issue questions only to endpoints that have a certain custom tag. Before you create a filter group, be sure to understand the difference between dynamic membership and manually defined membership. For more information, see Computer group membership on page 614.

TIP

Instead of creating a new filter group from scratch, cloning is usually easier if the group settings differ only slightly from an existing group.

You can edit the display name and content set assignment of a filter group. However, changing the display name does not change the object ID of a filter group. Also, you cannot change the group membership definition.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Permissions > Filter Groups** and perform one of the following steps:
    - **Create a new group from scratch**: Click **New Group**.
    - **Clone a group**: Select the filter group and click **Clone**.
    - **Edit a group**: Click the filter group **Name** and click **Edit Mode**.
2. Enter a **Name** of up to 255 characters to identify the group.
3. Assign the group to a **Content Set**.
4. Define which endpoints are **Members** of the filter group.

    You cannot change the **Members** definition after you save the filter group. However, if you configure dynamic membership and base it on a custom tag, you can change tag assignments on endpoints to adjust the group membership. For more information, see Manage computer group membership through custom tags on page 619.

    - **Dynamic membership** (best practice): Select a method for defining the membership filter:
        - **Filter Bar**: Use the same syntax as in the `from` clause of the Interact **Ask a Question** field. For more information, see Issue a free-form question on page 241.
        - **Filter Builder**: Use the same **from computers with** fields as in the Interact **Question Builder**. For more information, see Issue a question through the Question Builder on page 245.
    - **Manually defined membership**: Select **Manual Group** and enter a list of endpoint identifiers, which can be one of the following:
        - Computer names that match the results of the **Computer Name** sensor. Short forms or alternative names do not work.
        - Fully qualified domain names (FQDNs).
        - IP addresses that match the entries in the **Administration > Configuration > Client Status** page, **Network Location (from server)** column.
5. Review the list of endpoints that are members of the group and click **Save**.

Export or import filter groups

Export filter groups

Export filter groups as a file in the format required for your workflow:

© 2026 Tanium Inc. All Rights Reserved

- **CSV**

  You can use any application that supports CSV format to display the same filter group attributes (columns) as the Console **Filter Groups** grid shows and then customize the display. For example, you can use Microsoft Excel to create charts based on filter group attributes.

- **JSON**

  You can export multiple filter group configurations as a JSON file. Exporting configurations is useful if you want to import them into another Tanium environment. For example, you might test custom filter groups in a lab environment to ensure that they work as intended before importing the groups into your production environment. You must be assigned a role with the **Export Content** permission to export a JSON file. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.

Perform the following steps to export filter groups:

1. From the Main menu, go to **Administration > Permissions > Filter Groups**.
2. (Optional, CSV exports only) To add or remove attributes (columns) for the CSV file, click Customize Columns  in the grid and select **ID**.
3. Select rows in the grid to export only specific filter groups. If you want to export all filter groups, skip this step.
4. Click Export .
5. (Optional) Edit the default export **File Name**.

   The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.
6. Select an **Export Data** option: **All** filter groups in the grid or just the **Selected** filter groups.
7. Select the file **Format**:
   - **List of Filter Groups - CSV**
   - **Filter Group Definitions - JSON** (requires **Export Content** permission)
8. Click **Export**.

   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

Import filter groups

Importing is useful if you want to copy filter group configurations from another Tanium environment. For example, you might test filter groups in a lab environment to ensure that they work as intended. You can then export the groups from the lab environment and import them into your production environment. You can import filter groups and other content as a JSON or XML file.

You must be assigned a role with **Import Signed Content** permission to import content files.

© 2026 Tanium Inc. All Rights Reserved

1. (Non-Tanium-provided content only) Digitally sign the content file and ensure a public key is in place to validate the signature. For more information, see Authenticating content files on page 482.

   NOTE

   You do not have to generate keys or signatures for Tanium-provided solutions. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process.

   If you plan to import a file that another user signed, you can first perform an integrity check on the file. For more information, see Verify content file signatures on page 487.

2. From the Main menu, go to any of the following **Administration** pages:
   - **Configuration > Solutions**
   - **Permissions > Filter Groups**
   - Under **Content**, select **Sensors**, **Packages**, or **Saved Questions**
   - Under **Actions**, select **Scheduled Actions**, **All Pending Approvals**, or **Actions I Can Approve**
3. Select an **Import** option based on the source of the content:
   - **Import > Import Files**: Perform one of the following steps to select one or more files:
     - Drag and drop files from your file explorer.
     - Click **Browse for File**, select the files, and click **Open**.
   - **Import > Import URL**: Enter the URL in the **Import URL** field, and click **Import**.
4. For each file, expand the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts on page 135.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, **Include content set overwrite** is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Install**.

Copy filter group configuration details

Copy information from the **Filter Groups** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the content that you copy.

1. From the Main menu, go to **Administration > Permissions > Filter Groups**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy.
   - **Copy cell information**: Hover over the cell, click Options, and click Copy.

© 2026 Tanium Inc. All Rights Reserved

Delete filter groups

IMPORTANT

Do not delete the predefined filter groups that Tanium solutions provide. When you import solution updates, the update process restores any predefined filter groups that users deleted.

BEST PRACTICE

Instead of deleting custom filter groups, instruct users not to use them.

Before you delete filter groups, be sure to understand the consequences for scheduled actions and questions, and perform any prerequisite tasks. For more information, see Delete computer groups on page 623.

If you delete a filter group that also functions as a management group, it remains on the Tanium Server as a management group with filtering disabled; the **Administration > Permissions > Computer Groups** page continues displaying the group but the **Administration > Permissions > Filter Groups** page does not.

Perform the following steps to delete a filter group:

1. From the Main menu, go to **Administration > Permissions > Filter Groups**.
2. Select the filter group and click Delete .

© 2026 Tanium Inc. All Rights Reserved

Authenticating content files

Overview of content imports and exports

Exporting content (such as sensors and roles) enables you to review the content attributes offline in an application outside Tanium Console (such as in Microsoft Excel) or to import the content into another Tanium Server.

NOTE

For the user role permissions that are required to import or export content, see Import content files on page 101 and Export content files on page 101.

Supported file formats

You can export content as a file in one of the following formats:

- **JSON**
  A JSON file contains the configurations of content objects. Exporting configurations is useful if you want to import them into another Tanium environment. For example, you might test custom sensors in a lab environment to ensure that they work as intended before importing the sensors into your production environment. You must be assigned a role with the **Export Content** permission to export a JSON file. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.
- **CSV**
  A CSV file contains all the attributes of content objects that you see in various grids in Tanium Console. For example, if you export in CSV format from the **Sensors** page, the CSV file contains all the sensor attributes (columns) that you see in the grid on that page. CSV exports are useful for reviewing content attributes in applications that support CSV. For example, you can use Microsoft Excel to create charts based on sensor attributes.

Digital signatures and keys

In Tanium deployments with a production license, content that you import requires a digital signature by default. Signature validation helps to protect your deployment from imports of unauthorized files. A private key is used to create the signature. The Tanium Server uses the associated public key to validate the signature during the import process. You maintain the public keys of trusted signers on the Server. If none of the public keys in the Server key store can validate the signature, the Server does not import the content, and Tanium Console shows failure messages:

```
Error occurred beginning import: FAILURE
```

```
Import validation failed. The signature did not match. Please verify the file contents, validate the signature, and try again.
```

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

In Tanium deployments with a lab license, Tanium Console notifies you if the file you selected to import is unsigned and lets you choose whether to proceed. However, the best practice is to not import unsigned files in any deployment.

You do not have to generate keys or signatures for content that you import as a component of a Tanium solution. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process. For all other content, you must manually generate a public-private key pair to sign and validate the content files that you import.

As one-time tasks before importing content, you must generate the public-private key pair and copy the public key to the Tanium Server key store. You must then use the private key to sign each new content file that you import. If you plan to import a file that another user signed, you can first perform an integrity check on the file as described at Verify content file signatures on page 487.

Import and export permissions

Users who are assigned a role with **Import Signed Content** permission can import signed content files. Users who have the **Administrator** reserved role can export and import all content types. For other users, the ability to export varies by content type and role assignments. For more information, see Content management permissions on page 97.

Import and export procedures

For the steps to export content files, see Export content files on page 133.

For the steps to import content files after you digitally sign them, see Import content files on page 134.

NOTE

To troubleshoot content import issues, see Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform.

Create content authentication keys

The Tanium Server provides a command-line program to generate a cryptographic key pair for signing and validating content files. The program is **KeyUtility** on Windows and **TaniumKeyUtility** on Linux. The program and its associated files reside in the top-level installation directory of the Server. You can run the program from the Server installation directory (Windows only) or copy the files to a working directory on another system and run the program from that working directory.

© 2026 Tanium Inc. All Rights Reserved

Windows: Create content authentication keys

1. (Optional) To run **KeyUtility** from a working directory, set up the directory as follows:
   a. Copy the following files from the Tanium Server installation directory (such as `\Program Files\Tanium\Tanium Server`) or from the location where you unzipped the `KeyUtility-<release>.zip` file that Tanium Support provided:
      - `KeyUtility.exe`
      - `libeay32.dll`
      - `ssleay32.dll`
   b. Paste the files into the working directory.
2. Open the Windows **Command Prompt** (`cmd.exe`) and run the following command from the directory where the **KeyUtility** files reside. The `<file name>` argument defines the key-file names, but you do not have to specify the suffix. **KeyUtility** automatically appends the suffix `.pub` for the public key and `.pvk` for the private key.

   ```
   KeyUtility.exe makekeys <file name>
   ```

The following is an example of the command and the resulting contents of a working directory:

```
D:\Tanium\Working>KeyUtility.exe makekeys import

D:\Tanium\Working>dir

Directory of D:\Tanium\Working

09/05/2018  08:05 PM    <DIR>          .
09/05/2018  08:05 PM    <DIR>          ..
08/17/2018  03:04 AM         4,254,704 KeyUtility.exe
03/27/2018  07:03 PM         2,632,192 libeay32.dll
03/27/2018  07:03 PM           457,728 ssleay32.dll
09/05/2018  08:05 PM               158 import.pub
09/05/2018  08:05 PM               241 import.pvk
5 File(s)      7,345,023 bytes
2 Dir(s)  41,049,174,016 bytes free
```

Linux: Create content authentication keys

On a Tanium Appliance, running **TaniumKeyUtility** requires shell access, which is not available in most cases. The following steps describe how to run the program from another working directory instead.

© 2026 Tanium Inc. All Rights Reserved

1. Contact Tanium Support on page 724 to request the the `KeyUtility-<release>.tgz` file that contains **TaniumKeyUtility** and associated files:

   - `TaniumKeyUtility`
   - `libcrypto.so.1.0.0`
   - `libssl.so.1.0.0`

   You can also find the files in the Tanium Server installation directory (such as `/opt/Tanium/TaniumServer`).

2. Copy `KeyUtility-<release>.tgz` to the working directory and uncompress it:

   ```
   tar -xvf KeyUtility-<release>.tgz
   ```

3. Run the following command from the directory where **TaniumKeyUtility** resides. The `<file name>` argument defines the key-file names, but you do not have to specify the suffix. **TaniumKeyUtility** automatically appends the suffix `.pub` for the public key and `.pvk` for the private key.

   ```
   ./TaniumKeyUtility makekeys <file name>
   ```

The following is an example of the command and the resulting contents of a working directory:

```
./TaniumKeyUtility makekeys import

ls -l

-r-xr-x---  1 tanium tanium  7947792 Jun  1 13:39 TaniumKeyUtility
-r-xr-x---  1 tanium tanium  2947600 Jun  1 13:39 libcrypto.so.1.0.0
-r-xr-x---  1 tanium tanium   459272 Jun  1 13:39 libssl.so.1.0.0
-rw-r-----  1 tanium tanium      158 Jul 19 16:38 import.pub
-rw-r--r--  1 tanium tanium      241 Jul 19 16:38 import.pvk
```

Sign content files

After you create a public-private key pair for authenticating content files, use the private key to sign the files.

© 2026 Tanium Inc. All Rights Reserved

Windows: Sign content files

1. Copy the content file to a location that you can access from the directory where the **KeyUtility** and content-signing key files reside.

   The directory is either the Tanium Server installation directory (such as `\Program Files\Tanium\Tanium Server`) or a working directory that you set up. For more information, see Windows: Create content authentication keys on page 484.

2. Open the Windows **Command Prompt** (`cmd.exe`) and go to the directory where the **KeyUtility** and key files reside.

3. Sign the content file.

   ```
   KeyUtility.exe signcontent <private_key> <content_file>
   ```

   The following is an example of the command:

   ```
   KeyUtility.exe signcontent import.pvk sensors.json
   ```

4. Open the content file in a text editor and verify that a signature such as the following appears at the bottom:

   ```
   <!--
   hash=2a8bc7529c9fcdad037982bcbfc12306aa88ac8b9d95d02248ec369008188b7c0e356ad1
   811609c7
   54eb01dc97c09b9f2acb10331e2d9dbf77d309124c61950a;signature=01AF3D547A97CCBD62
   A022F398
   586DEAD4E29A30C29406283DA2E8F1E9FCF176194D66D4D9602538102F8F2FBBCFBC7AF370DB4
   4E839C04
   7253A246447E9A146706F00E94CD26D2CF29D8916E6EE0F21C77F0E13A6769905E5DDC0945891
   2A94BB74
   C1311C9B26301DB8D8C73AC043EBC6A5A836FB6815011F1ACB37E0248A30F100B631-->
   ```

Linux: Sign content files

1. Copy the content file to a location that you can access from the directory where the **TaniumKeyUtility** and content-signing key files reside.

2. Go to the directory where the **TaniumKeyUtility** and key files reside.

   ```
   cd <working directory>
   ```

3. Sign the content file.

   ```
   ./TaniumKeyUtility signcontent <private_key> <content_file>
   ```

   The following is an example of the command:

   ```
   ./TaniumKeyUtility signcontent import.pvk "sensors.json"
   ```

© 2026 Tanium Inc. All Rights Reserved

4. Open the content file in a text editor and verify that a signature such as the following appears at the bottom:

```
<!--
hash=2a8bc7529c9fcdad037982bcbfc12306aa88ac8b9d95d02248ec369008188b7c0e356ad1
811609c7
54eb01dc97c09b9f2acb10331e2d9dbf77d309124c61950a;signature=01AF3D547A97CCBD62
A022F398
586DEAD4E29A30C29406283DA2E8F1E9FCF176194D66D4D9602538102F8F2FBBCFBC7AF370DB4
4E839C04
7253A246447E9A146706F00E94CD26D2CF29D8916E6EE0F21C77F0E13A6769905E5DDC0945891
2A94BB74
C1311C9B26301DB8D8C73AC043EBC6A5A836FB6815011F1ACB37E0248A30F100B631-->
```

Verify content file signatures

Users might copy content files between systems to make the files accessible for importing. For example, after testing custom sensors in a lab environment, a user might export the sensors as a JSON file and copy it to a production environment. Before you import a file that another user digitally signed, you can verify the integrity of the file as a security measure. Signature verification ensures that the correct private key was used to sign the file and that no one modified the file after it was signed. To verify the signature of a private key, you specify its associated public key in the verification command.

Windows: Verify file signatures

1. Copy the content file to a location that you can access from the directory where the **KeyUtility** and content-signing key files reside.

   The directory is either the Tanium Server installation directory (such as `\Program Files\Tanium\Tanium Server`) or a working directory that you set up. For more information, see Windows: Create content authentication keys on page 484.

2. Open the Windows **Command Prompt** (`cmd.exe`) and go to the directory where the **KeyUtility** and key files reside.

3. Run the following command, where `<public_key>` is the public key associated with the private key that you are verifying:

   ```
   KeyUtility.exe verifycontent <public_key> <content_file>
   ```

   The following is an example of the command:

   ```
   KeyUtility.exe verifycontent import.pub sensors.json
   ```

   If the file passes verification, the output is:

   ```
   Signature Verified.
   ```

© 2026 Tanium Inc. All Rights Reserved

Linux: Verify file signatures

1. Copy the content file to a location that you can access from the directory where the **TaniumKeyUtility** and content-signing key files reside.
2. Go to the directory where the **TaniumKeyUtility** and key files reside.

   ```
   cd <working directory>
   ```

3. Run the following command, where `<public_key>` is the public key associated with the private key that you are verifying:

   ```
   ./TaniumKeyUtility verifycontent <public_key> <content_file>
   ```

   The following is an example of the command:

   ```
   ./TaniumKeyUtility verifycontent import.pub sensors.json
   ```

   If the file passes verification, the output is:

   ```
   Signature Verified.
   ```

Copy the public key to the key store

Before you import a content file, the Tanium Server keys directory must have a copy of the public key that the Server uses to validate the signature in the file. This is the public key that is associated with the private key that you use to sign content files, not the Server root public key `tanium.pub`.



In an active-active cluster, perform these steps for each active Tanium Server in the deployment. The Tanium Server does not synchronize content-signing keys between cluster members. If you copy the public key to only one Tanium Server, imports of content signed with the associated private key succeed on that Tanium Server but fail on the other Tanium Server, which can appear as an intermittent or random import failure.

Windows: Copy the public key to the key store

1. Copy the public key from the directory where you ran the key-generation command. The directory is either the Tanium Server installation directory (such as `\Program Files\Tanium\Tanium Server`) or a working directory that you set up. For more information, see Windows: Create content authentication keys on page 484.
2. Paste the public key into the `\Program Files\Tanium\Tanium Server\content_public_keys\content` directory.

© 2026 Tanium Inc. All Rights Reserved

Linux: Copy the public key to the key store

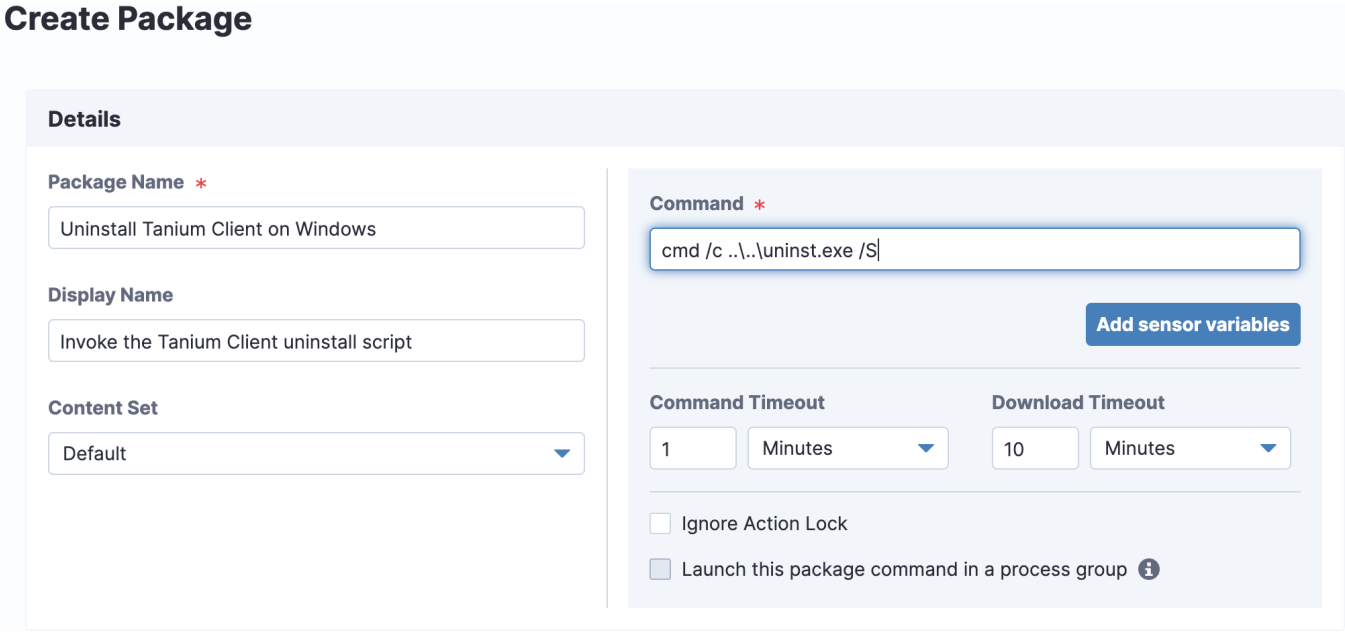
To add the public key to the Tanium Server in a Tanium Appliance deployment, perform the steps in Tanium Appliance Installation Guide: Enable import of user-created content. Because you already generated the keys, skip the steps to download the utility and generate keys.

© 2026 Tanium Inc. All Rights Reserved

Example: Package files

When you deploy actions, the Tanium Server distributes packages that run commands on the target endpoints. Some package commands depend on files that are distributed with the package. Other commands depend on utilities and resources that were previously installed in known locations on the endpoints. The following figure shows an example of a command that invokes the Tanium Client uninstallation utility `uninst.exe`. The utility file resides in the top-level installation folder on Windows, such as `C:\Program Files (x86)\Tanium\Tanium Client`.

Package that invokes the uninstallation utility



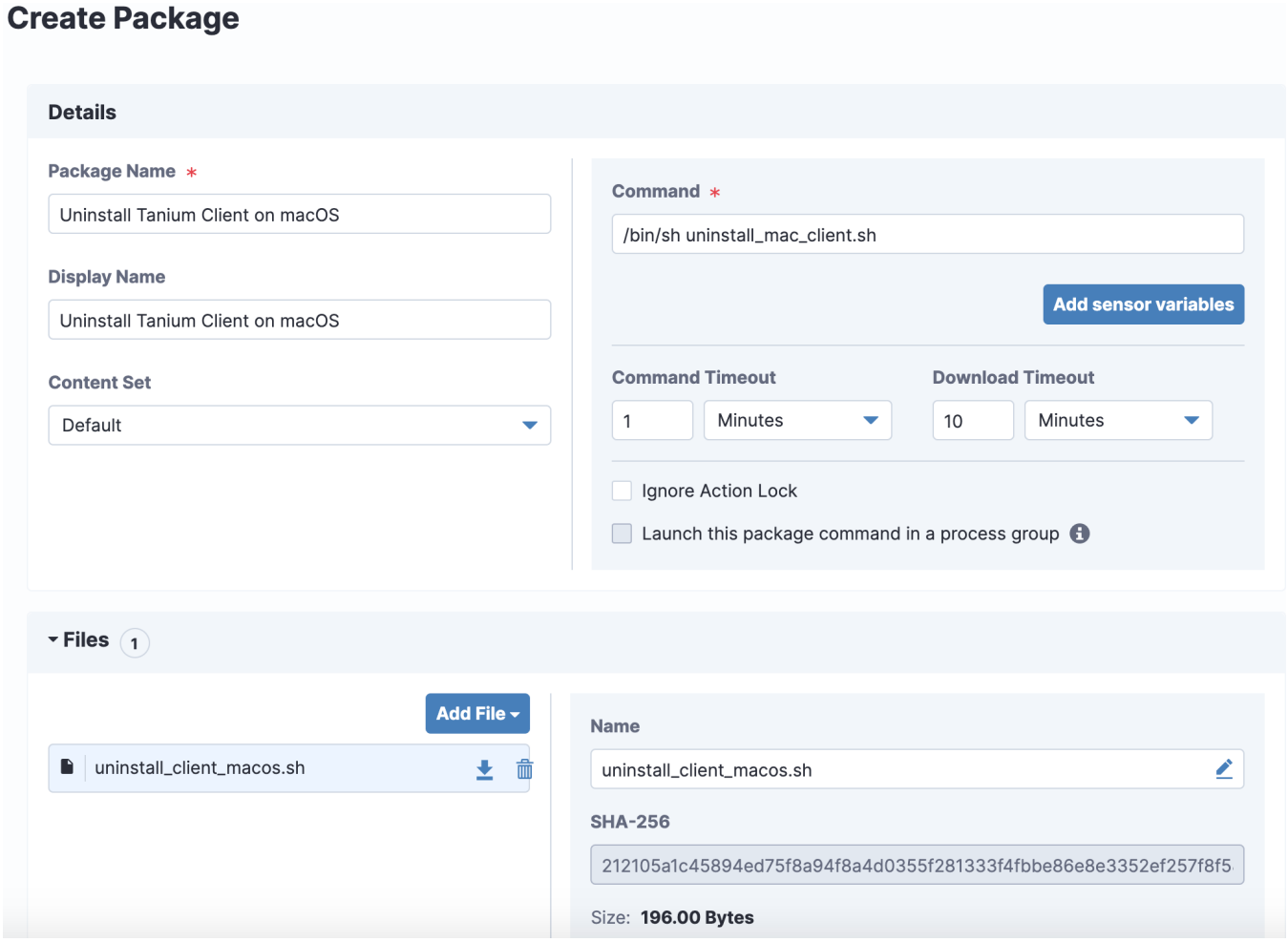
IMPORTANT

The syntax that you enter in the **Command** field of the package configuration must include all the appropriate command-line switches to ensure silent execution. For example, you can enter `setup.exe /S`, `msiexec.exe /i installme.msi /qn`, `installme.exe /S /D=DIR`, or `ipconfig /flushdns`.

On macOS, the Tanium Client distribution does not include an uninstall utility. You can create a shell script to uninstall the Tanium Client and use a package to deploy it. For more information, see Tanium Client Management User Guide: Uninstall using a script.

© 2026 Tanium Inc. All Rights Reserved

Package that distributes and runs an uninstall script



NOTE

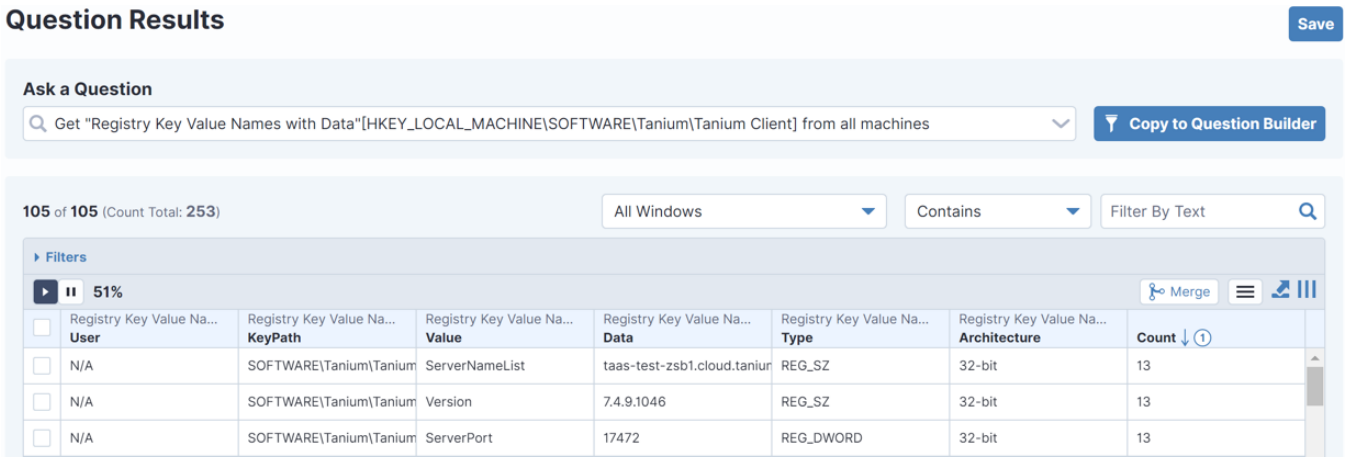
In these example actions, the Tanium Client is uninstalled. If an action to uninstall the Tanium Client succeeds, the endpoint does not send a final success message for the action. Because the Tanium Client is removed, the endpoint has no way to communicate with the Tanium Server.

© 2026 Tanium Inc. All Rights Reserved

Example: Multi-column sensors

Multi-column sensors collect multiple values of related data in a single answer from each Tanium Client. Create multi-column sensors for data that you want the **Question Results** page to show as a single record. For example, `Registry Key Value Names with Data` is an example of a Tanium-defined multi-column sensor. For the registry key that you specify, the sensor returns the **User** (if the key is associated with a user hive), **Key Path**, **Value**, **Data**, data **Type**, and OS **Architecture** type.

Results from a multi-column sensor

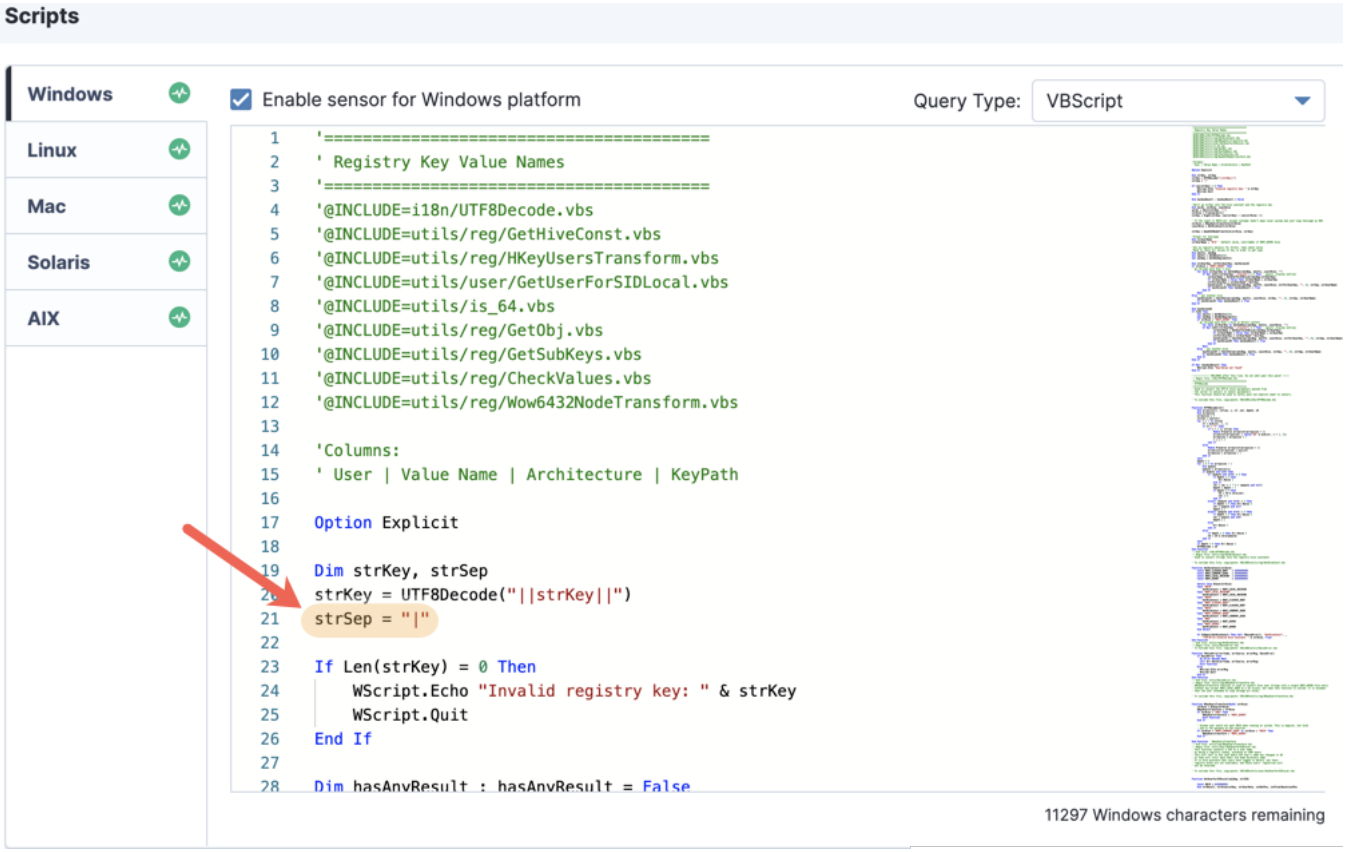


Sensor script for multi-column sensors

When you Create a sensor on page 427 with multiple columns, its script must add a delimiter between each property as it writes to the standard output channel. The delimiter in the script must match the delimiter in the **Use delimiter** field of the sensor configuration. In the following example, the delimiter is the pipe | character.

© 2026 Tanium Inc. All Rights Reserved

Multi-column delimiters in sensor script



Configure settings for multi-column sensors

When you Create a sensor on page 427, perform the following steps on the sensor configuration page to enable multiple columns:

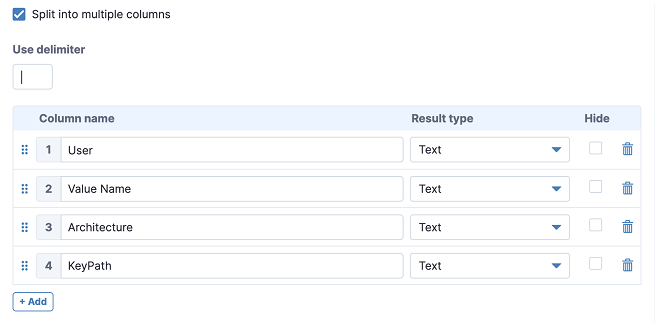
1. Go to the **Settings** section and select **Split into multiple columns**.
2. In the **Use delimiter** field, specify a string delimiter to separate result values in the sensor script. The pipe `|` character is a common choice.

   IMPORTANT

   When creating questions that filter multi-column sensors, single-column filtering works only if the sensor definition specifies column delimiters with a single character (such as `|`), not multiple characters (such as `|:`). For more information, see Use sensor column filters.
3. Enter each **Column Name** and corresponding **Result Type**. For more information about result types, see Sensor data types on page 424.
4. Drag the columns in the order that you want the Interact **Question Results** page to display them.
5. (Optional) Select **Hide** if you want to hide a column from the default view of the **Question Results** page.

© 2026 Tanium Inc. All Rights Reserved

Multi-column result settings



© 2026 Tanium Inc. All Rights Reserved

Example: Parameterized sensors

Overview of parameterized sensors

A parameterized sensor requires you to enter input (parameter values) before the sensor can collect results from endpoints. You enter the parameter values when issuing a dynamic question that uses the sensor. For example, when you issue a question with the **File Size** sensor, Interact prompts you to specify the name of the file for which the sensor collects size information. The Tanium Server then creates an object called a *temporary sensor*, which contains the substituted parameter values. The Server uses the temporary sensor in the question that it sends to Tanium Clients. The Clients then run the sensor to return an answer.

For more information about entering parameter values when issuing questions and about saving questions with parameterized sensors, see Questions with parameterized sensors on page 238.

To create a parameterized sensor, configure the **Scripts** and **Parameter Inputs** as described in the following sections when you perform the steps in Create a sensor on page 427:

- Script for a parameterized sensor on page 497
- Configure parameter inputs for a sensor on page 502



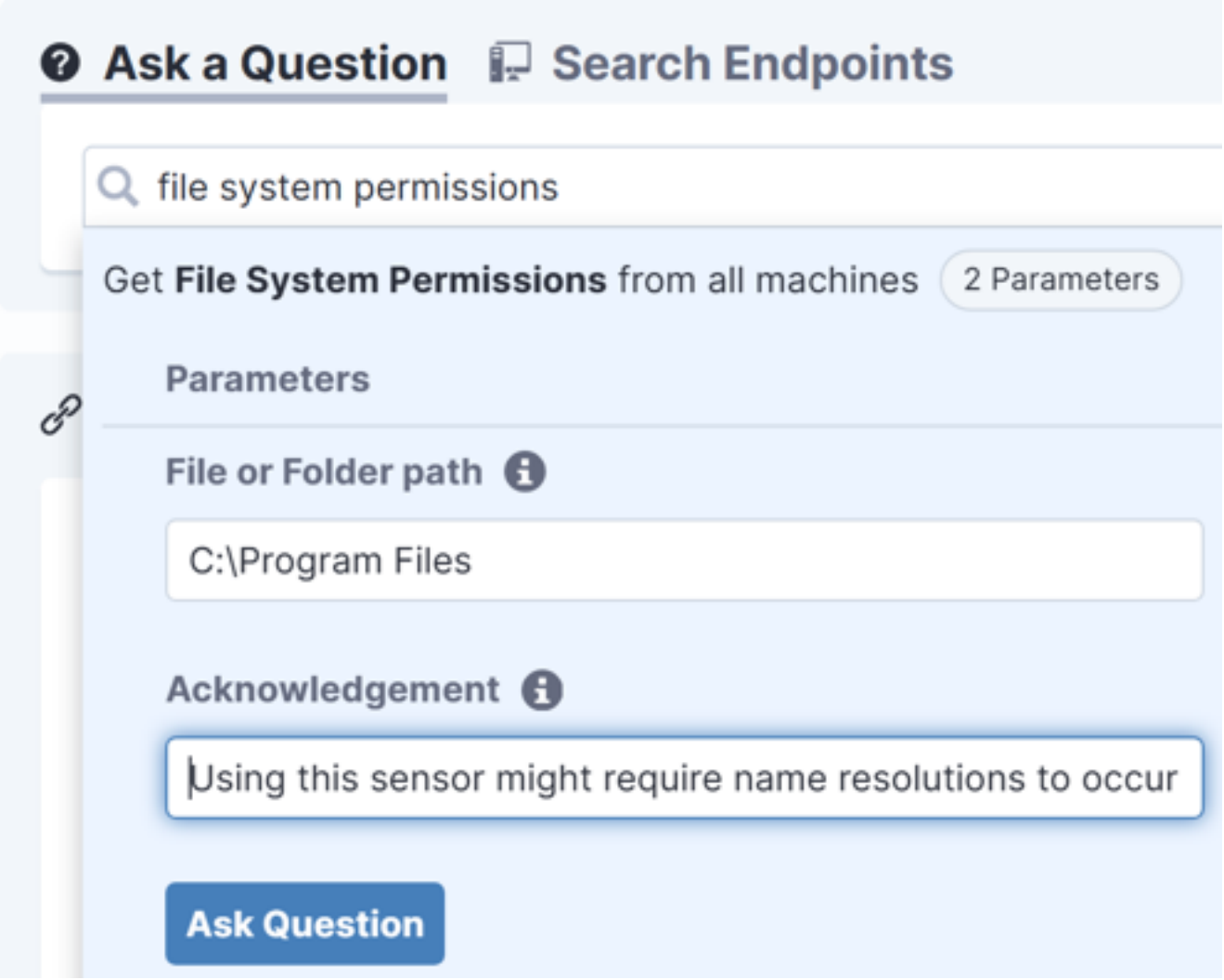
Before saving a question with a parameterized sensor, see Questions with parameterized sensors on page 238.

Sample question with parameterized sensor

File System Permissions is a Tanium-provided parameterized sensor. When you use that sensor in a dynamic question, Interact prompts you to specify values for the parameters **File or Folder Path** and **Acknowledgement**.

© 2026 Tanium Inc. All Rights Reserved

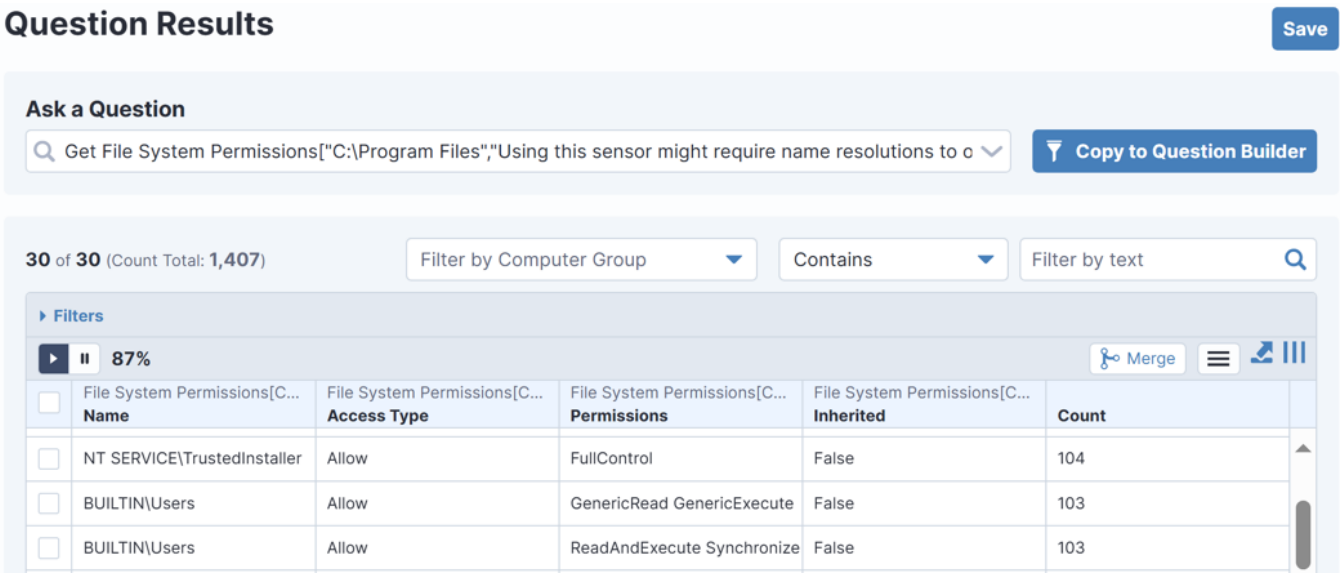
Dynamic question with parameterized sensor



After you enter values and click **Ask Question**, the Tanium Server issues the question to Tanium Clients. When Clients return results, the **Question Results** page shows the question with the values that you entered and the grid shows the results.

© 2026 Tanium Inc. All Rights Reserved

Parameterized sensor results



For more examples of questions with parameterized sensors, see Questions with parameterized sensors on page 238.

Script for a parameterized sensor

You add a sensor script in the sensor configuration page, as described in Create a sensor on page 427. The script for a parameterized sensor has the requirements described in Parameter names on page 497 and UTF-8 encoding and decoding on page 498.

BEST PRACTICE

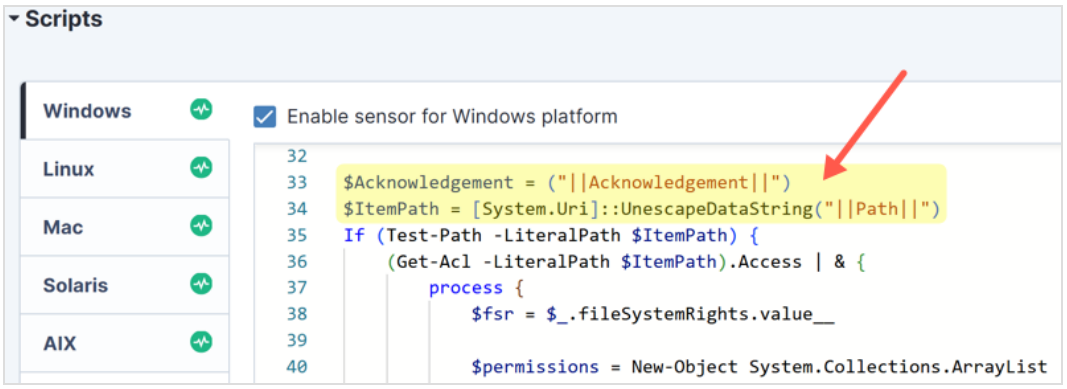
In the script text, include validation for the parameter types **List**, **Text Input**, and **Text Area**. For more information, see Validation expressions on page 507.

Parameter names

In the script for a parameterized sensor, enclose input parameters with double vertical bars (`||<parameter>||`), such as `||Acknowledgement||` and `||Path||` in the following example of a PowerShell sensor. You must specify the same parameter names when you configure the **Key** field for **Parameter Inputs** in the sensor configuration, as described in Configure parameter inputs for a sensor on page 502.

Example: sensor parameters in PowerShell script

© 2026 Tanium Inc. All Rights Reserved



Example: sensor parameters in VBScript script



UTF-8 encoding and decoding

When you issue a question with a parameterized sensor, The Tanium Server encodes the parameter values that you enter before passing the values to the sensor script. The Server includes the encoded values in the temporary sensor that it sends in the question to Tanium Clients. Clients then run the script to answer the question, and the script applies UTF-8 decoding to the encoded values.

PowerShell sensor scripts use the .NET method `[System.Uri]::UnescapeDataString()` to decode UTF-8 encoded parameters. For example, the script for the sensor **File System Permissions** uses that method for the parameter **File or Folder Path**:

```
$ItemPath = [System.Uri]::UnescapeDataString("||Path||")
```

Many sensor scripts in VBScript use a function for UTF-8 decoding, such as the following example.

UTF-8 decode function

© 2026 Tanium Inc. All Rights Reserved

```
'=======================================
' UTF8Decode
'=======================================
' Used to convert the UTF-8 style parameters passed from
' the server to sensors in sensor parameters.
' This function should be used to safely pass non english input to sensors.
'-----
'-----
Function UTF8Decode(str)
    Dim arraylist(), strLen, i, sT, val, depth, sR
    Dim arraysize
    arraysize = 0
    strLen = Len(str)
    for i = 1 to strLen
        sT = mid(str, i, 1)
        if sT = "%" then
            if i + 2 <= strLen then
                Redim Preserve arraylist(arraysize + 1)
                arraylist(arraysize) = cbyte("&H" & mid(str, i + 1, 2))
                arraysize = arraysize + 1
                i = i + 2
            end if
        else
            Redim Preserve arraylist(arraysize + 1)
            arraylist(arraysize) = asc(sT)
            arraysize = arraysize + 1
        end if
    next
    depth = 0
    for i = 0 to arraysize - 1
               Dim mybyte
        mybyte = arraylist(i)
        if mybyte and &h80 then
            if (mybyte and &h40) = 0 then
                if depth = 0 then
                    Err.Raise 5
                end if
                val = val * 2 ^ 6 + (mybyte and &h3f)
                depth = depth - 1
                if depth = 0 then
                    sR = sR & chrw(val)
```

© 2026 Tanium Inc. All Rights Reserved

```
                    val = 0
                end if
            elseif (mybyte and &h20) = 0 then
                if depth > 0 then Err.Raise 5
                val = mybyte and &h1f
                depth = 1
            elseif (mybyte and &h10) = 0 then
                if depth > 0 then Err.Raise 5
                val = mybyte and &h0f
                depth = 2
            else
                Err.Raise 5
            end if
        else
            if depth > 0 then Err.Raise 5
            sR = sR & chrw(mybyte)
        end if
    next
    if depth > 0 then Err.Raise 5
    UTF8Decode = sR
End Function
```

In shell scripts, you can use a function similar to the following `percent_decode` function to decode the parameter data.

percent_decode function

```
#!/bin/sh

percent_decode() {
        local data=$(echo "$1" | sed 's/%/\\\x/g')
        /usr/bin/printf '%b' "$data"
}

myVariable=`percent_decode "||parameter_value||"`
```

The printf utility might not be available or might not work correctly on all Linux, macOS, and UNIX platforms. The following implementation is more fool-proof but less elegant.

brute_force_percent_decode function

© 2026 Tanium Inc. All Rights Reserved

```
#!/bin/sh

brute_force_percent_decode() {
        # decode everything between 0x20-0x7E except:
        #0 1 2 3 4 5 6 7 8 9 (0x30-0x39)
        #A B C D E F G H I J K L M N O P Q R S T U V W X Y Z (0x41-0x5A)
        #a b c d e f g h i j k l m n o p q r s t u v w x y z (0x61-0x7A)
        echo "$1" | sed -e 's/%20/ /g' \
        -e 's/%21/!/g' \
        -e 's/%22/"/g' \
        -e 's/%23/#/g' \
        -e 's/%24/$/g' \
        -e 's/%25/%/g' \
        -e 's/%26/\&/g' \
        -e "s/%27/'/g" \
        -e 's/%28/(/g' \
        -e 's/%29/)/g' \
        -e 's/%2[aA]/*/g' \
        -e 's/%2[bB]/+/g' \
        -e 's/%2[cC]/,/g' \
        -e 's/%2[dD]/-/g' \
        -e 's/%2[eE]/./g' \
        -e 's#%2[fF]#/#g' \
        -e 's/%3[aA]/:/g' \
        -e 's/%3[bB]/;/g' \
        -e 's/%3[cC]/</g' \
        -e 's/%3[dD]/=/g' \
        -e 's/%3[eE]/>/g' \
        -e 's/%3[fF]/?/g' \
        -e 's/%40/@/g' \
        -e 's/%5[bB]/[/g' \
        -e 's/%5[cC]/\\/g' \
        -e 's/%5[dD]/]/g' \
        -e 's/%5[eE]/^/g' \
        -e 's/%5[fF]/_/g' \
        -e 's/%60/`/g' \
        -e 's/%7[bB]/{/g' \
        -e 's/%7[cC]/|/g' \
        -e 's/%7[dD]/}/g' \
        -e 's/%7[eE]/-/g'
}
```

© 2026 Tanium Inc. All Rights Reserved

```
myVariable=`brute_force_percent_decode "||parameter_value||"`
```

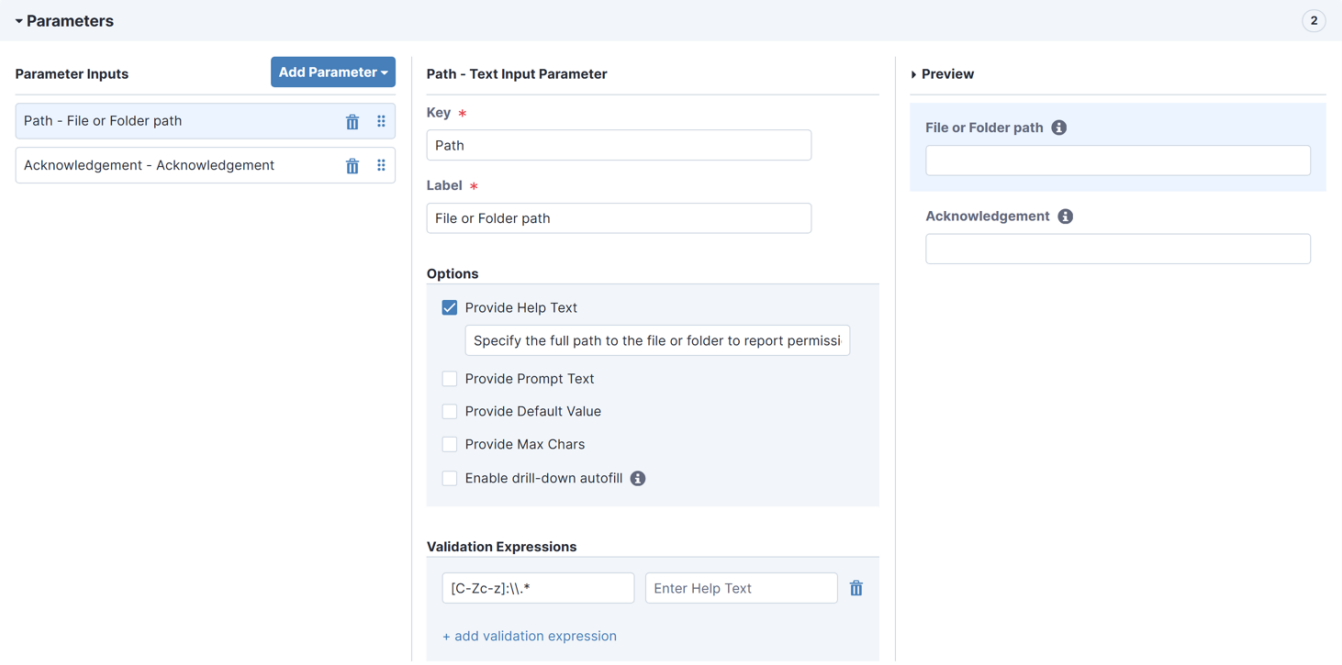
Configure parameter inputs for a sensor

Parameter Inputs that you add to a sensor configuration determine the prompts that a user must complete when issuing a question with the sensor. When you Create a sensor on page 427, add each parameter that the Script for a parameterized sensor on page 497 uses to reference the value that the user enters:

1. On the sensor configuration page, go to the **Parameters** section and select **Add Parameter > <*Type*>**. For descriptions of the types, see Parameter types on page 503.
2. In the **Key** field, specify the parameter name that the script uses (see Parameter names on page 497) but without the double vertical bars (||) that enclose the parameter in the script. Console includes the bars automatically when you add a parameter to the sensor configuration. The figure Parameter inputs on page 503 shows an example of the `Path` parameter.
3. Enter a **Label** to identify the parameter in the Interact workbench when users issue a question.
4. (Optional) Configure **Options** for the parameter. The options vary by parameter type. For more information, see Parameter options on page 504.
5. (Optional) Configure **Validation Expressions** for the parameter types **List**, **Text Area**, and **Text Input**. For more information, see Validation expressions on page 507.
6. Verify that the parameter looks and behaves as expected in the **Preview** section, which shows how users see the parameter when they issue a question. For example, you can enter values to test any limits that you configured in the **Options**.

© 2026 Tanium Inc. All Rights Reserved

Parameter inputs



Parameter types

The most common type of user-input widget for a parameter value is a text-entry field (**Text Input** type), but you can select any of the following types.

Parameter types

Parameter type	Description
Checkbox	Users select a checkbox to enable a setting (set the parameter value to 1) or clear the checkbox to disable the setting (set the value to 0).
Date	Users enter a date or select a date through the Calendar widget. Set the [1]time standard to **Local Time** or **UTC**. Set the [2]**Default Value** to **Now** or a **Specific** date.
Date Time	Users enter a date and time or select a date and time through the Calendar and Clock widgets. Set the [1]time standard to **Local Time** or **UTC**. Set the [2]**Default Value** to **Now** or a **Specific** date/time.
Date Time Range	Users specify a start date/time and end date/time. For the **End Date** setting, select **Require** if users must specify an end date/time or clear the checkbox if the end date/time is optional. Set the [1]time standard to **Local Time** or **UTC**.
Drop Down List	Users select only one item from a drop-down list. To specify each value that users can select, go to the **Values** section, click **+ add value** and enter the value.

© 2026 Tanium Inc. All Rights Reserved

Parameter types (continued)

Parameter type	Description
List	Users enter one or more values and use a pipe "|" to delimit multiple values. Entering a value is optional instead of required if List Is Optional on page 506 is selected in the parameter **Options**. To define the allowed values, see Validation expressions on page 507.
Numeric	Users enter a number.
Numeric Interval	Users enter a number and select the associated unit from a list. The unit has a numeric value (interval) that Interact multiplies by the user entry to determine the parameter value. For example, the list might include the units **Seconds**, **Minutes**, and **Hours** with the corresponding values 1, 60, and 3600 respectively. In this case, if a user enters `2` and selects **Hours**, the parameter value is 7200 (2 * 3600). To specify each unit that users can select, go to the **Interval Units** section, click **+ add interval**, enter a label for the unit, and enter its value.
Separator	This type is not a parameter input but a graphical separator that helps users to distinguish different sections of the user input form when entering parameter values. If a user must specify multiple values, you can use sections to visually organize related parameters in the input form. The **Separator text** that you specify appears as the section title and has a line below it.
Text Area	Users enter a large amount of text that can include multiple lines. To define the allowed values, see Validation expressions on page 507.
Text Input	Users enter a single line of text. To define the allowed values, see Validation expressions on page 507.
Time	Users enter a time or select a time through the Clock widget. Set the [1]time standard to **Local Time** or **UTC**. Set the [2]**Default Value** to **Now** or a **Specific** time.

[1] **Local Time** is local to the system that you use to access Console. **UTC** is Coordinated Universal Time.

[2] **Now** is the current date/time when users specify a value for the parameter.

Parameter options

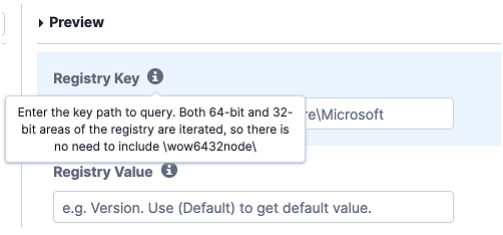
Use parameter **Options** to limit the range of values that users can enter, control how the Interact workbench presents a parameter, or provide help information that users see when entering values. The figure Parameter inputs on page 503 shows an example of information that you can specify for a **Text Input** parameter to help users understand what to enter. The options that are available vary by parameter type. Only the **Separator** type has no options.

NOTE

For the options of date/time parameters, set the time standard (**Local** or **UTC**) in the required settings of the parameters. For more information, see Parameter types on page 503.

© 2026 Tanium Inc. All Rights Reserved

Parameter options

Parameter option	Description	Parameter types
Date Limits	Restrict user entries to within a minimum and/or maximum date. For each limit, select a **Specific** date through the Calendar widget or select **Future Only** or **Past Only**.	Date Date Time
Enable drill-down autofill	This option applies only to parameterized sensors, not parameterized packages. Select the option to auto-populate a parameterized sensor in a drill-down question with the values of matching parameters in the results that the user selects in the **Question Results** grid. For more information, see Drill down into results on page 267.	All types
Default Start/End Date	Specify a default start and/or end date. For each date, select a **Specific** date through the Calendar widget or select **Future Only** or **Past Only**.	Date Time Range
Provide Default Value	Enter a default value to appear in the parameter input field. For list parameters, specify one value for each line. Users can overwrite the default value with a custom value.	List Numeric Numeric Interval Text Area Text Input
Provide Height in Lines	Specify the vertical height of a text area parameter. This option controls only the display size of the text-entry field, not the number of lines that users can enter. For example, if you enter `3`, the text-entry field appears 3 lines high but users can enter more than 3 lines of text.	Text Area
Provide Help Text	This option adds an Information icon beside the parameter name in the user input form. When a user hovers over the icon, a tooltip shows the text that you specify for this option. 	All types

© 2026 Tanium Inc. All Rights Reserved

Parameter options (continued)

Parameter option	Description	Parameter types
Provide Max Chars	Specify the maximum number of characters that users can enter for the parameter value.	Text Area Text Input
Provide Maximum Value	Specify the highest number that users can enter for the parameter.	Numeric Numeric Interval
Provide Minimum Value	Specify the lowest number that users can enter for the parameter.	Numeric Numeric Interval
Provide Prompt Text	Enter read-only text to appear in the parameter input field. The text is not a value for the parameter but typically explains what value to enter. If you also configure the **Provide Default Value** option, users initially see the default value and then see the prompt text only if they delete the default value.	Text Area Text Input
Provide Restrict Expression	Enter a regular expression that defines the allowed values. For example, the expression `A-Za-z` allows alphabetic characters but not numbers or special characters. TIP You can also use **Validation Expressions** to define the allowed values. For more information, see Validation expressions on page 507.	List
Provide Snap Interval	Use this option if the parameter value that a user enters must be divisible by the snap interval value.	Numeric Numeric Interval
Provide Step Size	Specify the amount by which users can increase or decrease the value of a numeric parameter. Enter a step size that is a multiple of the **Provide Snap Interval** value unless the snap interval is set to `0`.	Numeric Numeric Interval
List Is Optional	Select this option if entering a value for a **List** parameter is optional instead of required.	List
Selected	Select this option for a **Checkbox** parameter that must be selected by default. Users can manually clear the checkbox.	Checkbox

© 2026 Tanium Inc. All Rights Reserved

Parameter options (continued)

Parameter option	Description	Parameter types
Time Limits	Restrict user entries to within a minimum and/or maximum time. For each limit, select a **Specific** time through the Clock widget or select **Future Only** or **Past Only**.	Date Time Time

Validation expressions

For the parameter types **List**, **Text Area**, and **Text Input**, you can add **Validation Expressions** to define the allowed values. The expressions are based on Perl Compatible Regular Expressions (PCRE). Boolean AND logic applies if you add fields for multiple expressions. You can apply Boolean OR logic to multiple expressions by entering them as a single field entry with pipes "|" as separators. Each expression field has an adjacent text box where you can enter a description to help users understand the expression. For example, if the expression is `\S{5}`, you might enter the help text `Value must be at least 5 characters`.

BEST PRACTICE

Include validation for input parameters when you write the sensor script, not just in **Validation Expressions**. For more information, see Script for a parameterized sensor on page 497.

NOTE

The validation does not apply to custom sensors that you import or that you create through the Tanium API because it is Console that validates expressions, not the Tanium Server.

© 2026 Tanium Inc. All Rights Reserved

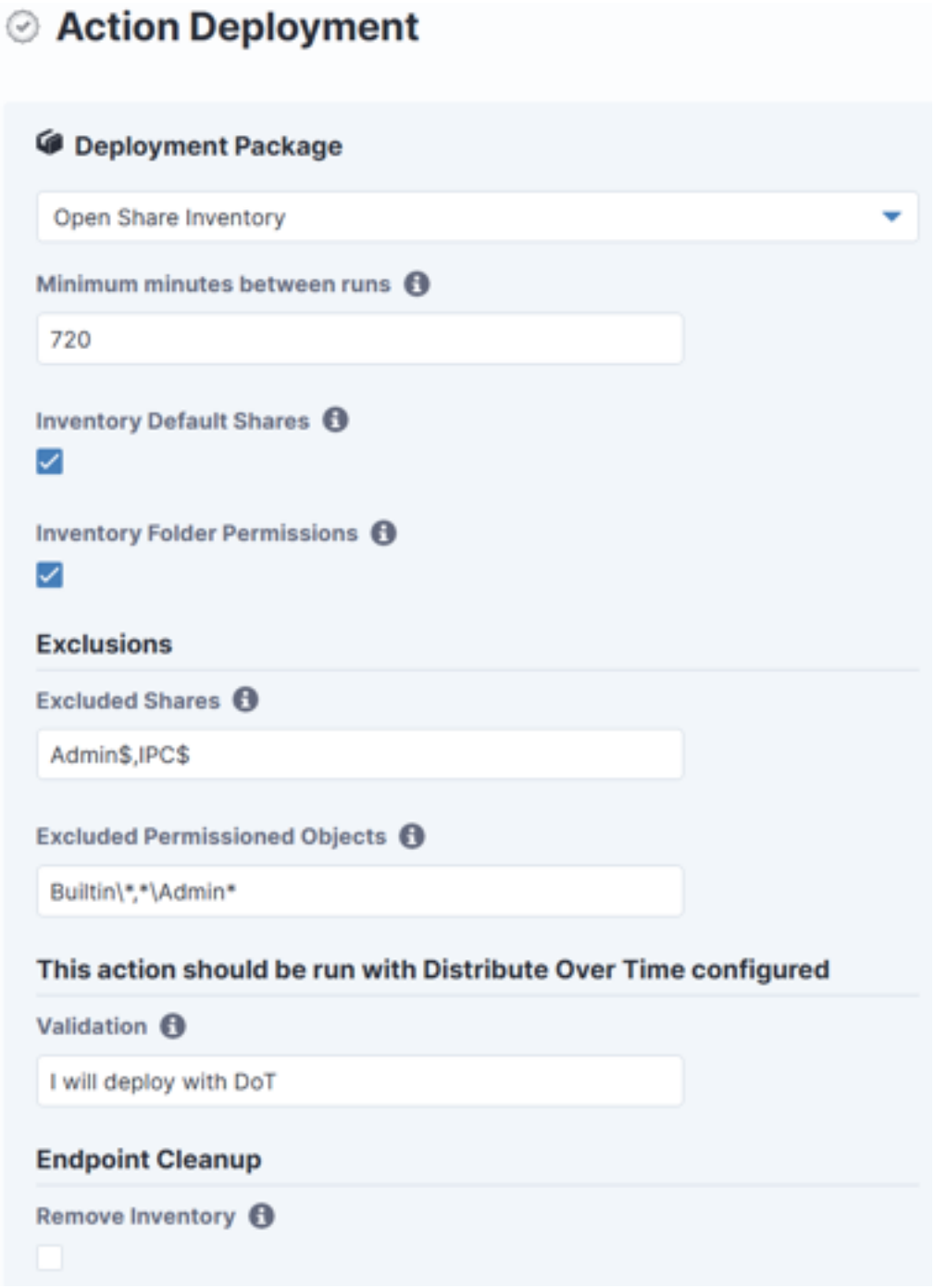
Example: Parameterized packages

Overview of parameterized packages

A parameterized package requires you to enter input (parameter values) when configuring an action that uses the package. For example, when you configure an action that uses the package **Open Share Inventory**, the **Action Deployment** page prompts you to enter the **Minimum minutes between runs** and other parameters. The package configuration specifies a command (such as `cmd.exe`) and script (such as `ShareInventory.ps1`) that require the parameters. When you configure the action, the Tanium Server saves the package definition in an object called a *temporary package*, which includes the parameter values that you entered. The Server then deploys the action with the temporary package to Tanium Clients, which run the package at the action start time.

© 2026 Tanium Inc. All Rights Reserved

Parameterized package



To create a parameterized package, configure the **Command**, script **Files**, and **Parameter Inputs** as described in the following sections when you perform the steps in Create a package on page 447:

- Package script and command-line parameters on page 510
- Configure parameter inputs for a package on page 516

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

For more information about the impact on scheduled actions when a parameterized package configuration is updated, see Scheduled action with parameterized package on page 443.

Package script and command-line parameters

When you Create a package on page 447 that uses parameters, the **Command** specifies an executable such as a script engine. The script for a parameterized package has the requirements described in Parameter positions on page 510 and UTF-8 encoding and decoding on page 512.

BEST PRACTICE

In the package script, include validation for the parameter types **List**, **Text Input**, and **Text Area**. For more information, see Validation expressions on page 521.

Parameter positions

In a package configuration, the command-line variables in the **Command** field must match the parameter numbers in the **Parameter Inputs** section. In the package **Open Share Inventory** for example, the **Command** includes variables that are numbered $1 to $7:

```
cmd.exe /d /c powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -NonInteractive -NoProfile -File "%CD%\ShareInventory.ps1" -MinMinsBetweenRuns $1 -InventoryDefaultShares $2 -InventoryFolderPerms $3 -ExcludedShares $4 -ExcludedPermissionedObjects $5 -Remove $7 -Validation $6
```

IMPORTANT

In the **Command** field, enclose parameters in quotation marks `"<parameter name>"` if their names have spaces.

The corresponding **Parameter Inputs** lists the parameters with numbers that match the **Command** variables:

© 2026 Tanium Inc. All Rights Reserved

Parameter positions in a package



© 2026 Tanium Inc. All Rights Reserved



Parameter numbers do not apply to the input type **Separator**, such as `- Exclusions -` in the preceding example.

The package configuration might include parameters that the script does not include. For example, the package **Open Share Inventory** specifies the `Validation $6` parameter because it requires user input. However, the associated PowerShell script `ShareInventory.ps1` does not process that parameter and therefore does not include it:

```
param (
       [int]$MinMinsBetweenRuns = 720,
       [int]$InventoryFolderPerms = 1,
       [int]$InventoryDefaultShares = 1,
       [string]$ExcludedShares = ' ',
       [string]$ExcludedPermissionedObjects = ' ',
       [int]$Remove = 0
)
```

The parameter numbering in the script for a VBScript package might not match the parameter numbering in the **Command** and **Parameter Inputs** of the package configuration. For example, the script parameters are numbered 0 to 4 in the `set-value.vbs` script for the package **Registry - Set Value** because VBScript treats an un-named argument list as a zero-based array:

```
targetArch = Trim(LCase(WScript.Arguments.Item(0)))
targetKey = UTF8Decode(WScript.Arguments.Item(1))
targetValueName = UTF8Decode(WScript.Arguments.Item(2))
targetValue = UTF8Decode(WScript.Arguments.Item(3))
targetValueType = UTF8Decode(WScript.Arguments.Item(4))
```

By contrast, the corresponding **Command** variables are numbered `$1` to `$5` in the package configuration:

```
cmd.exe /d /c ""%WinDir%\System32\cscript.exe" //E:VBScript //T:60 set-value.vbs "$1" "$2" "$3" "$4" "$5""
```

UTF-8 encoding and decoding

When you deploy an action with a parameterized package, the Tanium Server encodes the parameter values that you enter before passing the values to the package script. The Server includes the encoded values in the temporary package that it deploys in an action to Tanium Clients. When Clients start the action, they run the package script and the script applies UTF-8 decoding to the encoded values.

PowerShell package scripts use the .NET method `[System.Uri]::UnescapeDataString()` to decode UTF-8 encoded parameters. For example, the script `ShareInventory.ps1` for the package **Open Share Inventory** uses:

```
$ExcludedShares = [System.Uri]::UnescapeDataString($ExcludedShares)
```

Many package scripts in VBScript use a function for UTF-8 decoding, such as the following example.

© 2026 Tanium Inc. All Rights Reserved

UTF-8 decode function

```
'=======================================
' UTF8Decode
'=======================================
' Used to convert the UTF-8 style parameters passed from
' the server to sensors in sensor parameters.
' This function should be used to safely pass non english input to sensors.
'-----
'-----
Function UTF8Decode(str)
    Dim arraylist(), strLen, i, sT, val, depth, sR
    Dim arraysize
    arraysize = 0
    strLen = Len(str)
    for i = 1 to strLen
        sT = mid(str, i, 1)
        if sT = "%" then
            if i + 2 <= strLen then
                Redim Preserve arraylist(arraysize + 1)
                arraylist(arraysize) = cbyte("&H" & mid(str, i + 1, 2))
                arraysize = arraysize + 1
                i = i + 2
            end if
        else
            Redim Preserve arraylist(arraysize + 1)
            arraylist(arraysize) = asc(sT)
            arraysize = arraysize + 1
        end if
    next
    depth = 0
    for i = 0 to arraysize - 1
               Dim mybyte
        mybyte = arraylist(i)
        if mybyte and &h80 then
            if (mybyte and &h40) = 0 then
                if depth = 0 then
                    Err.Raise 5
                end if
                val = val * 2 ^ 6 + (mybyte and &h3f)
                depth = depth - 1
                if depth = 0 then
```

© 2026 Tanium Inc. All Rights Reserved

```
                    sR = sR & chrw(val)
                    val = 0
                end if
            elseif (mybyte and &h20) = 0 then
                if depth > 0 then Err.Raise 5
                val = mybyte and &h1f
                depth = 1
            elseif (mybyte and &h10) = 0 then
                if depth > 0 then Err.Raise 5
                val = mybyte and &h0f
                depth = 2
            else
                Err.Raise 5
            end if
        else
            if depth > 0 then Err.Raise 5
            sR = sR & chrw(mybyte)
        end if
    next
    if depth > 0 then Err.Raise 5
    UTF8Decode = sR
End Function
```

In shell scripts, you can use a function similar to the following `percent_decode` function to decode the parameter data.

percent_decode function

```
#!/bin/sh

percent_decode() {
        local data=$(echo "$1" | sed 's/%/\\\x/g')
        /usr/bin/printf '%b' "$data"
}

myVariable=`percent_decode "||parameter_value||"`
```

The printf utility might not be available or might not work correctly on all Linux, macOS, and UNIX platforms. The following implementation is more fool-proof but less elegant.

brute_force_percent_decode function

© 2026 Tanium Inc. All Rights Reserved

```
#!/bin/sh

brute_force_percent_decode() {
        # decode everything between 0x20-0x7E except:
        #0 1 2 3 4 5 6 7 8 9 (0x30-0x39)
        #A B C D E F G H I J K L M N O P Q R S T U V W X Y Z (0x41-0x5A)
        #a b c d e f g h i j k l m n o p q r s t u v w x y z (0x61-0x7A)
        echo "$1" | sed -e 's/%20/ /g' \
        -e 's/%21/!/g' \
        -e 's/%22/"/g' \
        -e 's/%23/#/g' \
        -e 's/%24/$/g' \
        -e 's/%25/%/g' \
        -e 's/%26/\&/g' \
        -e "s/%27/'/g" \
        -e 's/%28/(/g' \
        -e 's/%29/)/g' \
        -e 's/%2[aA]/*/g' \
        -e 's/%2[bB]/+/g' \
        -e 's/%2[cC]/,/g' \
        -e 's/%2[dD]/-/g' \
        -e 's/%2[eE]/./g' \
        -e 's#%2[fF]#/#g' \
        -e 's/%3[aA]/:/g' \
        -e 's/%3[bB]/;/g' \
        -e 's/%3[cC]/</g' \
        -e 's/%3[dD]/=/g' \
        -e 's/%3[eE]/>/g' \
        -e 's/%3[fF]/?/g' \
        -e 's/%40/@/g' \
        -e 's/%5[bB]/[/g' \
        -e 's/%5[cC]/\\/g' \
        -e 's/%5[dD]/]/g' \
        -e 's/%5[eE]/^/g' \
        -e 's/%5[fF]/_/g' \
        -e 's/%60/`/g' \
        -e 's/%7[bB]/{/g' \
        -e 's/%7[cC]/|/g' \
        -e 's/%7[dD]/}/g' \
        -e 's/%7[eE]/-/g'
}
```

© 2026 Tanium Inc. All Rights Reserved

```
myVariable=`brute_force_percent_decode "||parameter_value||"`
```

Configure parameter inputs for a package

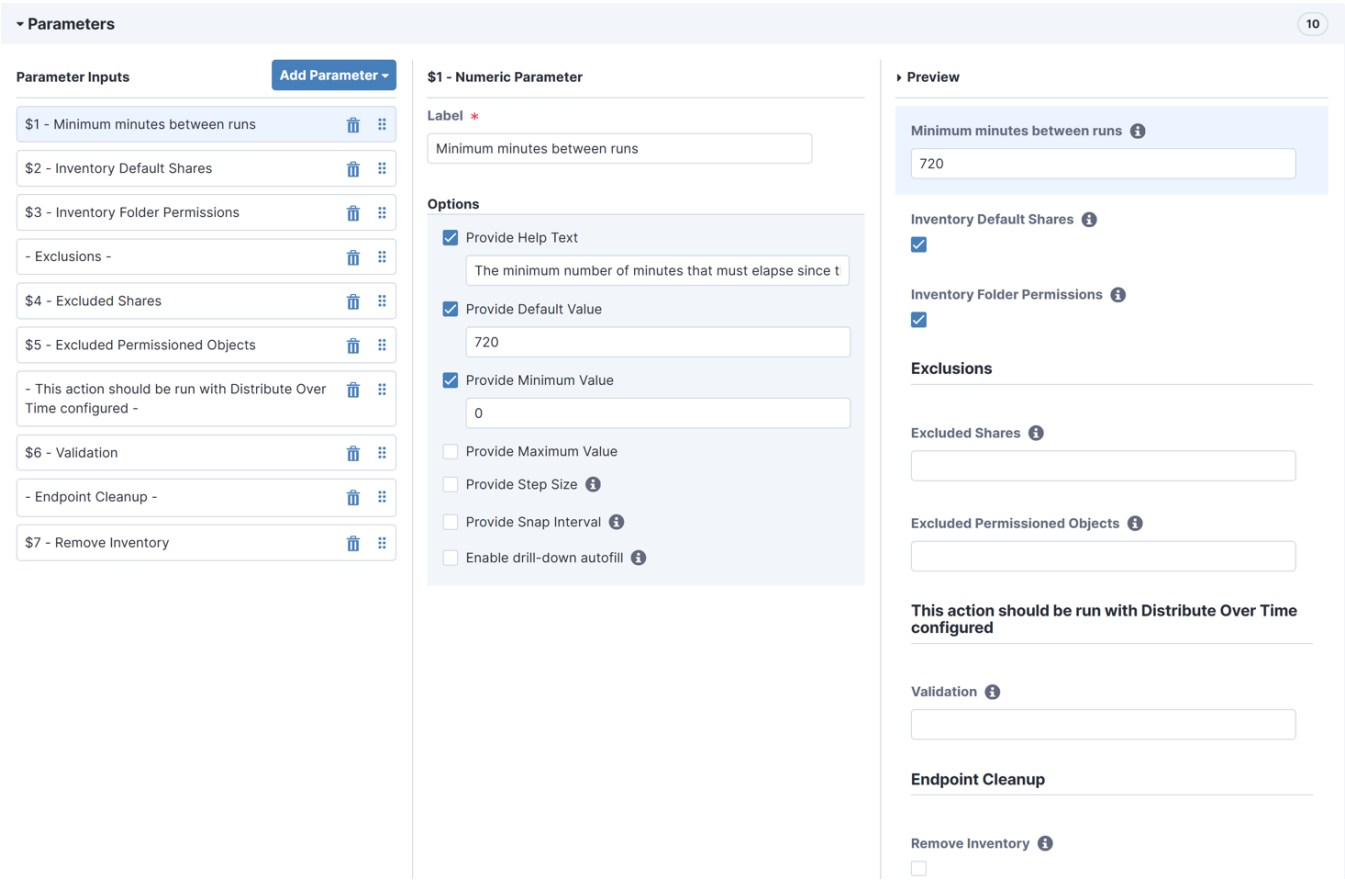
Parameter Inputs that you add to a package configuration determine the prompts that a user must complete when deploying an action that uses the package. On the package configuration page, add one parameter input at a time in an order that matches the corresponding command-line variables. The first parameter that you add is matched to command line variable $1, the second parameter is matched to variable $2, and so on as described under Parameter positions on page 510.

You can select and drag items in the **Parameter Inputs** list on the package configuration page to ensure that the items line up with the numbered parameters in the command.

1. When you Create a package on page 447, go to the **Parameters** section of the package configuration page and select **Add Parameter > <*Type*>**. For descriptions of the types, see Parameter types on page 517.
2. Enter a **Label** to identify the parameter in the Interact workbench when users deploy an action.
3. (Optional) Configure **Options** for the parameter. The options vary by parameter type. For more information, see Parameter options on page 518.
4. (Optional) Configure **Validation Expressions** for the parameter types **List**, **Text Area**, and **Text Input**. For more information, see Validation expressions on page 521.
5. Verify that the parameter looks and behaves as expected in the **Preview** section, which shows how users see the parameter when they deploy an action. For example, you can enter values to test any limits that you configured in the **Options**.

© 2026 Tanium Inc. All Rights Reserved

Parameter input settings



Parameter types

The most common type of user-input widget for a parameter value is a text-entry field (**Text Input** type), but you can select any of the following types.

Parameter types

Parameter type	Description
Checkbox	Users select a checkbox to enable a setting (set the parameter value to 1) or clear the checkbox to disable the setting (set the value to 0).
Date	Users enter a date or select a date through the Calendar widget. Set the [1]time standard to **Local Time** or **UTC**. Set the [2]**Default Value** to **Now** or a **Specific** date.
Date Time	Users enter a date and time or select a date and time through the Calendar and Clock widgets. Set the [1]time standard to **Local Time** or **UTC**. Set the [2]**Default Value** to **Now** or a **Specific** date/time.
Date Time Range	Users specify a start date/time and end date/time. For the **End Date** setting, select **Require** if users must specify an end date/time or clear the checkbox if the end date/time is optional. Set the [1]time standard to **Local Time** or **UTC**.

© 2026 Tanium Inc. All Rights Reserved

Parameter types (continued)

Parameter type	Description
Drop Down List	Users select only one item from a drop-down list. To specify each value that users can select, go to the **Values** section, click **+ add value** and enter the value.
List	Users enter one or more values and use a pipe "|" to delimit multiple values. Entering a value is optional instead of required if List Is Optional on page 520 is selected in the parameter **Options**. To define the allowed values, see Validation expressions on page 521.
Numeric	Users enter a number.
Numeric Interval	Users enter a number and select the associated unit from a list. The unit has a numeric value (interval) that Interact multiplies by the user entry to determine the parameter value. For example, the list might include the units **Seconds**, **Minutes**, and **Hours** with the corresponding values 1, 60, and 3600 respectively. In this case, if a user enters `2` and selects **Hours**, the parameter value is 7200 (2 * 3600). To specify each unit that users can select, go to the **Interval Units** section, click **+ add interval**, enter a label for the unit, and enter its value.
Separator	This type is not a parameter input but a graphical separator that helps users to distinguish different sections of the user input form when entering parameter values. If a user must specify multiple values, you can use sections to visually organize related parameters in the input form. The **Separator text** that you specify appears as the section title and has a line below it.
Text Area	Users enter a large amount of text that can include multiple lines. To define the allowed values, see Validation expressions on page 521.
Text Input	Users enter a single line of text. To define the allowed values, see Validation expressions on page 521.
Time	Users enter a time or select a time through the Clock widget. Set the [1]time standard to **Local Time** or **UTC**. Set the [2]**Default Value** to **Now** or a **Specific** time.

[1] **Local Time** is local to the system that you use to access Console. **UTC** is Coordinated Universal Time.

[2] **Now** is the current date/time when users specify a value for the parameter.

Parameter options

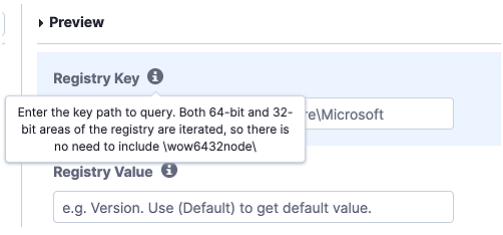
Use parameter **Options** to limit the range of values that users can enter, control how the Interact workbench presents a parameter, or provide help information that users see when entering values. The figure Parameter input settings on page 517 shows an example of information that you can specify for a **Text Input** parameter to help users understand what to enter. The options that are available vary by parameter type. Only the **Separator** type has no options.



For the options of date/time parameters, set the time standard (**Local** or **UTC**) in the required settings of the parameters. For more information, see Parameter types on page 517.

© 2026 Tanium Inc. All Rights Reserved

Parameter options

Parameter option	Description	Parameter types
Date Limits	Restrict user entries to within a minimum and/or maximum date. For each limit, select a **Specific** date through the Calendar widget or select **Future Only** or **Past Only**.	Date Date Time
Enable drill-down autofill	This option applies only to parameterized sensors, not parameterized packages. Select the option to auto-populate a parameterized sensor in a drill-down question with the values of matching parameters in the results that the user selects in the **Question Results** grid. For more information, see Drill down into results on page 267.	All types
Default Start/End Date	Specify a default start and/or end date. For each date, select a **Specific** date through the Calendar widget or select **Future Only** or **Past Only**.	Date Time Range
Provide Default Value	Enter a default value to appear in the parameter input field. For list parameters, specify one value for each line. Users can overwrite the default value with a custom value.	List Numeric Numeric Interval Text Area Text Input
Provide Height in Lines	Specify the vertical height of a text area parameter. This option controls only the display size of the text-entry field, not the number of lines that users can enter. For example, if you enter `3`, the text-entry field appears 3 lines high but users can enter more than 3 lines of text.	Text Area
Provide Help Text	This option adds an Information icon beside the parameter name in the user input form. When a user hovers over the icon, a tooltip shows the text that you specify for this option. 	All types

© 2026 Tanium Inc. All Rights Reserved

Parameter options (continued)

Parameter option	Description	Parameter types
Provide Max Chars	Specify the maximum number of characters that users can enter for the parameter value.	Text Area Text Input
Provide Maximum Value	Specify the highest number that users can enter for the parameter.	Numeric Numeric Interval
Provide Minimum Value	Specify the lowest number that users can enter for the parameter.	Numeric Numeric Interval
Provide Prompt Text	Enter read-only text to appear in the parameter input field. The text is not a value for the parameter but typically explains what value to enter. If you also configure the **Provide Default Value** option, users initially see the default value and then see the prompt text only if they delete the default value.	Text Area Text Input
Provide Restrict Expression	Enter a regular expression that defines the allowed values. For example, the expression `A-Za-z` allows alphabetic characters but not numbers or special characters. TIP You can also use **Validation Expressions** to define the allowed values. For more information, see Validation expressions on page 521.	List
Provide Snap Interval	Use this option if the parameter value that a user enters must be divisible by the snap interval value.	Numeric Numeric Interval
Provide Step Size	Specify the amount by which users can increase or decrease the value of a numeric parameter. Enter a step size that is a multiple of the **Provide Snap Interval** value unless the snap interval is set to `0`.	Numeric Numeric Interval
List Is Optional	Select this option if entering a value for a **List** parameter is optional instead of required.	List
Selected	Select this option for a **Checkbox** parameter that must be selected by default. Users can manually clear the checkbox.	Checkbox

© 2026 Tanium Inc. All Rights Reserved

Parameter options (continued)

Parameter option	Description	Parameter types
Time Limits	Restrict user entries to within a minimum and/or maximum time. For each limit, select a **Specific** time through the Clock widget or select **Future Only** or **Past Only**.	Date Time Time

Validation expressions

For the parameter types **List**, **Text Area**, and **Text Input**, you can add **Validation Expressions** to define the allowed values. The expressions are based on Perl Compatible Regular Expressions (PCRE). Boolean AND logic applies if you add fields for multiple expressions. You can apply Boolean OR logic to multiple expressions by entering them as a single field entry with pipes "|" as separators. Each expression field has an adjacent text box where you can enter a description to help users understand the expression. For example, if the expression is `\S{5}`, you might enter the help text `Value must be at least 5 characters`.

BEST PRACTICE

Include validation for input parameters when you write the package script, not just in **Validation Expressions**

NOTE

The validation does not apply to custom packages that you import or that you create through the Tanium API because it is Console that validates expressions, not the Tanium Server.

© 2026 Tanium Inc. All Rights Reserved

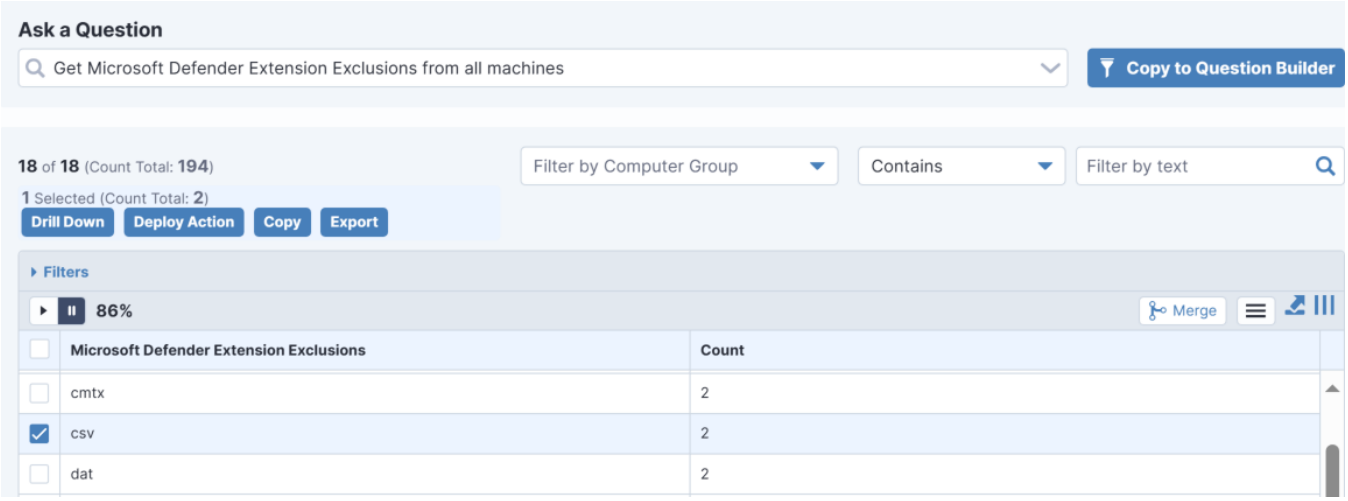
Example: Sensor-sourced packages

Overview of sensor-sourced packages

Sensor-sourced packages are designed like parameterized packages (see Example: Parameterized packages on page 508), but take sensor output instead of user input as run-time arguments. The command syntax requires a sensor result that the Tanium Server passes from the Interact **Question Results** grid when you initiate the action deployment workflow. For example, the following action workflow runs a package that removes the CSV file extension from the exclusions list of Microsoft Defender on Windows endpoints:

1. Issue a question with the sensor **Microsoft Defender Extension Exclusions**. Tanium Clients run the sensor and return results that you can select on the **Questions Results** page.
2. Select the `csv` result, which is from Clients on which Defender excludes that extension.
3. Deploy an action with the package **Microsoft Defender - Remove Extension Exclusion [Windows]**.

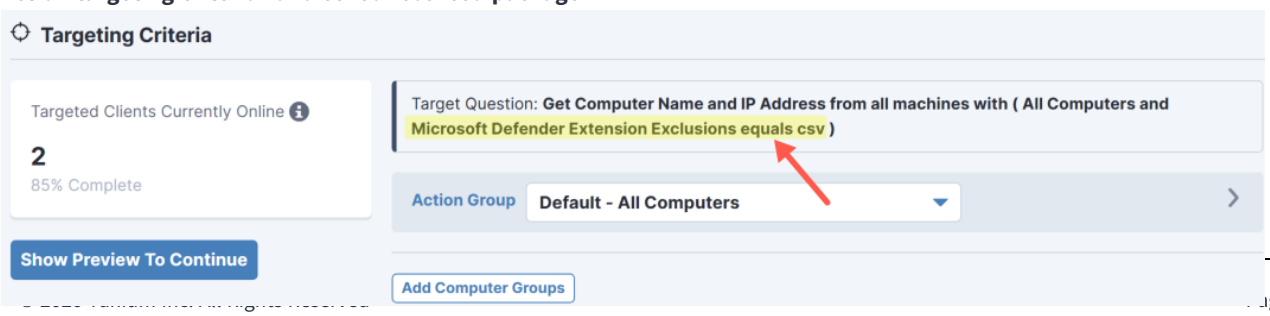
Question results for a sensor-sourced package



To deploy an action, you click **Deploy Action** on the **Question Results** page. The **Action Deployment** page then opens and provides the **Deployment Package** dropdown list for you to select the package. The list includes sensor-sourced packages only if your selections in the **Question Results** have a value to pass to the package. For example, if you select the result row with the value `csv`, the **Deployment Package** list shows the package **Microsoft Defender - Remove Extension Exclusion [Windows]**. If you select a result with the value `[no results]`, the list does not show that package.

On the **Action Deployment** page, the **Target Question** specifies the selected result. The Tanium Server passes this value to the package command line.

Action targeting criteria for a sensor-sourced package



To create a sensor-sourced package, configure the script and settings as described in the following sections when you perform the steps in Create a package on page 447:

- Script for a sensor-sourced package on page 523
- Configure settings for a sensor-sourced package on page 523

Script for a sensor-sourced package

When you deploy an action with a sensor-sourced package, the Tanium Server encodes the parameter values from sensor output before passing the values to the package script. The Server includes the encoded values in the temporary package that it deploys in an action to Tanium Clients. When Clients start the action, they run the package script, which applies UTF-8 decoding to the encoded values.

PowerShell package scripts use the .NET method `[System.Uri]::UnescapeDataString()` to decode UTF-8 encoded parameters. For example, the script `RemoveDefenderExtensionExclusion.ps1` for the package **Microsoft Defender - Remove Extension Exclusion [Windows]** uses:

```
$decoded_value = [System.Uri]::UnescapeDataString($args[0])
```

The VBScript script `startservice.vbs` for the package **Start Service - ||Stopped Service||** uses the following method for decoding:

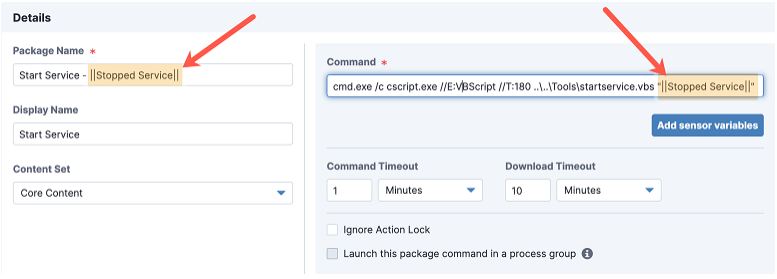
```
strService = Trim(UTF8Decode(colArguments.Item(0)))
```

For more information, see UTF-8 encoding and decoding on page 512.

Configure settings for a sensor-sourced package

To configure a sensor-sourced package, add sensors to the **Command** and (optionally) **Package Name** settings on the **Create Package** page when you perform the steps in Create a package on page 447.

Package name and command with sensor output arguments



Command setting

When you Create a package on page 447 that uses sensor-sourced parameters, add a sensor variable to the **Command** setting on the **Create Package** page:

© 2026 Tanium Inc. All Rights Reserved

1. Place the cursor where the sensor output is needed in the command and click **Add sensor variable**.
2. Select a sensor and click **Confirm**.



If the sensor output might have spaces, surround the sensor variable with quotation marks.

Package Name setting (optional)

When you Create a package on page 447 that uses sensor-sourced parameters, you can add the sensor output to the **Package Name** setting on the **Create Package** page. Place the cursor where you want the output to appear in the package name and type `||<sensor name>||`. This option helps you to distinguish among actions that use the same package but use different sensor output.

For example, the following workflow creates an action named `Deploy Start Service - Windows Defender Network Inspection Service`:

1. Issue a question that uses the sensor **Stopped Service**.
2. Select question results that have the sensor output `Windows Defender Network Inspection Service`.
3. Deploy an action that uses the package named **Start Service - ||Stopped Service||**.

If you select results with multiple output values for a sensor, the Tanium Server creates a separate action for each value. For example, if the package name includes the sensor **Computer Name**, the action deployment workflow automatically creates an action for each endpoint in the selected results because each has a unique computer name. Because you can select a maximum of 100 results for one action deployment, the Server creates a maximum of 100 actions for a single package that has a sensor in its name.



You cannot use a sensor that has an underscore character (_) in the name. The underscore is a delimiter for sensor sub-columns. If the sensor name has an underscore, it causes errors and unexpected results in sensor-sourced packages.

© 2026 Tanium Inc. All Rights Reserved

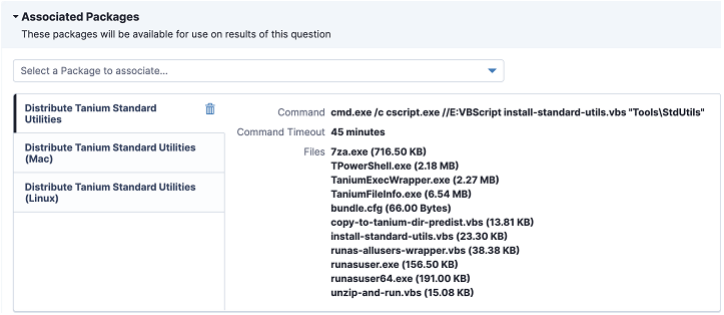
Example: Saved questions with associated packages

A saved question configuration can include optional *associated packages*, which are a recommendation from the question creator about the best packages to deploy when acting on results. An associated package is just a recommendation. The Tanium Server does not deploy it automatically and users can select any other package. Add associated packages to create workflow associations, especially when another person might use the saved question that you create as a tool to detect and remediate error states.

> **NOTE** For more information about the permissions required to manage associated packages, see Manage saved questions on page 99.

When you create or edit a saved question (see Managing saved questions in Console and Interact on page 455), use the **Associated Packages** section of the question configuration page to add a package. The following example shows packages that are added to the Tanium-provided saved question **Has Tanium Standard Utilities**.

Adding a package to a saved question



When you issue the question, it checks the Tanium Client installation directory for the existence of utilities that Tanium questions or actions rely on, and it returns `Yes`, `No`, or the names of missing files.

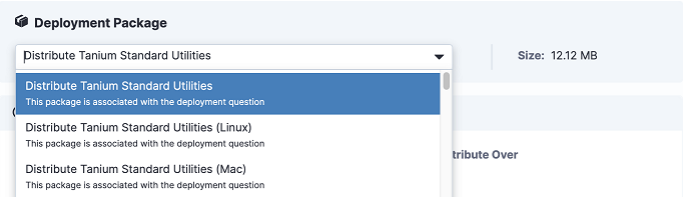
Saved question: Has Tanium Standard Utilities



© 2026 Tanium Inc. All Rights Reserved

When you click **Deploy Action**, the **Action Deployment** page automatically populates the **Deployment Package** with the first associated package that you added to the saved question configuration. All the packages that you added appear at the top of the **Deployment Package** dropdown list.

Action with preselected asssociated package



© 2026 Tanium Inc. All Rights Reserved

RBAC overview

Role-based access control (RBAC) enables you to configure granular permissions that control what individual Tanium users can see and do with Tanium solutions, and which endpoints those users can monitor and manage. For example, you can configure RBAC that allows all data center users to issue questions to data center servers but allows only administrators to deploy actions to those servers.

In the Tanium implementation of RBAC, permissions derive from roles and computer groups that are assigned to user accounts, personas, and user groups. Content such as sensors, packages, and saved questions are assigned to content sets, for which permissions control user access. For example, if your organization allows only data center administrators to reboot data center servers, you can create a role that includes **Package read** permission on the **Core Content** content set, which contains the packages for rebooting endpoints. You would also create a computer group that includes the servers, and then assign the role and computer group to the administrators.

To investigate and remediate RBAC issues, see Troubleshoot RBAC issues on page 713.



Review and, if necessary, update RBAC configurations on a quarterly basis to ensure that users can access all the Tanium features they need but without access to sensitive information they do not need. For more information, see Tanium Maintenance User Guide: Review and update RBAC permissions and authentication settings.

Roles and permissions

Permissions define the activities that users can perform in the Tanium Core Platform (see Permission-controlled Tanium activities on page 527), as well as the features and configuration objects that users can access during those activities (see Permission-controlled Tanium features and configuration objects on page 528). A role specifies *allow permissions* to enable access or *deny permissions* to prohibit access. You assign the roles to users, user groups, and personas.



For more information, see Managing access permissions through roles on page 569 and best practices for Roles on page 542.

Permission-controlled Tanium activities

Activity	Description
Read	Read permissions control object visibility. For example, the **Package read** permission allows users to open the **Administration > Content > Packages** page and view package configurations.
Write	Write permissions control the ability to manage (create, edit, or delete) objects. For example the **Package write** permission allows users to manage package configurations.

© 2026 Tanium Inc. All Rights Reserved

Permission-controlled Tanium activities (continued)

Activity	Description
Execute	Execute permissions control the ability to: • Run processes, such as initializing endpoints for Tanium™ Patch. • Use service accounts, such as the Tanium™ Connect service account. • Perform API operations, such as through the Tanium™ Detect API.
Delete	Delete permissions control the ability to delete objects that are beyond the scope of write permissions. For example, the **Threat Response Live Connection File delete** permission allows users to delete a file on an endpoint during a live connection.
Special	Special permissions control the ability to perform activities that are beyond the scope of other permissions. For example, most Tanium solutions have a **show** permission that allows users to view the solution workbench.

The configuration pages for roles, users, user groups, and personas group permissions based on the type of features and configuration objects for which the permissions control access:

Permission-controlled Tanium features and configuration objects

Feature or object type	Description
Platform content	Platform content permissions control access to content types that apply across all Tanium solutions and that are assigned to content sets. For example, you can assign permissions for sensors, packages, and saved questions in the **Default** content set. For more information, see Content sets on page 528.
Solution	Solution permissions control access to Tanium solution workbenches, features, and solution-specific content, such as Tanium Reporting dashboards.
Administration	Administration permissions control access to the **Administration > Permissions** and **Administration > Configuration** pages of Tanium Console.
Global	Global permissions control access to activities that are exclusively for reserved roles. For example, only the **Administrator** reserved role has permission to manage the Tanium license.

Content sets

A content set is a group of configuration objects (such as sensors, packages, and saved questions) for which permissions control access at the set level. For example, you can configure a role that applies **Sensor read** permission to all the sensors in the **Base** content set. A content set can contain solution-specific content (such as Tanium Reporting dashboards) or platform content that applies across all solutions (such as sensors). You cannot explicitly assign actions to a content set but they effectively belong to the same content set as their associated packages.

Tanium provides several predefined content sets through Tanium solutions. You can create a content set to contain custom content or to accommodate changes in the RBAC configuration of your Tanium deployment.

© 2026 Tanium Inc. All Rights Reserved

You can assign each content object to only one content set. For example, you cannot assign the **Domain Name** sensor to both the **Base** and **Default** content sets, although you can move the sensor from one set to another. A role can apply a permission to multiple content sets.

For more information, see Managing access to content through content sets on page 561 and best practices for Content sets on page 542.

Users

A Tanium user configuration associates the following RBAC components with a user account:

- **Roles**: A user is assigned one or more roles. Users have no permissions other than what their roles provide. A user with no roles can sign in to Tanium Console, but is directed to a page indicating insufficient permissions.
- **Computer groups**: A user is assigned one or more computer groups.
- **User groups**: A user is assigned zero or more user groups. The default persona of a user inherits roles and computer groups that are assigned to the default persona of every user group in which the user is a member.
- **Personas**: Every user is assigned a default persona and zero or more alternative personas. Users can select their assigned personas for Tanium sessions. Users can also select the alternative personas that are assigned to user groups in which the users are members.

To authenticate users when they access Tanium Console or the Tanium API, you can configure a remote authentication service or use the authentication service that is local to the Tanium Server. For more information, see User authentication on page 626.

For more information, see Managing users on page 625 and best practices for User permissions on page 543.

User groups

A Tanium user group configuration associates the following RBAC components with a set of users who inherit all the permissions of the user group:

- **Users**: A user group is assigned zero or more users.
- **Roles**: A user group is assigned one or more roles.
- **Computer groups**: A user group is assigned one or more computer groups.
- **Personas**: Every user group is assigned a default persona and zero or more alternative personas.

For more information, see Managing user groups on page 643 and best practices for User group permissions on page 543.

Personas

All user accounts have a predefined default persona, which is the persona that applies automatically when users sign in to Tanium Console. When using the default persona, a user has permissions derived from all the roles and computer groups that are assigned to that persona. The default persona of a user also provides permissions that are inherited from the default personas of user groups to which the user is assigned.

© 2026 Tanium Inc. All Rights Reserved

You can assign alternative personas directly to a user account or to the user groups in which the user is a member. After signing in for a Tanium session, the user can select any alternative persona that is assigned directly or inherited from a user group. After the user switches to an alternative persona, the user has only the permissions that are derived from the roles and computer groups that are assigned to that persona. An alternative persona does not inherit permissions from user groups to which the persona is assigned.

For more information, see Managing role and computer group permissions through personas on page 655.

Computer groups

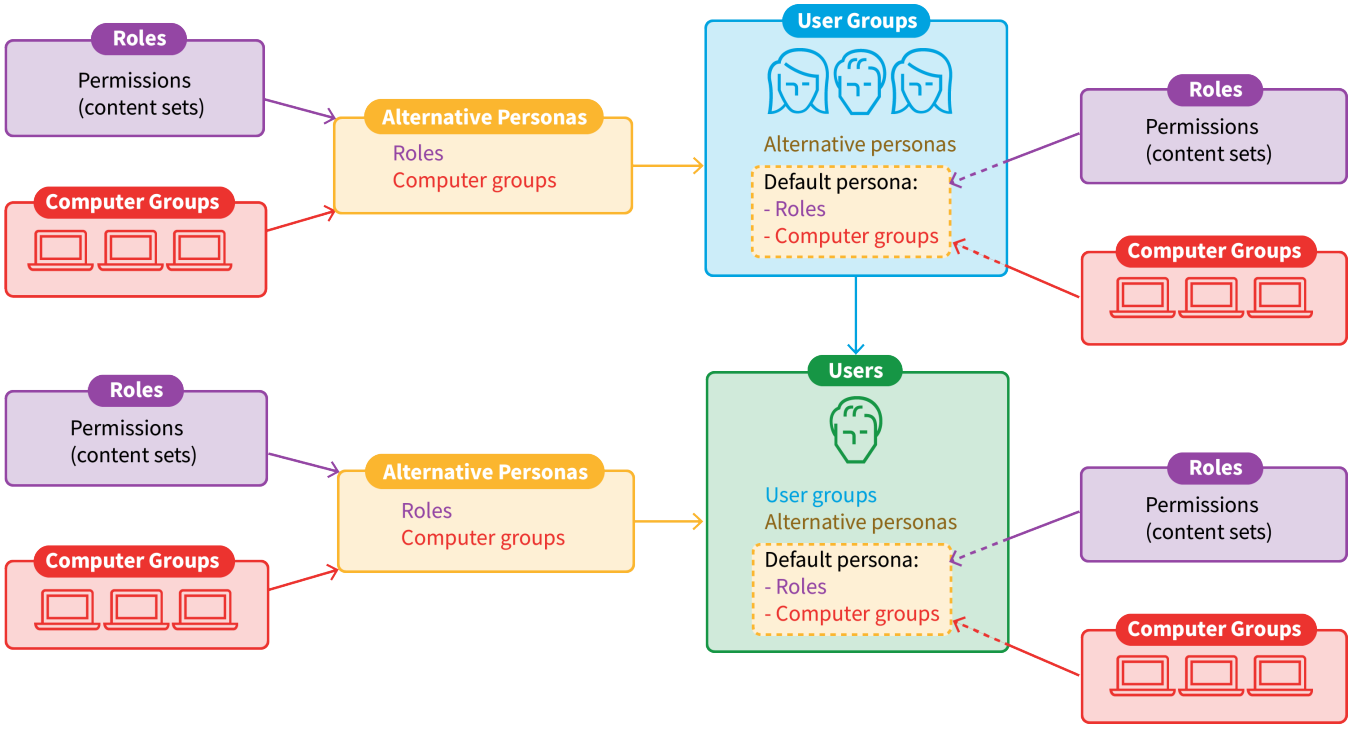
Tanium users can issue questions and deploy actions only to endpoints that belong to a *computer management group* that is assigned to those users or their user groups. For more information, see Controlling endpoint management rights through computer groups on page 610 and best practices for Computer groups on page 540.

Tanium users use computer *filter groups* as filters in questions and question results. Users can use only the filter groups that are assigned to a content set that is associated with a role, and the role must be assigned to those users or their user groups. For more information, see Managing filter groups for filtering questions and results on page 476.

RBAC configuration overview

The following figure illustrates the relationships among RBAC components. The arrows indicate how you assign the components to configure user permissions. Note that the roles and computer groups that you assign directly to user groups and user accounts are effectively assigned to the default persona of those user groups and users.

Relationships and assignments among RBAC components



© 2026 Tanium Inc. All Rights Reserved

The following tasks summarize the workflow for configuring RBAC and explain how RBAC components interact to define the effective permissions of users when they access Tanium Console under different personas. The figures in these tasks depict two user groups to illustrate the different implications of assigning roles and computer groups to alternative personas and default personas.

IMPORTANT

Before starting this workflow, review the important details and best practices described under Plan your RBAC implementation on page 539.

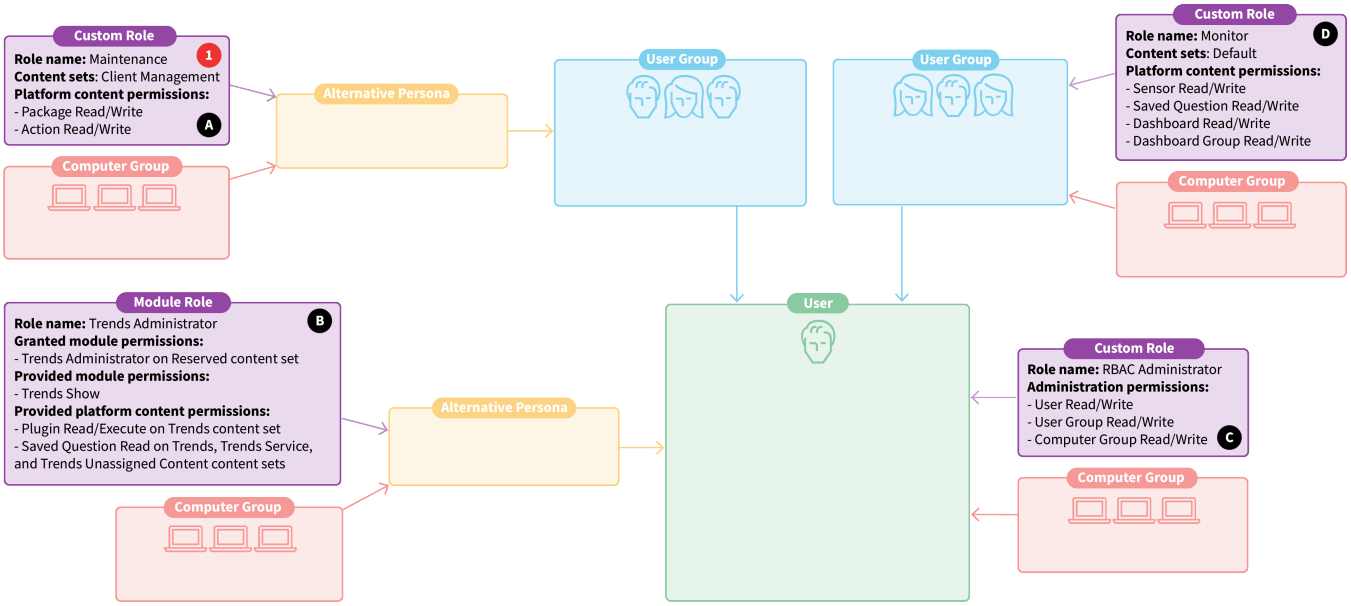
If you plan to import users and user groups from an LDAP or AD server, configure the imports before configuring RBAC. For more information, see Importing and authenticating users through LDAP on page 666.

1. Configure custom roles

Roles with platform content permissions and solution permissions apply permissions to content sets. Tanium solutions provide predefined content and content sets. You can also create custom content and content sets.

The following figure shows an example with one system role that defines solution permissions (B) and three custom roles (A, C, D).

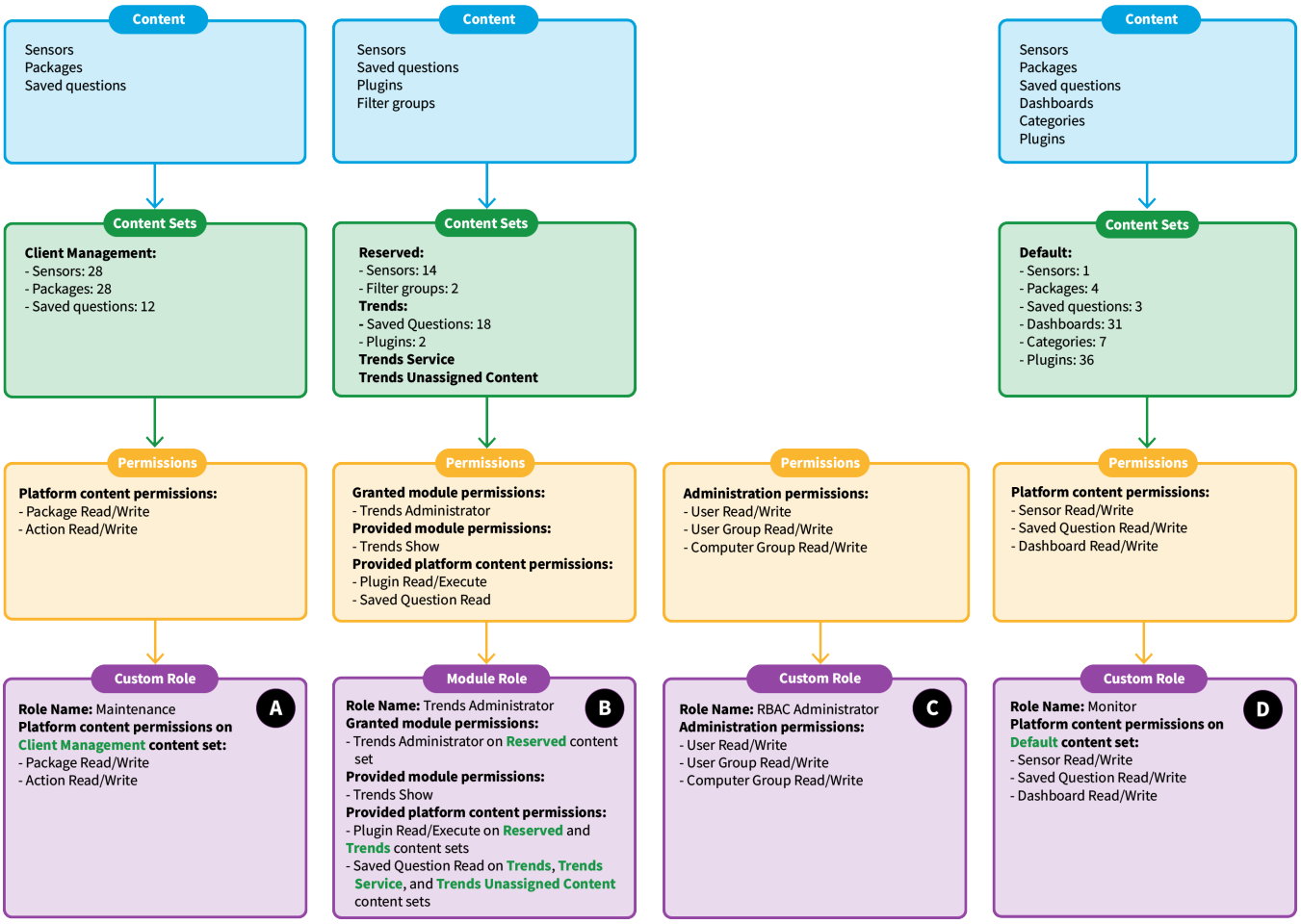
User role configurations



The next figure illustrates the relationships among content, content sets, and permissions in each example role configuration (roles A through D in the figure User role configurations on page 531).

© 2026 Tanium Inc. All Rights Reserved

Role permissions and content sets



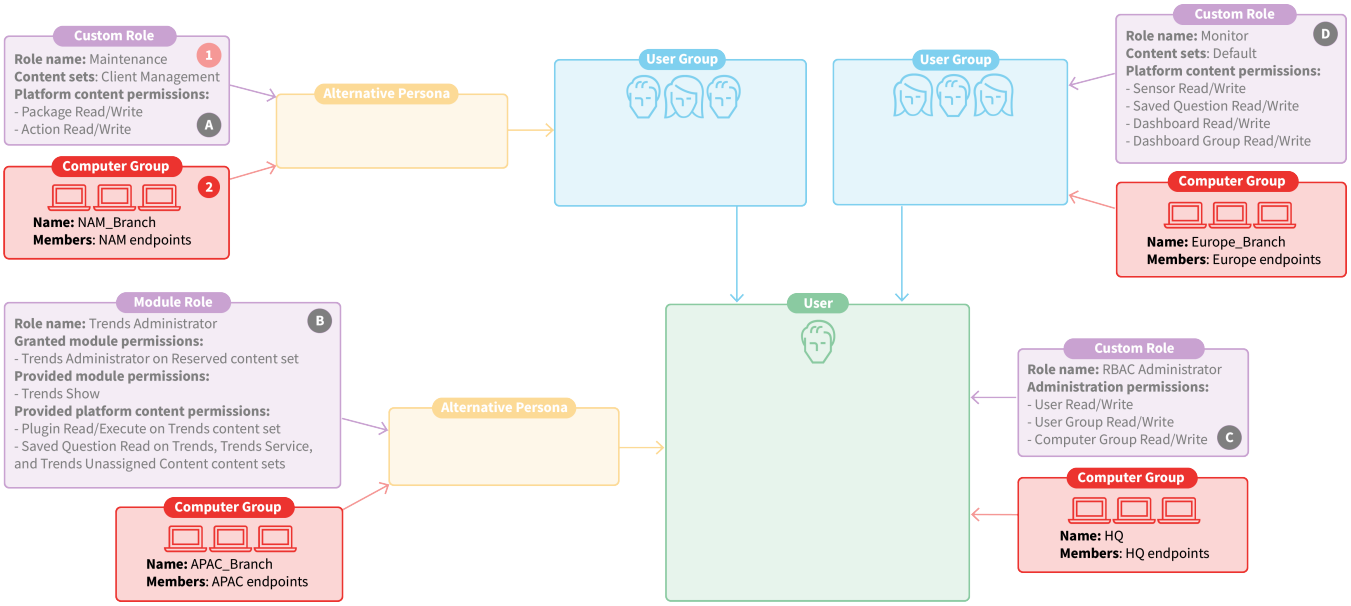
For more information, see Managing access permissions through roles on page 569.

2. Define computer management groups

You can assign computer management groups to user groups or directly to user accounts (default personas) and alternative personas.

© 2026 Tanium Inc. All Rights Reserved

Computer management group configurations

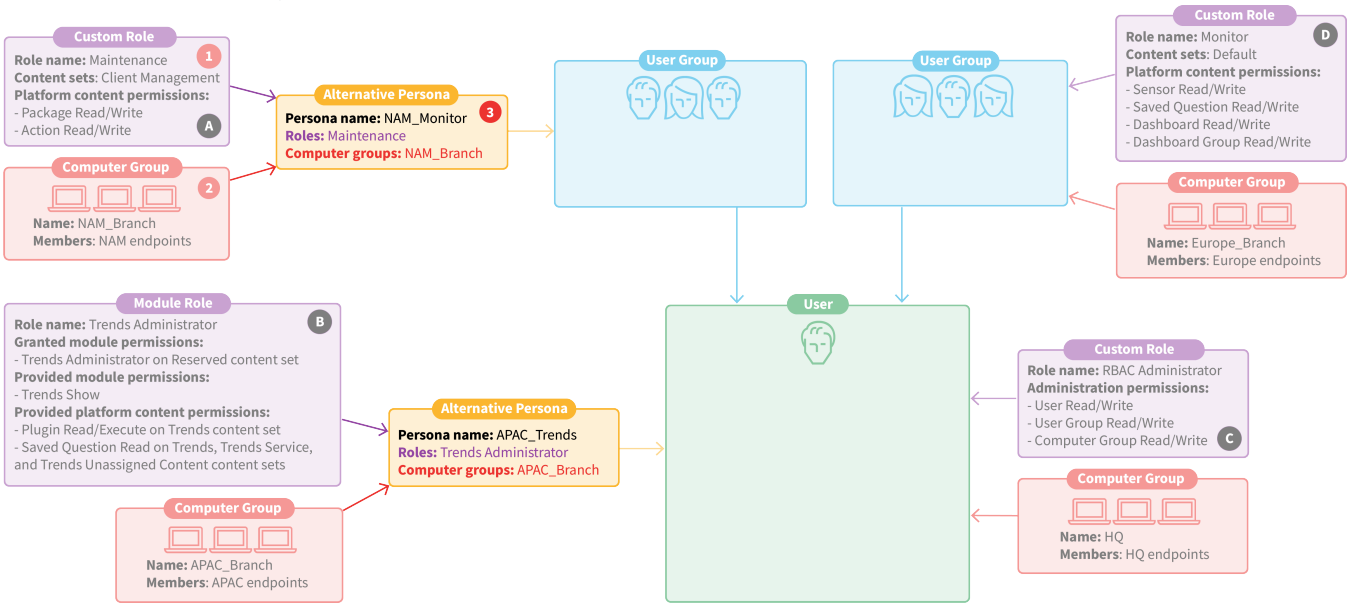


For more information, see Controlling endpoint management rights through computer groups on page 610.

3. Define alternative personas

Assign roles and computer management groups to each alternative persona.

Alternative persona configurations



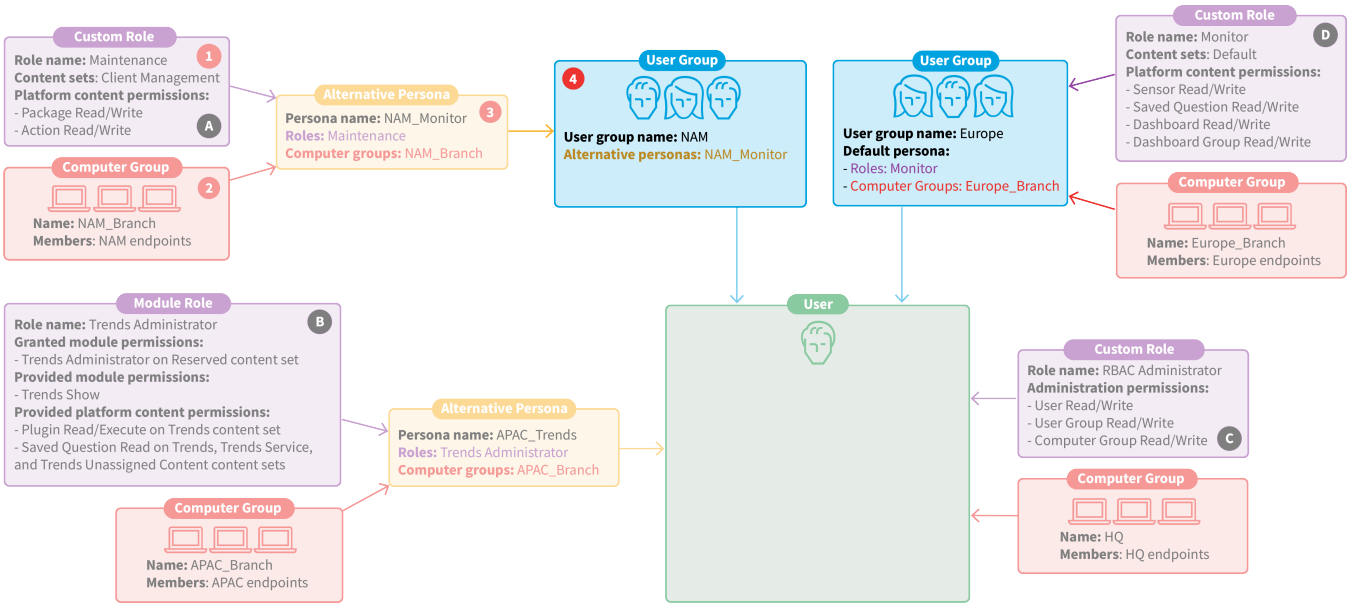
For more information, see Managing role and computer group permissions through personas on page 655.

© 2026 Tanium Inc. All Rights Reserved

4. Configure user groups

Configure the user groups that you imported from LDAP servers or manually add groups that are local to the Tanium Server. You can assign alternative personas to each user group, and assign roles and computer management groups to the default persona of each user group.

User group configurations



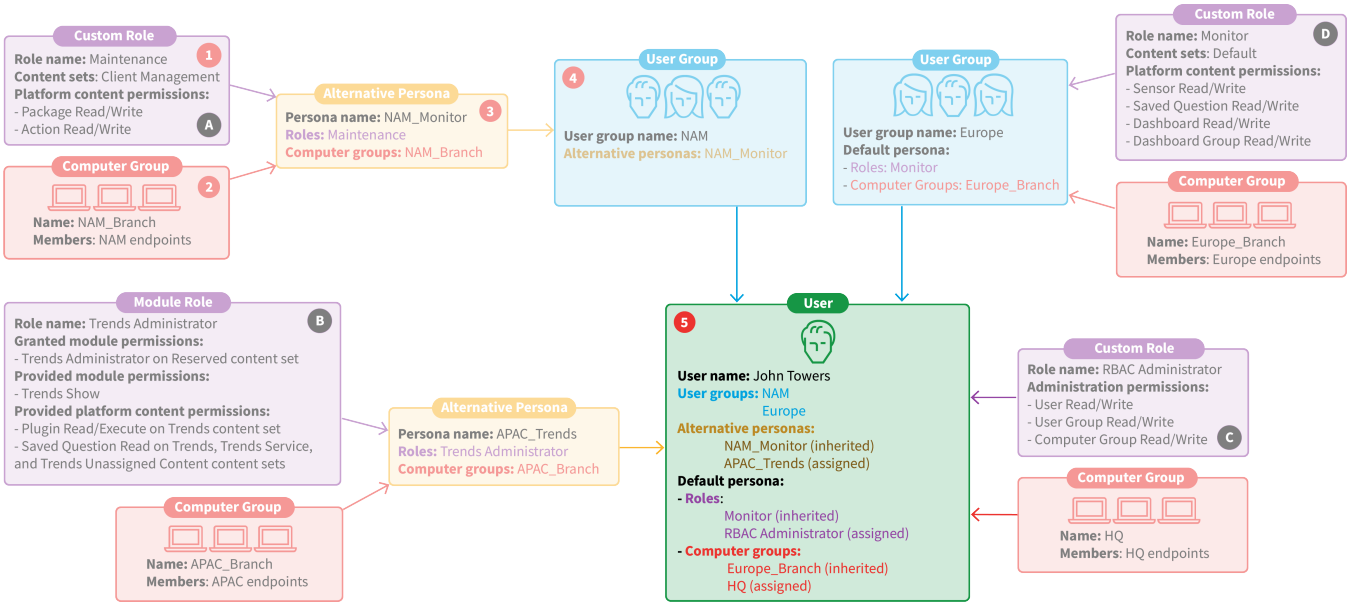
For more information, see Managing user groups on page 643.

5. Configure users

Configure the user accounts that you imported from LDAP servers or manually add accounts that are local to the Tanium Server. Assign alternative personas and user groups to each user. You can also assign roles and computer groups to the default persona of each user.

© 2026 Tanium Inc. All Rights Reserved

User configurations



For more information, see Managing users on page 625.

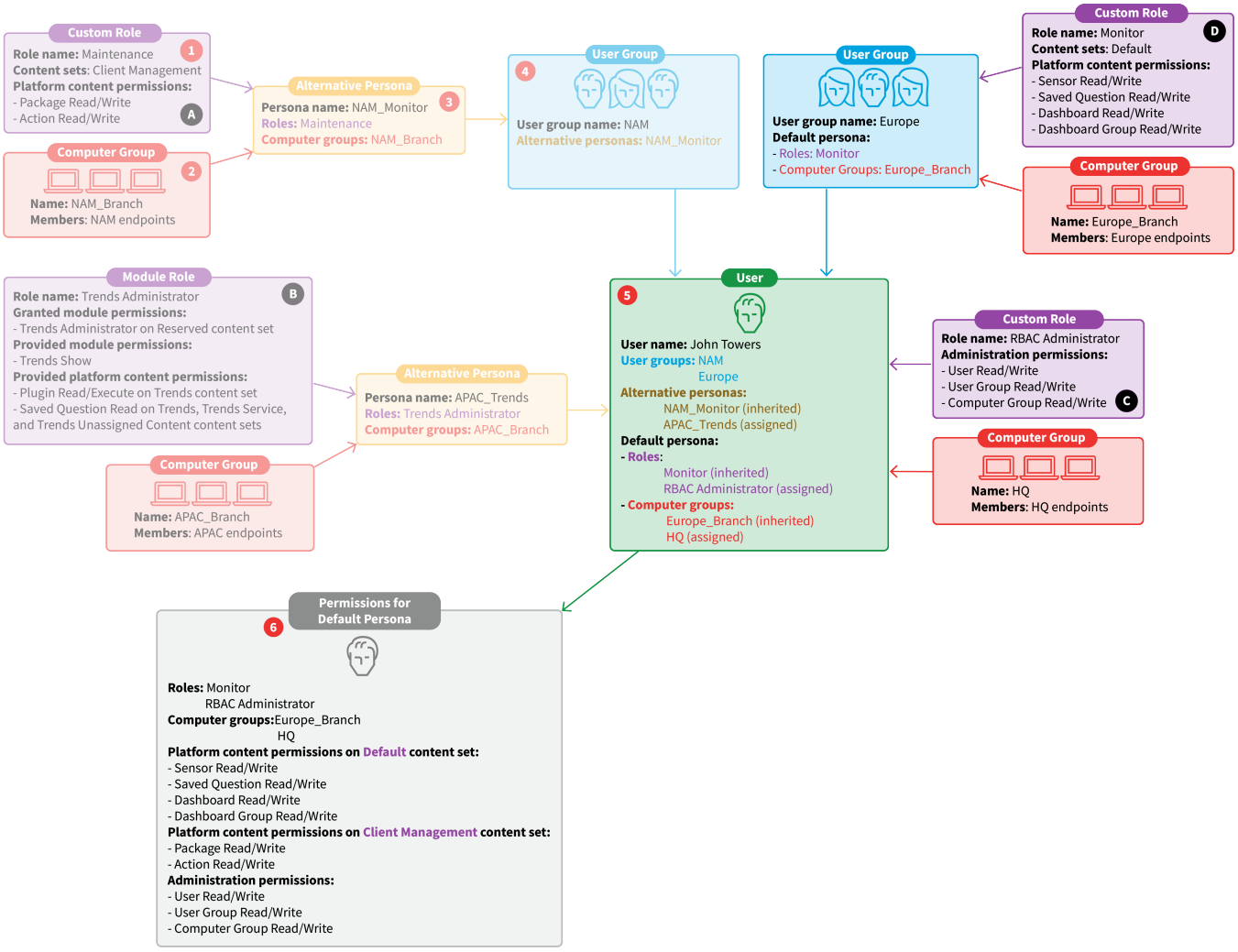
6. Sign in to Tanium Console to access the default persona

The default persona is active by default when a user sign in to Console. The default persona has permissions for all the roles and computer management groups that are directly assigned to the user account or that are inherited from the default personas of user groups.

In this example, the RBAC_Administrator role and HQ computer group are assigned to the default persona of the user. The user also inherits permissions from the Monitor role and Europe_Branch computer group that are assigned to the default persona of user group Europe.

© 2026 Tanium Inc. All Rights Reserved

Signing in as default persona



For more information, see Sign in to Console on page 49.

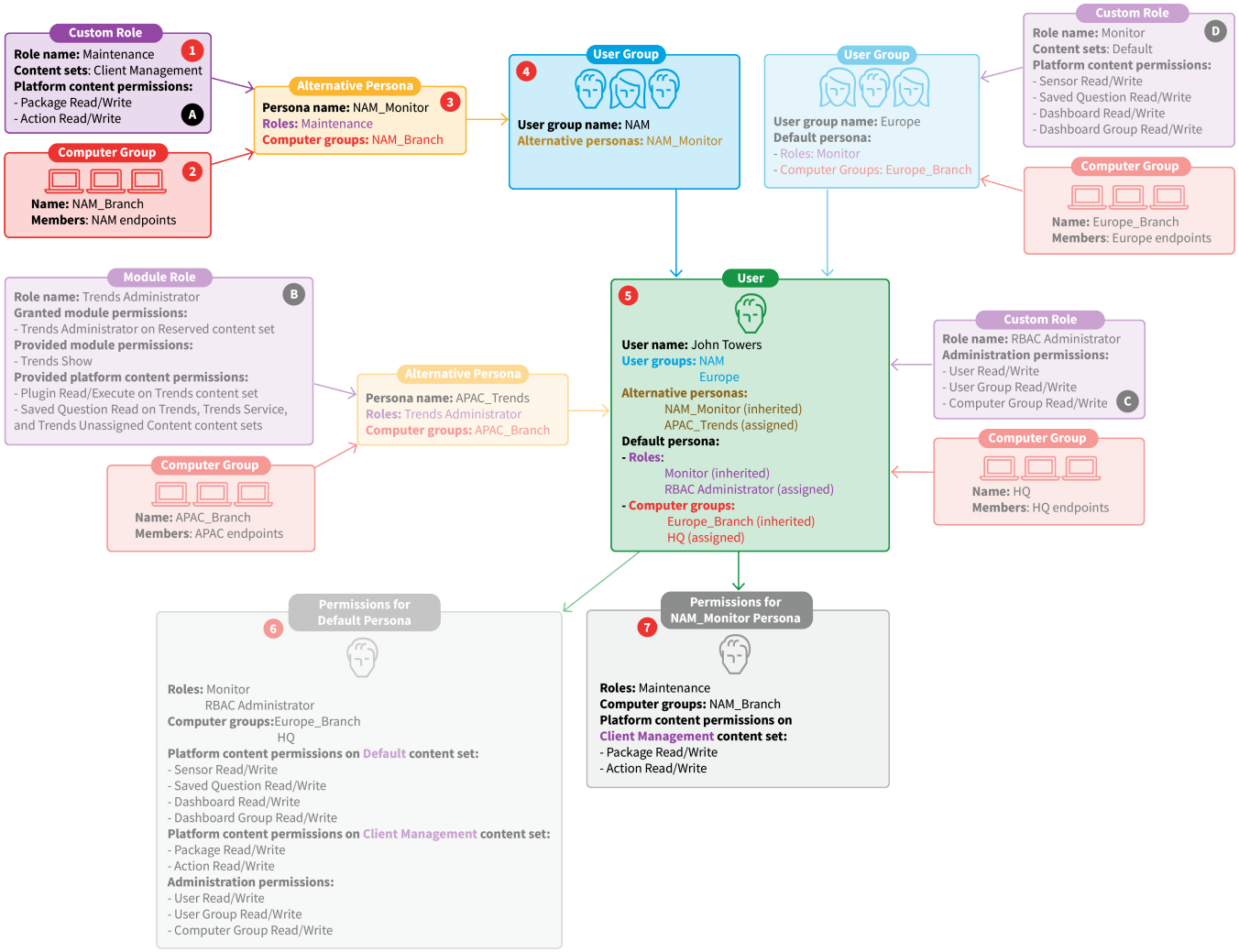
7. Switch to an alternative persona

When the user switches to an alternative persona for the Tanium Console session, that user has permissions only for the roles and computer management groups that are assigned to that persona.

In the following figure, the user selects the NAM_Monitor persona that is inherited from the NAM user group.

© 2026 Tanium Inc. All Rights Reserved

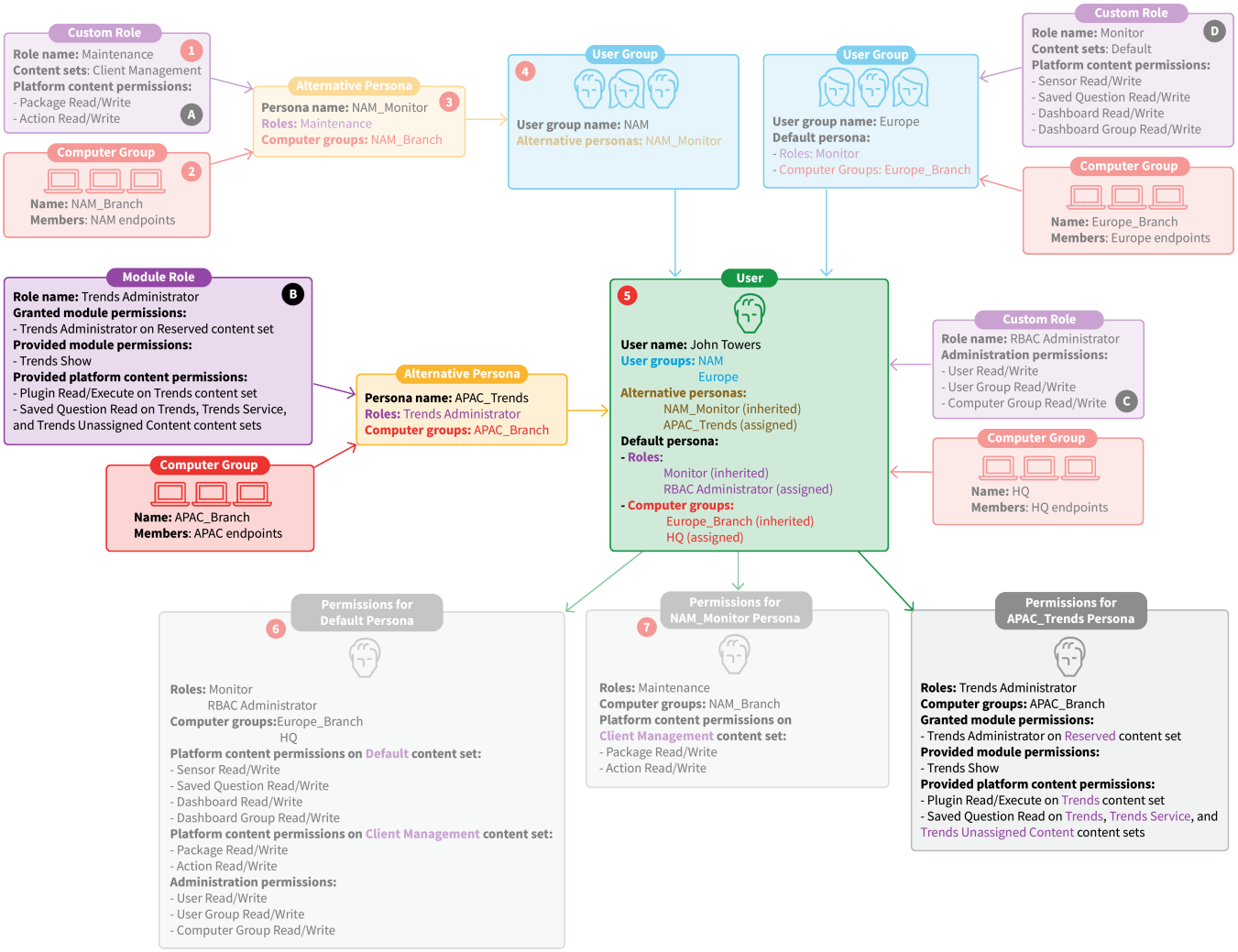
Selecting an alternative persona—example 1



In the next figure, the user selects the APAC_Trends persona that is assigned to the user account (default persona).

© 2026 Tanium Inc. All Rights Reserved

Selecting an alternative persona—example 2



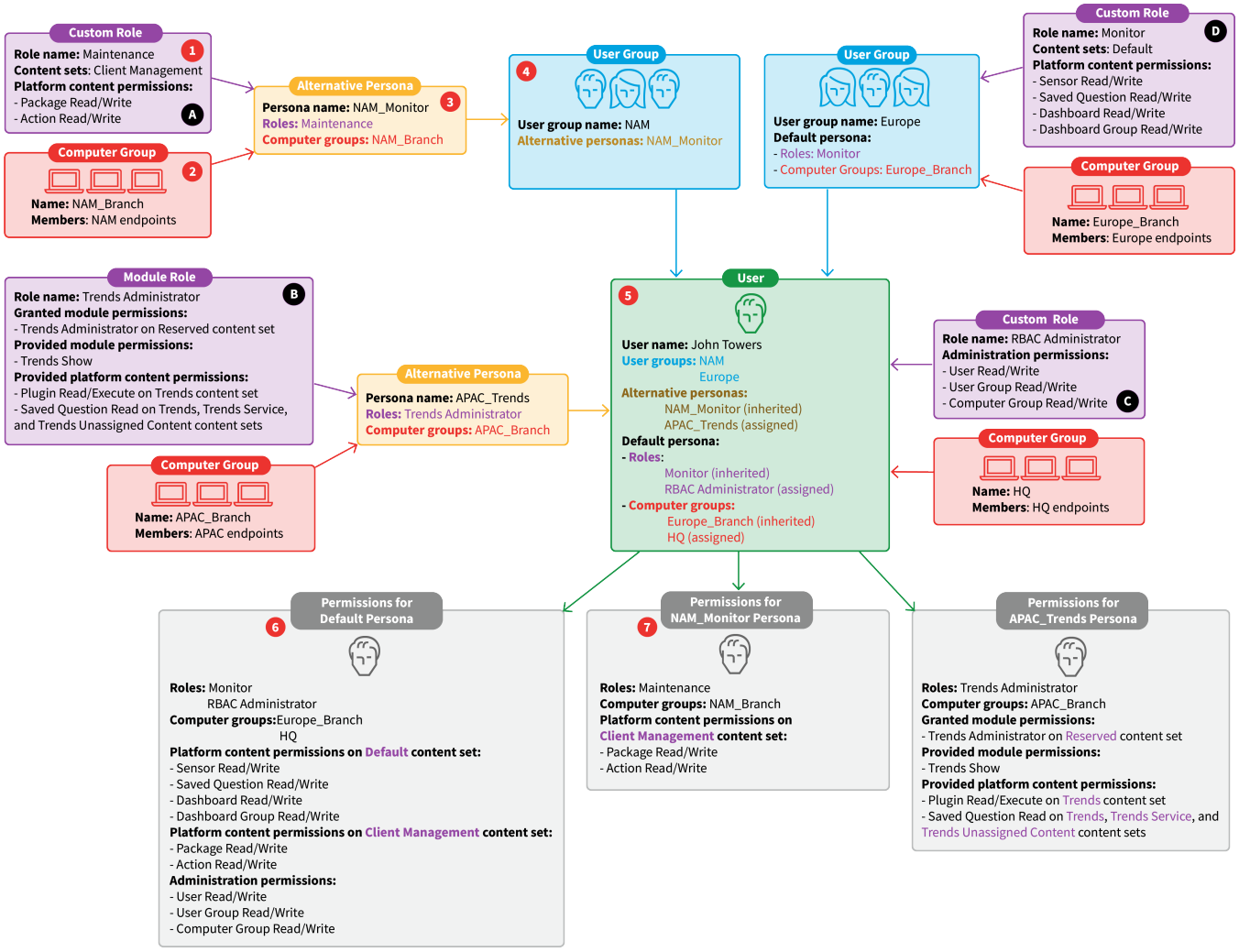
For more information, see Select a persona for your Console session on page 663.

Complete RBAC workflow

The following figure shows the complete workflow to configure the effective permissions of all three personas in this example.

© 2026 Tanium Inc. All Rights Reserved

RBAC configuration workflow



Plan your RBAC implementation

The following are important items and best practices to discuss with your team and Tanium Support (see Contact Tanium Support on page 724) when planning the RBAC implementation for your Tanium deployment.

- Naming convention on page 540
- Computer groups on page 540
- Content sets on page 542
- Roles on page 542
- Users and user groups on page 542

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

If you plan to import users and user groups from a Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server, do so before setting up RBAC. For more information, see Importing and authenticating users through LDAP on page 666.

BEST PRACTICE

For additional considerations and best practices, see the Tanium KB article 12 Things to Consider Before Planning Implementation of RBAC.

Naming convention

Before configuring custom roles, content sets, computer groups, and other RBAC objects, devise a naming convention that enables Tanium users to easily determine the purpose for each object and to distinguish it from similar Tanium-provided objects that are imported through Tanium solutions. Distinguishing custom objects is important because it is a best practice to avoid modifying Tanium-provided objects. For more information, see Tip 4: Limit customizations to Tanium content on page 138. For example, you can use the name of your organization as a prefix in the names of custom objects.

Computer groups

Consider the following best practices before you create custom computer management groups or filter groups for actions and questions.

MEMBERSHIP CRITERIA

Identify the sets of endpoints that you want to manage as a group for operations that Tanium users and solutions perform. Some user roles might be dedicated to certain functions, such as deploying patches to datacenter servers. In this case, you can create a computer group that targets those servers and assign the group to those users. Other operations might be restricted based on privacy laws that differ among locations, in which case you can create a computer group for each location.

For example, your organization might have separate users who are responsible for monitoring and managing endpoints in a particular regional office. For each region, you can create a computer group with a membership definition that includes all the endpoints in that region. If you use custom tags to define endpoint locations, a computer group for the Asia-Pacific (APAC) region might have the membership question `Custom Tags equals APAC`. After you assign that computer group to the corresponding user, that user can see results from all endpoints in the Asia-Pacific region for questions such as `Get Running Applications from all machines`. The user can also target the endpoints for actions, such as application updates.

RESOURCE USAGE FOR ACTIONS AND QUESTIONS

When a user issues a question or deploys an action, the Tanium Server sends it to endpoints within a message that includes all the computer groups that you assign to the user. Increasing the number and complexity of assigned computer groups increases the message size, which increases the networking and endpoint resources that the question or action consumes. The complexity and number of computer groups that you assign to an action group also increase the message size and therefore resource usage.

When you configure computer groups and assign them to users, personas, user groups, and action groups, the following best practices enable you to minimize the resource usage of questions and actions and to avoid unexpected targeting results:

© 2026 Tanium Inc. All Rights Reserved

- **Minimalistic assignments**
  - **Computer groups**: Assign only the computer groups that each user needs to perform the Tanium operations that are expected for the role of that user.

    For example, if a user has the authority to manage end-user systems but not servers, assign the **All Workstations** group but not the **All Windows** group, which includes Windows servers. As another example, instead of assigning the two groups **All Windows Servers - Physical** and **All Windows Servers - Virtual**, you can give a user the same management rights by assigning only **All Windows Servers**.
  - **Action groups**: When you configure an action group, assign only the computer groups that are necessary for the actions that you plan to deploy to that action group. If necessary, you can specify more computer groups and other filters in the **Targeting Criteria** of a specific action when you configure its settings. For more information, see Deploying actions and playbooks in Console and Interact on page 391.
- **Sensor- and tag-based groups**

  Define Computer group membership on page 614 using sensor-based filters instead of manually defined lists to enable granular control over which endpoints to include or exclude. You can achieve additional flexibility, while keeping the filtering clause simple, by defining computer groups with membership that is based on custom tags that you add to endpoints or remove as necessary. For more information, see Manage computer group membership through custom tags on page 619.
- **Precise membership expressions for fewer groups**

  One computer group with a precise membership expression is more efficient than multiple computer groups in which the combined membership exceeds what a user needs. For example, you might want to give a user management rights for all Windows endpoints that have x86 architecture. Instead of assigning the two groups **All Windows Servers - x86** and **All Windows Workstations - x86**, you can assign a single group with membership that is based on a sensor filter such as `"x64/x86?" starts with x86`.
- **Simple membership expressions**

  As much as possible, use simple expressions to define computer group membership. Complex expressions increase the processing load on endpoints. For example, you might want a computer group for Windows and macOS endpoints that use storage encryption. The membership expression `Storage Encryption Status equals "Encrypted"` is efficient because it selects only Windows and macOS endpoints, and only if they use storage encryption. By contrast, the expression `Is Windows equals true or Is Mac equals true` requires more sensors and is less precise because it selects Windows and macOS endpoints that might or might not use storage encryption. For more examples of complex expressions that increase the processing load, see Reference: Advanced question syntax in Console and Interact on page 731.
- **Negative targeting**

  As much as possible, avoid negative targeting in sensor-based filter expressions when you create computer groups with dynamic membership. Negative targeting is the use of negative conditions to target endpoints, such as expressions that use the filter operators `not contains`, `is not equal to`, and `does not match`. Negative targeting can be unpredictable and unintentionally include or exclude endpoints.
- **Maximum sensor or data age**

  Do not lower the default **Max Sensor Age** or **Maximum Data Age** for any sensor that defines endpoint membership in a computer group. For more information, see Best practices for saved questions on page 456.

© 2026 Tanium Inc. All Rights Reserved

NOTE

For more information about the options available for sensor filters in the membership expressions of computer groups, see Filter operators on page 733. For examples of regular expressions that you can use, see Use regular expression filters on page 739.

Content sets

Determine how to organize content set permissions for controlling access to specific data and deploying actions on endpoints. As a best practice, ensure that the content in any particular content set is similar to minimize the risk of assigning unintended permissions to user roles. You can organize content sets based on the following:

- **Capability**: Read or write permissions
- **Content type**: For example, saved questions, sensors, or packages
- **Subject matter**: For example, Tanium Client administration or Windows system administration

BEST PRACTICE

For content that is provided through Tanium solutions, keep the content objects in their original Tanium-provided content sets. To sustain this practice when moving content between content sets, create copies of Tanium-provided content and move the copies instead of the original versions. Contact Tanium Support before proceeding if you need to move original Tanium-provided content. For more information, see Contact Tanium Support on page 724.

Roles

The following are best practices for managing roles:

- **Configuration order**: Configure custom roles that specify solution permissions before configuring roles that specify platform content or administration permissions. Solution permissions allow access to a specific solution and often provide additional platform content and administration permissions.
- **Modularity**: When configuring roles, take advantage of their modularity and cumulative effect on user permissions. For example, instead of creating a role with all the permissions that a particular user needs, and creating another role with only slightly different permissions for another user, create several roles with smaller but unique permissions sets. You can then mix and match these minimalistic roles among various users to achieve the same effective permissions as individual roles that have comprehensive permissions. For more information, see View effective role permissions on page 588.

Users and user groups

LDAP SUPPORT

If you plan to import users and user groups from a Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server, set up the imports before you perform other RBAC tasks. The Tanium Server automatically synchronizes with the LDAP server every five minutes, and you can manually synchronize at any time. The synchronization updates the Tanium Server with any changes that

© 2026 Tanium Inc. All Rights Reserved

occurred on the LDAP server, including any new or deleted users, new or deleted user groups, and changes to group membership. Optionally, you can use an LDAP server to authenticate the imported users. For more information, see Importing and authenticating users through LDAP on page 666.

USER GROUP PERMISSIONS

Control permissions at the user group level as much as possible instead of at the user level. Assigning computer groups, roles, personas, and users to user groups minimizes the administrative effort required to update your RBAC configuration. For example, instead of modifying role assignments for the personas of each user who might join or leave your organization, or whose responsibilities might change, you can configure user groups that use sensor-based filters to dynamically adjust group membership when such changes occur.

USER PERMISSIONS

To identify which permissions are needed, consider what each team in your organization needs to accomplish through the Tanium system. In particular, consider the following:

- **Solution access**: Which users require access to which Tanium solution workbenches and solution content?
- **Administrator permissions**: Do you want to use the **Administrator** reserved role to assign full administrator permissions to a few users or assign granular administration permissions that allow or deny page-specific read and write access to the **Administration > Configuration** pages?

SAML AUTHENTICATION

You can use a Security Assertion Markup Language (SAML) identity provider (IdP) to provide single sign-on authentication for Tanium Console users. For more information, see Enabling SSO through SAML on page 684.

© 2026 Tanium Inc. All Rights Reserved

RBAC overview

Role-based access control (RBAC) enables you to configure granular permissions that control what individual Tanium users can see and do with Tanium solutions, and which endpoints those users can monitor and manage. For example, you can configure RBAC that allows all data center users to issue questions to data center servers but allows only administrators to deploy actions to those servers.

In the Tanium implementation of RBAC, permissions derive from roles and computer groups that are assigned to user accounts, personas, and user groups. Content such as sensors, packages, and saved questions are assigned to content sets, for which permissions control user access. For example, if your organization allows only data center administrators to reboot data center servers, you can create a role that includes **Package read** permission on the **Core Content** content set, which contains the packages for rebooting endpoints. You would also create a computer group that includes the servers, and then assign the role and computer group to the administrators.

To investigate and remediate RBAC issues, see Troubleshoot RBAC issues on page 713.



Review and, if necessary, update RBAC configurations on a quarterly basis to ensure that users can access all the Tanium features they need but without access to sensitive information they do not need. For more information, see Tanium Maintenance User Guide: Review and update RBAC permissions and authentication settings.

Roles and permissions

Permissions define the activities that users can perform in the Tanium Core Platform (see Permission-controlled Tanium activities on page 544), as well as the features and configuration objects that users can access during those activities (see Permission-controlled Tanium features and configuration objects on page 545). A role specifies *allow permissions* to enable access or *deny permissions* to prohibit access. You assign the roles to users, user groups, and personas.



For more information, see Managing access permissions through roles on page 569 and best practices for Roles on page 559.

Permission-controlled Tanium activities

Activity	Description
Read	Read permissions control object visibility. For example, the **Package read** permission allows users to open the **Administration > Content > Packages** page and view package configurations.
Write	Write permissions control the ability to manage (create, edit, or delete) objects. For example the **Package write** permission allows users to manage package configurations.

© 2026 Tanium Inc. All Rights Reserved

Permission-controlled Tanium activities (continued)

Activity	Description
Execute	Execute permissions control the ability to: • Run processes, such as initializing endpoints for Tanium™ Patch. • Use service accounts, such as the Tanium™ Connect service account. • Perform API operations, such as through the Tanium™ Detect API.
Delete	Delete permissions control the ability to delete objects that are beyond the scope of write permissions. For example, the **Threat Response Live Connection File delete** permission allows users to delete a file on an endpoint during a live connection.
Special	Special permissions control the ability to perform activities that are beyond the scope of other permissions. For example, most Tanium solutions have a **show** permission that allows users to view the solution workbench.

The configuration pages for roles, users, user groups, and personas group permissions based on the type of features and configuration objects for which the permissions control access:

Permission-controlled Tanium features and configuration objects

Feature or object type	Description
Platform content	Platform content permissions control access to content types that apply across all Tanium solutions and that are assigned to content sets. For example, you can assign permissions for sensors, packages, and saved questions in the **Default** content set. For more information, see Content sets on page 545.
Solution	Solution permissions control access to Tanium solution workbenches, features, and solution-specific content, such as Tanium Reporting dashboards.
Administration	Administration permissions control access to the **Administration > Permissions** and **Administration > Configuration** pages of Tanium Console.
Global	Global permissions control access to activities that are exclusively for reserved roles. For example, only the **Administrator** reserved role has permission to manage the Tanium license.

Content sets

A content set is a group of configuration objects (such as sensors, packages, and saved questions) for which permissions control access at the set level. For example, you can configure a role that applies **Sensor read** permission to all the sensors in the **Base** content set. A content set can contain solution-specific content (such as Tanium Reporting dashboards) or platform content that applies across all solutions (such as sensors). You cannot explicitly assign actions to a content set but they effectively belong to the same content set as their associated packages.

Tanium provides several predefined content sets through Tanium solutions. You can create a content set to contain custom content or to accommodate changes in the RBAC configuration of your Tanium deployment.

© 2026 Tanium Inc. All Rights Reserved

You can assign each content object to only one content set. For example, you cannot assign the **Domain Name** sensor to both the **Base** and **Default** content sets, although you can move the sensor from one set to another. A role can apply a permission to multiple content sets.

For more information, see Managing access to content through content sets on page 561 and best practices for Content sets on page 559.

Users

A Tanium user configuration associates the following RBAC components with a user account:

- **Roles**: A user is assigned one or more roles. Users have no permissions other than what their roles provide. A user with no roles can sign in to Tanium Console, but is directed to a page indicating insufficient permissions.
- **Computer groups**: A user is assigned one or more computer groups.
- **User groups**: A user is assigned zero or more user groups. The default persona of a user inherits roles and computer groups that are assigned to the default persona of every user group in which the user is a member.
- **Personas**: Every user is assigned a default persona and zero or more alternative personas. Users can select their assigned personas for Tanium sessions. Users can also select the alternative personas that are assigned to user groups in which the users are members.

To authenticate users when they access Tanium Console or the Tanium API, you can configure a remote authentication service or use the authentication service that is local to the Tanium Server. For more information, see User authentication on page 626.

For more information, see Managing users on page 625 and best practices for User permissions on page 560.

User groups

A Tanium user group configuration associates the following RBAC components with a set of users who inherit all the permissions of the user group:

- **Users**: A user group is assigned zero or more users.
- **Roles**: A user group is assigned one or more roles.
- **Computer groups**: A user group is assigned one or more computer groups.
- **Personas**: Every user group is assigned a default persona and zero or more alternative personas.

For more information, see Managing user groups on page 643 and best practices for User group permissions on page 560.

Personas

All user accounts have a predefined default persona, which is the persona that applies automatically when users sign in to Tanium Console. When using the default persona, a user has permissions derived from all the roles and computer groups that are assigned to that persona. The default persona of a user also provides permissions that are inherited from the default personas of user groups to which the user is assigned.

© 2026 Tanium Inc. All Rights Reserved

You can assign alternative personas directly to a user account or to the user groups in which the user is a member. After signing in for a Tanium session, the user can select any alternative persona that is assigned directly or inherited from a user group. After the user switches to an alternative persona, the user has only the permissions that are derived from the roles and computer groups that are assigned to that persona. An alternative persona does not inherit permissions from user groups to which the persona is assigned.

For more information, see Managing role and computer group permissions through personas on page 655.

Computer groups

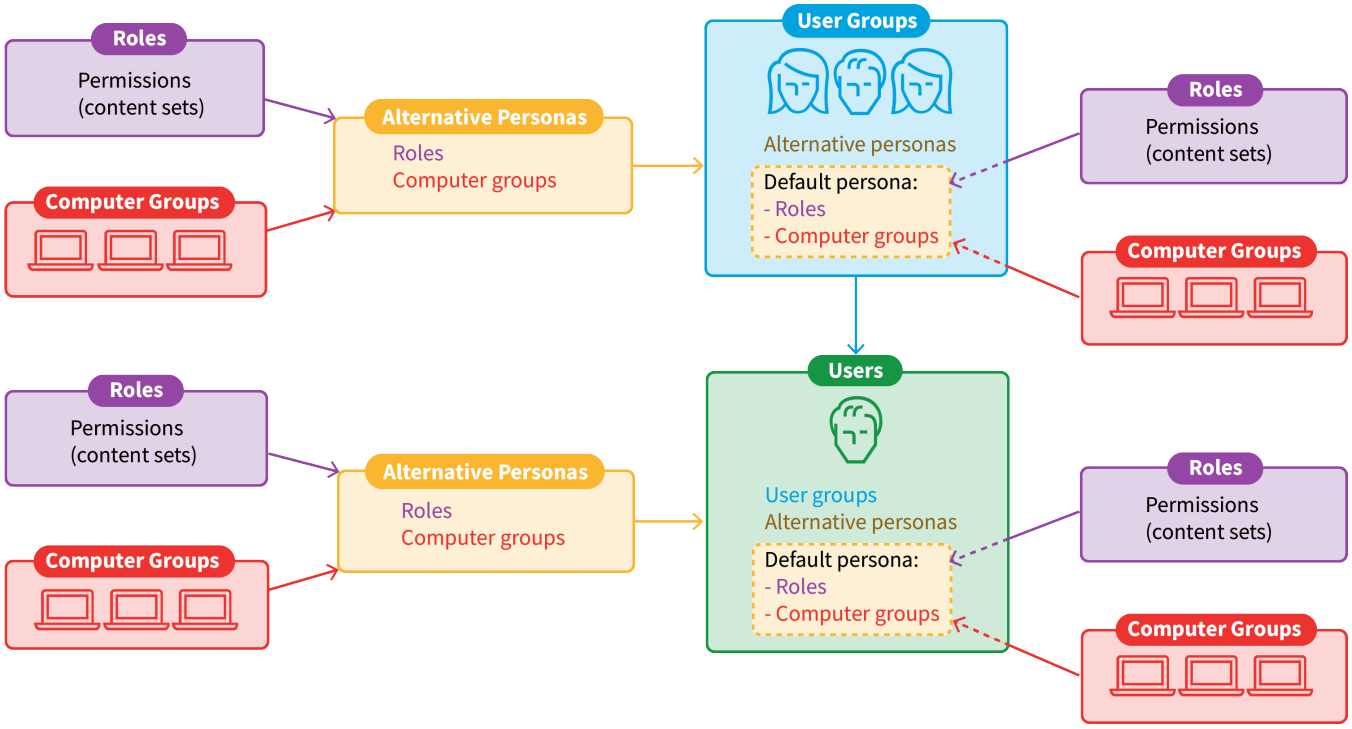
Tanium users can issue questions and deploy actions only to endpoints that belong to a *computer management group* that is assigned to those users or their user groups. For more information, see Controlling endpoint management rights through computer groups on page 610 and best practices for Computer groups on page 557.

Tanium users use computer *filter groups* as filters in questions and question results. Users can use only the filter groups that are assigned to a content set that is associated with a role, and the role must be assigned to those users or their user groups. For more information, see Managing filter groups for filtering questions and results on page 476.

RBAC configuration overview

The following figure illustrates the relationships among RBAC components. The arrows indicate how you assign the components to configure user permissions. Note that the roles and computer groups that you assign directly to user groups and user accounts are effectively assigned to the default persona of those user groups and users.

Relationships and assignments among RBAC components



© 2026 Tanium Inc. All Rights Reserved

The following tasks summarize the workflow for configuring RBAC and explain how RBAC components interact to define the effective permissions of users when they access Tanium Console under different personas. The figures in these tasks depict two user groups to illustrate the different implications of assigning roles and computer groups to alternative personas and default personas.

IMPORTANT

Before starting this workflow, review the important details and best practices described under Plan your RBAC implementation on page 556.

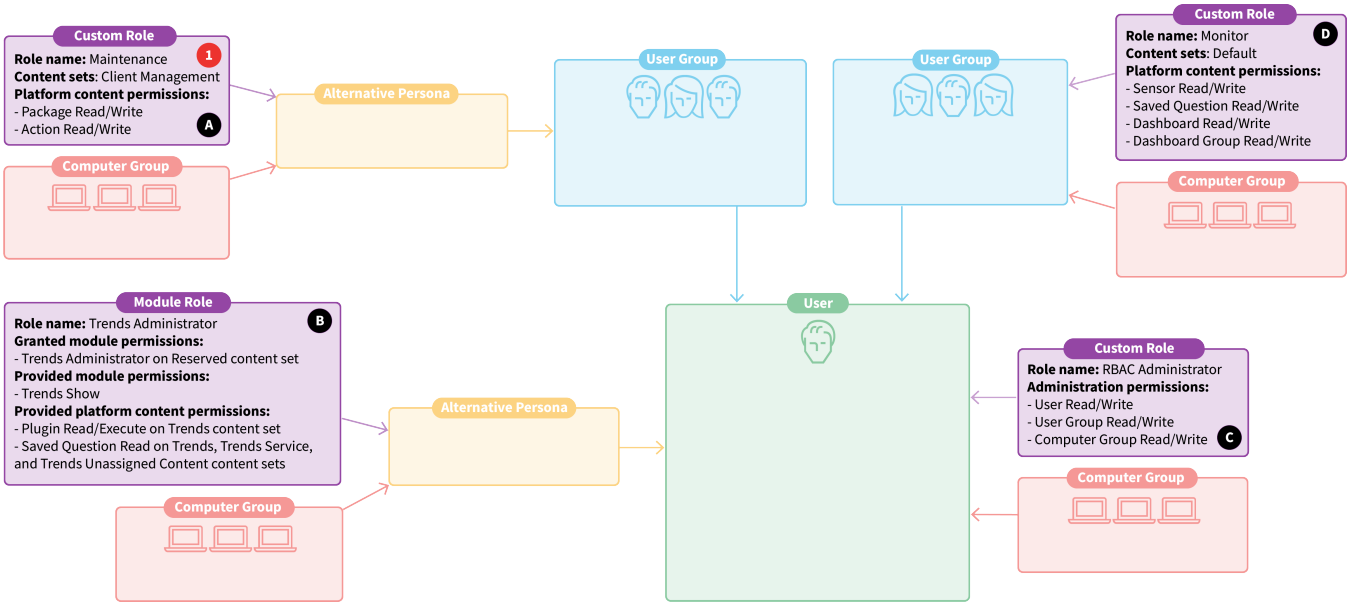
If you plan to import users and user groups from an LDAP or AD server, configure the imports before configuring RBAC. For more information, see Importing and authenticating users through LDAP on page 666.

1. Configure custom roles

Roles with platform content permissions and solution permissions apply permissions to content sets. Tanium solutions provide predefined content and content sets. You can also create custom content and content sets.

The following figure shows an example with one system role that defines solution permissions (B) and three custom roles (A, C, D).

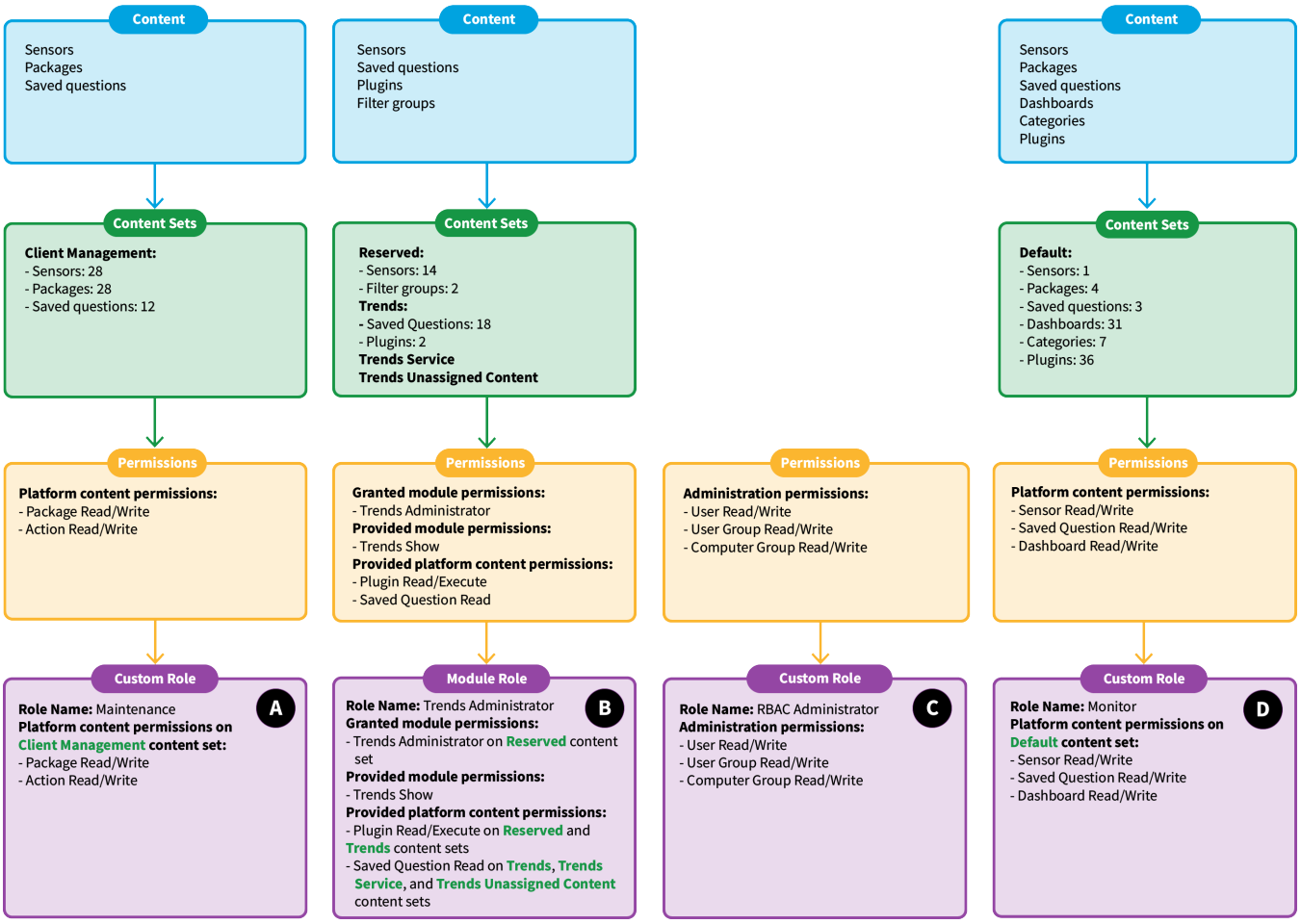
User role configurations



The next figure illustrates the relationships among content, content sets, and permissions in each example role configuration (roles A through D in the figure User role configurations on page 548).

© 2026 Tanium Inc. All Rights Reserved

Role permissions and content sets



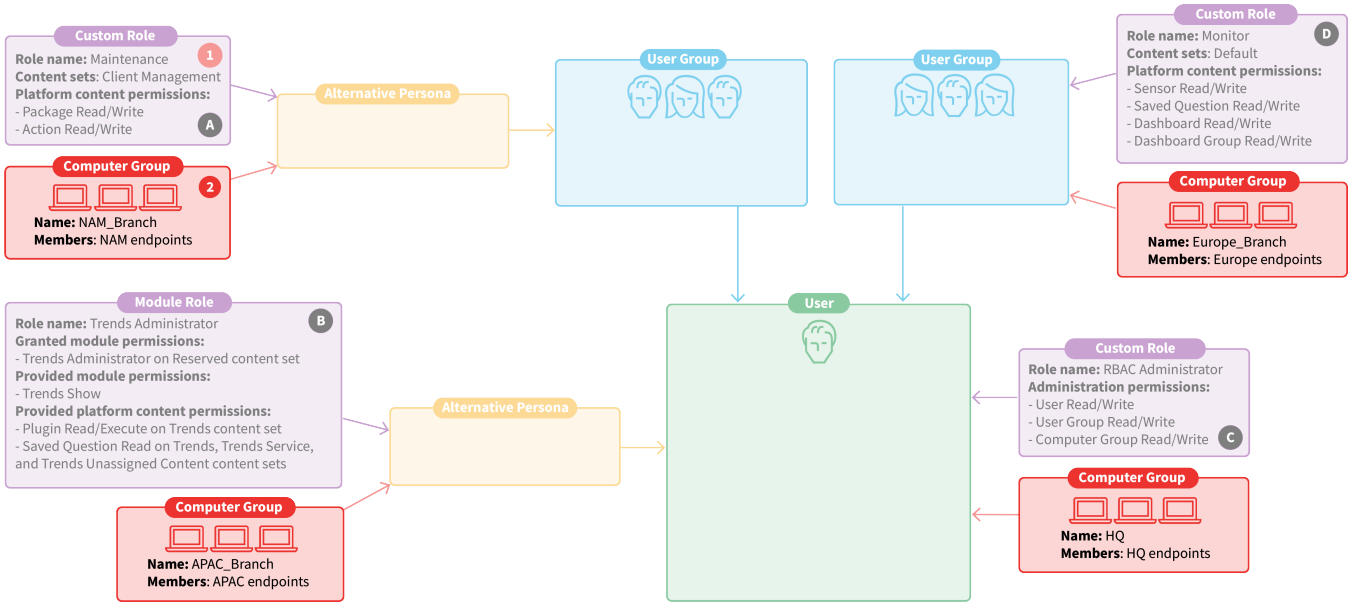
For more information, see Managing access permissions through roles on page 569.

2. Define computer management groups

You can assign computer management groups to user groups or directly to user accounts (default personas) and alternative personas.

© 2026 Tanium Inc. All Rights Reserved

Computer management group configurations

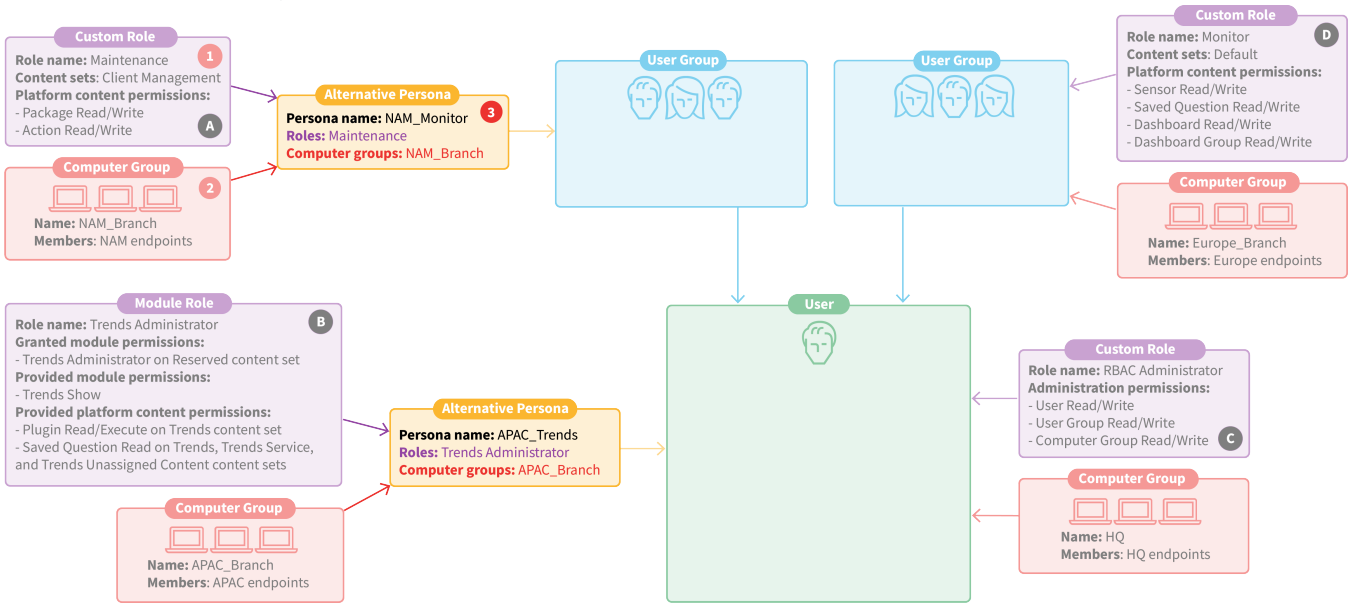


For more information, see Controlling endpoint management rights through computer groups on page 610.

3. Define alternative personas

Assign roles and computer management groups to each alternative persona.

Alternative persona configurations



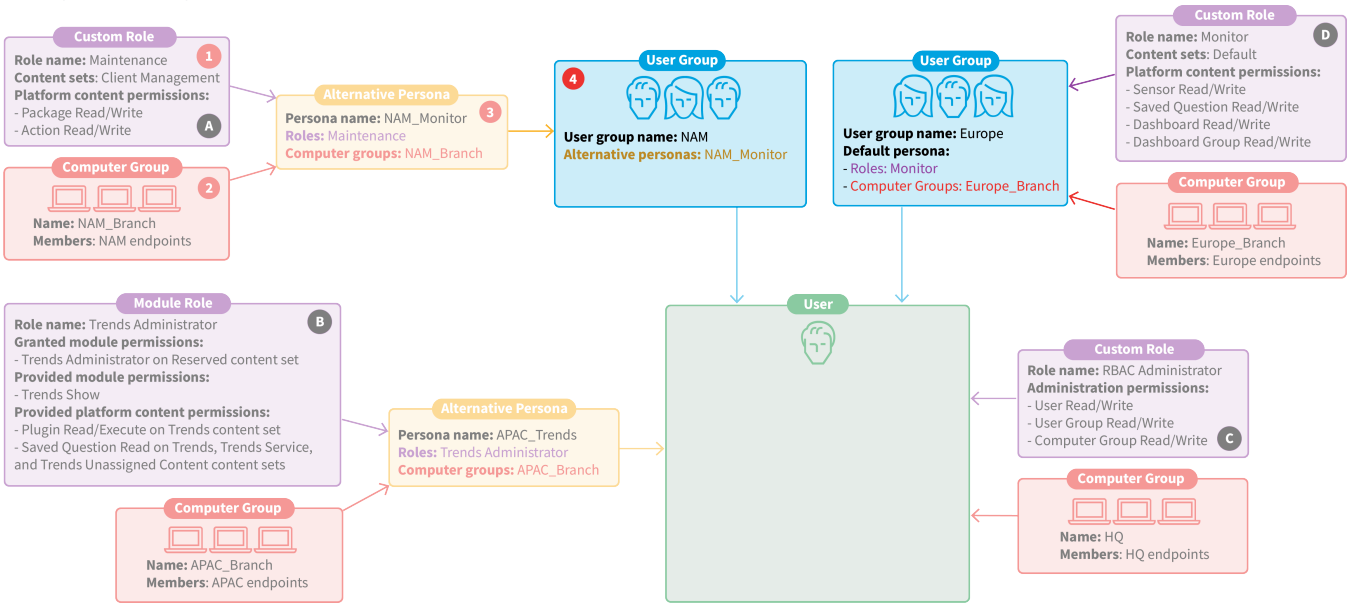
For more information, see Managing role and computer group permissions through personas on page 655.

© 2026 Tanium Inc. All Rights Reserved

4. Configure user groups

Configure the user groups that you imported from LDAP servers or manually add groups that are local to the Tanium Server. You can assign alternative personas to each user group, and assign roles and computer management groups to the default persona of each user group.

User group configurations



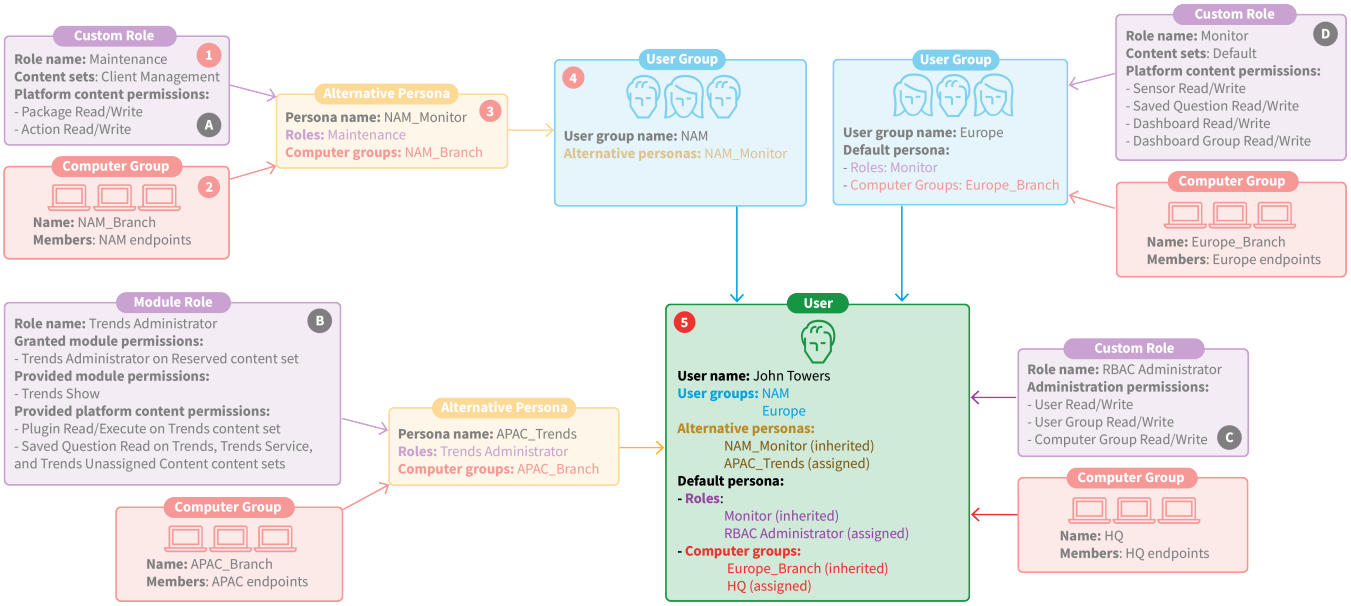
For more information, see Managing user groups on page 643.

5. Configure users

Configure the user accounts that you imported from LDAP servers or manually add accounts that are local to the Tanium Server. Assign alternative personas and user groups to each user. You can also assign roles and computer groups to the default persona of each user.

© 2026 Tanium Inc. All Rights Reserved

User configurations



For more information, see Managing users on page 625.

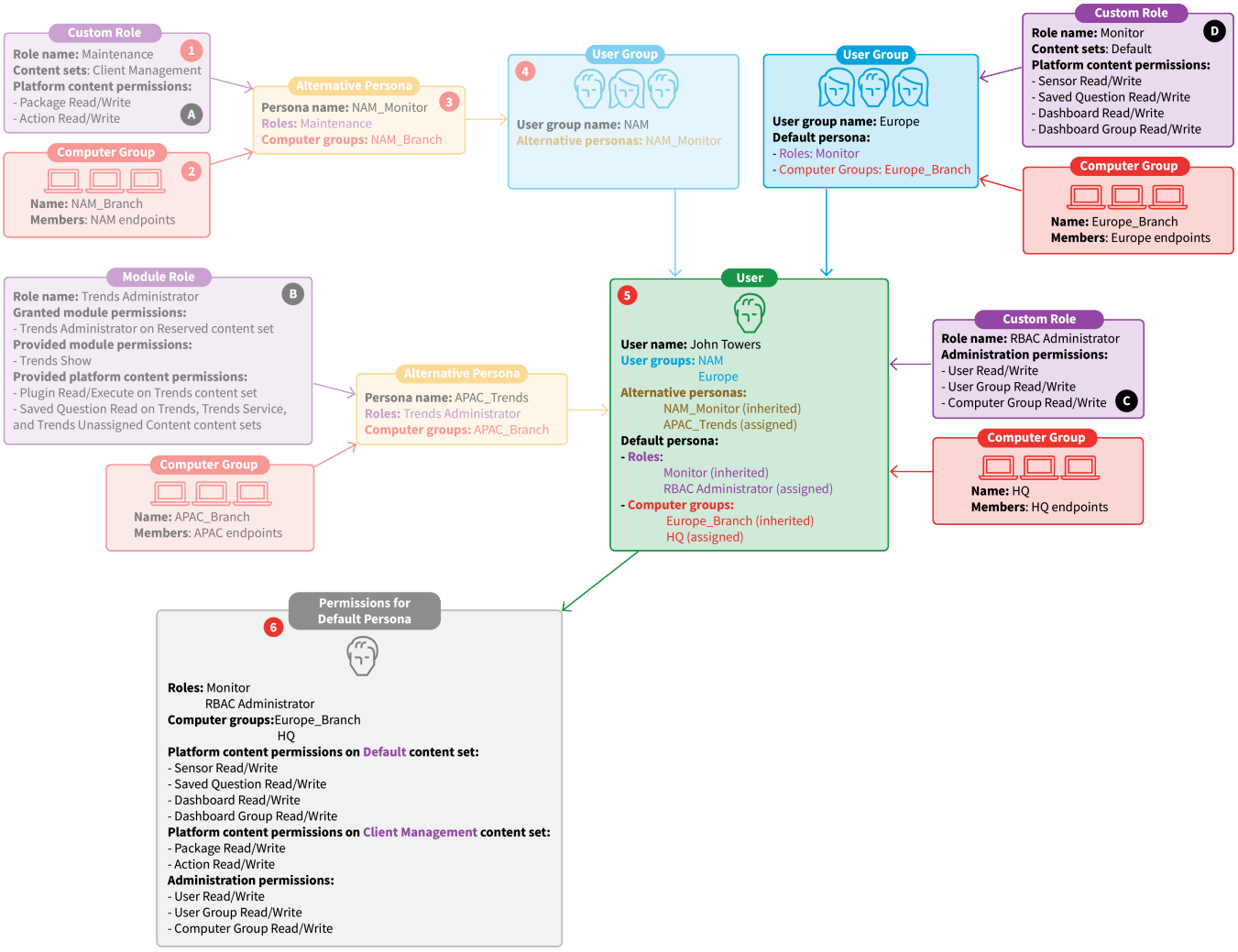
6. Sign in to Tanium Console to access the default persona

The default persona is active by default when a user sign in to Console. The default persona has permissions for all the roles and computer management groups that are directly assigned to the user account or that are inherited from the default personas of user groups.

In this example, the RBAC_Administrator role and HQ computer group are assigned to the default persona of the user. The user also inherits permissions from the Monitor role and Europe_Branch computer group that are assigned to the default persona of user group Europe.

© 2026 Tanium Inc. All Rights Reserved

Signing in as default persona



For more information, see Sign in to Console on page 49.

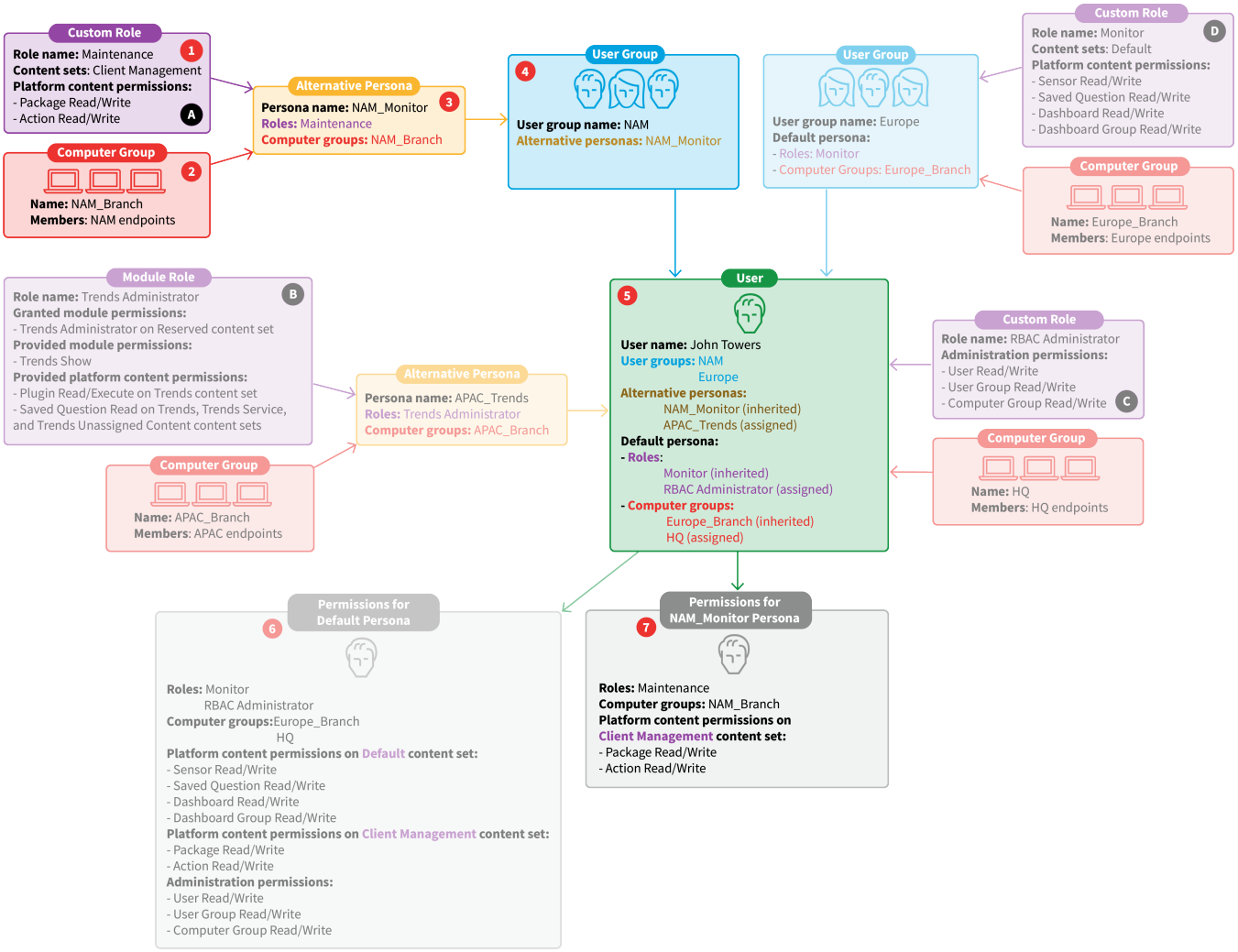
7. Switch to an alternative persona

When the user switches to an alternative persona for the Tanium Console session, that user has permissions only for the roles and computer management groups that are assigned to that persona.

In the following figure, the user selects the NAM_Monitor persona that is inherited from the NAM user group.

© 2026 Tanium Inc. All Rights Reserved

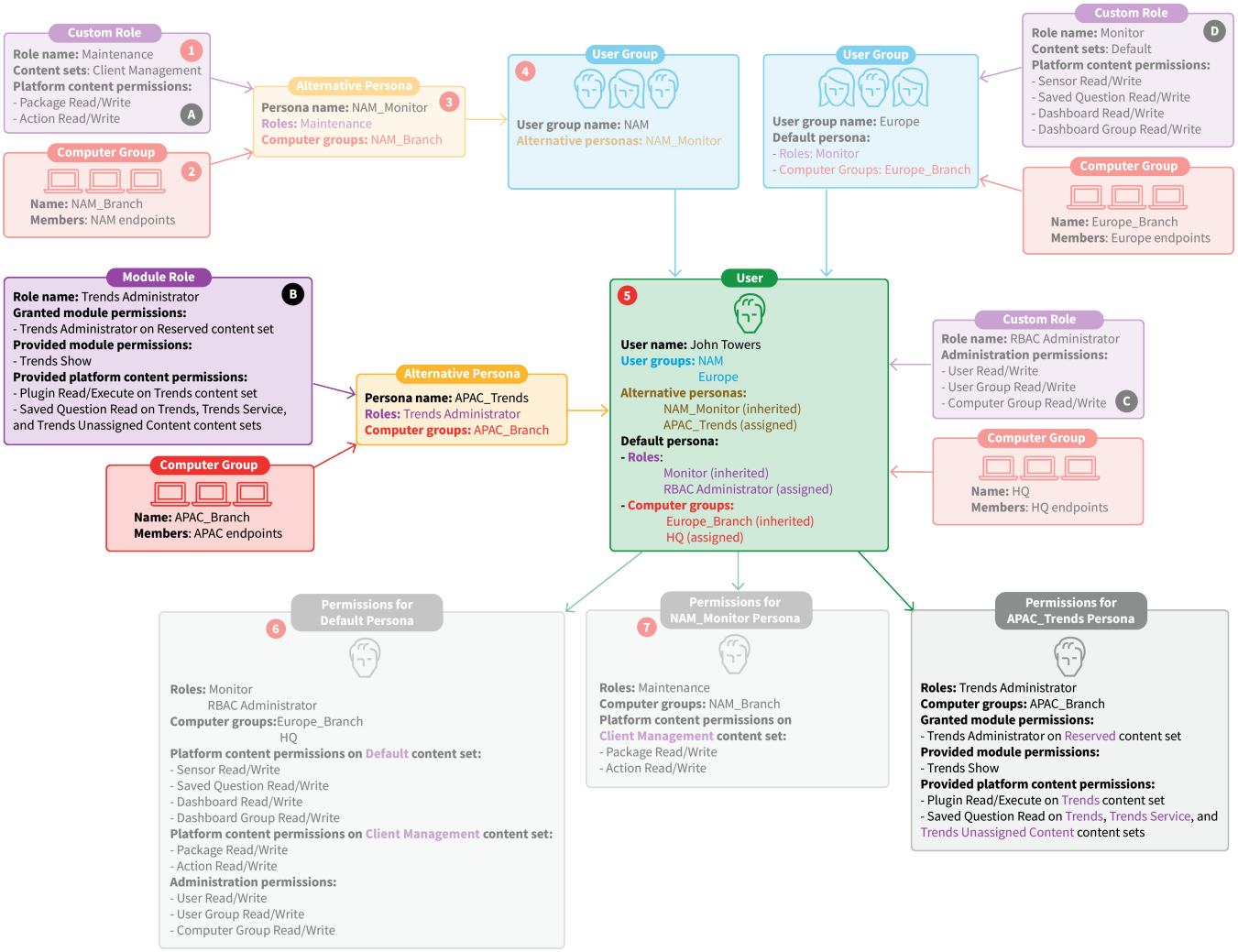
Selecting an alternative persona—example 1



In the next figure, the user selects the APAC_Trends persona that is assigned to the user account (default persona).

© 2026 Tanium Inc. All Rights Reserved

Selecting an alternative persona—example 2



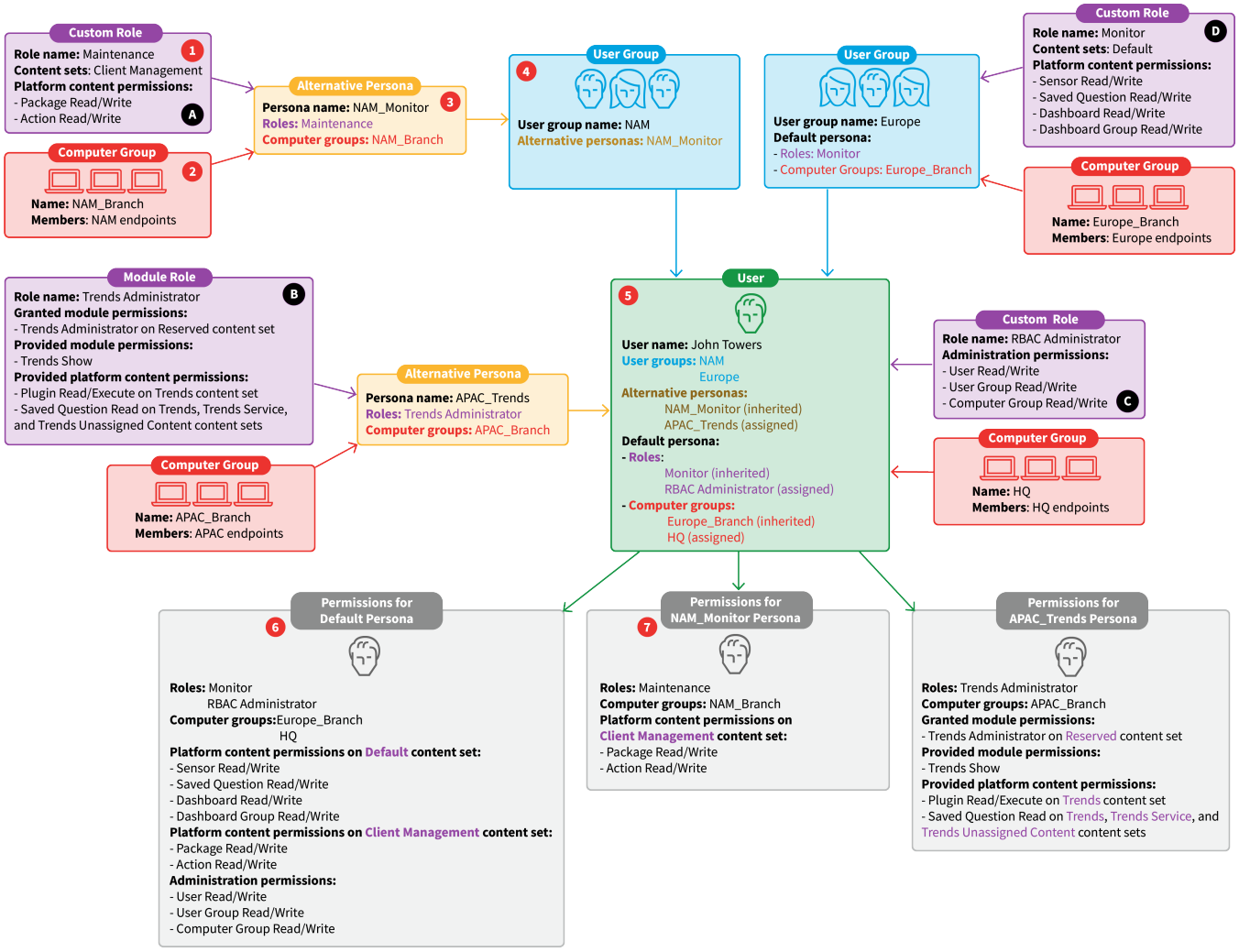
For more information, see Select a persona for your Console session on page 663.

Complete RBAC workflow

The following figure shows the complete workflow to configure the effective permissions of all three personas in this example.

© 2026 Tanium Inc. All Rights Reserved

RBAC configuration workflow



Plan your RBAC implementation

The following are important items and best practices to discuss with your team and Tanium Support (see Contact Tanium Support on page 724) when planning the RBAC implementation for your Tanium deployment.

- Naming convention on page 557
- Computer groups on page 557
- Content sets on page 559
- Roles on page 559
- Users and user groups on page 559

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

If you plan to import users and user groups from a Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server, do so before setting up RBAC. For more information, see Importing and authenticating users through LDAP on page 666.

BEST PRACTICE

For additional considerations and best practices, see the Tanium KB article 12 Things to Consider Before Planning Implementation of RBAC.

Naming convention

Before configuring custom roles, content sets, computer groups, and other RBAC objects, devise a naming convention that enables Tanium users to easily determine the purpose for each object and to distinguish it from similar Tanium-provided objects that are imported through Tanium solutions. Distinguishing custom objects is important because it is a best practice to avoid modifying Tanium-provided objects. For more information, see Tip 4: Limit customizations to Tanium content on page 138. For example, you can use the name of your organization as a prefix in the names of custom objects.

Computer groups

Consider the following best practices before you create custom computer management groups or filter groups for actions and questions.

MEMBERSHIP CRITERIA

Identify the sets of endpoints that you want to manage as a group for operations that Tanium users and solutions perform. Some user roles might be dedicated to certain functions, such as deploying patches to datacenter servers. In this case, you can create a computer group that targets those servers and assign the group to those users. Other operations might be restricted based on privacy laws that differ among locations, in which case you can create a computer group for each location.

For example, your organization might have separate users who are responsible for monitoring and managing endpoints in a particular regional office. For each region, you can create a computer group with a membership definition that includes all the endpoints in that region. If you use custom tags to define endpoint locations, a computer group for the Asia-Pacific (APAC) region might have the membership question `Custom Tags equals APAC`. After you assign that computer group to the corresponding user, that user can see results from all endpoints in the Asia-Pacific region for questions such as `Get Running Applications from all machines`. The user can also target the endpoints for actions, such as application updates.

RESOURCE USAGE FOR ACTIONS AND QUESTIONS

When a user issues a question or deploys an action, the Tanium Server sends it to endpoints within a message that includes all the computer groups that you assign to the user. Increasing the number and complexity of assigned computer groups increases the message size, which increases the networking and endpoint resources that the question or action consumes. The complexity and number of computer groups that you assign to an action group also increase the message size and therefore resource usage.

When you configure computer groups and assign them to users, personas, user groups, and action groups, the following best practices enable you to minimize the resource usage of questions and actions and to avoid unexpected targeting results:

© 2026 Tanium Inc. All Rights Reserved

- **Minimalistic assignments**
    - **Computer groups**: Assign only the computer groups that each user needs to perform the Tanium operations that are expected for the role of that user.

      For example, if a user has the authority to manage end-user systems but not servers, assign the **All Workstations** group but not the **All Windows** group, which includes Windows servers. As another example, instead of assigning the two groups **All Windows Servers - Physical** and **All Windows Servers - Virtual**, you can give a user the same management rights by assigning only **All Windows Servers**.
    - **Action groups**: When you configure an action group, assign only the computer groups that are necessary for the actions that you plan to deploy to that action group. If necessary, you can specify more computer groups and other filters in the **Targeting Criteria** of a specific action when you configure its settings. For more information, see Deploying actions and playbooks in Console and Interact on page 391.
- **Sensor- and tag-based groups**

  Define Computer group membership on page 614 using sensor-based filters instead of manually defined lists to enable granular control over which endpoints to include or exclude. You can achieve additional flexibility, while keeping the filtering clause simple, by defining computer groups with membership that is based on custom tags that you add to endpoints or remove as necessary. For more information, see Manage computer group membership through custom tags on page 619.
- **Precise membership expressions for fewer groups**

  One computer group with a precise membership expression is more efficient than multiple computer groups in which the combined membership exceeds what a user needs. For example, you might want to give a user management rights for all Windows endpoints that have x86 architecture. Instead of assigning the two groups **All Windows Servers - x86** and **All Windows Workstations - x86**, you can assign a single group with membership that is based on a sensor filter such as `"x64/x86?" starts with x86`.
- **Simple membership expressions**

  As much as possible, use simple expressions to define computer group membership. Complex expressions increase the processing load on endpoints. For example, you might want a computer group for Windows and macOS endpoints that use storage encryption. The membership expression `Storage Encryption Status equals "Encrypted"` is efficient because it selects only Windows and macOS endpoints, and only if they use storage encryption. By contrast, the expression `Is Windows equals true or Is Mac equals true` requires more sensors and is less precise because it selects Windows and macOS endpoints that might or might not use storage encryption. For more examples of complex expressions that increase the processing load, see Reference: Advanced question syntax in Console and Interact on page 731.
- **Negative targeting**

  As much as possible, avoid negative targeting in sensor-based filter expressions when you create computer groups with dynamic membership. Negative targeting is the use of negative conditions to target endpoints, such as expressions that use the filter operators `not contains`, `is not equal to`, and `does not match`. Negative targeting can be unpredictable and unintentionally include or exclude endpoints.
- **Maximum sensor or data age**

  Do not lower the default **Max Sensor Age** or **Maximum Data Age** for any sensor that defines endpoint membership in a computer group. For more information, see Best practices for saved questions on page 456.

© 2026 Tanium Inc. All Rights Reserved

NOTE

For more information about the options available for sensor filters in the membership expressions of computer groups, see Filter operators on page 733. For examples of regular expressions that you can use, see Use regular expression filters on page 739.

Content sets

Determine how to organize content set permissions for controlling access to specific data and deploying actions on endpoints. As a best practice, ensure that the content in any particular content set is similar to minimize the risk of assigning unintended permissions to user roles. You can organize content sets based on the following:

- **Capability**: Read or write permissions
- **Content type**: For example, saved questions, sensors, or packages
- **Subject matter**: For example, Tanium Client administration or Windows system administration

BEST PRACTICE

For content that is provided through Tanium solutions, keep the content objects in their original Tanium-provided content sets. To sustain this practice when moving content between content sets, create copies of Tanium-provided content and move the copies instead of the original versions. Contact Tanium Support before proceeding if you need to move original Tanium-provided content. For more information, see Contact Tanium Support on page 724.

Roles

The following are best practices for managing roles:

- **Configuration order**: Configure custom roles that specify solution permissions before configuring roles that specify platform content or administration permissions. Solution permissions allow access to a specific solution and often provide additional platform content and administration permissions.
- **Modularity**: When configuring roles, take advantage of their modularity and cumulative effect on user permissions. For example, instead of creating a role with all the permissions that a particular user needs, and creating another role with only slightly different permissions for another user, create several roles with smaller but unique permissions sets. You can then mix and match these minimalistic roles among various users to achieve the same effective permissions as individual roles that have comprehensive permissions. For more information, see View effective role permissions on page 588.

Users and user groups

LDAP SUPPORT

If you plan to import users and user groups from a Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server, set up the imports before you perform other RBAC tasks. The Tanium Server automatically synchronizes with the LDAP server every five minutes, and you can manually synchronize at any time. The synchronization updates the Tanium Server with any changes that

© 2026 Tanium Inc. All Rights Reserved

occurred on the LDAP server, including any new or deleted users, new or deleted user groups, and changes to group membership. Optionally, you can use an LDAP server to authenticate the imported users. For more information, see Importing and authenticating users through LDAP on page 666.

USER GROUP PERMISSIONS

Control permissions at the user group level as much as possible instead of at the user level. Assigning computer groups, roles, personas, and users to user groups minimizes the administrative effort required to update your RBAC configuration. For example, instead of modifying role assignments for the personas of each user who might join or leave your organization, or whose responsibilities might change, you can configure user groups that use sensor-based filters to dynamically adjust group membership when such changes occur.

USER PERMISSIONS

To identify which permissions are needed, consider what each team in your organization needs to accomplish through the Tanium system. In particular, consider the following:

- **Solution access**: Which users require access to which Tanium solution workbenches and solution content?
- **Administrator permissions**: Do you want to use the **Administrator** reserved role to assign full administrator permissions to a few users or assign granular administration permissions that allow or deny page-specific read and write access to the **Administration > Configuration** pages?

SAML AUTHENTICATION

You can use a Security Assertion Markup Language (SAML) identity provider (IdP) to provide single sign-on authentication for Tanium Console users. For more information, see Enabling SSO through SAML on page 684.

© 2026 Tanium Inc. All Rights Reserved

Managing access to content through content sets

Content sets overview

A *content set* is a group of Tanium content objects to which a permission applies. You apply content set permissions through role configurations that you assign to users. The association between content sets and permissions ensures that only authorized users can use content that might have a significant impact on managed endpoints.

For example, the **Core Content** set contains sensors, packages, saved questions, dashboards, and filter groups that you use for many common Interact tasks. One such package is **Restart Service - ||Service Details_Service Name||**, which you can use to restart a service that is stopped on Windows endpoints. You require **Package read** permission on the **Core Content** set to deploy an action with that package.

Tanium provides several predefined content sets through Tanium modules, shared services, and content-only solutions. You can create a content set to contain custom content or to accommodate RBAC changes in your organization. For example, you can create a content set for sensors and packages related to Tanium Client maintenance, and then configure roles that allow a wide group of users read access to the content but allow write access to a smaller group of users.

BEST PRACTICE

Understand the best practices for content sets before you create or edit custom sets. For more information, see Content sets on page 559.

NOTE

For more information and procedures related to specific content types, see Solution content overview on page 418.

For the user role permissions required to manage content sets, see Manage content sets on page 102.

Role permissions for content sets

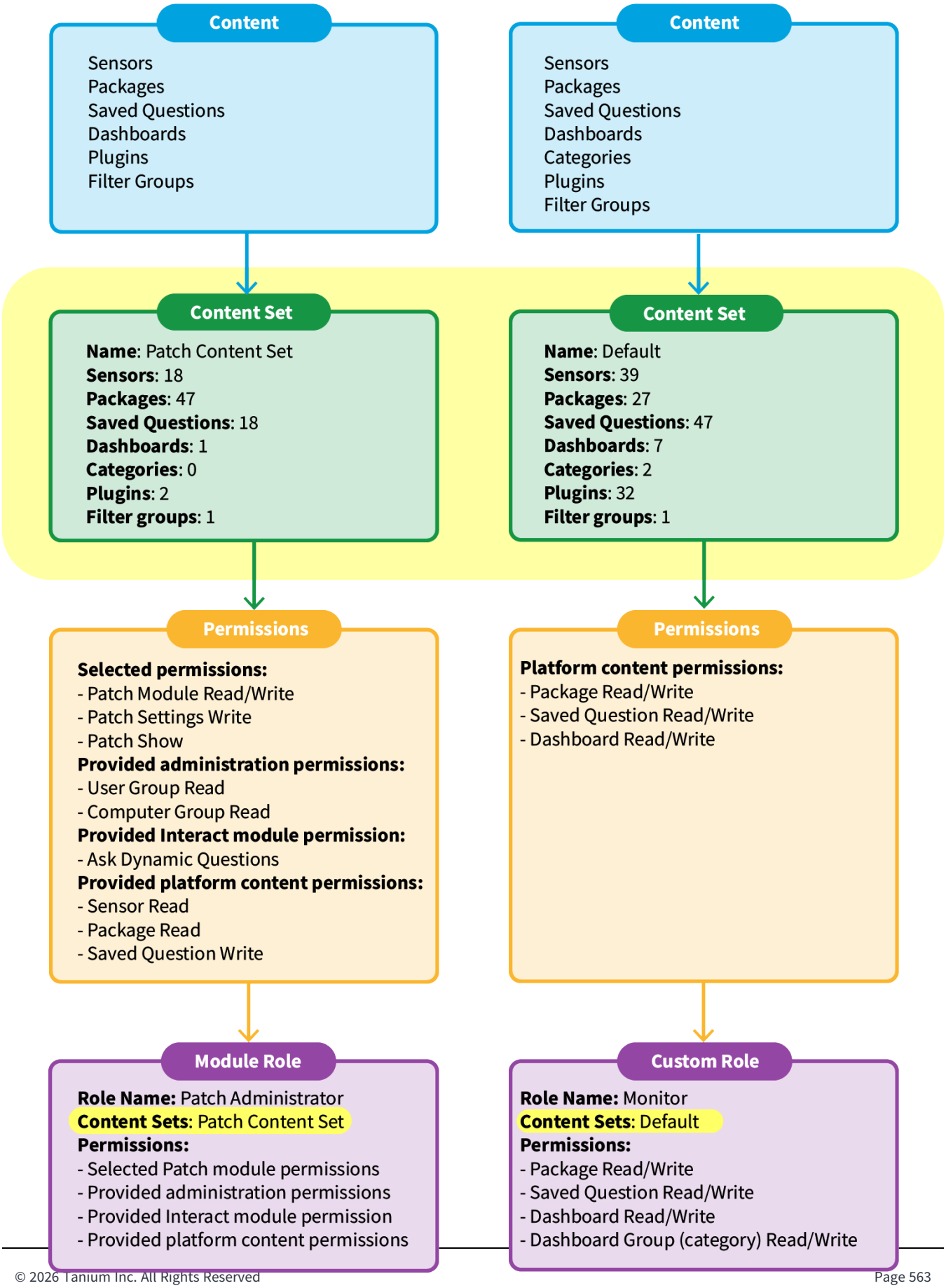
You can assign content to only one content set. A role can specify permissions for multiple content sets. Configure custom roles to define platform content permissions for content that is used across all Tanium solutions and solution permissions for solution-specific content. Tanium also provides pre-defined solution roles for solution-specific content.

The following figure shows the relationship between contents sets and content, permissions, and roles.

© 2026 Tanium Inc. All Rights Reserved

Content sets in relation to content, permissions, and roles

© 2026 Tanium Inc. All Rights Reserved



© 2026 Tanium Inc. All Rights Reserved

To manage content set permissions for a role, see Manage content set permissions for a role on page 605.

View content set details

Viewing content set attributes (columns) can help you manage RBAC for your organization. For example, the **Used By** column indicates which Tanium solutions use the content in each content set, which can help you decide whether it makes sense to move content between sets.

> NOTE
>
> If the **Used By** column displays no value for a content set, that means its content is used across the Tanium Core Platform and is not solution-specific.

1. From the Main menu, go to **Administration > Permissions > Content Sets**.

   The **Content Sets** grid shows attributes (such as **Name**) to identify each content set and to indicate which solutions use its content.

   > NOTE
   >
   > The **Used By** column shows `Data` to indicate Tanium Reporting uses the content.

2. (Optional) Enter a search string in the **Filter items** field to find specific content sets based on **Name** or **Description** values.

3. Click the **Name** of the content set for which you want to review content and permissions.

   > NOTE
   >
   > A content set might list two types of dashboards:
   >
   > - **Interact dashboard**: This is a group of related saved questions. The **Preview Content Sets** page use an icon to identify this dashboard type. For more information, see Interact dashboards and categories on page 457.
   > - **Reporting dashboard**: This is a group of related panels that provide charts (visualizations of report data), text, and action deployment options. For more information, see Tanium Reporting User Guide: Dashboards.

4. Expand the content type that you want to review.

   The top grid lists all the objects of that type in the content set.

   The bottom grid displays the Roles, Users, and User Groups with permissions that are associated with the content.

5. When you finish reviewing, click **Exit** to return to the **Content Sets** summary page.

Create a content set

Create custom content sets if your organization has RBAC requirements that existing sets do not satisfy. For example, you might create a content set to contain custom packages that only privileged users can use.

© 2026 Tanium Inc. All Rights Reserved

NOTE

After you save a content set, you cannot edit its name or description, but you can move its content to another set.

1. From the Main menu, go to **Administration > Permissions > Content Sets** and click **New Content Set**.
2. Enter a **Content Set Name** of up to 255 characters and an optional **Description**, and then click **Save**.
3. Perform the following tasks to assign content to the content set:
    - Move content between content sets on page 565
    - Specify a content set when you create or edit content:
        - Managing sensors for collecting endpoint data on page 421
        - Managing packages for platform actions on page 442
        - Managing saved questions in Console and Interact on page 455
        - Managing filter groups for filtering questions and results on page 476

Move content between content sets

Move custom content between content sets to accommodate RBAC changes in your organization. For example, if a sensor collects sensitive information from endpoints, you might want to move that sensor to a content set that only highly privileged user roles can access.

To move content between content sets, you require the **Administrator** or **Content Set Administrator** reserved role or a role that has write permission on the content and content sets. You can move content between any content sets except:

- The **Reserved** content set, which includes fundamental sensors that the Tanium Core Platform uses.
- Certain Tanium solution-based content sets.

Before you begin

Before moving content, be sure that you understand how the move affects workflows. For example, if a user configures a scheduled action, and you later move the associated package to a content set for which that user does not have permission, the Tanium Server does not deploy the action.

TIP

Content attributes might influence the content set you that you assign. For example, if a sensor description indicates the sensor collects hardware information, you would not move it to a set for virtualization-related content. Use the **Administration > Content** pages to review content attributes. Optionally, you can also reassign content sets through those pages by editing the content. For more information, see:

© 2026 Tanium Inc. All Rights Reserved

TIP

- Edit a sensor on page 429
- Edit a package on page 450
- Edit a saved question on page 465
- Managing filter groups for filtering questions and results on page 476

Move content to a different content set

Perform the following steps to move content.

TIP

As a workaround for solution-based content sets that do not allow moving content, you can clone the content, move the clones to other content sets, and instruct users to use the clones in their workflows instead of the original content.

1. From the Main menu, go to **Administration > Permissions > Content Sets**.
2. Click the **Name** of the content set that contains the content you want to move.
3. Expand the content type and select the content that you want to move.
4. Click **Move to Content Set**, select the target content set, and click **Confirm**.

Export or import content sets

Export content sets

Export content sets as a file in the format required for your workflow:

- **CSV**
  You can use any application that supports CSV format to display the same content set attributes (columns) as the Console **Content Sets** grid shows and then customize the display. For example, you can use Microsoft Excel to create charts based on content set attributes.
- **JSON**
  You can export multiple content set configurations as a JSON file. Exporting configurations is useful if you want to import them into another Tanium environment. You must be assigned a role with the **Export Content** permission to export a JSON file. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.

Perform the following steps to export content sets:

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Permissions > Content Sets**.
2. (Optional, CSV exports only) To add or remove attributes (columns) for the CSV file, click Customize Columns  in the grid and select the attributes.
3. Select rows in the grid to export only specific content sets. If you want to export all content sets, skip this step.
4. Click Export .
5. (Optional) Edit the default export **File Name**.

   The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.
6. Select an **Export Data** option: **All** content sets in the grid or just the **Selected** content sets.
7. Select the file **Format**:
   - **List of Content Sets - CSV**
   - **Content Set Definitions - JSON** (**Administrator** or **Content Set Administrator** reserved role only)
8. Click **Export**.
   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

Import content sets

Importing is useful if you want to copy content set configurations from another Tanium environment. You can import content sets and other content as a JSON or XML file.

You must be assigned a role with **Import Signed Content** permission to import content files through the following steps.

1. (Non-Tanium-provided content only) Digitally sign the content file and ensure a public key is in place to validate the signature. For more information, see Authenticating content files on page 482.

   You do not have to generate keys or signatures for Tanium-provided solutions. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process.

   If you plan to import a file that another user signed, you can first perform an integrity check on the file. For more information, see Verify content file signatures on page 487.
2. From the Main menu, go to any of the following **Administration** pages:
   - **Configuration > Solutions**
   - **Permissions > Filter Groups**
   - Under **Content**, select **Sensors**, **Packages**, or **Saved Questions**
   - Under **Actions**, select **Scheduled Actions**, **All Pending Approvals**, or **Actions I Can Approve**

© 2026 Tanium Inc. All Rights Reserved

3. Select an **Import** option based on the source of the content:
    - **Import > Import Files**: Perform one of the following steps to select one or more files:
        - Drag and drop files from your file explorer.
        - Click **Browse for File**, select the files, and click **Open**.
    - **Import > Import URL**: Enter the URL in the **Import URL** field, and click **Import**.
4. For each file, expand  the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, **Include content set overwrite** is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Install**.

Delete a content set



Do not delete the predefined content sets that Tanium solutions provide. When you import solution updates, the update process restores any predefined content sets that users have deleted.

Delete a custom content set only if it is no longer needed to control permissions for accessing content.

You must empty a content set configuration before you can delete it. You have the following options to empty a content set:

- Move its content to another set. For more information, see Move content between content sets on page 565.
- Delete its content. For more information, see Managing content on page 419.

Perform the following steps when you are ready to delete a content set:

1. From the Main menu, go to **Administration > Permissions > Content Sets** and click the content set **Name**.
2. Click **Delete Content Set**.

© 2026 Tanium Inc. All Rights Reserved

Managing access permissions through roles

Roles overview

In the context of Tanium role-based access control (RBAC), a role assigns *allow permissions* to specify allowed activities or assigns *deny permissions* to specify prohibited activities. You assign roles to users, user groups, and personas to control what users can see and do with Tanium solutions. For example, you can configure a role that allows bypassing action approval and assign it only to users who have the authority to deploy actions without approval. For more information, see Roles and permissions on page 544.

IMPORTANT

If you plan to import users and user groups from a Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server, do that before configuring or assigning roles. For more information, see Importing and authenticating users through LDAP on page 666.

BEST PRACTICE

Understand the best practices for roles before you create or edit custom roles. For more information, see Roles on page 559.

NOTE

To add, edit, or delete roles, you require the **Administrator** or **Content Set Administrator** reserved role. However, a **Content Set Administrator** cannot manage the assignment of personas or reserved roles to users and user groups.

If Tanium Console displays RBAC errors, such as `RBACInsufficientPrivilege`, see Troubleshoot permission issues on page 713.

Custom and system roles

The Tanium implementation of RBAC supports two role categories, which the **Administration > Permissions > Roles** page distinguishes with icons in the **Role Name** column: system roles and custom roles.

CUSTOM ROLES

You can create, edit, or delete custom roles, which allow or deny any combination of administration, platform content, and solution permissions. For more information, see Configure a custom role on page 586.

SYSTEM ROLES

Tanium provides predefined system roles that you cannot edit or delete. These roles include:

© 2026 Tanium Inc. All Rights Reserved

- **Solution roles**

  These roles allow or deny permissions for access to solution workbenches, features, and content sets. Some solution permissions automatically enable additional *provided permissions*. For example, the **Patch Module** write permission automatically grants the **Ask Dynamic Questions**, which is a solution permission for Tanium Interact.

- **Reserved roles**

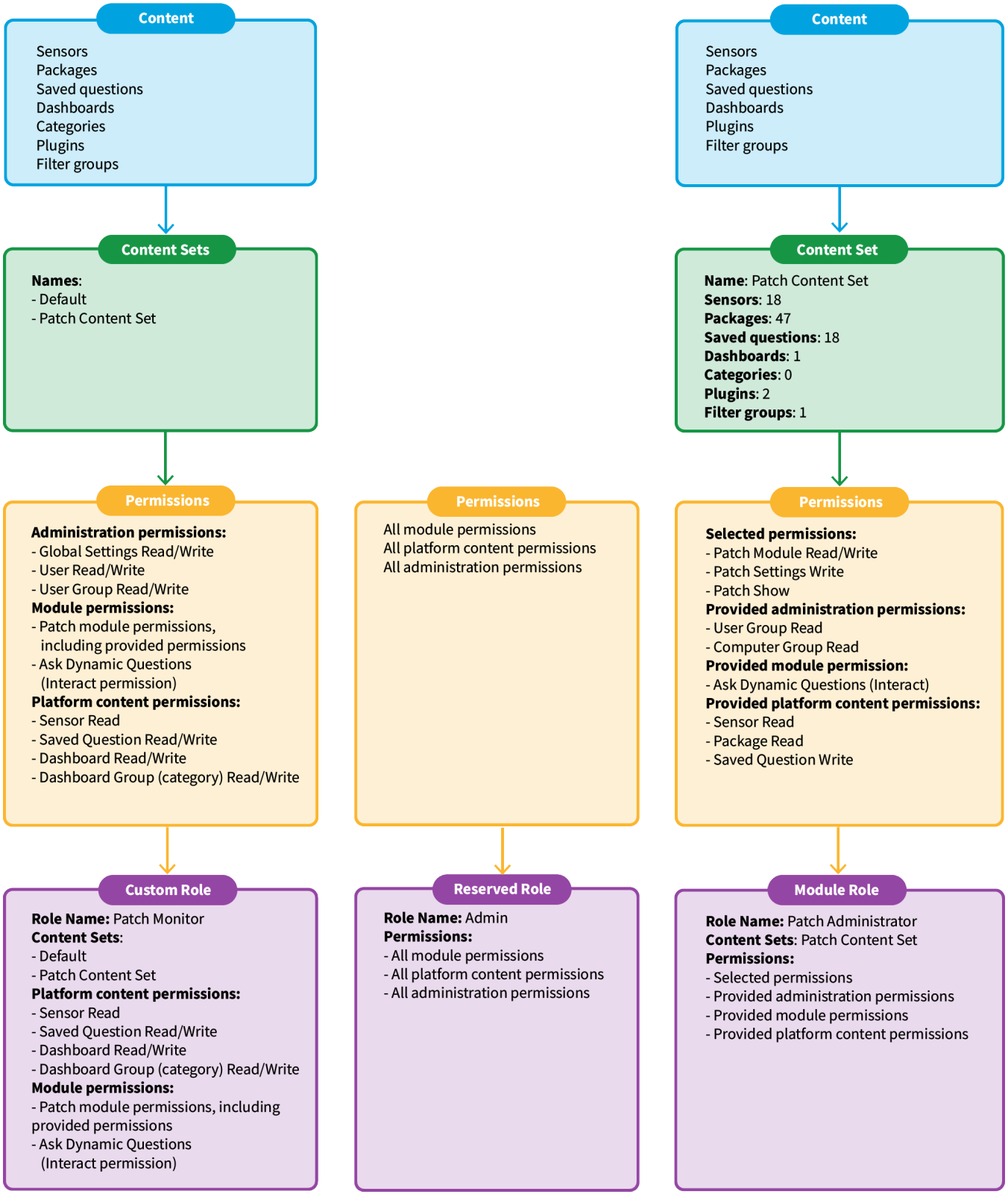
  These roles assign permissions for a range of tasks that, in many organizations, are commonly exclusive to a few users. For example, organizations typically have a small set of users who oversee all Tanium operations and require the full administrative permissions that the **Administrator** reserved role provides. For more information, see Reserved roles on page 581.

Role components

The following figure shows the configurable components of roles, along with example permissions and the order in which you assign the components:

© 2026 Tanium Inc. All Rights Reserved

Components and assignments in role configurations



Note the following considerations when you configure and assign roles for these RBAC components:

© 2026 Tanium Inc. All Rights Reserved

- **Cumulative assignments**

  Roles have a many-to-many relationship with users, personas, and user groups. For example, all Tanium Interact users can have the predefined **Interact Show** role, and each of those users can have additional custom roles that provide access to the sensors and questions that they use in Interact. Similarly, you can configure permissions for the same content set across multiple roles and each role can specify permissions across multiple content sets.

- **User groups**

  Users and personas inherit roles from the user groups that you assign those users and personas. For more information, see Inherited roles on page 580.

- **Personas**

  For a given Tanium Console session, only the permissions of the currently selected persona are available to a user, even if multiple personas are assigned to that user or to the user group in which the user is a member. For more information, see Managing role and computer group permissions through personas on page 655.

- **Computer groups**

  Roles control access to filter groups (see Managing filter groups for filtering questions and results on page 476) but not to computer management groups (see Manage computer management groups on page 103) or action groups (see Targeting actions through action groups on page 400). However, roles do control the permissions that you require to view, add, edit, and delete computer group and action group configurations.

For more information about how roles relate to content sets, personas, users, user groups, and computer groups, see RBAC overview on page 544.

Allow and deny roles

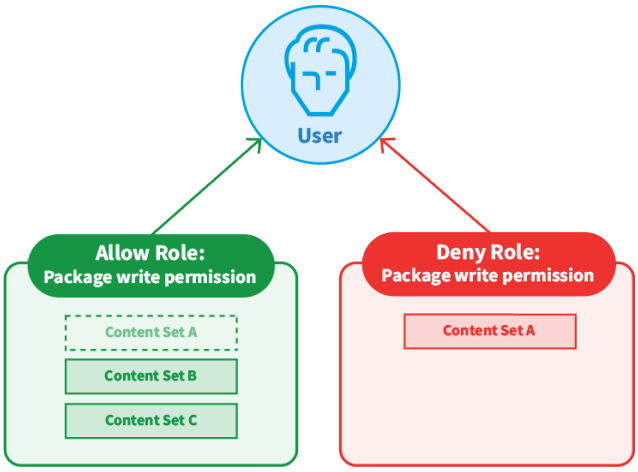
On the **Roles** page, the **Type** column indicates if a role allows or denies permissions. You can assign multiple allow or deny roles to a user or user group. The Tanium Server bases the effective permissions of a user or group on the cumulative effect of all the roles that are assigned to that user or group: all explicitly granted or implicitly provided allow permissions minus explicit deny permissions.

You can view the View effective role permissions on page 588 of a user or user group in Tanium Console.

In custom roles, a permission and content set in the deny role must match a permission and content set in the allow role to negate the allow permission. In the following example, the deny **Package write** permission on Content Set A matches the allow **Package write** permission on Content Set A, so the allow permission is negated.

© 2026 Tanium Inc. All Rights Reserved

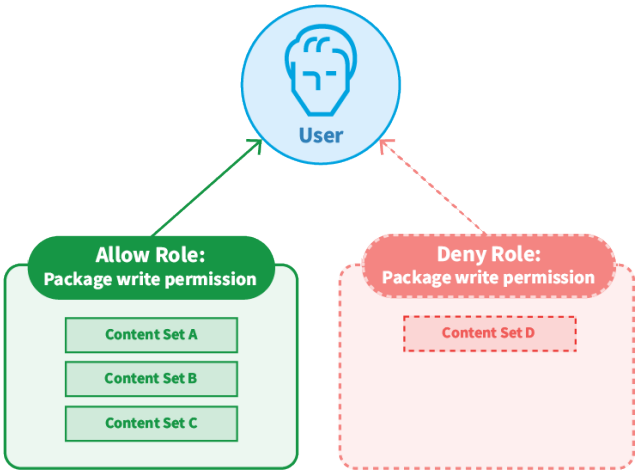
Example: Allow and deny roles on content set permissions (match)



© 2026 Tanium Inc. All Rights Reserved

In the following example, the deny **Package write** permission on Content Set D does not match any allow permissions. Therefore, the deny permission has no impact on the effective permissions of the user.

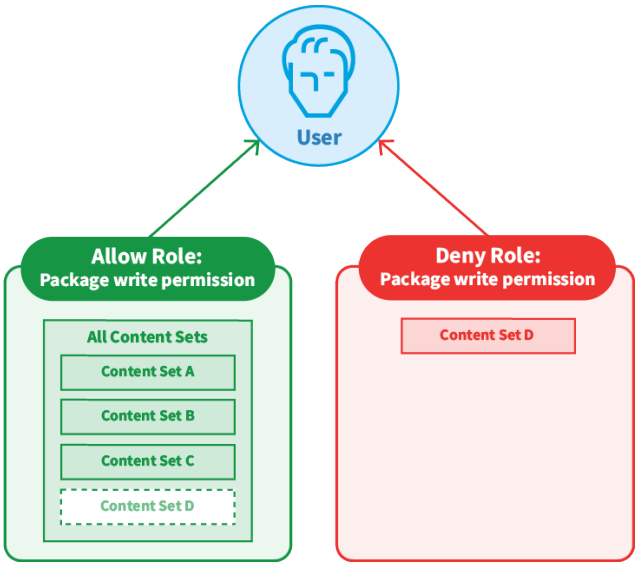
Example: Allow and deny roles on content set permissions (no match)



© 2026 Tanium Inc. All Rights Reserved

When you assign content sets to permissions in custom roles, the **Add all Content Sets that exist or will exist to the permissions** option is equivalent to listing every content set. The following figure illustrates an example where the deny **Package write** permission on Content Set D has an effect.

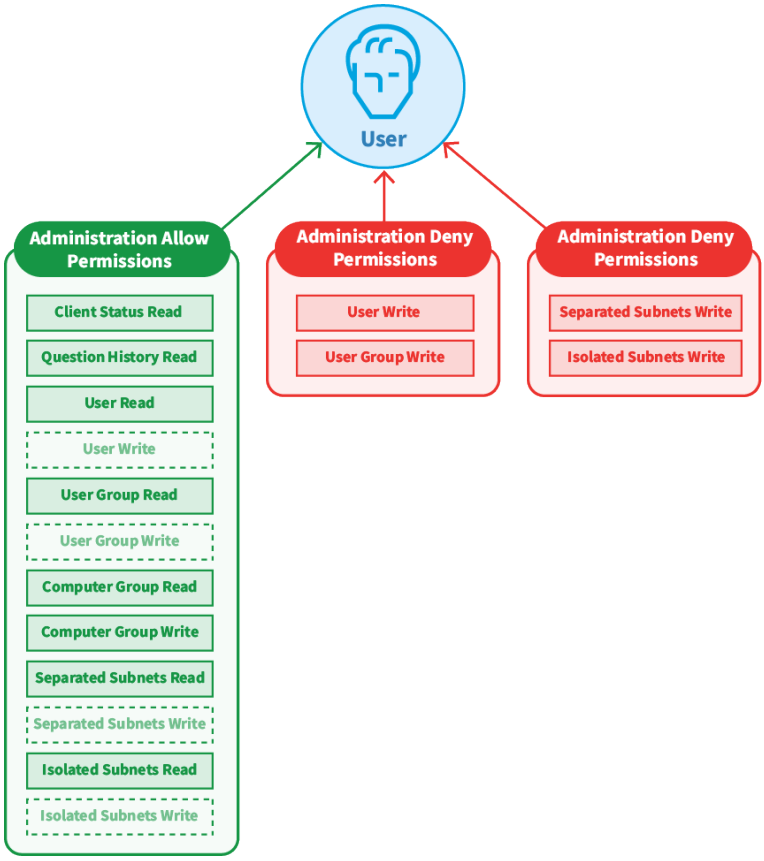
Example: Add All Content Sets option



© 2026 Tanium Inc. All Rights Reserved

Allow and deny matching also applies to administration permissions. In the following example, the user has one allow role and two deny roles that specify administration permissions. The Tanium Server factors out exact matches between allow and deny permissions. The user has all of the capabilities that the allow role specifies, minus the capabilities that the deny roles specify.

Example: Allow and deny roles on administration permissions



Provided role permissions

Some permissions automatically provide additional permissions because of dependencies. For example, the **Package write** permission that enables creating packages depends on the **Package read** permission that enables accessing the **Packages** page. Similarly, the **Interact Execute action** permission that enables action deployment depends on the **Action write** permission that enables action configuration.

NOTE

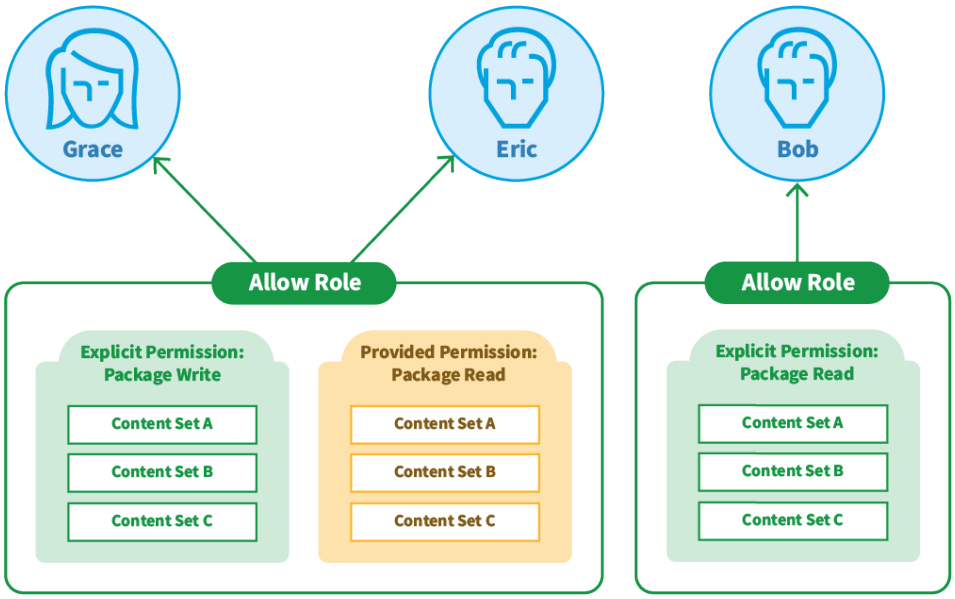
The configuration pages for roles, users, user groups, and personas use different icons to distinguish between explicitly assigned and implicitly provided permissions. For more information, see View effective role permissions on page 588.

© 2026 Tanium Inc. All Rights Reserved

Dependencies between read-write permissions

In allow roles, every write permission implicitly provides the associated read permission. In the following example, the custom role that is assigned to Eric and Grace has the **Package write** permission on the specified content sets, and therefore the configuration does not need to specify the **Package read** permission. A role that has only the **Package read** permission on the same content set is created for users who must have read-only permissions, like Bob in this example.

Example: Users effectively have both read and write permissions

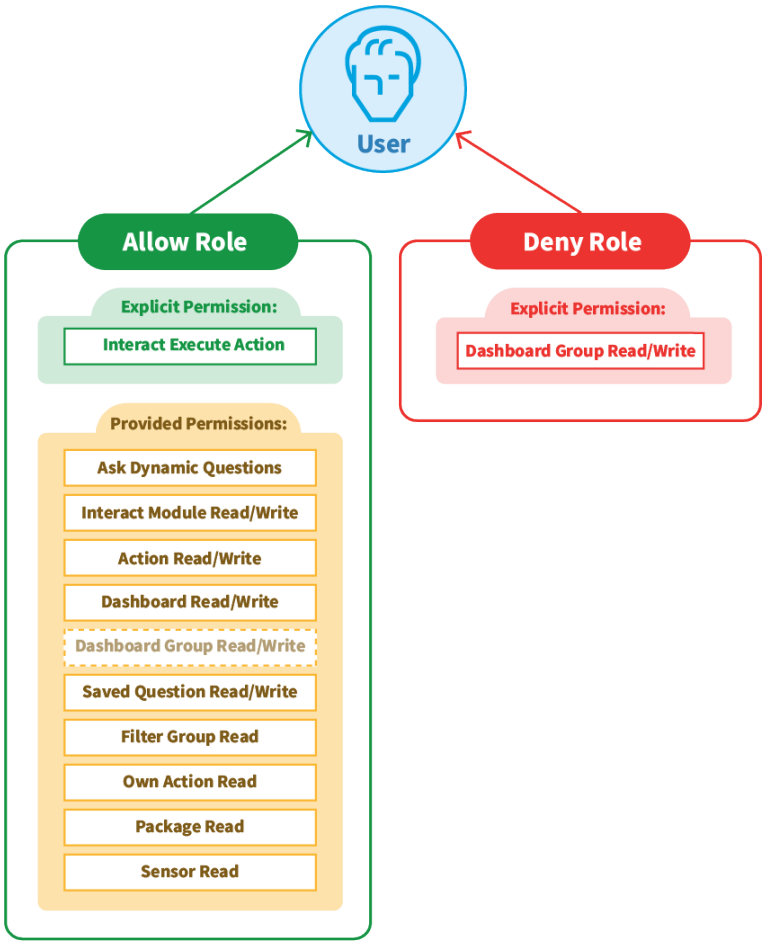


Task-based dependencies among permissions

Some solution permissions and platform content permissions implicitly provide additional permissions because of dependencies that are unrelated to read-write associations. For example, the **Interact Execute action** permission provides several additional permissions that are required to deploy and configure actions.

© 2026 Tanium Inc. All Rights Reserved

Example: Permission dependencies

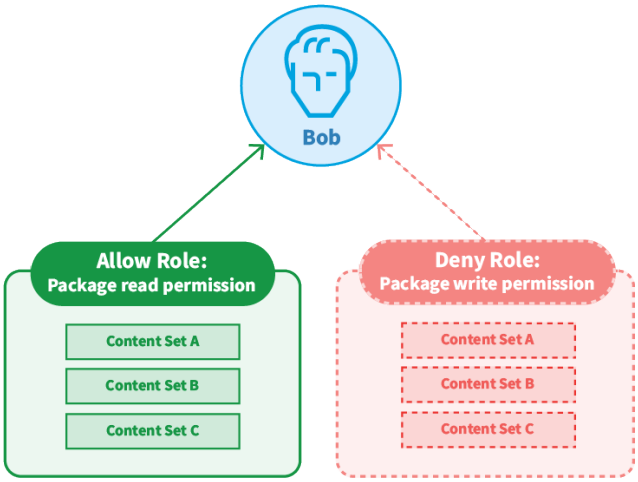


Interaction between deny and provided permissions

© 2026 Tanium Inc. All Rights Reserved

Deny roles do not implicitly provide associated permissions. For deny roles to have an effect, they must explicitly specify permissions and those permissions must exactly match the permissions that an allow role specifies. For example, if a deny role specifies that **Package write** permission is denied on a content set, the role does not also deny **Package read** permission. In the following example, the deny role permissions do not exactly match any allow role permissions. Therefore, the deny role is disregarded and Bob still has **Package read** permission on the specified content sets.

Example: User effectively has read permissions



If the roles assigned to a user conflict with respect to implicitly provided permissions and deny permissions, the provided permissions take precedence to ensure that permission assignments work as intended. To ensure the correct precedence, the Tanium Server evaluates permissions in the following order:

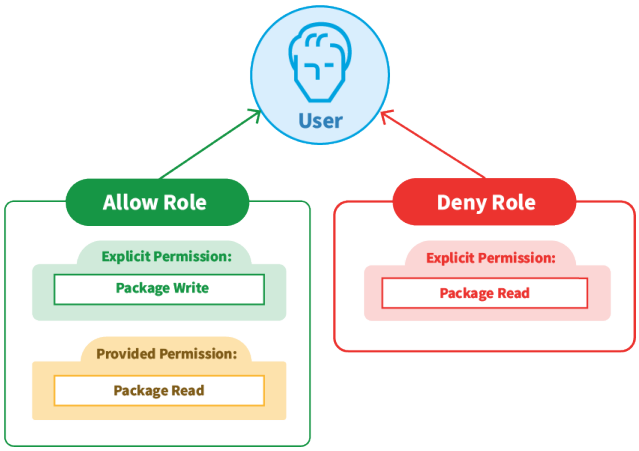
1. Allow permissions are granted.
2. Deny permissions deny allowed permissions.
3. Permissions that the allow permissions implicitly provide are granted.

For example, the Tanium Server performs the following processing if you assign a role that allows **Package write** permission and another role that denies **Package read** permission:

1. Grants **Package write** permission and its implied **Package read** permission.
2. Denies **Package read** permission.
3. Re-grants **Package read** permission because **Package write** provides it. Re-granting the read permission is necessary because a user cannot perform write functions (add, edit, or delete packages) unless that user can also perform the read function (view packages).

© 2026 Tanium Inc. All Rights Reserved

Example: User effectively has read and write permissions



Provided permissions on content sets

Provided permission automatically apply to content set assignments. For example, if you assign the **Action write** permission to the **Base** content set, it automatically provides **Package read** permission for the **Base** content set. If you assign **Sensor write** permission to the **Default** content set, it automatically provides **Sensor read** permission for the **Default** content set.

Inherited roles

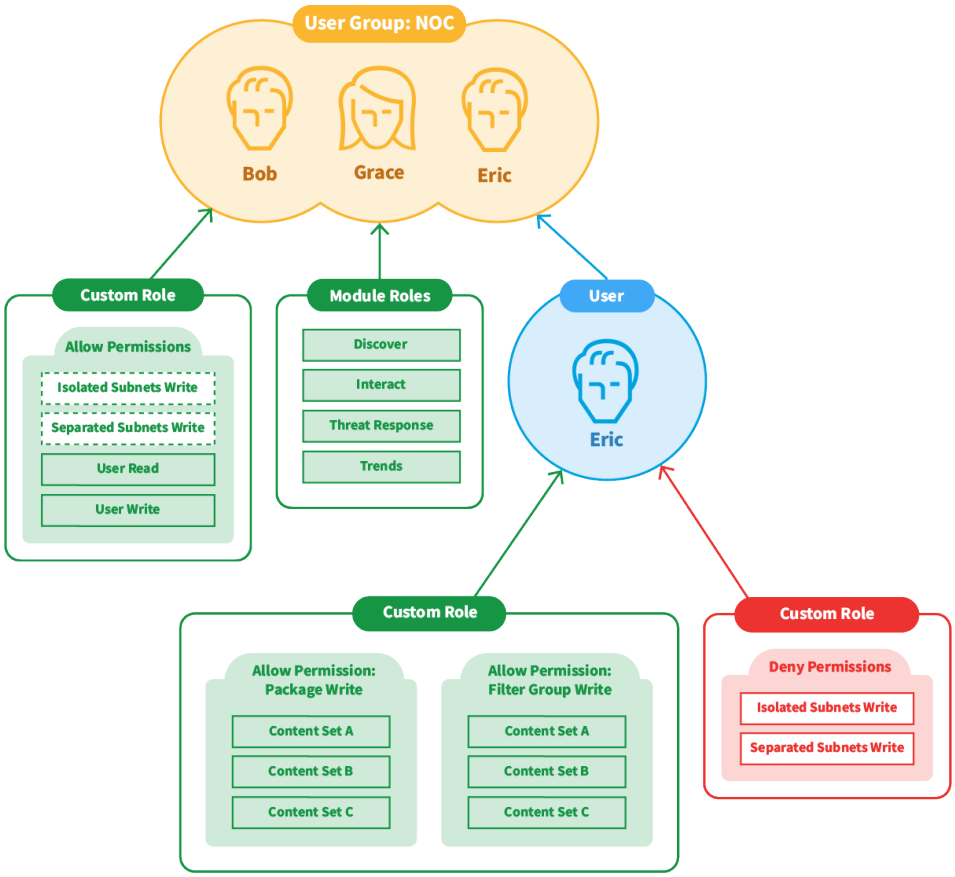
Users inherit role permissions from their user groups. In the following example, a user named Eric inherits permissions from the roles that are assigned to the NOC user group. He also has permissions that are assigned directly to his user account. The Tanium Server enforces the net effect. In this example, even though Eric inherits the **Isolated Subnets write** permission and **Separated Subnets write** permission from the user group, the deny role that is assigned directly to his user account negates those permissions. Because no deny roles are assigned to the accounts of Bob and Grace, they have all the permissions that are inherited from the user group, including **Isolated Subnets write** and **Separated Subnets write** permissions.

NOTE

If you assign an alternative persona to a user group, that persona does not inherit role permissions from the group. Persona assignments to a user group just enable the users in that group to select the persona for a Tanium session.

© 2026 Tanium Inc. All Rights Reserved

Example: Inherited roles



Roles for personas

When you select an alternative persona for a Tanium session, you can select any persona that is assigned to your user account or to a user group in which you are a member. However, an alternative persona does not have permissions derived from the roles that are assigned to your user account (default persona) or user groups. You must assign roles directly to an alternative persona to provide permissions to that persona. For more information, see View effective role permissions for a persona on page 658.

Reserved roles

The predefined reserved roles assign permissions for a range of tasks that, in many organizations, are commonly exclusive to a few users. For example, organizations typically have a small set of users who oversee all Tanium operations and require the full administrative permissions that the **Administrator** reserved role provides.

Reserved roles can include special permissions, such as managing the Tanium license, that are not available to non-reserved roles. In addition to the special permissions, reserved roles can have some or all of the platform content, administration, and solution permissions that are associated with other roles. You cannot edit or delete reserved roles. Special logic applies when you assign both a reserved role and non-reserved role to a user or user group, as described in the following sections.

© 2026 Tanium Inc. All Rights Reserved

Administrator reserved role

Assign the **Administrator** reserved role to users who manage all Tanium content, solutions, and administrative functionality.

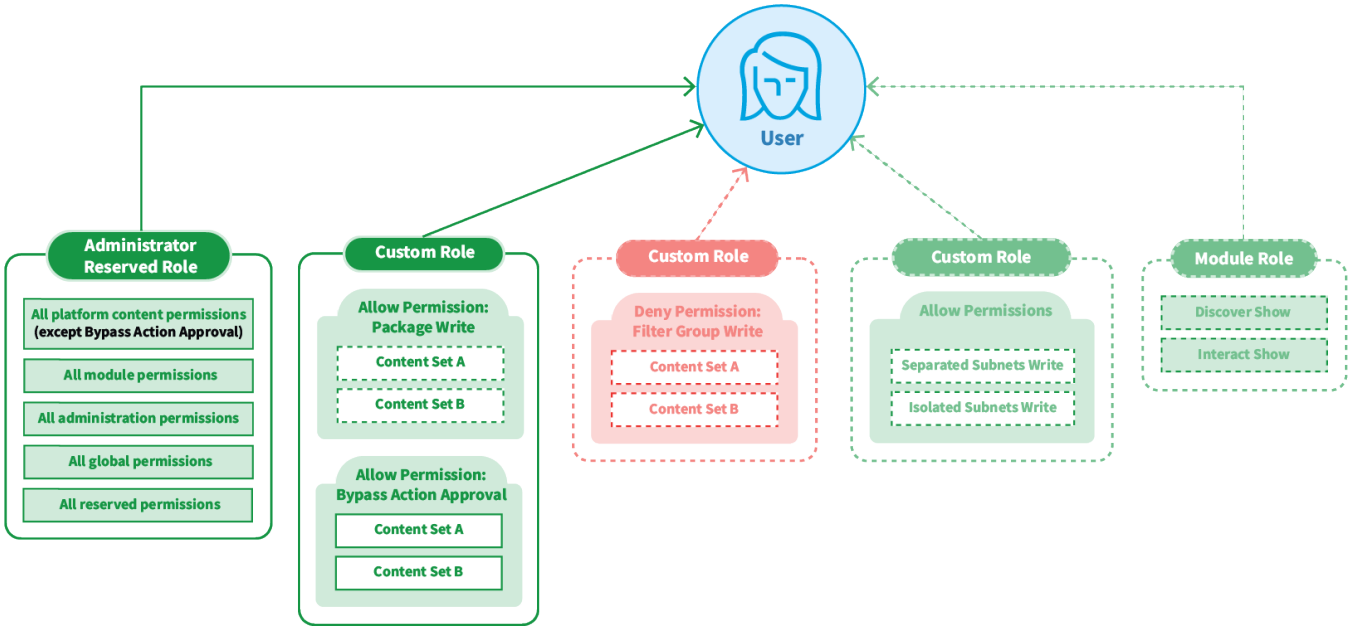
This role can perform the following tasks:

- Import, export, update, uninstall, and use all Tanium solutions
- Configure all Tanium Core Platform settings (such as bandwidth throttles) and customize Tanium Console
- Manage the Tanium license and manage trust among platform components (such as Tanium Servers and Tanium Zone Servers)
- View, create, edit, and delete all RBAC configurations, including users, user groups, personas, roles, computer groups, LDAP server configurations, SAML IdP connections, and API tokens
- View, create, edit, delete, import, and export all content configurations such as sensors, packages, and actions

When you assign the **Administrator** role, other allow roles are superfluous and deny roles are ineffective, with the following exceptions:

- **Bypass Action Approval**: A custom role with the **Bypass Action Approval** permission does have effect when it is assigned to a user who has the **Administrator** reserved role. The **Administrator** reserved role does not have this permission by default. Due to the sensitive nature of bypassing approval, you must explicitly assign this permission in all cases.
- **Deny All**: The Deny All reserved role on page 584 negates all the permissions of the **Administrator** reserved role.

Administrator reserved role



Content Set Administrator reserved role

Assign the **Content Set Administrator** reserved role to users who manage content set and role configurations.

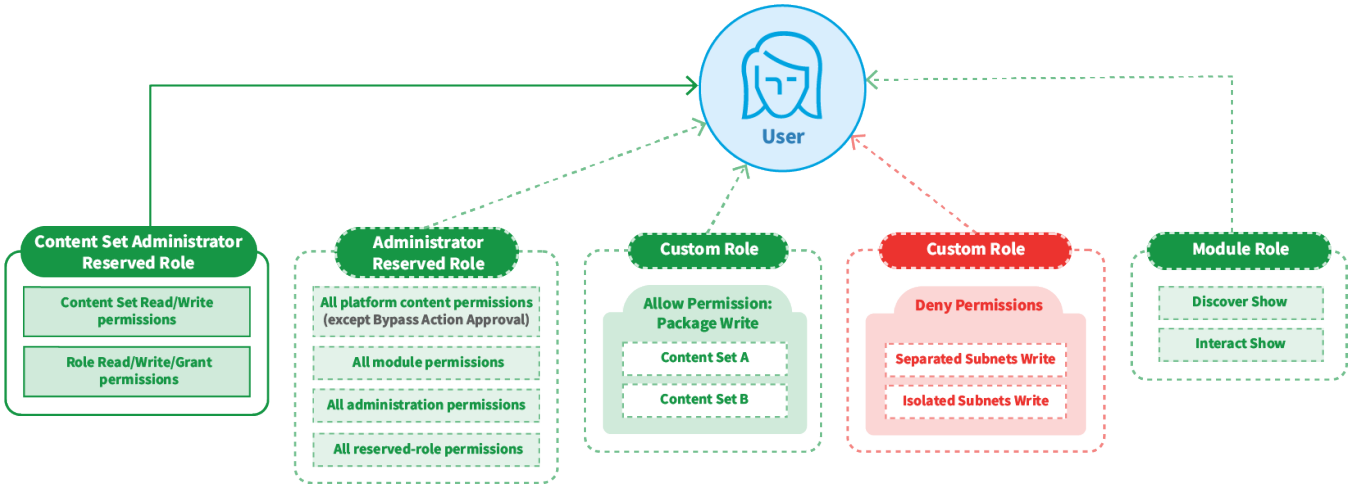
This role can perform the following tasks:

© 2026 Tanium Inc. All Rights Reserved

- View, create, edit, delete, import, or export content set configurations
- Manage content assignments to content sets
- View, create, edit, delete, import, or export user role configurations
- Manage role assignments to users, user groups, and personas

The **Content Set Administrator** role makes all other allow roles superfluous. The Deny All reserved role on page 584 is the only role that can affect a user who has the **Content Set Administrator** role.

Content Set Administrator reserved role



IMPORTANT

Notice the result when both the **Content Set Administrator** and **Administrator** roles are assigned. Only the **Content Set Administrator** role remains effective. Be careful not to assign the **Content Set Administrator** role to users who must have other roles. Be careful not to assign (directly or by user group inheritance) the **Content Set Administrator** role to users who are assigned the **Administrator** role.

Content Administrator reserved role

Assign the **Content Administrator** reserved role to users who manage content and actions.

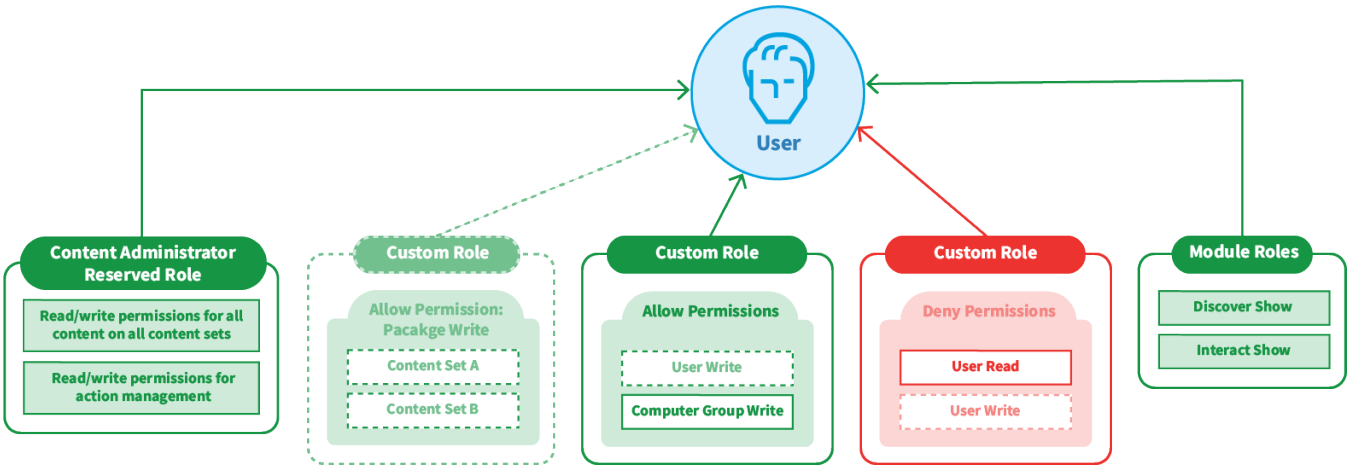
This role can perform the following tasks:

- View, create, edit, and delete all content configurations (such as sensors, packages, and saved questions) across all content sets
- View, create, edit, deploy, and delete actions

When the Tanium Server evaluates effective permissions for a user who has the **Content Administrator** role, the Server disregards the content permissions in other roles but evaluates other types of permissions.

© 2026 Tanium Inc. All Rights Reserved

Content Administrator reserved role



Deny All reserved role

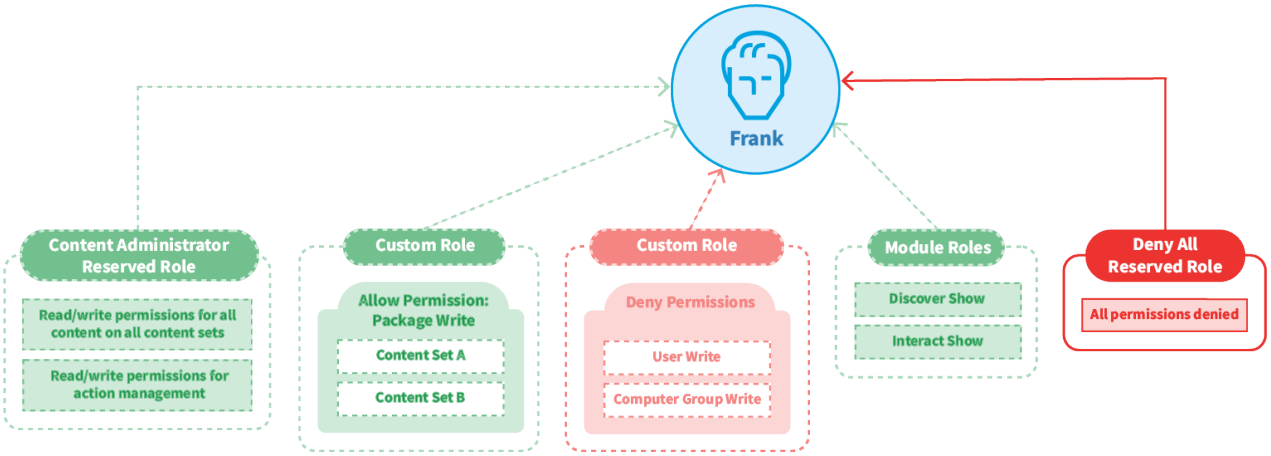
Assign the **Deny All** reserved role to user accounts that you must disable even though you have not yet deleted those accounts. Users who have the **Deny All** role cannot access anything in the Tanium Core Platform, regardless of any other role that you assign to them, including the **Administrator** reserved role. In the figure Example: Deny All on page 584, the only role assigned to Frank that has any effect is **Deny All**.

NOTE

Assigning **Deny All** to a user account affects the default persona of that user but does not affect any alternative persona that is assigned to the user. To disable an alternative persona instead of deleting it, assign **Deny All** to that persona. For more information, see View effective role permissions for a persona on page 658.

Assigning **Deny All** to a user group disables all the user accounts that are members of the group. For more information, see Inherited roles on page 580.

Example: Deny All



© 2026 Tanium Inc. All Rights Reserved

Tasks that require reserved roles

To perform the following Tanium Console tasks, a user must have a reserved role because the tasks are not associated with administration permissions that you can assign to custom roles.

Console tasks that require a reserved role

Task	Administrator	Content Administrator	Content Set Administrator
Manage content sets Create, edit, or delete content set configurations.	✓	✗	✓
Manage role configurations and assignments Edit roles and edit the role assignments of users, user groups, and personas.	✓	✗	✓
Manage Tanium solutions Manage Tanium modules, shared services, and content-only solutions on the **Administration > Configuration > Solutions** page.	✓	✗	✗
Manage Tanium Core Platform configuration View or manage many of the **Administration > Configuration** pages, including those for proxy settings, logging levels, plugins, plugin schedules, sensor threshold indicators, package file repository, Tanium licenses, Tanium root keys, downloads authentication, trust among Tanium Core Platform servers, LDAP servers, SAML, and Tanium Console customizations.	✓	✗	✗

View role details

Viewing role attributes can help you manage RBAC for your organization. For example, the **Roles** page can show you at a glance if the highly privileged **Administrator** role is assigned to too many users. You can also open the full configuration of a single role to view all its assigned permissions.

1. From the Main menu, go to **Administration > Permissions > Roles**.
   The page displays each role name and type, and the number of users, user groups, and personas to which each role is assigned. The **Total Users** column indicates the sum of all the users who are assigned the role through their user accounts or who inherit the role from user groups.
2. (Optional) To display attributes that the grid hides by default, click Customize Columns and select the attributes.

© 2026 Tanium Inc. All Rights Reserved

3. (Optional) Use the following filter types to find specific roles:
    - **Text**: Enter a text string in the **Filter items** field to filter the grid by column values.
    - **Attribute**: Expand the **Filters** section, select a role attribute (such as **Role Name**), select an operator (such as **contains**), enter a text string that contains all or part of the attribute value, and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.
    - **Category**: By default, the grid shows roles of **All** categories but you can click a **Category** button to show only System roles on page 569 or Custom roles on page 569.
    - **Type**: By default, the grid shows roles of **All** types but you can click a **Type** button to show only **Allow** or **Deny** roles. For more information, see Allow and deny roles on page 572.
4. (Optional) View the permissions (and associated content sets), users, and user groups that are assigned to a role by clicking the **Role Name**.

To view or edit the configuration of an assigned user or user group, click the user or group name.
For more information about the icons in the **Permissions** and **Content Sets** grids, see View effective role permissions on page 588.
To view the roles that are assigned to a persona, see Manage persona assignments for a role on page 587.

Configure a custom role

Configure custom roles if the Tanium-defined roles do not address all the RBAC needs of your organization. For example, you might create a role that assigns the **Bypass Action Approval** permission and then assign the role to users who have the authority to deploy actions without approval.

A custom role can include any combination of administration, platform content, and Tanium solution permissions. When you configure a custom role with platform content or solution permissions that are associated with content, such as sensors and packages, you also select the content sets to which those permissions apply.

To add a role that has many settings in common with an existing role, cloning the existing role and then modifying the clone is often a quicker method than configuring a new role.

1. From the Main menu, go to **Administration > Permissions > Roles**.
2. Perform one of the following steps:
    - **Create a role from scratch**: Click **New Role**.
    - **Clone a role**: Select a role and click **Clone**.
    - **Edit a role**: Click a **Role Name** and click **Edit Mode**.
3. Specify a **Role Name** of up to 255 characters to identify the role.

© 2026 Tanium Inc. All Rights Reserved

4. Set the **Permission Type** to **Allow** or **Deny**.
   For more information, see Allow and deny roles on page 572.
5. Configure the RBAC assignments and permissions as described in the following tasks, and then click **Save**.

   NOTE

   You configure persona assignments in the persona configuration page instead of the role configuration pages. For more information, see Manage persona assignments for a role on page 587.

   - Manage user and user group assignments for a role on page 587
   - Configure role permissions on page 591
   - Manage content set permissions for a role on page 605

Manage user and user group assignments for a role

Skip the first step if you opened the **Create Role** or **Edit Role** page in a previous task.

1. From the Main menu, go to **Administration > Permissions > Roles**, click the **Role Name**, and click **Edit Mode**.
2. Expand the **Users** section, click **Manage Users**, select or deselect users, and click **Select**.

   TIP

   If you are editing a role that already has users assigned, click the number above the **Users** field in the **Role Details** section to go to the **Users** section and expand it.
   To view or edit the configuration of a particular user, click the user **Name** in the **Users** section. The **Edit User** page opens in a new tab.
3. Expand the **User Groups** section, click **Manage User Groups**, select or deselect groups, and click **Select**.

   TIP

   If you are editing a role that already has user groups assigned, click the number above the **User Groups** field in the **Role Details** section to go to the **User Groups** section and expand it.
   To view or edit the configuration of a particular user group, click the group **Name** in the **User Groups** section. The **Edit User Group** page opens in a new tab.
4. Click **Save**.

Manage persona assignments for a role

Assign a role to a persona to provide the permissions of that role to users who select the persona for a Tanium session.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Permissions > Personas**.
2. Click the persona **Name** and click **Edit Mode**.
3. In the **Roles** section, click **Manage Roles**.
4. Select or deselect roles and click **Apply**.

   You cannot assign the **Content Administrator** or **Content Set Administrator** reserved role to a persona.
5. (Optional) Review the **Permissions** and **Content Sets** that are associated with the selected roles.
6. Click **Save**.

Manage role permissions

For an overview of how roles determine the effective permissions of users, and to view the permissions and associated content sets that are assigned to a role, see View effective role permissions on page 588.

To assign or unassign permissions for a role, see Configure role permissions on page 591.

For descriptions of the permissions that you can assign to roles, see:

- Administration permissions on page 594
- Solution permissions on page 598 (such as **Interact** or **Patch** permissions)
- Platform content permissions on page 600

View effective role permissions

The effective permissions of a user account are based on the cumulative effect of all roles that are assigned to the account or inherited from user groups, including:

- Permissions specified in allow roles minus permissions specified in deny roles
- Implicitly provided permissions in allow roles
- Roles that are assigned to the persona that a user selects for a Tanium Console session. The persona can be assigned directly to the user account or inherited from a user group to which the user belongs.

Perform the following steps to see the effective permissions for a role:

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Permissions > Roles**, click the **Role Name**, and click **Edit Mode**.
2. Review the **Permissions** and **Content Sets**. The page displays icons to indicate how permissions are derived:



Allow permissions that you explicitly assign and that automatically provide additional permissions because of dependencies. For example, when you assign the **Interact Module write** permission, it automatically provides the **Ask Dynamic Questions** permission. For more information, see Provided role permissions on page 576. The icons are grayed out for permissions that are not assigned.



Allow permissions that you explicitly assign but that do not provide additional permissions. The icons are grayed out for permissions that are not assigned.



Allow permissions that are implicitly assigned because other permissions provide them. You can hover over the icon to show a tool tip that indicates how the permission was derived from an explicit permission .



Deny permissions that you explicitly assign.



When you view the configuration page for reserved roles (such as **Administrator**), it displays a single **special** permission  under **Global Permissions**. When you view the configuration page for a custom role, the **Global Permissions** of reserved roles are hidden because you cannot assign them.

You can Expand  individual solution content permissions (such as **Trends Administrator** permission) and **Platform Content Permissions** (such as **Sensor read** permission) to see the content sets to which the permission applies. The following icons indicate how content set assignments are derived:



Content set that is explicitly assigned to the permission.



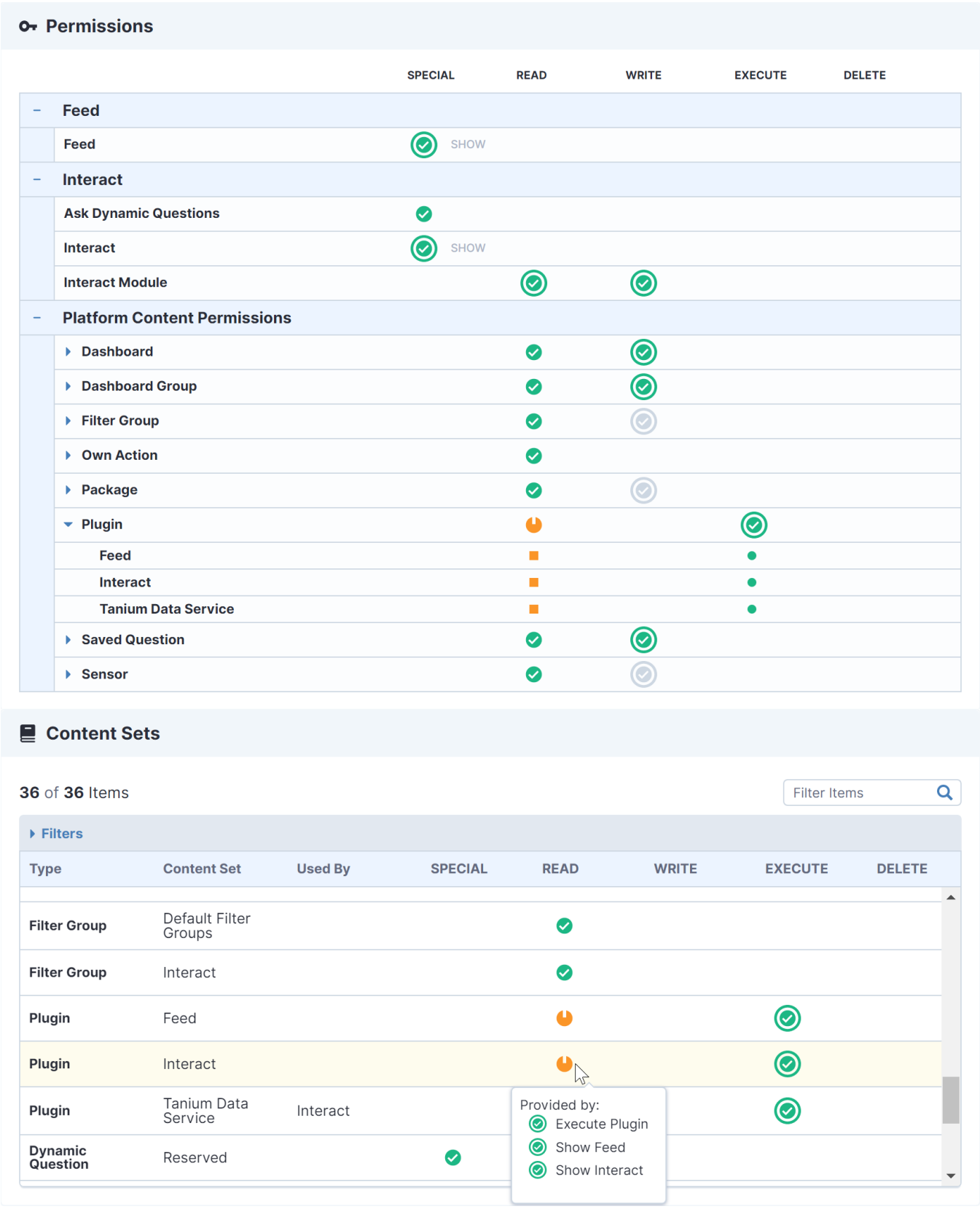
Content set that is assigned because another permission implicitly provides it. You can hover over the icon to show a tool tip that indicates how the content set assignment was derived from an explicit permission .



Content set that is assigned to a deny permission.

© 2026 Tanium Inc. All Rights Reserved

Effective permissions for a role



© 2026 Tanium Inc. All Rights Reserved

To review the effective permissions for a user, user group, or persona, see:

- View effective role permissions for a user on page 631
- View effective role permissions for a user group on page 646
- View effective role permissions for a persona on page 658

Configure role permissions

Perform one of the following tasks to assign or unassign permissions in a new or existing role:

- (New or existing role) Assign or unassign permissions for a single role on page 591

  NOTE

  For a single role, to assign content sets to permissions that are associated with content, see Manage content set permissions for a role on page 605.

- (Existing roles) Assign permissions and content sets to multiple roles on page 592
- (Existing roles) Unassign permissions and content sets from multiple roles on page 594

ASSIGN OR UNASSIGN PERMISSIONS FOR A SINGLE ROLE

Perform the following steps to assign or unassign permissions for a role. Skip the first step if you opened the **Create Role** or **Edit Role** page in a previous task.

1. From the Main menu, go to **Administration > Permissions > Roles**, click the **Role Name**, and click **Edit Mode**.
2. Expand the section that corresponds to the type of permissions that you want to assign or unassign:
   - Administration permissions on page 594
   - Solution permissions on page 598 (such as **Interact** or **Patch** permissions)
   - Platform content permissions on page 600
3. Assign or unassign permissions by clicking the appropriate icons in the **Special**, **Read**, **Write**, **Execute**, or **Delete** column. For more information about the icons, see View effective role permissions on page 588.

   TIP

   Click an icon in a column header to select all the permissions of that type. For example, in the **Administration** permissions header, click the **Special** icon to assign all the available special administration permissions.

4. (Optional) Review all the permissions that you selected.

   TIP

   Click **Preview** at the top right of the page to display only the permissions that you selected. When you finish reviewing, click **Edit Mode** to continue configuring the role.

© 2026 Tanium Inc. All Rights Reserved

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

ASSIGN PERMISSIONS AND CONTENT SETS TO MULTIPLE ROLES

1. From the Main menu, go to **Administration > Permissions > Roles** and select the roles to edit.
2. Select  **> Add Permissions**.
3. Go to the **Permissions** section and expand  the section that corresponds to the type of permissions that you want to assign:

   - Administration permissions on page 594
   - Solution permissions on page 598 (such as **Interact** or **Patch** permissions)
   - Platform content permissions on page 600
4. Assign permissions by clicking the appropriate icons in the **Special**, **Read**, **Write**, **Execute**, or **Delete** column, and then click **Next**.

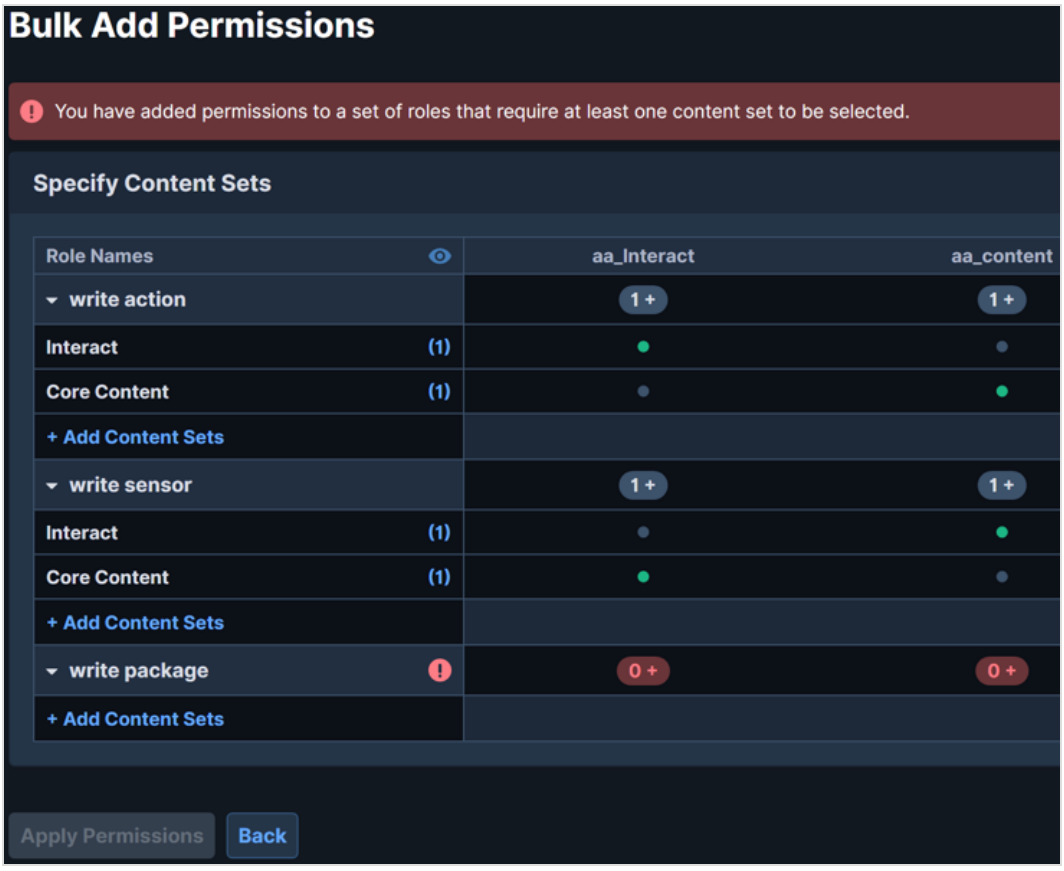
   For more information about the icons, see View effective role permissions on page 588.

   Click an icon in a column header to select all the permissions of that type. For example, in the **Administration** permissions header, click the **Special** icon to assign all the available special administration permissions.

   To show only the **Permissions** that you added, click **Preview** at the top right of the page. After reviewing the permissions, revert to **Edit Mode** before proceeding to the next step.
5. If any permissions that you assigned are associated with content, such as **Package write** permission, click **Next** and perform the remaining steps to assign content sets to those permissions. Otherwise, click **Apply Permissions** to complete the procedure.
6. Assign content sets to permissions that are associated with content.

   In the grid, the first column shows the name of each permission, the content sets that you assigned to it (initially none ), and the number of roles (initially **0**) to which you assigned the permission-content set pairing. For each role, an additional column shows the total number of permission-content set pairings that you assigned (initially **0**) and an assigned  or not assigned  icon for each pairing. The **Apply Permissions** button is disabled until you assign at least one content set to every permission that is associated with content.

© 2026 Tanium Inc. All Rights Reserved



You can assign permission-content set pairings to multiple roles or a single role:

- **Multiple roles**:
    a. For each permission, click **Add Contents Sets**, select content sets, and click **Select**.
    b. For each permission-content set pairing that you added, click the content set name, select roles, and click **Select**.
- **Single role**: For each permission, click **0+** in a role column, select content sets, and click **Select**.

TIP

After you assign permission-content set pairings on the **Bulk Add Permissions** page, you can change any assignments that you added during the current workflow (that is, before you click **Apply Permissions**). You cannot remove any permission-content set pairings that were assigned before you started the current **Bulk Add Permissions** workflow. To change assignments that you added during the current workflow:

© 2026 Tanium Inc. All Rights Reserved

TIP

- **Single assignment**: For each pairing, click an icon in a role column to toggle between assigned or unassigned for that role.
- **Multiple assignments**: For each permission, click a number in a role column and then select or deselect multiple content sets for that permission.

To change permission-content set assignments after you complete the **Bulk Add Permissions** workflow, see Unassign permissions and content sets from multiple roles on page 594.

7. Click **Apply Permissions**.

UNASSIGN PERMISSIONS AND CONTENT SETS FROM MULTIPLE ROLES

1. From the Main menu, go to **Administration > Permissions > Roles** and select the roles to edit.
2. Click **> Remove Permissions**.
3. Go to the **Permissions** section.
   The listed permissions are assigned to one or more of the **Selected Roles**. When you deselect permissions in the list, they are unassigned from any of those roles.
4. Deselect permissions by clicking the or icons in the **Special**, **Read**, **Write**, **Execute**, or **Delete** column.
   For more information about the icons, see View effective role permissions on page 588.
5. Click **Apply Changes**.

Administration permissions

The following table describes administration permissions.

Administration permissions

Permission	Description
Action Group	Read permission enables users to view and export action group configurations in the **Action Groups** page. NOTE **Action Group read** permission overrides the **Visibility** setting. A user who has **Action Group read** and action deployment permissions can select any action group when deploying an action. A user who has **Action Group read** and **Approve Action** permissions can approve actions that target any action group. However, the computer groups that are assigned to a user still control which endpoints run an action that the user deploys to the selected action group. Write permission enables users to create, edit, and delete action group configurations. Write permission provides the **Action Group read** permission.

© 2026 Tanium Inc. All Rights Reserved

Administration permissions (continued)

Permission	Description
Allowed URLs	Read permission enables users to view allowed URL configurations on the **Allowed URLs** page and to export the configurations in CSV format. The **Export Content** administrationmicro admin permission is required to export in JSON format. Write permission enables users to create, edit, and delete allowed URL configurations. Write permission provides **Allowed URLs read** permission.
Audit	Read permission enables users to view: • **Last Sign In** information on the **Users** page • **Last Modified** information on the user configuration page • **Last Modification** information on the **Settings** page
Computer Group	Read permission enables users to view computer management groups and export them in CSV format. The **Export Content** permission is required to export in JSON format.  NOTE Additional permissions are required to view the user group, user, and persona assignments of computer management groups. For more information, see Manage computer management groups on page 103. Write permission enables users to create, edit, and delete computer management groups. Write permission provides the **Computer Group read** permission. To create a computer management group in which membership is based on a sensor filter, users require the following permissions in addition **Computer Group write**: • **Sensor** (platform content): Read permission on the **Reserved** content set, which includes content that is used to ask preview questions • **Interact Module** (solution): Write permission Computer groups with manually defined membership do not require the **Sensor read** or **Interact Module write** permissions.

© 2026 Tanium Inc. All Rights Reserved

Administration permissions (continued)

Permission	Description
Export Content	Enables users to export the following content types in JSON format: • Actions • Allowed URLs • Computer management groups • Content sets • Filter groups • Packages • Roles • Saved questions • Scheduled actions • Sensors  NOTE Only the **Administrator** reserved role can export categories and dashboards.
Import Signed Content	Enables users to import digitally signed content files, such as for sensor configurations.
Global bandwidth throttles	Read permission enables users to view global bandwidth throttle configurations on the **Bandwidth Throttles** page. Write permission enables users to create, edit, and delete global bandwidth throttles.
Global Settings	Read permission enables users to view the platform settings of Tanium Core Platform servers and Tanium Clients on the **Settings** page. Write permission enables you to edit, create, or delete platform settings. Write permission provides the **Global Settings read** permission.
Https Certificates	Read permission enables users to view information about certificates and certificate signing requests (CSRs) on the **Administration > Configuration > SSL Certificates** page. Only the **Administrator** reserved role can generate CSRs and upload new certificates.
Intentional Subnets	Read permission enables users to view and export intentional Client subnet configurations on the **Administration > Configuration > Subnets** page. Write permission enables users to create, edit, and delete intentional Client subnet configurations. Write permission provides **Intentional Subnets read** permission.

© 2026 Tanium Inc. All Rights Reserved

Administration permissions (continued)

Permission	Description
Isolated Subnets	Read permission enables users to view and export isolated Client subnet configurations on the **Administration > Configuration > Subnets** page. Write permission enables users to create, edit, and delete isolated Client subnet configurations. Write permission provides **Isolated Subnets read** permission.
Metrics	Read permission enables users to view the **Monitor Usage** tab on the **Bandwidth Throttles** page. For the tab charts, **Global Bandwidth Throttles read** permission is required to view global bandwidth usage and **Subnet Bandwidth Throttles read** permission is required to view site bandwidth usage.
Persona	Read permission enables users to view and export persona details. Write permission enables users to create, edit, and delete personas. Write permission provides the **Persona read** permission. NOTE Users require additional permissions to edit the assignment of other RBAC objects (such as users) to personas. For more information, see Manage personas on page 106.
Public Key	Read permission enables Tanium REST API users to download the Tanium public key (`tanium.pub`) or initialization file (`tanium-init.dat`). Only the **Administrator** reserved role can access the **Infrastructure** page to download those files through Tanium Console.

Question History	Read permission enables users to view the **Question History** page.
	
	To issue a question from the **Question History** page, users also require the following permissions:
	
	• **Interact** solution permissions:
	  ◦ **Interact show**
	  ◦ **Interact Module read**
	• **Platform Content Permissions**:
	  ◦ **Saved Question read** permission on the content sets that contain the questions that the user is allowed to issue.
	  ◦ **Sensor read** permission on the content sets that contain the sensors that are used in the questions that the user is allowed to issue.

Separated Subnets	Read permission enables users to view and export separated Client subnet configurations on the **Subnets** page. Write permission enables users to create, edit, and delete isolated Client subnet configurations. Write permission provides **Separated Subnets read** permission.

© 2026 Tanium Inc. All Rights Reserved

Administration permissions (continued)

Permission	Description
Server Status	Read permission enables users to view the `https://<Tanium_Server>/info` page. For more information, see View the Tanium Server info page on page 723.
Subnet bandwidth throttles	Read permission enables users to view site-specific bandwidth throttle configurations on the **Bandwidth Throttles** page. Write permission enables users to create, edit, and delete site-specific bandwidth throttles.
Client Status	Read permission enables users to view the **Client Status** page.
Token - Revoke	Enables users to create or revoke API tokens of any user.
Token - Use	Enables a user to create, view, rotate, or revoke his or her own API tokens. This permission does not enable the user to perform these tasks for the tokens of other users.
Token - View	Enables users to view the **API Tokens** page and view the tokens of all users.
Token - Rotate	Enables users to rotate the API tokens of any user. Rotation deletes the selected token and creates a new one. The expiration timer of the new token is reset and has the same interval as the deleted token.
User	Read permission enables users to view and export user configurations on the **Users** page. Write permission enables users to create, edit, and delete user configurations. Write permission provides **User** read permission. NOTE Additional permissions are required to view and edit the role, user group, and persona assignments of users. For more information, see Manage users on page 104.
User Group	Read permission enables users to view and export user group configurations on the **User Groups** page. Write permission enables users to create, edit, and delete user group configurations. Write permission provides **User Group read** permission. NOTE Additional permissions are required to view and edit the role, user, and persona assignments of user groups. For more information, see Manage user groups on page 105.

Solution permissions

Tanium solutions provide predefined roles with permissions that allow users to access solution workbenches and content. For information about solution-specific permissions, see the following Tanium user guides.

© 2026 Tanium Inc. All Rights Reserved

NOTE

Some solution permissions require content set assignments. For more information, see Manage content set permissions for a role on page 605.

- Asset
- Automate
- Benchmark
- Certificate Manager
- Client Management
- Cloud Workloads
- Comply
- Connect
- Criticality
- Deploy
- Direct Connect
- Directory Query
- Discover
- Endpoint Configuration
- End-User Notifications
- Enforce
- Engage
- Gateway
- Guide
- Health Check
- Impact
- Integrations Gallery
- Integrity Monitor
- Interact
- Investigate
- Jump Gate
- Patch

© 2026 Tanium Inc. All Rights Reserved

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

Platform content permissions

The following table describes the permissions for Tanium Core Platform content. After assigning these permissions to a role, you must apply them to content sets. For more information, see Manage content set permissions for a role on page 605.

© 2026 Tanium Inc. All Rights Reserved

Platform content permissions

Permission	Description
Action	**Action read** permission enables users to perform the following tasks on the **Scheduled Actions**, **All Pending Approvals**, **Action History**, and **Ring Deployment Status** pages. These tasks are enabled only for Tanium platform actions that use packages in a content set to which **Action read** permission is assigned. • View actions. • Export the actions in CSV format. The **Export Content** administration permission is required to export actions in JSON format. • Copy the actions to the clipboard. • View action status on page 96, when combined with other content permissions. **Action write** permission enables users to perform the following tasks on the **Scheduled Actions**, **All Pending Approvals**, **Action History**, and **Ring Deployment Status** pages. These tasks are enabled only for Tanium platform actions that use packages in a content set to which **Action write** permission is assigned. • Reissue or edit actions, when combined with **Sensor read** permissions on the **Reserved** content set. The **Reserved** content set includes content that you use to ask preview questions. • View the status of, and re-download, packages that are associated with actions. • Disable or enable actions. • Change the action groups that actions target. • Create copies of action configurations. • Delete actions. • Stop actions. • Pause or resume adaptive (ring-based) actions. **Action read** permission provides **Own Action read** permission. **Action write** permission provides **Own Action read**, **Package read**, and **Show Preview** permissions.  NOTE Users who view, deploy, and manage adaptive actions require additional permissions. For more information, see Manage deployment plans on page 91.

© 2026 Tanium Inc. All Rights Reserved

Platform content permissions (continued)

Permission	Description
Action for Saved Question	Write permission enables users to: • Access the **Scheduled Actions** page and see the actions they have deployed. • See and use the **Deploy Action** button on the **Question Results** grid for saved questions that have associated packages. The **Package read** permission is not required for the associated packages. If the saved question does not have associated packages, the **Deploy Action** button does not appear. Write permission provides **Own Action read** and **Show Preview** permissions. Use the **Action for Saved Question write** permission instead of the **Action write** permission to limit use by action users who use Tanium products to execute standard operating procedures that someone else created.
Approve Action	Enables users to perform the following tasks on the **Actions I Can Approve** page: • View actions that require approval. Users cannot view their own actions on this page. • Approve actions that other users own, when combined with **Sensor read** permission. Users cannot approve their own actions. • Export the actions in CSV format. **Export Content** (administration) permission is required to export actions in JSON format. • Copy the actions to the clipboard.
Bypass Action Approval	Actions created by a user with this permission are not subject to approval requirements. No role, including the **Administrator** reserved role, includes this permission by default. This is the one platform content permission that has effect when granted to a user with the **Administrator** role.
Dashboard	Read permission enables users to view dashboards in the Interact **Content** page, if those users also have **Interact show** permission. The users also require read permissions for **Saved Question** and **Sensor** on related content to use the dashboard. Write permission enables users to create, edit, and delete dashboard configurations. Write permission provides **Dashboard read** permission.
Dashboard Group	Read permission enables users to view categories in the Interact **Content** page, if those users also have **Interact show** permission. Users also require read permissions for **Dashboard**, **Saved Question**, and **Sensor** on the related content to use the category. Write permission enables users to create, modify, and delete category configurations. Write permission provides the **Category read** permission.

© 2026 Tanium Inc. All Rights Reserved

Platform content permissions (continued)

Permission	Description
Deployment Plan	Read permission enables users to view deployment plan configurations and select plans for actions. Write permission enables users to create, modify, and delete plans. For more information, see Manage deployment plans on page 91.
Filter Group	Read permission enables users to: • View the **Filter Groups** page • Use filter groups for filtering questions, question results, and various lists in Tanium Console • Export filter groups in CSV format. The **Export Content** administration permission is required to export in JSON format. Write permission enables users to create, edit, and delete filter group configurations. Write permission provides the **Filter Group read** permission.
Own Action	Enables users to perform the following tasks on their own actions (not those of other users) on the **Scheduled Actions**, **All Pending Approvals**, and **Action History** pages. These tasks are enabled only for actions that use packages in a content set to which **Own Action read** permission is assigned. • View the actions. • Export the actions in CSV format. The **Export Content** administration permission is required to export actions in JSON format. • Copy the actions to the clipboard. • View action status on page 96, when combined with other content permissions. The following permissions provide **Own Action read** permission: • **Action read** • **Action write** • **Action for Saved Question write**  NOTE User cannot create their own actions unless they have **Action write** and **Interact Module read** permissions.

© 2026 Tanium Inc. All Rights Reserved

Platform content permissions (continued)

Permission	Description
Package	Read permission enables users to: • View packages in the **Deployment Package** list of the **Action Deployment** page. • View packages in the **Packages** page. • Export packages in CSV format. The **Export Content** administration permission is required to export in JSON format. Write permission enables users to create, edit, and delete package configurations. Write permission provides **Package read** and **Show Preview** permissions.
Associated Packages	**Associated Packages read** permission is not an explicit permission; the **Action for Saved Question write** permission provides **Associated Packages read** permission.
Plugin	Certain solution permissions provide **Plugin read** and **execute** permissions to enable functionality that varies by solution. You do not need to select these permissions for custom roles.
Progression Criteria Set	Read permission enables users to view the progression criteria that are defined in a deployment plan. Write permission enables users to create, modify, and delete progression criteria in a deployment plan. For more information, see Manage deployment plans on page 91.
Ring Set	Read permission enables users to view the rings that are defined in a deployment plan. Write permission enables users to create, modify, and delete rings in a deployment plan. For more information, see Manage deployment plans on page 91.
Saved Question	Read permission enables users to: • View saved questions in the **Question Results** grid drill-down and similar user interfaces. • View saved questions in the Interact **Overview** page, if the user also has **Interact** show permission. • Issue saved questions, if the user also has **Sensor read** permission on the content sets that contain the sensors in those questions. • View the **Saved Questions** page. • Export saved questions in CSV format. The **Export Content** administration permission is required to export in JSON format. Write permission enables users to create, edit, and delete saved question configurations. Write permission provides **Saved Question read** permission but does not provide **Ask Dynamic Questions** permission.

© 2026 Tanium Inc. All Rights Reserved

Platform content permissions (continued)

Permission	Description
Sensor	Read permission enables users to: • View sensor configurations. • View sensors in the **Question Builder** and similar user interfaces throughout Tanium Console. • Use sensors in questions if the user also has the ability to ask questions. Write permission enables users to create, edit, and delete sensor configurations. Write permission provides **Sensor read** and **Show Preview** permissions.
Show Preview	**Show Preview** is not an explicit permission. The write permissions for **Action**, **Action for Saved Question**, **Sensor**, and **Package** provide **Show Preview**. **Show Preview** enables users to ask questions that are necessary to preview the impact of new and changed action, sensor, and package configurations. To ask preview questions, the user also needs **Sensor read** permission on the **Reserved** content set, which includes content that is used to ask the preview questions.

Manage content set permissions for a role

When you configure a role with permissions for Tanium solution content (such as **Report write** permission) or platform content (such as **Sensor read** permission), you must assign **Content Sets** to the pertinent permissions.

Manage content set permissions for multiple roles

You can add or remove content set assignments in bulk for multiple roles when you configure role permissions:

- Assign permissions and content sets to multiple roles on page 592
- Unassign permissions and content sets from multiple roles on page 594

Manage content set permissions for a single role

Skip the first step in this procedure if you opened the **Create Role** or **Edit Role** page in a previous task.

1. From the Main menu, go to **Administration > Permissions > Roles**, click the **Role Name**, and click **Edit Mode**.
2. Perform one of the following sub-steps:
    - To assign all existing and future content sets to all the pertinent content permissions that you selected, select **Add all Content Sets that exist or will exist to the permissions selected above**. This option is useful, for example, when you want a user to always be able to read sensors or never be able to write actions, regardless of content set assignments. This option is not available for implied permissions. You must select (explicitly assign) a permission before applying this option.

© 2026 Tanium Inc. All Rights Reserved

- To assign specific content sets to all the pertinent content permissions that you selected, click **Apply Content Sets**, select the sets, and click **Select**. The **Content Sets** selection dialog shows a check mark ☑ for any contents sets that are already assigned to all the selected permissions and shows a dash — for content sets that are applied to some (but not all) of the selected permissions.

  > NOTE
  >
  > Content sets that you select in the **Content Sets** selection dialog are assigned to all currently selected permissions. Content sets that you deselect in the dialog are removed from all currently selected permissions. For example, if you previously assigned the **Interact** content set specifically to the **Sensor read** permission but then deselect that content set during the **Apply Content Sets** workflow, the **Sensor read** permission does not apply to the **Interact** content set.

- To assign specific content sets to a specific permission:

  a. Go to the **Permissions** section and click the number beside the permission icon, such as:

  b. Select the content sets and click **Select**.

  > NOTE
  >
  > Content sets that you assign to specific permissions are added to any previous assignments. For example, if you assigned the **Base** content set to all pertinent content permissions (**Apply Content Sets** workflow) and subsequently assigned the **Interact** content set specifically to the **Sensor read** permission, then both the **Base** and **Interact** content sets are assigned to the **Sensor read** permission.

> TIP
>
> To create a custom content set without leaving the role configuration page, click **New Content Set**, enter a **Name** to identify the set, and click **Save**. You can then assign the new content set to permissions.

3. (Optional) Review the content set assignments.

   > NOTE
   >
   > The role configuration pages use icons to indicate how permissions and content set assignments are derived. For more information, see View effective role permissions on page 588.

   - To review the content set assignments of a specific permission, expand it ▶ in the **Permissions** section.
   - To review the content set assignments for all permissions, see the **Content Sets** grid.

4. Click **Save** to save your changes.

© 2026 Tanium Inc. All Rights Reserved

Export and import roles

Export roles

Export roles as a file in the format required for your workflow:

- **CSV**

  You can use any application that supports CSV format to display the same role attributes (columns) as the Console **Roles** page shows and (optionally) list the RBAC assignments of each role. Displaying the grid in a CSV application is useful when you want to customize the display. For example, you can use Microsoft Excel to create charts based on role attributes.

- **JSON**

  You can export multiple role configurations as a JSON file. Exporting configurations is useful if you want to import them into another Tanium environment. For example, you might test roles in a lab environment to ensure that they work as intended before importing the roles into your production environment. You must be assigned a role with the **Export Content** permission to export a JSON file. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.

Perform the following steps to export roles:

1. From the Main menu, go to **Administration > Permissions > Roles**.
2. (Optional, CSV exports only) To add or remove attributes (columns) for the CSV file, click Customize Columns  in the grid and select the attributes.
3. Select rows in the grid to export only specific roles. If you want to export all roles, skip this step.
4. Click Export .
5. (Optional) Edit the default export **File Name**.

   The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.
6. Select an **Export Data** option: **All** roles in the grid or just the **Selected** roles.
7. Select the file **Format**:

   - **List of Roles - CSV**

     Optionally, select **With RBAC Details** to include the number of users, user groups, and personas to which the roles are assigned, along with the permissions that are assigned to the roles. The report includes a **Total Users** column that shows the total number of users to which each role is assigned either through direct assignment to user accounts or through assignments inherited from user groups.

   - **Role Definitions - JSON** (**Administrator** reserved role only)
8. Click **Export**.

   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

© 2026 Tanium Inc. All Rights Reserved

Import roles

Importing is useful if you want to copy role configurations from another Tanium environment. For example, you might test custom roles in a lab environment to ensure that they work as intended. You can then export the roles from the lab environment and import them into your production environment. You can import roles and other content as a JSON or XML file.

You must be assigned a role with **Import Signed Content** permission to import content files through the following steps.

1. (Non-Tanium-provided content only) Digitally sign the content file and ensure a public key is in place to validate the signature. For more information, see Authenticating content files on page 482.

   NOTE

   You do not have to generate keys or signatures for Tanium-provided solutions. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process.

   If you plan to import a file that another user signed, you can first perform an integrity check on the file. For more information, see Verify content file signatures on page 487.

2. From the Main menu, go to any of the following **Administration** pages:
   - **Configuration > Solutions**
   - **Permissions > Filter Groups**
   - Under **Content**, select **Sensors**, **Packages**, or **Saved Questions**
   - Under **Actions**, select **Scheduled Actions**, **All Pending Approvals**, or **Actions I Can Approve**
3. Select an **Import** option based on the source of the content:
   - **Import > Import Files**: Perform one of the following steps to select one or more files:
     - Drag and drop files from your file explorer.
     - Click **Browse for File**, select the files, and click **Open**.
   - **Import > Import URL**: Enter the URL in the **Import URL** field, and click **Import**.
4. For each file, expand the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, **Include content set overwrite** is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Install**.

Copy role configuration details

Copy information from the **Roles** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the content that you copy.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Permissions > Roles**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy .
   - **Copy cell information**: Hover over the cell, click Options , and click Copy .

Delete a role



Do not delete the predefined roles that Tanium solutions provide. When you import solution updates, the update process restores any deleted predefined roles.

Deleting a role removes it from any user, user group, and persona to which it was assigned.

As a best practice, perform the following tasks before deleting a role:

1. Delete the user assignments from the role configuration: Manage user and user group assignments for a role on page 587.
2. Delete the user group assignments from the role configuration: Manage user and user group assignments for a role on page 587.
3. Go to the effective permissions page for your users and review the resulting impact on the effective permissions: View effective role permissions for a user on page 631.

To delete a role:

1. From the Main menu, go to **Administration > Permissions > Roles**.
2. Select the role and click Delete .

© 2026 Tanium Inc. All Rights Reserved

Controlling endpoint management rights through computer groups

Computer groups overview

A *computer group* defines a set of endpoints that you want to manage as a group with respect to operations that Tanium users and solutions perform. For example, you can define a computer group that includes all endpoints that are in a data center, and assign the group only to users who will issue questions and deploy actions to data center endpoints.

Computer groups are the building blocks of *action groups*, which filter the target endpoints for actions. For more information, see Targeting actions through action groups on page 400.

You can also use computer groups to filter questions, question results, and various lists in Tanium Console, such as on the **Administration > Permissions > Users** page.

NOTE

For the role permissions required to manage computer groups, see Manage computer management groups on page 103 and Manage filter groups on page 101.

BEST PRACTICE

Review computer groups on a quarterly basis and delete any that are no longer useful. For more information, see Tanium Maintenance User Guide: Delete unnecessary computer groups.

Understand the best practices for computer groups before you create or edit custom groups. For more information, see Computer groups on page 557.

Computer group types

Based on the permissions that you want users to have when querying or deploying actions to sets of endpoints, you can create the following types of computer groups:

- Computer management groups on page 611
- Computer filter groups on page 611
- Computer management and filter groups on page 612

NOTE

The name for each type of computer group reflects how users apply it to retrieve or filter the results of questions issued to endpoints. All three types can use sensor-based filters to define which endpoints are group members. For more information, see Computer group membership on page 614.

© 2026 Tanium Inc. All Rights Reserved

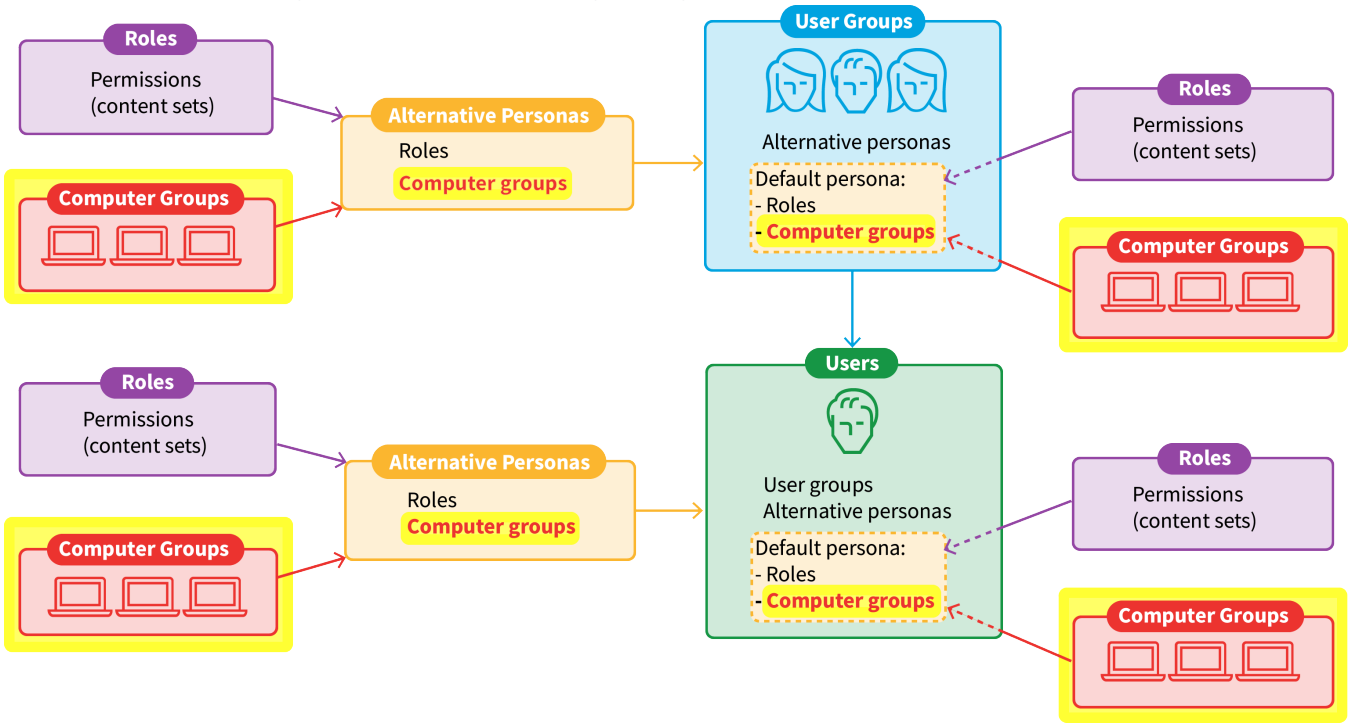
COMPUTER MANAGEMENT GROUPS

A Tanium user can view question results from, and deploy actions to, only those endpoints that belong to a computer management group that is assigned to the user or persona selected for the current session. Use the **Administration > Permissions > Computer Groups** page to manage computer groups that function exclusively as management groups, not filter groups.

Roles do not control access to computer management groups, but roles do control which content is available to the user for questions and actions. For example, you might want a user to see the processes running on endpoints in a data center. You must assign that user a role with **Sensor read** permissions on the content set containing the **Running Processes** sensor and also assign the user a computer management group that contains the data center endpoints.

The following figure illustrates the relationship between computer management groups and other Tanium role-based access control (RBAC) components.

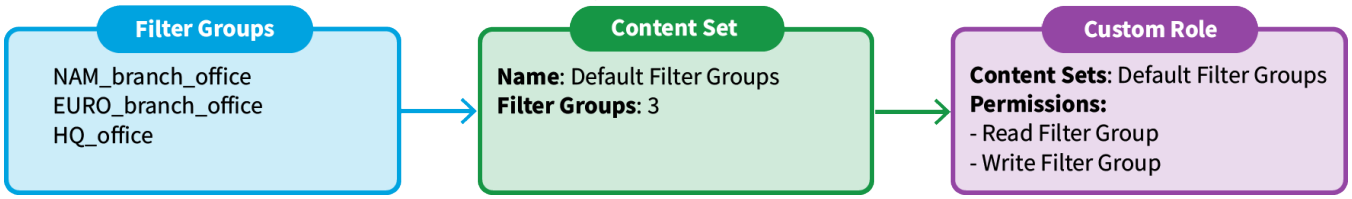
RBAC components and assignments in computer management groups



COMPUTER FILTER GROUPS

Tanium users use computer filter groups as filters in questions (see Use filter groups) and question results (see Filter question results on page 259). Users acquire permissions for a filter group when you assign it to a content set, grant filter group permissions to that content set in roles, and assign the role to user accounts, personas, or user groups. The following figure shows an example of a custom role that grants **Filter Group read** and **write** permissions to the **Default Filter Groups** content set:

RBAC components and assignments in computer filter groups



© 2026 Tanium Inc. All Rights Reserved

Users cannot receive question results from endpoints in a filter group unless those endpoints also belong to a computer management group and you assign that management group to users, personas, or user groups.

To manage computer groups that function exclusively as filter groups, use the **Administration > Permissions > Filter Groups** page. For more information, see Managing filter groups for filtering questions and results on page 476.

COMPUTER MANAGEMENT AND FILTER GROUPS

You can configure computer groups to function as both management groups and filter groups. The reserved computer groups **All Computers** and **No Computers** function as both types. These reserved groups are in the **Reserved** content set, and you cannot edit them. When you first sign in to Tanium Console after a fresh installation of the Tanium Server, the Server automatically imports additional predefined computer groups that function as both filter groups and management groups. For more information, see Default computer groups on page 615.

Use the **Administration > Permissions > Computer Groups** page to manage computer groups that function as both management groups and filter groups.

Computer groups in questions

Understanding how Tanium Clients process questions can help you understand the interaction between computer management groups and filter groups, and how best to use them. The figure Computer management groups and filter groups in a question on page 614 illustrates an example of how assigning computer groups and roles to a user account determines which question results the user can view and filter on the Interact **Question Results** page.

The example in the figure uses computer management groups named **UK** and **France**, which contain Tanium Clients in the corresponding branch offices. The sensors that define membership in the groups filter Clients based on their country codes (44 and 33). The organization headquarters is based in the U.S. (country code 1) and therefore the two groups do not contain any Clients in headquarters. The example user can retrieve question results from branch office Clients in the U.K. or France because the **UK** and **France** computer management groups are assigned to that user. The user cannot retrieve question results from Clients in headquarters because those Clients do not belong to a computer management group that is assigned to the user.

Example: Computer management groups

Name	Membership filter	Tanium Clients
UK	Country Code equals 44	UK_win_1, UK_win_2, UK_mac_1, UK_mac_2
France	Country Code equals 33	FRA_win_1, FRA_win_2, FRA_mac_1, FRA_mac_2

The user is also assigned a role (**euro_admin**) that provides access to the **Default** content set, which includes filter groups named **All Windows** and **All Macs**. Therefore, the user can use those filter groups to filter question results. Each group contains all the Tanium Clients with a specific operating system across all branch offices and headquarters.

Example: Filter groups

Name	Membership filter	Tanium Clients
All Windows	Is Windows equals True	UK_win_1, UK_win_2, FRA_win_1, FRA_win_2, HQ_win_1, HQ_win_2
All Macs	Is Mac equals True	UK_mac_1, UK_mac_2, FRA_mac_1, FRA_mac_2, HQ_mac_1, HQ_mac_2

© 2026 Tanium Inc. All Rights Reserved

In this example, the user issues the following question:

```
Get Computer Name and PowerShell Version equals 2.0 from all machines with Country Code equals 44
```

All Tanium Clients that are online receive the question and process its components in the following order:

1. Computer group management permissions

   Each Tanium Client first evaluates whether it belongs to a computer management group that is assigned to the user who issued the question. If not, the Client does not process the question further. In the example, only the Clients in the **UK** and **France** management groups continue processing the question.

   The **All Windows** and **All Mac** filter groups bestow only filtering permissions, not the permission to receive answers from Clients. Therefore, the Windows and macOS Clients in headquarters (**HQ_***) do not continue processing the question because they do not belong to any computer management group that is assigned to the user.

2. Target filter (`from`) clause

   The `from` clause specifies whether question results are required from all Tanium Clients (`from all machines`) or only from Clients that evaluate the filtering sensor to true. The example question targets endpoints with country code 44, which corresponds to the U.K. Therefore, only the **UK** Clients match the target filter clause `from all machines with Country Code equals 44` and continue to process the question.

3. Select statement (`get`) clause

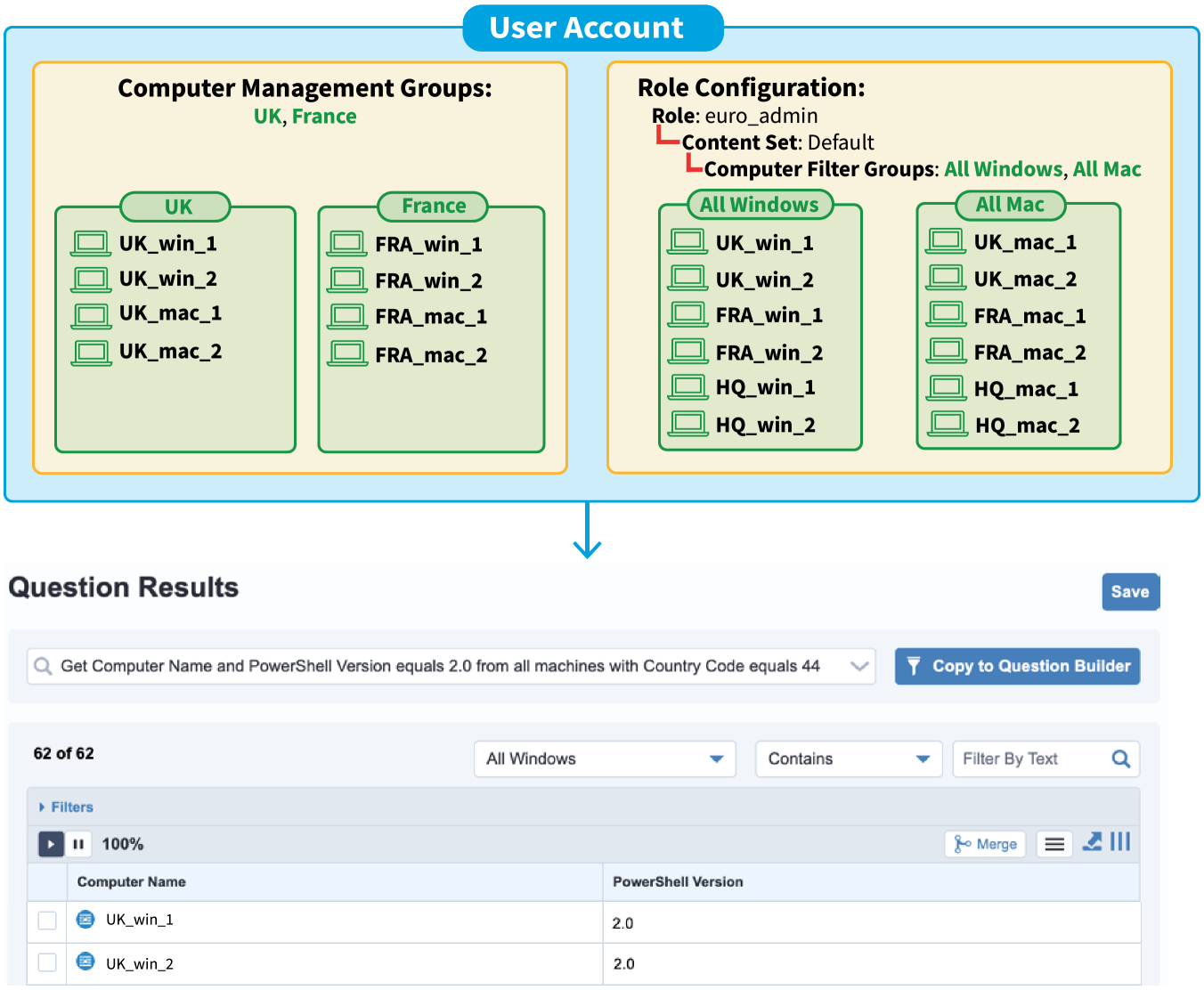
   The `get` clause specifies the sensors that Clients run to answer the question. If the clause has a filter, Clients apply the filter to the sensor results and return the filtered results to the Tanium Server. Interact then shows the filtered results in the **Question Results** page.

   In the example, the **UK** Clients run the sensors `Computer Name` and `PowerShell Version`, process the `equals 2.0` filter for the `PowerShell Version` sensor, and return the filtered results to the Tanium Server. Interact then displays results only for **UK** Clients that have PowerShell version 2.0 installed.

In the example, the user wants the **Question Results** page to show results only for Clients that run Windows. Therefore, the user selects the **All Windows** filter group in the **Filter by Computer Group** dropdown list. The Tanium Server reissues the question using both `Country Code equals 44` and `Is Windows` in the target filter clause. The **Question Results** page then shows results only for Tanium Clients **UK_win_1** and **UK_win_2** because only those Clients match both filters.

© 2026 Tanium Inc. All Rights Reserved

Computer management groups and filter groups in a question



Computer group membership

Before you create a computer management group (see Configure a computer group on page 617) or filter group (see Configure a filter group on page 477), be sure to understand the following options for defining which endpoints are members. After creating a group, you cannot change its membership definition.

Dynamic membership

Dynamic membership in a computer group is based on the results of a sensor filter expression, such as `is Windows equals true`. Tanium Clients process the expression to determine whether their endpoints belong to the group. For more information about using filter expressions, see Use question filters on page 731.

© 2026 Tanium Inc. All Rights Reserved

Whenever possible, define computer group membership based on sensors. Only groups based on a sensor dynamically adjust their membership as endpoints join or leave your network. For example, you might create a manual group called Critical Servers for three special servers. If you later add a fourth server to the cluster, you cannot change the Critical Servers membership. Instead, you would have to: create a new manual computer group; assign it to users; and re-create pertinent action groups and saved questions that you want to target the new computer group. A better approach is to define the computer group based on a sensor that identifies which servers qualify as critical, so that the fourth server automatically becomes a member.



When you configure a computer group with membership based on a parameterized sensor, the Tanium Server creates an object called a *temporary sensor*, which contains the substituted parameter values and a link to the actual sensor. The Tanium Client runs the temporary sensor to process questions or actions that target the computer group. If the sensor definition changes on the Server, the Client receives the new definition after its next registration interval. The Client then applies the parameter values to the updated sensor definition for subsequent questions or actions that target the computer group.

If you base the sensor filter on a custom tag, you can change tag assignments on endpoints to adjust the membership of a computer group. For more information, see Manage computer group membership through custom tags on page 619.

Manually defined membership

Manually defined membership in a computer group is based on a manually entered list of computer names, IP addresses, or fully qualified domain names (FQDNs). The Tanium Client obtains configuration information for the computer groups when registering with the Tanium Server.

Default computer groups

When you first sign in to Tanium Console after a fresh installation of the Tanium Server, the Server automatically imports a content-only solution named Default Computer Groups, which includes predefined computer groups. They all function as both management groups and filter groups, and are assigned to the **Default Filter Groups** content set.

To list the defaults groups:

1. Go to on the **Administration > Permissions > Computer Groups** page and expand the **Filters** section.
2. Click **Add Row**, add the following filter, and click Apply:
   - **Attribute**: **Content Set**
   - **Operator**: **is equal to**
   - **Value**: **Default Filter Groups**

© 2026 Tanium Inc. All Rights Reserved

3. Click Add, select **Add Row**, add the following filter, and click Apply:

    a. **Attribute**: **Created By**

    b. **Operator**: **is equal to**

    c. **Value**: **Administrator**

> NOTE
>
> The Tanium Server creates additional default computer groups as part of Initial content on page 48 during installation.
>
> The Server does not import default computer groups when you upgrade the Server.

View computer group details

Viewing computer group attributes can help you to determine if new groups are necessary and to manage or troubleshoot existing groups. For example, you might check the **Expression** attribute of a group to diagnose issues related to action targeting.

> BEST PRACTICE
>
> As part of quarterly maintenance for your Tanium environment, review the custom computer groups and Delete computer groups on page 623 that are no longer useful or that have memberships that duplicate other groups.

1. From the Main menu, go to **Administration > Permissions > Computer Groups**.
   The **Computer Groups** grid shows the following attributes for each computer group:

    - **Name**: The name that identifies the computer group.
    - **Type**: Indicates whether group membership is sensor-based (`Standard`) or manually defined (`Manual`). For more information, see Computer group membership on page 614.
    - **Management**: Indicates whether you can (`true`) or cannot (`false`) use the group as a computer management group.
    - **Content Set** (filter groups only): The content set to which the group is assigned.
    - **Expression**: The filter used to define membership in the computer group. The value is `[Manual List]` for groups with manually defined membership.
    - **Modified By (Persona)**: The name of the user who last modified the computer group. If the user used an alternative persona during the modification, the persona appears in parentheses.
    - **Last Modification**: The date and time when a user last modified the computer group.

© 2026 Tanium Inc. All Rights Reserved

2. (Optional) Use the filters to find specific computer groups:
    - **Filter by text**: Enter a text string in the **Filter items** field to filter the grid by computer group **Name** or membership **Expression**.
    - **Filter by attribute**: Expand the **Filters** section, select a group attribute (such as **Content Set** assignment), select an operator (such as **contains**), enter a text string that contains all or part of the attribute value, and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.
3. To see a list of endpoints that are members of a group, click the group **Name** and go to the **Members** section.

    TIP

    Clicking the icon for an endpoint opens the **Endpoint Details** dialog, where you can View details for a single endpoint on page 270.

Configure a computer group

Considerations for creating computer groups

Create a custom computer group if the Tanium-defined groups do not address all the scenarios for managing endpoints in your environment. For example, you might want to deploy actions only to endpoints that have a certain custom tag. Before you create a computer group, be sure to understand the difference between dynamic membership and manually defined membership. For more information, see Computer group membership on page 614.

TIP

Cloning an existing computer group is usually easier than creating a group from scratch if the new group has settings that differ only a little from the original group.

To create a computer group that functions exclusively as a filter group and not as a computer management group, see Configure a filter group on page 477.

Considerations for editing computer groups

For existing computer groups, you can edit the name and enable or disable their use as filter groups. However, changing the name does not change the object ID of a computer group. Also, you cannot change the group membership definition. However, if you configure a new group with dynamic membership and base it on a custom tag, you can change tag assignments on endpoints to adjust the group membership. For more information, see Manage computer group membership through custom tags on page 619.

© 2026 Tanium Inc. All Rights Reserved

Create, clone, or edit a computer group

1. From the Main menu, go to **Administration > Permissions > Computer Groups** and perform one of the following steps:
   - **Create a computer group from scratch**: Click **New Computer Group**.
   - **Clone a computer group**: Select the computer group and click **Clone**.
   - **Edit a computer group**: Click the computer group **Name** and click **Edit Mode**.
2. Specify a **Name** of up to 255 characters to identify the group.
3. Under **Additional Options**, select whether users can (**Enable**) or cannot (**Disable**) use this group as a filter group. If you enable the filter group function, select a content set. To use the filter group, users require a role that specifies permissions for that content set.
4. Define which endpoints are **Members** of the computer group.
   - **Dynamic membership** (best practice): Select a method for defining the membership filter:
     - **Filter Bar**: Use the same syntax as in the `from` clause of the Interact **Ask a Question** field. For more information, see Issue a free-form question on page 241.
     - **Filter Builder**: Use the same **from computers with** fields as in the Interact **Question Builder**. For more information, see Issue a question through the Question Builder on page 245.
   - **Manually defined membership**: Select **Manual Group** and enter a list of endpoint identifiers, which can be one of the following:
     - Computer names that match the results of the **Computer Name** sensor. Short forms or alternative names do not work.
     - Fully qualified domain names (FQDNs).
     - IP addresses that match the entries in the **Administration > Configuration > Client Status** page, **Network Location (from server)** column.
5. Review the list of endpoints that are members of the group and click **Save**.

Clicking the icon for an endpoint opens the **Endpoint Details** dialog, where you can View details for a single endpoint on page 270.

Assign computer groups

Assign computer management groups to enable users to view question results from, and deploy actions to, the endpoints in those groups. You can assign up to 255 computer management groups to each user, persona, or user group. The user limit does not include computer groups that a user inherits from user groups. For example, if you assign 255 computer groups to a user, that user can still inherit up to 255 computer groups from each user group to which the user belongs.

A user account or persona that has the **Unrestricted Management Rights** option enabled can view question results from, and deploy actions to, all computer groups. You cannot enable the option for user groups.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

Tanium strongly recommends that you do not assign **Unrestricted Management Rights**, unless you want the user or persona to be able to manage all endpoints across all computer groups regardless of security considerations.

Perform the following tasks to assign or unassign computer groups:

- Manage computer group assignments for a user on page 636
- Manage computer group assignments for a user group on page 651
- Manage computer group assignments for a persona on page 662

NOTE

Tanium Data Service (TDS) automatically registers sensors that define membership in custom computer groups when you assign those groups to users, personas, and (under certain conditions) user groups. For more information, see Tanium Interact User Guide: Sensor registration and unregistration.

TIP

To target computer groups for action deployment, assign them to action groups. For more information, see Create an action group on page 401.

BEST PRACTICE

Computer group assignments affect the processing load on endpoints. To optimize processing usage, see Computer group membership on page 614.

Manage computer group membership through custom tags

A custom tag is a user-defined label that you can assign to, or unassign from, endpoints. Tags are useful for defining computer group membership if you sometimes want to change which endpoints are members. For example, you can configure a computer group with the **Members** setting set to the filter `Custom Tags contains "test"`. Then you can add or remove the tag `test` on endpoints that move in or out of the environment to change the group membership.

You use the **Custom Tags** sensor to define membership for a computer group that is based on custom tags. Before you create tag-based computer groups, review Dynamic membership on page 614 for important details about using sensors to define membership.

NOTE

To configure computer groups based on enhanced tags, see Enhanced Tags Documentation.

Review custom tags

To see which custom tags are assigned to endpoints, ask a question using the `Custom Tags` sensor, such as:

```
Get Custom Tags from all machines
```

© 2026 Tanium Inc. All Rights Reserved

To see which endpoints have a specific custom tag, ask a question using the `Custom Tag Exists` parameterized sensor, such as:

```
Get Tanium Client Version from all machines with Custom Tag Exists[lab,1] equals true
```

For more information about asking questions, see Part 6: Exploring and accessing endpoints in Console and Interact on page 231.

Add custom tags

1. Ask a question to target the endpoints that require custom tags. Because different packages add tags for Windows or non-Windows endpoints, ask a question that specifies the distinction, such as:
   `Get Tanium Client Version from all machines with Is Windows equals true`
2. Select the endpoints to target and click **Deploy Action**.

   You can drill-down or merge questions to refine the results before selecting endpoints.
3. Select one of the following packages as the Deployment Package:
   - **Custom Tagging - Add Tags** for Windows endpoints
   - **Custom Tagging - Add Tags (Non-Windows)**
4. Enter a list of tag names with spaces as delimiters.

   (Windows only) To include any tag names with spaces, use the character sequence `#|#` as a delimiter. To apply a single tag that includes spaces, enter the character sequence `#|#` after the tag name.
5. Configure the remaining action settings. For more information, see Configure action settings.
6. Click **Show Preview To Continue**, review the list of targeted endpoints, and click **Deploy Action**.

Remove custom tags

1. Ask a question to target the endpoints from which to remove custom tags. Because different packages remove tags for Windows or non-Windows endpoints, ask a question that specifies the distinction, such as:
   `Get Custom Tags from all machines with ( Is Windows equals true and Computer Name contains ABC )`
2. Select the **Question Results** rows for the tags that you want to remove and click **Deploy Action**.

   You can drill-down or merge questions to refine the results before selecting endpoints.
3. Select one of the following packages as the Deployment Package:
   - **Custom Tagging - Remove Tags** for Windows endpoints
   - **Custom Tagging - Remove Tags (Non-Windows)**

© 2026 Tanium Inc. All Rights Reserved

4. Configure the remaining action settings. For more information, see Configure action settings.
5. Click **Show Preview To Continue**, review the list of targeted endpoints, and click **Deploy Action**.

Export or import computer groups

Export computer groups

Export computer groups as a file in the format required for your workflow:

- **CSV**
  You can use any application that supports CSV format to display the same computer group attributes (columns) as the Console **Computer Groups** grid shows and then customize the display. For example, you can use Microsoft Excel to create charts based on computer group attributes.
- **JSON**
  You can export multiple computer group configurations as a JSON file. Exporting configurations is useful if you want to import them into another Tanium environment. For example, you might test custom computer groups in a lab environment to ensure that they work as intended before importing the groups into your production environment. You must be assigned a role with the **Export Content** permission to export a JSON file. If you have **Import Signed Content** permission, you can then import the file into another Tanium Server. The **Administrator** reserved role has export and import permissions.

Perform the following steps to export computer groups:

1. From the Main menu, go to **Administration > Permissions > Computer Groups**.
2. (Optional, CSV exports only) To add or remove attributes (columns) for the CSV file, click Customize Columns  in the grid and select the attributes.
3. Select rows in the grid to export only specific computer groups. If you want to export all computer groups, skip this step.
4. Click Export .
5. (Optional) Edit the default export **File Name**.

   
   NOTE

   The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.
6. Select an **Export Data** option: **All** computer groups in the grid or just the **Selected** computer groups.
7. Select the file **Format**:
   - **List of Computer Groups - CSV**
   - **Computer Group Definitions - JSON** (requires **Export Content** permission)
8. Click **Export**.
   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

© 2026 Tanium Inc. All Rights Reserved

Import computer groups

Importing is useful if you want to copy computer group configurations from another Tanium environment. For example, you might test custom computer groups in a lab environment to ensure that they work as intended. You can then export the groups from the lab environment and import them into your production environment. You can import computer groups and other content as a JSON or XML file.

You must be assigned a role with **Import Signed Content** permission to import content files through the following steps.

1. (Non-Tanium-provided content only) Digitally sign the content file and ensure a public key is in place to validate the signature. For more information, see Authenticating content files on page 482.

   You do not have to generate keys or signatures for Tanium-provided solutions. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process.

   If you plan to import a file that another user signed, you can first perform an integrity check on the file. For more information, see Verify content file signatures on page 487.

2. From the Main menu, go to any of the following **Administration** pages:
   - **Configuration > Solutions**
   - **Permissions > Filter Groups**
   - Under **Content**, select **Sensors**, **Packages**, or **Saved Questions**
   - Under **Actions**, select **Scheduled Actions**, **All Pending Approvals**, or **Actions I Can Approve**
3. Select an **Import** option based on the source of the content:
   - **Import > Import Files**: Perform one of the following steps to select one or more files:
     - Drag and drop files from your file explorer.
     - Click **Browse for File**, select the files, and click **Open**.
   - **Import > Import URL**: Enter the URL in the **Import URL** field, and click **Import**.
4. For each file, expand the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, **Include content set overwrite** is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Install**.

Copy computer group configuration details

Copy information from the **Computer Groups** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the content that you copy.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Permissions > Computer Groups**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy.
   - **Copy cell information**: Hover over the cell, click Options, and click Copy.

Delete computer groups

IMPORTANT

Do not delete the predefined computer groups that Tanium solutions provide. When you import solution updates, the update process restores any predefined computer groups that users deleted.

BEST PRACTICE

Instead of deleting custom computer groups, instruct users not to use them.

Review the following considerations before you delete computer management groups:

- **RBAC assignments**

  Account for user and user group configurations that might reference the computer management group through personas. Be prepared to modify those configurations as needed.

- **Content associations**

  Account for other configurations that might have referenced the computer group, such as action groups, scheduled actions, and saved questions. The scheduled actions and saved questions that are configured to target the computer group continue to do so because they do not depend on the computer group ID, just the information that the computer group provided at the time it was created.

- **Scheduled content**

  If you intend to stop the scheduled activities (such as scheduled actions and saved questions) that target those computers, you must disable, edit, or delete the corresponding configurations.

- **Question targeting**

  Endpoints continue to match targeting questions as long as they match the sensor filter expression or manual group ID. The manual group ID obtained during registration is never erased from the Tanium Client configuration, so targeting questions based on a manual group ID continue to match as well.

- **Filter/management groups**

  Deleting a computer management group through the **Administration > Permissions > Computer Groups** page removes all instances of the group from the Tanium Server even if the group also functions as a filter group. However, if you use the **Content > Filter Groups** page to delete a filter group that also functions as a management group, the group remains on from the Server as a management group with filtering disabled.

NOTE

To delete a filter group, see Delete filter groups on page 481.

© 2026 Tanium Inc. All Rights Reserved

When you are ready to delete the computer management group, perform the following steps.

1. From the Main menu, go to **Administration > Permissions > Computer Groups**.
2. Select the computer group and click Delete .

© 2026 Tanium Inc. All Rights Reserved

Managing users

Users overview

A user configuration defines which personas, user groups, computer management groups, and roles are assigned to a user account. Add or remove users based on personnel changes and update the assignments to accommodate RBAC changes in your environment. For example, you might want certain users to have a role that enables approving the actions that other users deploy.

BEST PRACTICE

Review and, if necessary, update user accounts on a quarterly basis to ensure that account configurations reflect personnel changes as users leave, join, or change roles in your organization. For more information, see Tanium Maintenance User Guide: Review and update Console user accounts.

Understand the best practices for users before you create or edit user accounts. For more information, see User permissions on page 560.

NOTE

For the user role permissions required to manage users, see Manage users on page 104.

If you imported Tanium solutions with default settings, the service account that the solutions use to run background processes is the user account that performed the import. For more information, see Manage service accounts for solutions on page 144.

Local and imported user accounts

You can create user accounts locally on the Tanium Server or import them from a Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server.

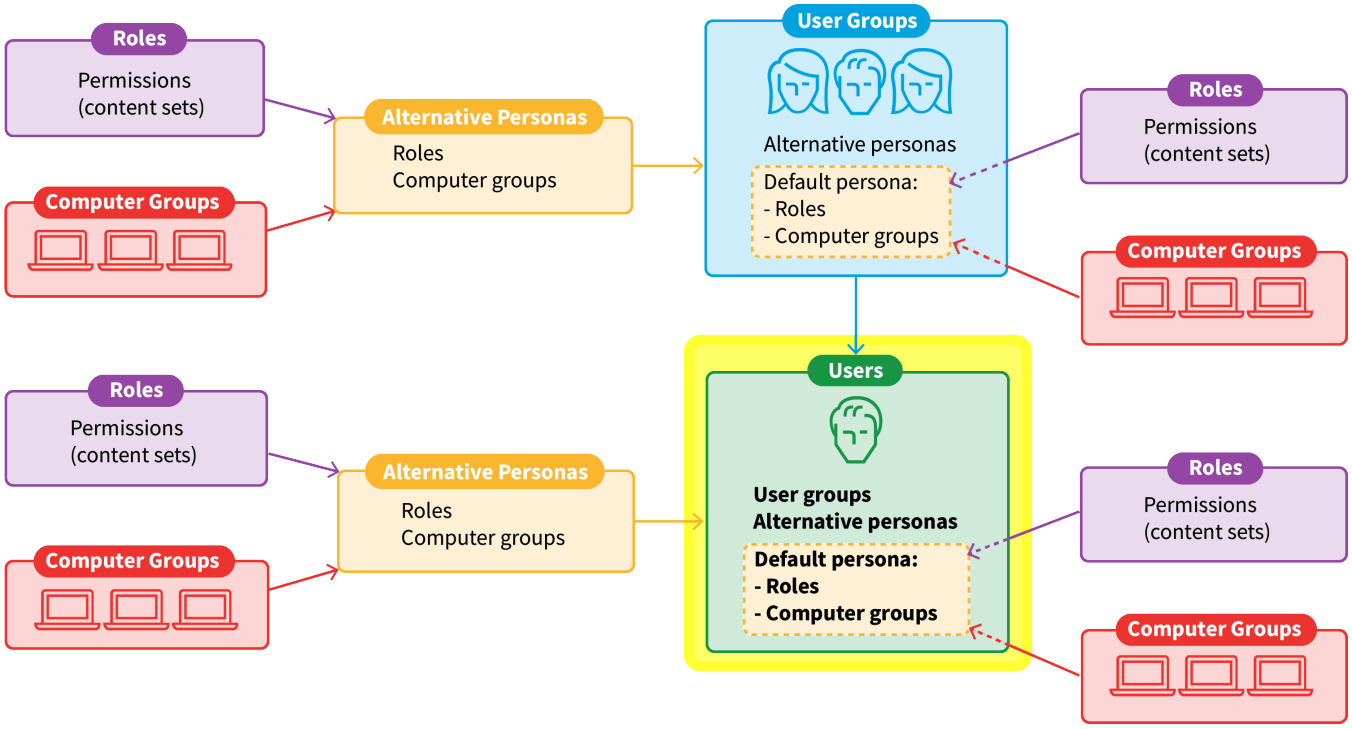
If your deployment requires both local and imported users, configure the imports first. For more information, see Importing and authenticating users through LDAP on page 666.

User assignments in Tanium RBAC

The following figure illustrates the relationship between users and other RBAC components in a Tanium environment:

© 2026 Tanium Inc. All Rights Reserved

RBAC components and assignments in user configurations



User authentication

Users must authenticate when they access Tanium Console or the Tanium API as a measure to help secure your environment.

You can configure the following authentication methods:

User authentication methods for Console and API access

Authentication method	Description
LDAP server	If you import users from an LDAP server, you have the option to use the server as the authentication source. For more information, see Importing and authenticating users through LDAP on page 666.
SAML	You can configure single sign-on (SSO) if your Tanium environment integrates with a Security Assertion Markup Language (SAML) identity provider (IdP). For more information, see Enabling SSO through SAML on page 684.
AD server	(Windows only) Users can authenticate through the AD server for the domain to which the Tanium Server is joined.
Windows authentication	(Windows only) Windows authentication is available for accounts that are defined locally on a Tanium Server. The user passwords are stored in the Windows user database, not in the Tanium database.
Local authentication service	(Appliance only) Users can authenticate through a local service. For more information, see Tanium Appliance User Guide: Configure the local authentication service.

© 2026 Tanium Inc. All Rights Reserved

NOTE

For more information about settings and events that affect the duration of Tanium Console sessions and how often users must re-authenticate, see Configure Console user preferences on page 155 and Sign in to Console on page 49.

If users have issues signing in to Tanium Console, see Troubleshoot Console access on page 702.

BEST PRACTICE

If you use an external service for authentication, maintain at least one user account that relies on local authentication and assign the **Administrator** reserved role to that account. If the external service ever becomes unavailable (for example, the connection to the LDAP server or SAML IdP goes down), this local user can still access Tanium Console and reconfigure the connection to the external service as necessary. Optionally, you can use the default user that is created during Tanium Server installation for this purpose.

Default user

The Tanium Server installation process creates a Tanium Console user account that has permissions similar to the root or admin superuser in some operating systems. This initial user is assigned the **All Computers** computer group and the **Administrator** reserved role, enabling this user to perform any Tanium workflow. However, this user is not a built-in user like root or admin, so you can modify or delete the account. For more information about creating the default user during Server installation, see the guide for your infrastructure:

- Tanium Appliance Deployment Guide: Install Tanium roles
- Tanium Core Platform User Guide for Windows Deployments: Install the Tanium Server: See the **Set Administrator Account** settings.

View user details

As part of quarterly maintenance for your Tanium environment, review user settings and update them if necessary to ensure that account configurations and permissions reflect personnel changes as users leave, join, or change roles in your organization. In particular, ensure that users can access all the Tanium features they need but without access to sensitive information they do not need. Also review how users are configured to authenticate for Tanium Console and API access.

1. From the Main menu, go to **Administration > Permissions > Users**.
   The **Users** grid displays the following basic attributes of each user.

   TIP

   To show columns that are hidden by default, click Customize Columns and select the columns.

© 2026 Tanium Inc. All Rights Reserved

User account attributes

Attribute	Description
ID (hidden by default)	The identifier that the Tanium Server assigns to the user account when it is created or initially imported. The ID uniquely identifies the user within the Tanium environment.
Name	The user name of the account.
Display Name	An optional name that appears in square brackets [ ] beside the user name in the Environment details on page 56 and Part 2: Getting started with Console and Interact on page 47 of the Console header. To edit the **Display Name**, see Configure user display name and properties on page 631.
Status (hidden by default)	Shows whether the user is active or deleted. For more information, see Delete, un-delete, or lock out a user on page 640.
Domain	The Active Directory (AD) domain that the Tanium Server joins to authenticate users that it imports from an AD server. This column is blank if the Tanium Server does not import from an AD server. For more information, see Importing and authenticating users through LDAP on page 666.
Computer Groups	The number of computer management groups that are assigned to the user account. The value `Unrestricted` indicates that the user has management rights for all endpoints. For more information, see Manage computer group assignments for a user on page 636.
User Groups	The number of user groups to which the user is assigned. For more information, see Manage user group assignments for a user on page 635.
Locked Out	Shows whether the user is locked out. For more information, see Locked-out users on page 641.
Last Sign In	The date and time when the user last signed in to Tanium Console.
Created Date	The date and time when the user account was created on, or initially imported into, your Tanium environment.
Source (hidden by default)	Shows whether the user account is: • **Local** to the Tanium Server and uses a local authentication service. For more information, see Disable or enable local user access on page 642. • **External**, which means that the Tanium Server imported the account from an IdP, AD server, or LDAP server. For more information, see Importing and authenticating users through LDAP on page 666 or Enabling SSO through SAML on page 684.
The following attributes appy only if System for Cross-domain Identity Management (SCIM) is configured in your environment. Otherwise, the columns are blank. These attributes can help you troubleshoot if user accounts fall out of sync between Tanium Cloud and your IdP. For more information, see Tanium Cloud User Guide: Configure SCIM provisioning.	
External ID (hidden by default)	Shows the identifier that is assigned to the user account on the SCIM server.

© 2026 Tanium Inc. All Rights Reserved

User account attributes (continued)

Attribute	Description
Reflected ID (hidden by default)	Shows the identifier that Tanium Cloud assigns to the user account to uniquely identify it on the IdP. Tanium Cloud uses the **Reflected ID** of a user because its value never overlaps with the **Reflected ID** of a user group. By contrast, a user and user group might have the same ID on page 628 value, in which case that value could not uniquely identify the user or group on the IdP.
SCIM Server Name (hidden by default)	The name of the SCIM server. This matches the **Identify Provider Name** that is configured in Tanium Cloud.

2. (Optional) Use the filters to find specific users:
   - **Status**: By default, the **Users** toggle is set to **Active**, and the grid does not show user accounts that are deleted or locked out. To show all accounts regardless of status, set the toggle to **All**.
   - **Text**: Enter a text string in the **Filter items** field to filter the grid by user name, display name, or domain name.
   - **Attribute**: Expand the **Filters** section, select a user attribute (such as **Name**), select an operator (such as **contains**), enter a text string that contains all or part of the attribute value, and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.
3. (Optional) Click the user **Name** to see the names of user groups, computer groups, personas, roles, and permissions that are assigned to a user. For more information, see View effective role permissions for a user on page 631.

Create a user

All users who require access to Tanium Console and the Tanium API require user configurations on the Tanium Server. Users access Console and the API by authenticating through services such as an LDAP server or SAML IdP. The roles, computer groups, and other RBAC components that you assign to users control access to specific solutions and features.

LDAP integrations

Create only the user configurations that the Tanium Server does not import from an AD or LDAP server. For more information, see Importing and authenticating users through LDAP on page 666.

SAML integrations

If you create users who are local to the Tanium Server and who authenticate through a SAML IdP, work with the IdP administrator to ensure that their user accounts are also configured in the remote identity store. For more information, see Enabling SSO through SAML on page 684.

RBAC assignments

Assigning roles, alternative personas, and computer groups to a user account is optional. However, a user with no roles cannot access anything after signing in to Tanium Console. You can assign roles and computer groups directly to the user (default persona) or assign them to alternative personas and user groups that you assign to the user. If you Set the default user group on page 652, all new users are automatically assigned to it. Otherwise, you must manually assign users to groups.

© 2026 Tanium Inc. All Rights Reserved

BEST PRACTICE

Managing user role, computer group, and persona assignments through user groups is a best practice. By combining that practice with a default user group, you can automatically provision new users with all the RBAC permissions that they need.

Create a local or AD user

1. From the Main menu, go to **Administration > Permissions > Users** and click **New User**.
2. Specify a **User Name** that matches one of the following:
   - **Local account**: Enter the name of a user account that is defined locally on the Tanium Server. If the account does not yet exist on the Server, a later step in this procedure describes how to add it.
   - **AD account** (Windows deployment only). Enter just the user name, not the domain name. The Tanium Server uses Windows Authentication, and does not store or manage sign-in credentials for the user.

   NOTE

   The name cannot exceed 255 characters.
3. Configure any settings that the user requires but does not inherit from a default user group, and then click **Save**. If necessary, you can reassign the user to a user group other than the default group.
   - Configure user display name and properties on page 631
   - Configure role assignments for a user on page 635
   - Manage user group assignments for a user on page 635
   - Manage computer group assignments for a user on page 636
   - Manage persona assignments for a user on page 635
4. (Tanium Appliance deployment only) Add the user account on the Appliance and configure the local authentication service as described in Tanium Appliance User Guide: Configure the local authentication service.
5. (Windows deployment, local account only) Add the user account on the Tanium Server if it does not yet exist there:
   a. Sign in to the Tanium Server host as the **Administrator** user.
   b. From the Windows menu, open the **Control Panel**.
   c. Select **User Accounts**, click **Manage another account**, and click **Add a user account**.
   d. Complete the following fields and click **Next**:
      - **User name**
      - **Password**
      - **Reenter password**

© 2026 Tanium Inc. All Rights Reserved

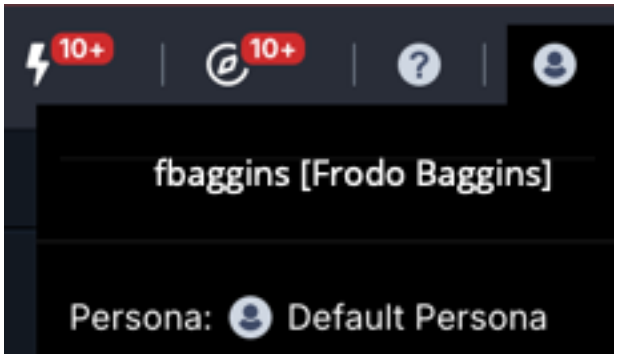
- **Password hint**

e. Click **Finish** and verify that the list of accounts includes the one that you just added.

Configure user display name and properties

When you open the user dropdown list in the Console header, it shows the user name of the signed-in account. Optionally, you can add a display name for each user to appear in brackets beside the user name. For example, you might enter display names that users more easily recognize than user names that follow a less familiar convention. You can also configure user properties, which are name-value pairs that record optional details. For example, you might find it useful to add email addresses and phone numbers for the sake of administrators who might want to contact users.

User display name in Console header



1. From the Main menu, go to **Administration > Permissions > Users**.
2. Click the user **Name** and click **Edit Mode**.
3. Enter a **Display Name**.
4. Update properties as follows and then click **Save**:
   - **Add**: Click **Add properties** or, if the user already has some properties, click Add, and then enter a name-value pair in the text fields.
   - **Edit**: Overwrite the entries of existing name-value pairs.
   - **Delete**: Click Delete beside a name-value pair.

Manage role assignments for a user

For an overview of how effective permissions are derived for a user, and to view the roles and associated content sets that are assigned to a user, see View effective role permissions for a user on page 631.

To assign or unassign roles and associated content sets for a user, see Configure role assignments for a user on page 635.

View effective role permissions for a user

The effective permissions of a user are based on the cumulative effect of all the assigned and inherited roles, including:

© 2026 Tanium Inc. All Rights Reserved

- Permissions specified in allow roles minus permissions specified in deny roles
- Implicitly provided permissions in allow roles

Perform the following steps to view the effective permissions for a user:

1. From the Main menu, go to **Administration > Permissions > Users** and click the user **Name**.
2. Review the assigned and inherited roles, permissions, and content sets. The page displays icons to indicate:
   Allow roles or permissions
   Deny roles or permissions

   > NOTE
   >
   > The role configuration pages indicate whether permissions are explicitly assigned or implicitly provided. For more information, see View effective role permissions on page 588.
   >
   > If you assign reserved roles (such as **Administrator**), they appear under **Global Permissions** with a single **special** permission .
3. (Optional) Expand an individual permission to review the content sets that are assigned to it. Only solution content permission (such as **Trends Administrator** permission) and platform content permissions (such as **Sensor** read permission) are associated with content sets. The page displays icons to indicate the type of permission to which the content sets are assigned:
   Allow permission
   Deny permission

© 2026 Tanium Inc. All Rights Reserved

Effective permissions for a user

© 2026 Tanium Inc. All Rights Reserved

Permissions

	SPECIAL	READ	WRITE	EXECUTE	DELETE
Administration					
Action Group		✓	✓		
Computer Group		✓	✓		
Server Status		⊘			
Feed					
Feed	✓ SHOW				
Interact					
Ask Dynamic Questions	✓				
Interact	✓ SHOW				
Interact Module		✓	✓		
Platform Content Permissions					
Approve Action	⊘				
Default Filter Groups	●				
Interact	●				
Bypass Action Approval	⊘				
Dashboard		✓	✓		
Dashboard Group		✓	✓		
Filter Group		✓			
Own Action		✓			
Package		✓			
Default Filter Groups		●			
Interact		●			
Plugin		✓		✓	
Saved Question		✓	✓		
Sensor		✓			

Content Sets

40 of **40** Items

Filter Items

Filters

Type	Content Set	Used By	SPECIAL	READ	WRITE	EXECUTE	DELETE
Interact Module	Reserved			✓	✓		
Show	Reserved		✓				
Package	Default Filter Groups			✓			
Package	Interact			✓			
Own Action	Default Filter Groups			✓			
Own Action	Interact			✓			

Configure role assignments for a user

Perform the following steps to update the role assignments for the default persona of a user.

> **NOTE** To configure roles through an alternative persona, edit the persona configuration and assign the persona to the user. For more information, see Manage role assignments for a persona on page 658 and Manage persona assignments for a user on page 635.

1. From the Main menu, go to **Administration > Permissions > Users**.
2. Click the user **Name** and click **Edit Mode**.
3. In the **Roles** section, click **Manage Roles**.
4. Select or deselect roles and click **Apply**.
5. (Optional) Review the **Permissions** and **Content Sets** that are associated with the selected roles. For more information, see View effective role permissions for a user on page 631.
6. Click **Save**.

Manage user group assignments for a user

A user inherits roles, computer groups, and alternative personas from the user groups that you assign to the user.

1. From the Main menu, go to **Administration > Permissions > Users**.
2. Click the user **Name** and click **Edit Mode**.
3. Expand the **User Groups** section and click **Manage User Groups**.
4. Select or deselect user groups and click **Select**.
5. Review the inherited **Roles**, **Permissions**, **Content Sets**, and **Computer Groups**, and then click **Save**.

Manage persona assignments for a user

After a user signs in for a Tanium session, the user can switch the session to any persona that you assign to the user account. The Tanium Server automatically assigns a default persona to new user accounts. You must manually assign alternative personas through the following steps.

> **NOTE** For more information about personas, see Managing role and computer group permissions through personas on page 655.

© 2026 Tanium Inc. All Rights Reserved

1. Sign in to Tanium Console as a user who is assigned the **Administrator** reserved role.
2. From the Main menu, go to **Administration > Permissions > Users**.
3. Click the user **Name** and click **Edit Mode**.
4. Expand the **Personas** section and click **Manage Personas**.
5. Select or deselect personas, and click **Select**.
6. Review the assigned **Personas** and click **Save**.

Manage computer group assignments for a user

A user can view question results from, and deploy actions to, only the endpoints that belong to a computer management group that is assigned to the user. You can assign up to 255 computer management groups to each user. The user limit does not include computer groups that a user inherits from user groups. For example, if you assign 255 computer groups to a user, that user can still inherit up to 255 computer groups from each user group to which the user belongs.

Perform the following steps to update the computer management group assignments for the default persona of a user.

NOTE

To assign computer groups through alternative personas, add the groups to the personas and assign the personas to the user or a user group to which the user belongs. For more information, see Manage computer group assignments for a persona on page 662, Manage persona assignments for a user on page 635, and Manage persona assignments for a user group on page 650.

To provide a user access to computer filter groups, assign a role with filter group permissions to the user. For more information, see Managing filter groups for filtering questions and results on page 476 and Manage role assignments for a user on page 631.

1. From the Main menu, go to **Administration > Permissions > Users**.
2. Click the user **Name** and click **Edit Mode**.
3. Expand the **Computer Groups** section.
4. If you want the user to have management rights for all endpoints, select **Unrestricted Management Rights** and click **Save** (you can skip the remaining steps).

IMPORTANT

Tanium strongly recommends that you do not assign **Unrestricted Management Rights**, unless you want the user to be able to manage all endpoints across all computer groups regardless of security considerations.

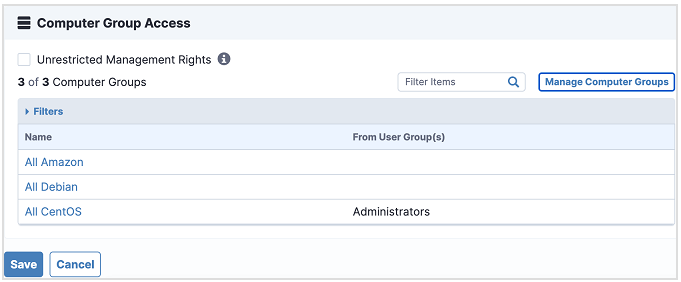
© 2026 Tanium Inc. All Rights Reserved

5. Click **Manage Computer Groups**, select or deselect computer management groups, and click **Select**.

   NOTE

   Selections are logically combined. For example, the union of **All Computers** and **No Computers** is effectively **All Computers**.

6. Review the list of computer groups that you assigned or that the user inherits from user groups, and then click **Save**.



Delete content or transfer ownership

By default, the user account or persona that a user selects for a Tanium Console or API session is the owner of any content that the user creates during the session. Consider transferring ownership of content if you plan to perform any of the following operations for user accounts or personas:

- **Delete users or personas**: Scheduled content (such as an action) stops running if you delete the user accounts or personas that own the content. Transferring content ensures that it continues running.
- **Change RBAC assignments**: Unassigning role permissions or computer groups from a user account or persona can affect scheduled content that the user or persona owns. For example, if you unassign the **All Windows** computer group from a user who owns scheduled actions, those actions stop deploying to Windows endpoints. To prevent RBAC-related disruptions to scheduled content, transfer the content before unassigning role permissions or computer groups from the current owners of that content.

You can delete content instead of transferring it if the owner no longer needs the content and no other user or persona needs it.

BEST PRACTICE

The best practice is to transfer content before deleting a user or persona to ensure content continues running without interruption. However, you can also transfer content after the deletion. For more information, see Considerations when deleting users on page 640.

NOTE

You require the **Administrator** reserved role to transfer or delete content through the **Manage Content** page as described in the following tasks. For the permissions to delete content through other pages, see Content management permissions on page 97.

© 2026 Tanium Inc. All Rights Reserved

Delete or transfer the content of an active user

Transfer content ownership or delete content for one user at a time as described in the following steps.



Transfer content only to personas and active (not locked out) user accounts that have the same role and computer group assignments as the current owners. To review the role and computer group assignments of users or personas, see View user details on page 627 or View persona details on page 656.

1. From the Main menu, go to **Administration > Permissions > Users**.
2. Select the user that owns the content and click **Transfer**. If an alternative persona owns the content, select a user to whom the persona is assigned.
3. Select a **Persona** to list the **Content** that it owns:
    - ***<Persona name>***: List the content of a specific alternative persona that is assigned to the user.
    - **All Personas**: List the content of the user account (default persona) and all the alternative personas that are assigned to the user.
    - **(Default Persona)**: List the content of the user account.
4. Select **Content** that requires the same transfer or delete operation. For example, select all the actions and questions that you want to transfer to the same user. To transfer content to multiple users, you must repeat this step and the next step for each user.

    To reassign content to a different content set before transferring, click the name in the **Content Set** column to open the configuration page for that content set. After you reassign content, return to the first step in the content transfer workflow. For more information, see Move content between content sets on page 565.
5. Click one of the following buttons:
    - **Transfer**: The **Select the persona that will receive the content** dropdown lists each user and persona in the format ***<user>, <persona>***. Select the user and persona of the new owner and click **Transfer** to proceed.
    - **Delete**: Review the content that you selected and click **Delete** to proceed.

Delete or transfer the content of a non-active user

The **Deleted User Content** page lists user accounts that are deleted or locked out and that own content. Use the page to delete the content or transfer its ownership.



Transfer content only to personas and active (not locked out) user accounts that have the same role and computer group assignments as the current owners. To review the role and computer group assignments of users or personas, see View user details on page 627 or View persona details on page 656.

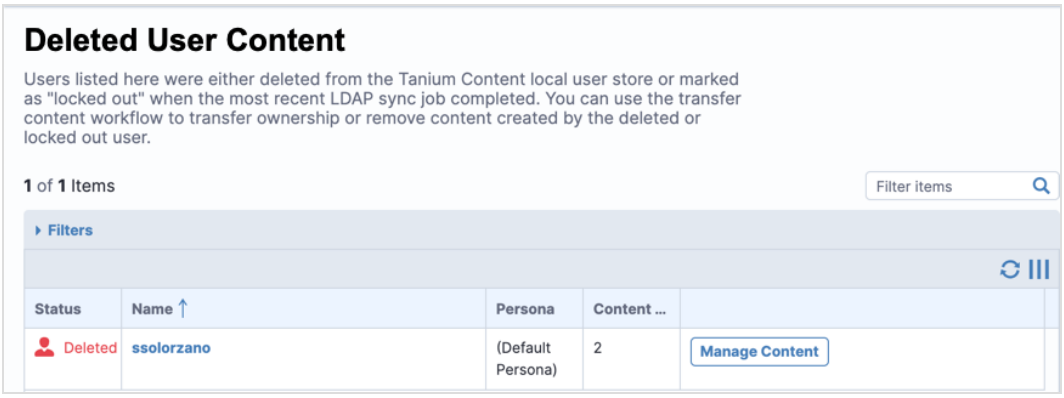
© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

You cannot delete a persona that owns content.

Delete content or transfer content ownership for one user at a time:

1. From the Main menu, go to **Administration > Permissions > Deleted User Content**.
2. Click **Manage Content** in the row of the user account (persona) for which you want to transfer content.



3. Select content that requires the same transfer or delete operation. For example, select all the actions and questions that you want to transfer to the same user. To transfer content to multiple users, you must repeat this step and the next step for each user.

   TIP

   To reassign content to a different content set before transferring, click the name in the **Content Set** column to open the configuration page for that content set. After you reassign content, return to the first step in the content transfer workflow. For more information, see Move content between content sets on page 565.

4. Click one of the following buttons:
   - **Transfer**: Select the user name (persona) of the new owner and click **Transfer** to proceed.
   - **Delete**: Review the content that you selected and click **Delete** to proceed.

Export user details

You can export user account details as a CSV file. When you open the file in an application that supports CSV format, it lists the users with the same attributes (columns) as the Console **Users** grid displays and (optionally) lists the RBAC assignments of each user. Displaying the grid in a CSV application is useful when you want to customize the display. For example, you can use Microsoft Excel to create charts based on user attributes.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Permissions > Users**.
2. (Optional) To add or remove attributes (columns) for the CSV file, click Customize Columns in the grid and select the attributes.
3. Select rows in the grid to export only specific users. If you want to export all users, skip this step.
4. Click Export.
5. (Optional) Edit the default export **File Name**. The Tanium Server automatically appends the file suffix (`.csv`).
6. Select an **Export Data** option: **All** users in the grid or just the **Selected** users.
7. Set the file **Format** to **List of Users - CSV**. Optionally, select **With RBAC Details** to include the names of user groups, roles, personas, and computer groups that are assigned to users. For users that are members of user groups, the exported data includes the names of roles, personas, and computer groups that the users inherit.
8. Click **Export**.
   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

Copy user configuration details

Copy configuration details from the grid in the **Users** page to your clipboard for pasting into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the content that you copy.

1. From the Main menu, go to **Administration > Permissions > Users**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy.
   - **Copy cell information**: Hover over the cell, click Options, and click Copy.

Delete, un-delete, or lock out a user

You have the following options for locking down user access to the Tanium environment when users leave your organization:

- Assign the Deny All role to the user. The user can still sign in to Tanium Console, but cannot access any Console functionality.
- Delete the Console configuration for a manually created user.
- Disable the AD or LDAP user account that is associated with the Console user configuration, or change the password if it is an administrator alias account. If the Tanium Server imported the user through an LDAP server, it is important to modify the user details on the LDAP server so that the Tanium Server does not import the user again at the next synchronization. When you disable a user account on the LDAP server, the account has locked out status on the Tanium Server. For more information, see Locked-out users on page 641.

Considerations when deleting users

When you delete a user or persona, scheduled content that the user or persona owns stops running, including:

© 2026 Tanium Inc. All Rights Reserved

- Plugin schedules
- Scheduled saved questions
- Scheduled actions
- Tasks for specific Tanium solutions

Locked-out users

The Tanium Server designates imported user accounts as *locked out* when the associated account on the LDAP server or IdP is disabled or (LDAP only) when the data is missing. While the account has locked-out status, the user cannot sign in, but scheduled content that the user owns continues to run.



Locked-out status is applicable for IdP user accounts only if the accounts are provisioned through System for Cross-Domain Identity Management (SCIM).



When off-boarding employees, disable LDAP accounts rather than delete them to avoid deleting associated records.

The **Administration > Permissions > Users** page shows the **Locked out** status of users:

- **Locked out - Disabled**: The latest data from the LDAP server or IdP indicates that the user account is disabled.
- **Locked out - Missing**: The latest LDAP synchronization returned no data for the user. Data might be missing if the user was deleted from the LDAP server or otherwise no longer matches the filter expression that the LDAP server uses.

Check the policy of your organization for managing locked-out users. One option is to delete them and transfer the content that they own to another user. For more information, see Delete content or transfer ownership on page 637.

Delete a user

1. From the Main menu, go to **Administration > Permissions > Users** and select the user.
2. Click Delete and **Confirm**.

To display deleted users, set the **Users** toggle to **All** (default is **Active** users only). The **Status** column indicates which users are active or deleted.

To transfer or delete content that the deleted user owned, see Delete content or transfer ownership on page 637.

Un-delete a user

By default, the persona that a user selects for a Tanium Console or API session is the owner of any content that the user creates during the session. When you un-delete users who own content, you can delete or transfer ownership of that content.

© 2026 Tanium Inc. All Rights Reserved

Un-delete one user at a time:

1. From the Main menu, go to **Administration > Permissions > Users**.
2. Set the **Users** toggle to **All** (default is **Active** users only).
   The **Status** column indicates which users are active or deleted .
3. Select the row for the deleted user, click Undelete User , and click **Confirm**.

Disable or enable local user access

By default, users whose accounts are local to the Tanium Server can access Tanium Console. However, if you transition to an external authentication service such as an LDAP server or SAML IdP and you want to ensure all user access is through that service, disable local authentication.

BEST PRACTICE

Maintain at least one user account that relies on local authentication and assign the **Administrator** reserved role to that account. If the external authentication service ever becomes unavailable (for example, the connection to the LDAP server or SAML IdP goes down), this local user can still access Tanium Console and reconfigure the connection to the external service as necessary. Optionally, you can use the default user that is created during Tanium Server installation for this purpose.

Local users on a Tanium Appliance

To disable or re-enable Tanium Console access for user accounts that are local to a Tanium Appliance, see Tanium Appliance User Guide: Configure the local authentication service.

Local users on a Windows server

Perform the following steps to disable or re-enable Tanium Console access for user accounts that are local to a Tanium Server installed on a Windows server.

IMPORTANT

If you disable local account sign ins and the remote authentication service later stops working (for example, the connection to the LDAP server or SAML IdP goes down), no users can access Tanium Console, including the default user. In such cases, you must re-enable local authentication through the CLI by running the following command from the Tanium Server installation folder:

```
TaniumReceiver global-settings set soap_enable_local_auth 1
```

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.
2. In the **Name** column, click **soap_enable_local_auth**.
3. In the **Value**, enter `0` to disable or `1` to enable local authentication, and then click **Save**.

© 2026 Tanium Inc. All Rights Reserved

Managing user groups

User groups overview

A user group configuration defines which personas, users, computer management groups, and roles are assigned to a user group. The assigned users inherit personas, computer groups, and roles from the user groups. You can add or remove user groups based on organizational changes and update the assignments to accommodate RBAC changes in your environment. For example, you might want users in a certain user group to inherit a role that enables approving the actions that other users deploy.

BEST PRACTICE

Understand the best practices for user groups before you create or edit groups. For more information, see User group permissions on page 560.

NOTE

For the role permissions that are required to manage user groups, see Manage user groups on page 105.

If Tanium Console displays permission errors (such as `RBACInsufficientPrivilege`) for permissions that you expected your user account to inherit from a user group, see Troubleshoot permission issues on page 713.

Local and imported user groups

You can create user groups locally on the Tanium Server or import them from a Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server. After you create or import user groups, you must assign roles, computer groups, and personas to them. For user groups that you create locally, you must also assign users.

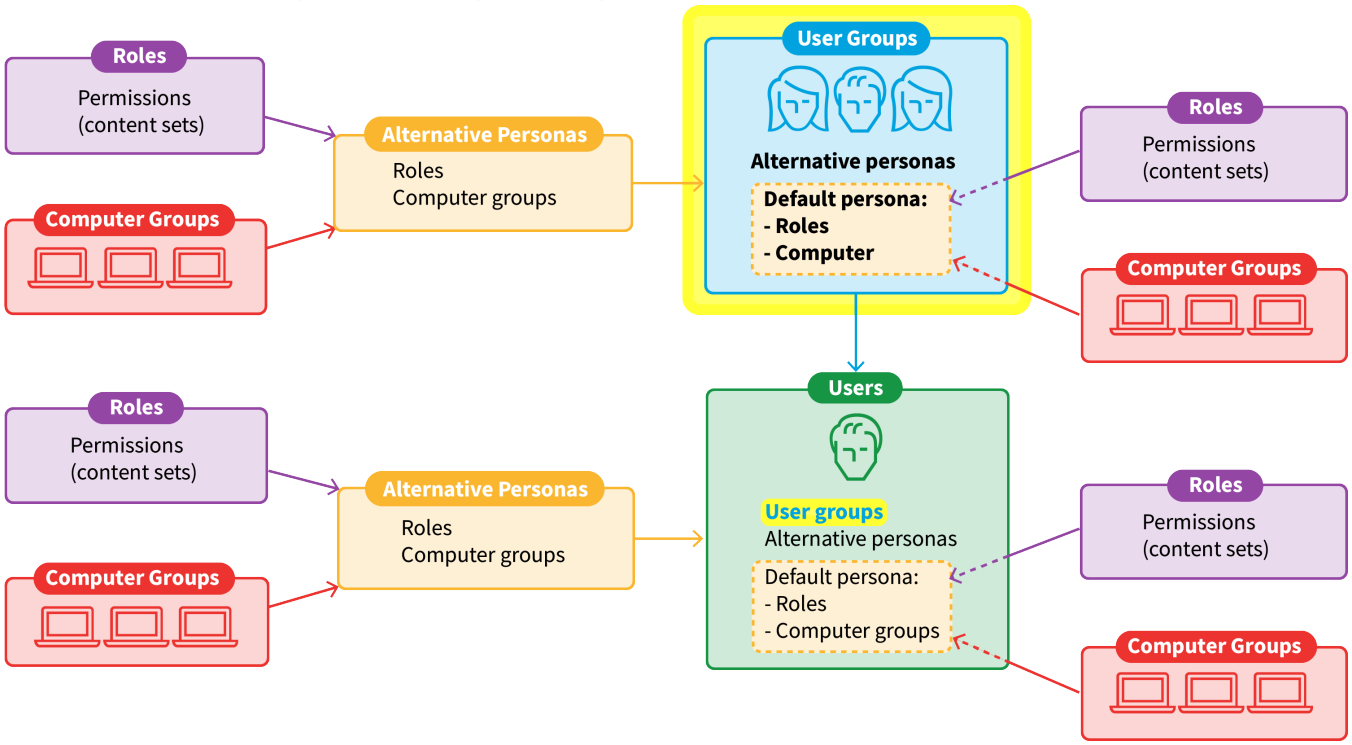
If your deployment requires both local and imported groups, configure the imports first. For more information, see Importing and authenticating users through LDAP on page 666.

User group assignments in Tanium RBAC

The following figure illustrates the relationship between user groups and other RBAC components in a Tanium environment:

© 2026 Tanium Inc. All Rights Reserved

RBAC components and assignments in user group configurations



View user group details

As part of quarterly maintenance for your Tanium environment, review user group settings and update them if necessary to ensure that the permissions that users inherit from the groups reflect personnel changes as users leave, join, or change roles in your organization. In particular, ensure that user groups provide users with access to all the Tanium features that they need but without access to sensitive information they do not need.

1. From the Main menu, go to **Administration > Permissions > User Groups**.

   The **User Groups** grid displays the following basic attributes of each user group.

   > TIP To show columns that are hidden by default, click Customize Columns and select the columns.

   User group attributes

Attribute	Description
ID (hidden by default)	The identifier that the Tanium Server assigns to the user group when it is created or initially imported. The ID uniquely identifies the group within the Tanium environment.
Name	The name of the user group. A star beside the name indicates the default user group. For more information, see Set the default user group on page 652.

© 2026 Tanium Inc. All Rights Reserved

User group attributes (continued)

Attribute	Description
Computer Groups	The number of computer management groups that are assigned to the user group. For more information, see Manage computer group assignments for a user group on page 651.
Users	The number of users that are assigned to the user group. For more information, see Manage user assignments for a user group on page 650.
Source (hidden by default)	Shows whether the user group is: • **Local** to the Tanium Server. • **External**, which means that the Tanium Server imported the group from an IdP, AD server, or LDAP server. For more information, see Importing and authenticating users through LDAP on page 666 or Enabling SSO through SAML on page 684.
The following attributes apply only if System for Cross-domain Identity Management (SCIM) is configured in your environment. Otherwise, the columns are blank. These attributes can help you troubleshoot if user groups fall out of sync between Tanium Cloud and your IdP.	
External ID (hidden by default)	Shows the identifier that is assigned to the user group on the SCIM server.
Reflected ID (hidden by default)	Shows the identifier that Tanium Cloud assigns to the user group to uniquely identify it on the IdP. Tanium Cloud uses the **Reflected ID** of a group because its value never overlaps with the **Reflected ID** of a user account. By contrast, a user group and user might have the same ID on page 644 value, in which case that value could not uniquely identify the group or user on the IdP.
SCIM Server Name (hidden by default)	The name of the SCIM server. This matches the **Identify Provider Name** that is configured in Tanium Cloud.

2. (Optional) Use the filters to find specific user groups:
   - **Text**: Enter a text string in the **Filter items** field to filter the grid by user group name.
   - **Attribute**: Expand the **Filters** section, select a group attribute (such as **Name**), select an operator (such as **contains**), enter a text string that contains all or part of the attribute value, and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.
3. Click the user group **Name** to see the names of users, computer groups, personas, roles, and permissions that are assigned to a user group. For more information, see View effective role permissions for a user group on page 646.

Configure a user group

You can create a user group for each set of role, persona, and computer group assignments that multiple users share. Perform the following steps to configure a user group that is local to the Tanium Server. Do not create configurations for groups that you import from an LDAP server. For more information, see Importing and authenticating users through LDAP on page 666.

© 2026 Tanium Inc. All Rights Reserved

TIP

To add a user group that has many settings in common with an existing group, cloning the existing group and then modifying the clone is often a quicker method than configuring a new group from scratch.

1. From the Main menu, go to **Administration > Permissions > User Groups** and perform one of the following steps:
   - **Create a user group from scratch**: Click **New User Group**.
   - **Clone a user group**: Select the user group and click **Clone**.
   - **Edit a user group**: Click the user group **Name** and click **Edit Mode**.
2. Enter a **User Group Name** of up to 255 characters to identify the group.
3. Assign roles, users, computer groups, and personas to the user group:
   - Manage role assignments for a user group on page 646
   - Manage user assignments for a user group on page 650
   - Manage persona assignments for a user group on page 650
   - Manage computer group assignments for a user group on page 651
4. Review the assignments and click **Save**.

Manage role assignments for a user group

For an overview of how effective permissions are derived for a user group, and to view the roles and associated content sets that are assigned to a user group, see View effective role permissions for a user group on page 646.

To assign or unassign roles and associated content sets for a user group, see Configure role assignments for a user group on page 650.

View effective role permissions for a user group

The effective permissions of a user group are based on the cumulative effect of all the assigned roles, including:

- Permissions specified in allow roles minus permissions specified in deny roles
- Implicitly provided permissions in allow roles

Perform the following steps to see the effective permissions for a user group:

1. From the Main menu, go to **Administration > Permissions > User Groups** and click the user group **Name**.
2. Review the assigned and inherited roles, permissions, and content sets. The page displays icons to indicate:
   Allow roles or permissions
   Deny roles or permissions

© 2026 Tanium Inc. All Rights Reserved

NOTE

The role configuration pages indicate whether permissions are explicitly assigned or implicitly provided. For more information, see View effective role permissions on page 588.

If you assign reserved roles (such as **Administrator**), they appear under **Global Permissions** with a single **special** permission .

3. (Optional) Expand an individual permission to review the content sets that are assigned to it. Only solution content permission (such as **Trends Administrator** permission) and platform content permissions (such as **Sensor read** permission) are associated with content sets. The page displays icons to indicate the type of permission to which the content sets are assigned:

   Allow permission

   Deny permission

© 2026 Tanium Inc. All Rights Reserved

Effective permissions of a user group

© 2026 Tanium Inc. All Rights Reserved

Permissions

	SPECIAL	READ	WRITE	EXECUTE	DELETE
Administration					
Action Group		✓	✓		
Computer Group		✓	✓		
Server Status		⊘			
Feed					
Feed	✓ SHOW				
Interact					
Ask Dynamic Questions	✓				
Interact	✓ SHOW				
Interact Module		✓	✓		
Platform Content Permissions					
Approve Action	⊘				
Default Filter Groups	●				
Interact	●				
Bypass Action Approval	⊘				
Dashboard		✓	✓		
Dashboard Group		✓	✓		
Filter Group		✓			
Own Action		✓			
Package		✓			
Default Filter Groups		●			
Interact		●			
Plugin		✓		✓	
Saved Question		✓	✓		
Sensor		✓			

Content Sets

40 of **40** Items

Filter Items

Filters

Type	Content Set	Used By	SPECIAL	READ	WRITE	EXECUTE	DELETE
Interact Module	Reserved			✓	✓		
Show	Reserved		✓				
Package	Default Filter Groups			✓			
Package	Interact			✓			
Own Action	Default Filter Groups			✓			
Own Action	Interact			✓			

Configure role assignments for a user group

Perform the following steps to update role assignments for the default persona of a user group.

> **NOTE** To configure roles through an alternative persona, assign the roles to the persona and assign the persona to the user group. For more information, see Manage role assignments for a persona on page 658 and Manage persona assignments for a user group on page 650.

1. From the Main menu, go to **Administration > Permissions > User Groups**.
2. Click the user group **Name** and click **Edit Mode**.
3. In the **Roles** section, click **Manage Roles**, select or deselect roles, and click **Apply**.
4. (Optional) Review the **Permissions** and **Content Sets** that are associated with the selected roles. For more information, see View effective role permissions for a user group on page 646.
5. Click **Save**.

Manage user assignments for a user group

A user inherits roles and computer management groups from the default persona of the user groups to which you assign that user. When a user selects a persona for a Tanium session, the user can also select any alternative persona that is assigned to the user groups.

1. From the Main menu, go to **Administration > Permissions > User Groups**.
2. Click the user group **Name** and click **Edit Mode**.
3. Expand the **Users** section and click **Manage Users**.
4. Select or deselect users, and click **Select**.
5. Review the assigned **Users** and click **Save**.

Manage persona assignments for a user group

After a user signs in for a Tanium session, the user can switch the session to any persona that you assign to user groups in which the user is a member. The Tanium Server automatically assigns a default persona to new user groups. You must manually update the assignment of alternative personas through the following steps.

> **NOTE** Alternative personas do not inherit roles or computer groups from the user groups to which those personas are assigned. For more information, see Personas overview on page 655.

© 2026 Tanium Inc. All Rights Reserved

1. Sign in to Tanium Console as a user who is assigned the **Administrator** reserved role.
2. From the Main menu, go to **Administration > Permissions > User Groups**.
3. Click the user group **Name** and click **Edit Mode**.
4. Expand the **Personas** section and click **Manage Personas**.
5. Select or deselect personas, and click **Select**.
6. Review the assigned **Personas** and click **Save**.

Manage computer group assignments for a user group

A user inherits computer management groups from the user groups to which you assign the user. You can assign up to 255 computer management groups to each user group.

NOTE

To configure computer group assignments through an alternative persona, assign computer groups to the persona and assign the persona to the user group. For more information, see Manage computer group assignments for a persona on page 662 and Manage persona assignments for a user group on page 650.

To assign filter group permissions to a user group, configure the permissions in the roles that you assign to the user groups. For more information, see Managing filter groups for filtering questions and results on page 476 and Configure role assignments for a user group on page 650.

1. From the Main menu, go to **Administration > Permissions > User Groups**.
2. Click the user group **Name** and click **Edit Mode**.
3. Expand the **Computer Groups** section.

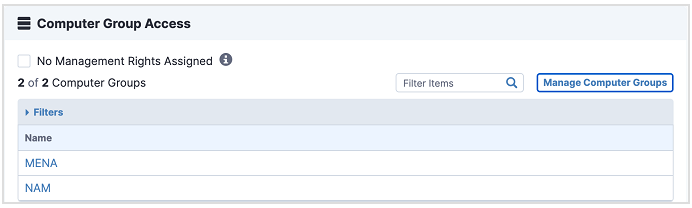
   By default, **No Management Rights Assigned** is selected.
4. If you do not want users to inherit computer groups from this user group, leave **No Management Rights Assigned** selected and click **Save** (skip the remaining steps).
5. Deselect **No Management Rights Assigned**, click **Manage Computer Groups**, select or deselect computer management groups, and click **Select**.

   NOTE

   Selections are logically combined. For example, the union of **All Computers** and **No Computers** is effectively **All Computers**.

© 2026 Tanium Inc. All Rights Reserved

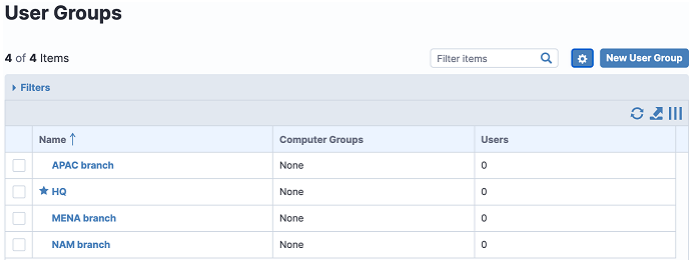
6. Review the assigned computer groups and click **Save**.



Set the default user group

Configuring a default user group is useful in deployments where you expect many new users to belong to the same group. After you set a user group as the default, the Tanium Server automatically assigns it to user accounts that are subsequently added to your remote identity store. The group that is the default has a star beside its name on the **User Groups** page.

Default user group on the User Groups page



NOTE

Write permissions for **User Group** and **Global Settings** are required to set the default user group.

The default user group applies only to users who authenticate through Security Assertion Markup Language (SAML) and are not synchronized with an LDAP server. For more information, see Enabling SSO through SAML on page 684.

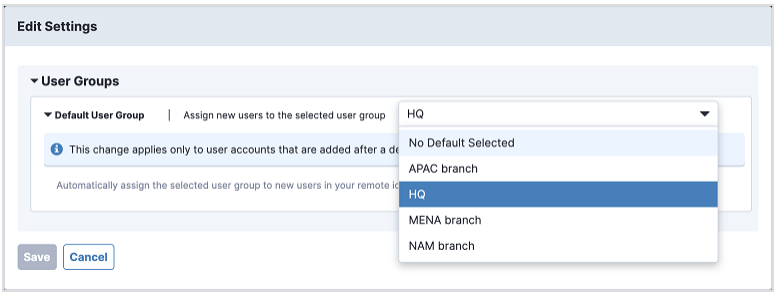
If no user groups are defined, the **User Groups** page does not display the Settings for configuring a default group.

You can also see and modify the default user group on the **Administration > Configuration > Settings > Platform Settings** page through the **Default User Group** setting. For more information, see Manage platform settings on page 163.

Perform the following steps to set the default user group. Select the **No Default Selected** option if you do not want any default user group.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Permissions > User Groups**.
2. Click Settings, select a **Default User Group**, and click **Save**.



Export user group details

You can export user group details as a CSV file. When you open the file in an application that supports CSV format, it lists the groups with the same attributes (columns) as the Console **User Groups** grid displays and (optionally) lists the RBAC assignments of each group. Displaying the grid in a CSV application is useful when you want to customize the display. For example, you can use Microsoft Excel to create charts based on user group attributes.

1. From the Main menu, go to **Administration > Permissions > User Groups**.
2. (Optional) To add or remove attributes (columns) for the CSV file, click Customize Columns in the grid and select the attributes.
3. Select rows in the grid to export only specific user groups. If you want to export all user groups, skip this step.
4. Click Export.
5. (Optional) Edit the default export **File Name**. The Tanium Server automatically appends the file suffix (`.csv`).
6. Select an **Export Data** option: **All** user groups in the grid or just the **Selected** user groups.
7. Set the file **Format** to **List of User Groups - CSV**. Optionally, select **With RBAC Details** to include the names of users, roles, computer groups, and personas that are assigned to the user groups.
8. Click **Export**.
   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

Copy user group configuration details

Copy configuration details from the grid in the **User Groups** page to your clipboard for pasting into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the content that you copy.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Permissions > User Groups**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy.
   - **Copy cell information**: Hover over the cell, click Options, and click Copy.

Delete a user group

When you delete a user group configuration, users stop inheriting personas, computer management groups, and roles from it.

BEST PRACTICE

Before deleting a user group:

1. Delete the persona and user assignments from the user group. For the steps, see Manage user assignments for a user group on page 650 and Manage persona assignments for a user group on page 650.
2. Review the impact that deleting persona and user assignments from the user group has on the effective permissions of users. For the steps, see View effective role permissions for a user group on page 646.

Delete a user group as follows:

1. From the Main menu, go to **Administration > Permissions > User Groups**.
2. Select the group, click Delete Selected, and click **Confirm**.

© 2026 Tanium Inc. All Rights Reserved

Managing role and computer group permissions through personas

Personas overview

A persona is a set of roles and computer groups that a user selects for a Tanium session. Assigning multiple personas to a user account enables you to enforce different sets of restrictions on what that user can see and do with Tanium solutions, based on the work scope for a given session, without having to configure multiple accounts for the user.

For example, users might manage endpoints across multiple countries, each with unique privacy laws restricting the actions that users can deploy to specific endpoints based on security clearance. You might configure one persona with a role that allows actions relating only to Tanium Client maintenance on all computer groups for a particular country. You could give the same user another persona that allows security patch installations but only for the subset of computer groups that the user directly manages.



For the role permissions that are required to manage personas, see Manage personas on page 106.

If Tanium Console displays RBAC errors (such as `RBACInsufficientPrivilege`) when you try to access certain features after switching to a persona, see Troubleshoot permission issues on page 713.



If you plan to import users and user groups from a Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server, do so before configuring and assigning personas. For more information, see Importing and authenticating users through LDAP on page 666.

Persona types

Tanium RBAC includes default and alternative personas.

DEFAULT PERSONA

The permissions of a default persona derive from roles and computer groups that are assigned directly to its associated user account or user group. The default persona of a user inherits permissions and computer groups from the default persona of any user group to which the user is assigned. The Tanium Server automatically assigns the default persona to new users and user groups. Each user and group has only one default persona and it is unique; multiple users and groups cannot share a default persona. You cannot delete default personas or reassign them to different users or groups. The default persona automatically applies when users sign in to Tanium Console.

ALTERNATIVE PERSONA

The permissions of an alternative persona derive only from roles and computer groups that are assigned to the persona. A user can inherit multiple alternative personas from user groups, but only the permissions of the single persona that the user selects for the current Tanium session apply. When you assign alternative personas to a user group, the personas do not inherit permissions from

© 2026 Tanium Inc. All Rights Reserved

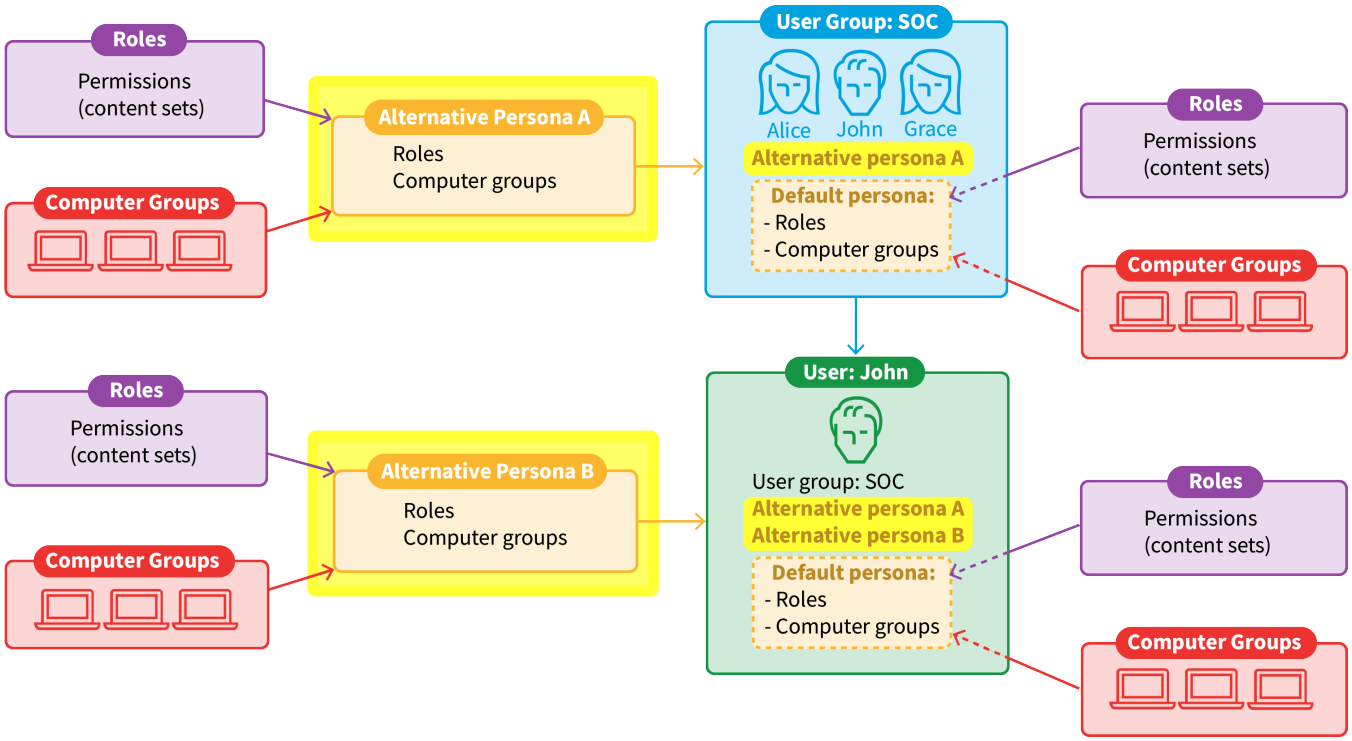
that group. In the example that the figure RBAC components and assignments in persona configurations on page 656 illustrates, persona A is assigned to user group SOC, in which user John is a member. If John switches to persona A, his permissions are limited to the roles and computer groups that are assigned to persona A. As long as John uses persona A, he has none of the permissions that are assigned to the default persona of his user account or that his account inherits from the default persona of user group SOC. John can inherit roles and computer groups from SOC only by switching back to his default persona.

You can assign an alternative persona to multiple users and user groups. Each user and group can have zero or more alternative personas.

Persona assignments in Tanium RBAC

The following figure illustrates the relationship between personas and other RBAC components in a Tanium environment:

RBAC components and assignments in persona configurations



For more information about how personas interact with users, user groups, computer groups, and roles to determine the effective permissions of a user, see RBAC overview on page 544.

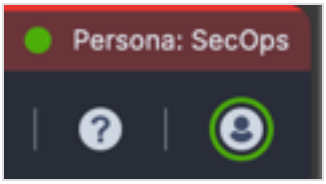
View persona details

Periodically review persona settings and update them if necessary to ensure that the assigned permissions reflect RBAC changes in your organization. In particular, ensure that personas enable users to access all the Tanium features they need but without access to sensitive information they do not need.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Permissions > Personas**.

   The **Personas** grid shows attributes that identify each persona. For example, the **Color** appears in the Console header to help you identify the persona that you selected for the current Tanium session.

2. (Optional) Use the filters to find specific personas:

   - **Filter by text**: Enter a text string in the **Filter items** field to filter the grid by column values.
   - **Filter by attribute**: Expand the **Filters** section, select a persona attribute (such as **Name**), select an operator (such as **contains**), enter a text string that contains all or part of the attribute value, and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.

3. View the effective permissions of a persona and the assigned roles, computer groups, users, and user groups by clicking the persona **Name**. For more information, see View effective role permissions for a persona on page 658.

Configure a persona

You can create a persona for each set of role and computer group assignments that multiple users or user groups share. Edit existing personas to reflect RBAC changes in your organization.

> TIP
>
> To add a persona that has many settings in common with an existing persona, cloning the existing persona and then modifying the clone is often a quicker method than configuring a new persona from scratch.

1. From the Main menu, go to **Administration > Permissions > Personas** and perform one of the following steps:

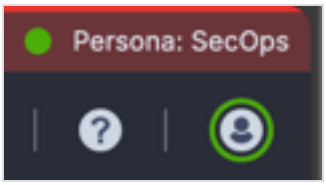
   - **Create a persona from scratch**: Click **New Persona**.
   - **Clone a persona**: Select a persona and click **Clone**.
   - **Edit a persona**: Click the persona **Name** and click **Edit Mode**.

2. Specify a **Persona Name** of up to 255 characters to identify the persona.

3. (Optional) Specify a **Description** that helps other users understand the purpose for this persona. The **Personas** page shows your entry in the **Display Name** column. Users also see the description when they switch personas.

© 2026 Tanium Inc. All Rights Reserved

4. Select the **Color** that the Console header shows to help you quickly identify the persona that you selected for your current Tanium session.



5. Configure the role, user group, user, and computer group assignments:
   - Configure role assignments for a persona on page 662
   - Manage user and user group assignments for a persona on page 662
   - Manage computer group assignments for a persona on page 662
6. Review the assignments and click **Save**.

Manage role assignments for a persona

For an overview of how effective permissions are derived for a persona, and to view the roles and associated content sets that are assigned to a persona, see View effective role permissions for a persona on page 658.

To assign or unassign roles and associated content sets for a persona, see Configure role assignments for a persona on page 662.

View effective role permissions for a persona

The effective permissions of an alternative persona are based on the cumulative effect of all the roles that you assign to the persona, including:

- Permissions specified in allow roles minus permissions specified in deny roles
- Implicitly provided permissions in allow roles

> NOTE
>
> An alternative persona does not have permissions derived from the roles of user accounts (default personas) or user groups to which you assign the persona. You must assign roles directly to an alternative persona to provide permissions to that persona.

Perform the following steps to see the effective permissions for a persona:

1. From the Main menu, go to **Administration > Permissions > Personas** and click the persona **Name**.
2. Review the assigned and inherited roles, permissions, and content sets. The page displays icons to indicate:
   Allow roles or permissions
   Deny roles or permissions

© 2026 Tanium Inc. All Rights Reserved

NOTE

The role configuration pages indicate whether permissions are explicitly assigned or implicitly provided. For more information, see View effective role permissions on page 588.

If you assign reserved roles (such as **Administrator**), they appear under **Global Permissions** with a single **special** permission .

3. (Optional) Expand an individual permission to review the content sets that are assigned to it. Only solution content permission (such as **Trends Administrator** permission) and platform content permissions (such as **Sensor read** permission) are associated with content sets. The page displays icons to indicate the type of permission to which the content sets are assigned:

   Allow permission

   Deny permission

© 2026 Tanium Inc. All Rights Reserved

Effective permissions of a persona

© 2026 Tanium Inc. All Rights Reserved

Permissions

	SPECIAL	READ	WRITE	EXECUTE	DELETE
Administration					
Action Group		✓	✓		
Computer Group		✓	✓		
Server Status		⊘			
Feed					
Feed	✓ SHOW				
Interact					
Ask Dynamic Questions	✓				
Interact	✓ SHOW				
Interact Module		✓	✓		
Platform Content Permissions					
Approve Action	⊘				
Default Filter Groups	●				
Interact	●				
Bypass Action Approval	⊘				
Dashboard		✓	✓		
Dashboard Group		✓	✓		
Filter Group		✓			
Own Action		✓			
Package		✓			
Default Filter Groups		●			
Interact		●			
Plugin		✓		✓	
Saved Question		✓	✓		
Sensor		✓			

Content Sets

40 of **40** Items

Filter Items

Filters

Type	Content Set	Used By	SPECIAL	READ	WRITE	EXECUTE	DELETE
Interact Module	Reserved			✓	✓		
Show	Reserved		✓				
Package	Default Filter Groups			✓			
Package	Interact			✓			
Own Action	Default Filter Groups			✓			
Own Action	Interact			✓			

Configure role assignments for a persona

Assign a role to a persona to provide the permissions of that role to users who select the persona for a Tanium session.

1. From the Main menu, go to **Administration > Permissions > Personas**.
2. Click the persona **Name** and click **Edit Mode**.
3. In the **Roles** section, click **Manage Roles**.
4. Select or deselect roles and click **Apply**.

   NOTE: You cannot assign the **Content Administrator** or **Content Set Administrator** reserved role to a persona.
5. (Optional) Review the **Permissions** and **Content Sets** that are associated with the selected roles.
6. Click **Save**.

Manage user and user group assignments for a persona

A user can select any persona that is assigned to his or her account after signing in to Tanium Console. Assign a persona to a user group to enable users who are members of that group to select the persona for a Tanium session.

NOTE: Alternative personas do not inherit roles or computer groups from the user groups to which those personas are assigned. For more information, see Personas overview on page 655.

1. From the Main menu, go to **Administration > Permissions > Personas**.
2. Click the persona **Name** and click **Edit Mode**.
3. Expand the **User Groups** section, click **Manage User Groups**, select or deselect user groups, and click **Select**.
4. Expand the **Users** section, click **Manage Users**, select or deselect users, and click **Select**.
5. Review the assignments and click **Save**.

Manage computer group assignments for a persona

Assign a computer group to an alternative persona to provide management for the endpoints in that group to users who select the persona for a Tanium session. You can assign up to 255 computer management groups to each persona.

1. From the Main menu, go to **Administration > Permissions > Personas**.
2. Click the persona **Name** and click **Edit Mode**.
3. Expand the **Computer Groups** section.

© 2026 Tanium Inc. All Rights Reserved

4. If you want the persona to have management rights for all endpoints, select **Unrestricted Management Rights** and click **Save** (you can skip the remaining steps).

   IMPORTANT

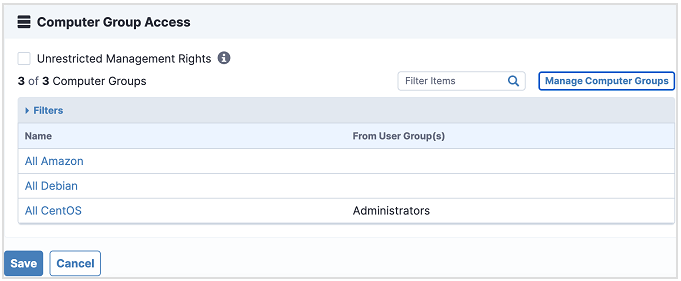
   Tanium strongly recommends that you do not assign **Unrestricted Management Rights**, unless you want the users with the persona to be able to manage all endpoints across all computer groups regardless of security considerations.

5. Click **Manage Computer Groups**, select or deselect computer management groups, and click **Select**.

   NOTE

   Selections are logically combined. For example, the union of **All Computers** and **No Computers** is effectively **All Computers**.

6. Review the list of computer groups that you assigned or that derive from user group assignments, and then click **Save**.



Transfer content that a persona owns

By default, the user account (default persona) or alternative persona that a user selects for a Tanium session is the owner of any content that the user creates during the session. Consider transferring content ownership if you plan to delete a persona or change the roles or computer groups that are assigned to a persona. You cannot delete a persona that owns content. For more information, see Delete content or transfer ownership on page 637.

Select a persona for your Console session

In the Tanium Console header, a colored ring around the user icon indicates that an alternative persona is selected for the Console session. The ring matches the color that is assigned in the persona configuration. If you select the default persona, the icon has no colored ring. When you sign in, the **Default Persona** for your user account applies automatically. To switch to an alternative persona or revert to the **Default Persona**, perform the following steps.

TIP

Hovering over the user icon / opens a menu that displays the name of the current persona.

© 2026 Tanium Inc. All Rights Reserved

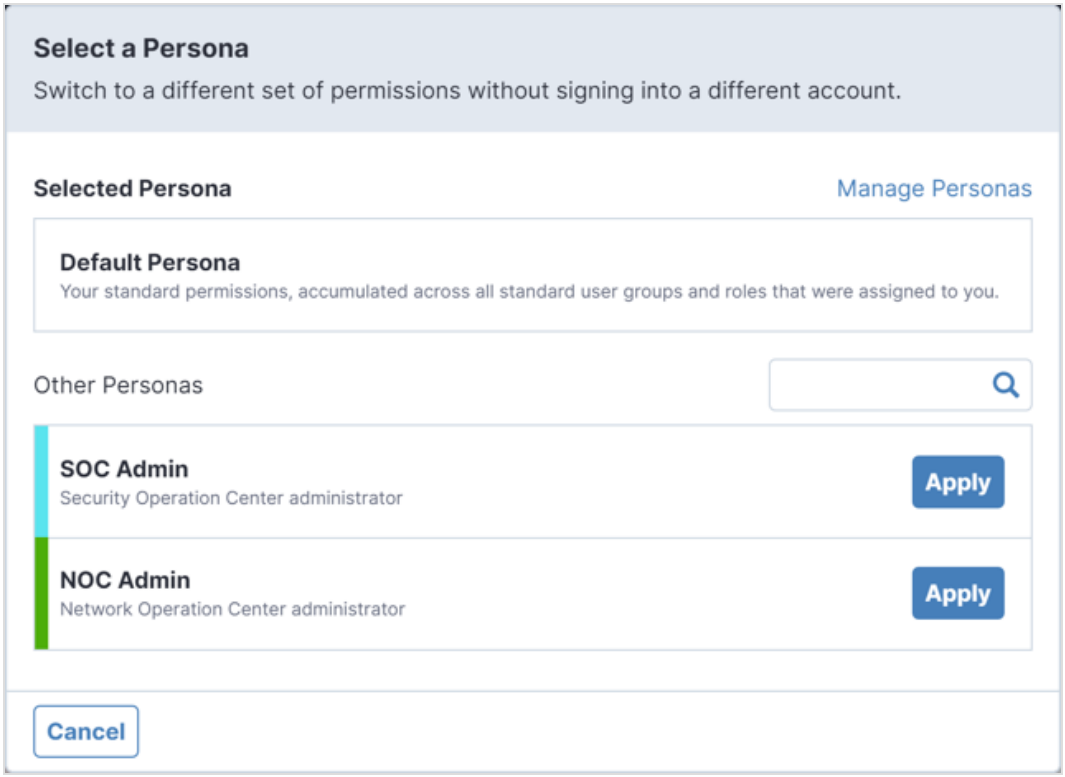
1. In the Console header, hover over the user icon and click **Persona:** ***<current persona>***.

   The **Select a Persona** dialog then lists the personas that are assigned to your user account or to the user groups to which you belong. The dialog identifies personas by their name, description (if specified), and color.

2. Click **Apply** beside the persona that you want to use.

   Console then refreshes to show only the features and solutions for which the selected persona has access permissions.

Persona selection for a Console session



Export persona details

You can export persona details as a CSV file. When you open the file in an application that supports CSV format, it lists the personas with the same attributes (columns) as the Console **Personas** grid displays and (optionally) lists the RBAC assignments of each persona. Displaying the grid in a CSV application is useful when you want to customize the display. For example, you can use Microsoft Excel to create charts based on persona attributes.

1. From the Main menu, go to **Administration > Permissions > Personas**.
2. (Optional) To add or remove attributes (columns) for the CSV file, click Customize Columns in the grid and select the attributes.
3. Select rows in the grid to export only specific personas. If you want to export all personas, skip this step.
4. Click Export.

© 2026 Tanium Inc. All Rights Reserved

5. (Optional) Edit the default export **File Name**. The Tanium Server automatically appends the file suffix (`.csv`).
6. Select an **Export Data** option: **All** personas in the grid or just the **Selected** personas.
7. Set the file **Format** to **List of Personas - CSV**. Optionally, select **With RBAC Details** to include the computer groups and roles that are assigned to the personas.
8. Click **Export**.
   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

Copy persona configuration details

Copy information from the **Personas** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string in the content that you copy.

1. From the Main menu, go to **Administration > Permissions > Personas**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy.
   - **Copy cell information**: Hover over the cell, click Options, and click Copy.

Delete a persona

You can delete alternative personas but not the default persona that is assigned to each user. When you delete a persona, the Tanium Server removes the persona from any user or user group configurations that included it.

You cannot delete a persona that owns content. Transfer content to another persona before deleting the persona. For more information, see Delete content or transfer ownership on page 637.

BEST PRACTICE

Before deleting a persona, delete the user and user group assignments from the persona configuration. For more information, see Manage user and user group assignments for a persona on page 662 and Manage user and user group assignments for a persona on page 662.

1. From the Main menu, go to **Administration > Permissions > Personas** and select the persona that you want to delete.
2. Click Delete Selected and click **Confirm**.

© 2026 Tanium Inc. All Rights Reserved

Importing and authenticating users through LDAP

LDAP overview

Lightweight Directory Access Protocol (LDAP) is a standard, cross-platform, client-server protocol for interacting with directory services such as Active Directory (AD) over an Internet Protocol (IP) network. The Tanium Core Platform supports LDAP for authenticating users and importing users and user groups.

You can configure the Tanium Server to synchronize with multiple LDAP servers. In each LDAP server configuration, you specify whether to authenticate synchronized users through the LDAP server. Otherwise, the Tanium Server applies whatever other user authentication methods you configured. For more information, see User authentication on page 626.

IMPORTANT

Configure the integration with LDAP servers before performing other role-based access control (RBAC) configuration tasks.

NOTE

You require the **Administrator** reserved role to see and use the **Administration > Configuration > LDAP/AD Sync Configurations** page.

LDAP synchronization

The Tanium Server automatically synchronizes with each LDAP server every five minutes and you can manually synchronize at any time. In an active-active deployment, only one Tanium Server synchronizes with LDAP servers at any given time. Synchronization updates the Tanium Server with any changes that occurred on the LDAP server, including:

- New, updated, disabled, or deleted users
- New, updated, or deleted user groups
- Changes to user group membership

RBAC configuration for new users and user groups

Assign roles, computer groups, and personas to new users and user groups after the Tanium Server imports them from an LDAP server. If you import any user accounts that are not assigned to user groups, you must manually configure those assignments also. For more information, see:

- Managing users on page 625
- Managing user groups on page 643

© 2026 Tanium Inc. All Rights Reserved

LDAP logs and troubleshooting

If synchronization with an Active Directory server does not return all of the expected users or user groups, you might need to change the page size. For more information, see the `ldap_page_size` setting in Reference: Tanium Core Platform settings on page 765.

If a user account that is imported from an LDAP server cannot sign in to Tanium Console, ask the LDAP administrator to check the account status.

To troubleshoot other issues with your LDAP integration, review the LDAP logs:

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

> **NOTE** In an active-active deployment, only the Tanium Server that is currently synchronizing with LDAP servers records synchronization events in its LDAP logs.

Example: LDAP synchronization and authentication

The figure LDAP synchronization and authentication on page 668 illustrates LDAP synchronization and authentication for the following example deployment:

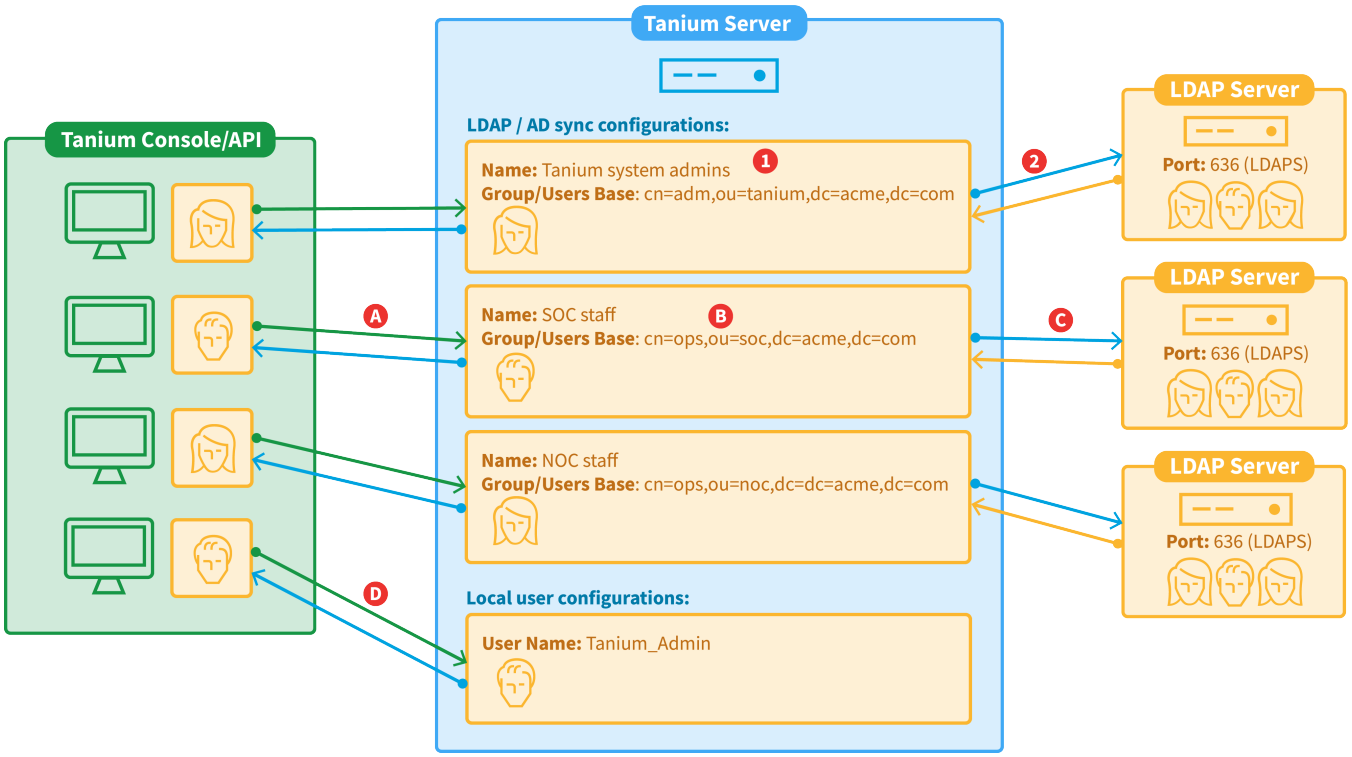
- The Tanium Server is installed on a Tanium Appliance and uses Secure LDAP (LDAPS) encryption for connections to LDAP servers.

  > **NOTE** The available Encryption on page 676 options depend on the operating systems of the Tanium Server and LDAP servers.

- All the LDAP configurations specify that the LDAP servers will authenticate the imported users.
- One account (Tanium_Admin) with the **Administrator** reserved role is not imported from an LDAP server, and the Tanium Appliance uses its local authentication service for that user. This configuration ensures that at least one user can access Tanium Console even if LDAP connections go down.

© 2026 Tanium Inc. All Rights Reserved

LDAP synchronization and authentication



The following steps (matching the numbers in the figure LDAP synchronization and authentication on page 668) summarize the LDAP synchronization process for this example deployment.

1 Each LDAP server configuration identifies which users and user groups to synchronize with which LDAP server. For configuration details, see User and user group filtering on page 669 and Configure LDAP server connections on page 673.

2 The Tanium Server initiates connections with the LDAP servers to perform the initial import of users and user groups and to periodically query for updates. All the LDAP server configurations specify LDAPS encryption in this example, so the Tanium Server connects to port 636 on the LDAP servers.

The following steps (matching the letters in the figure LDAP synchronization and authentication on page 668) summarize the LDAP authentication process for this example deployment.

A A synchronized user enters a domain (if required), user name, and password to sign in to Tanium Console.

B The Tanium Server uses the specified user name to find the corresponding external identifier (such as objectGUID) in the Tanium database. (In the LDAP server configuration, the **User Unique ID Property** specifies this identifier).

C The Tanium Server uses the external identifier to query the LDAP server for the matching distinguished name (DN) of the user, such as `cn=jdoe,ou=noc,dc=acme,dc=com`. (The query is based on the same settings as those used for synchronization. For more information, see User and user group filtering on page 669 and Configure LDAP server connections on page 673.) The LDAP server then authenticates the user based on the DN and sign in password. After the LDAP server returns an authentication success message, the Tanium Server provides the user access to Tanium Console.

D When a user configured locally (Tanium_Admin) enters sign in credentials, the Tanium Server uses the local authentication service to authenticate the user, and then provides access to Tanium Console.

© 2026 Tanium Inc. All Rights Reserved

User and user group filtering

Before configuring LDAP server connections, be sure to understand the interactions among the settings in the table LDAP settings for user and user group filtering on page 669. The Tanium Server uses these settings to filter users and user groups that it synchronizes.

For example, because the best practice is to configure RBAC for Tanium users based on user group permissions instead of user permissions, you might want to exclude users who are not assigned to groups. The figures Filtering on LDAP servers on page 670 and LDAP user and group filtering on page 671 illustrate an example of the steps that the servers perform in that scenario, with separate workflows for filtering users on the LDAP servers and Tanium Server.

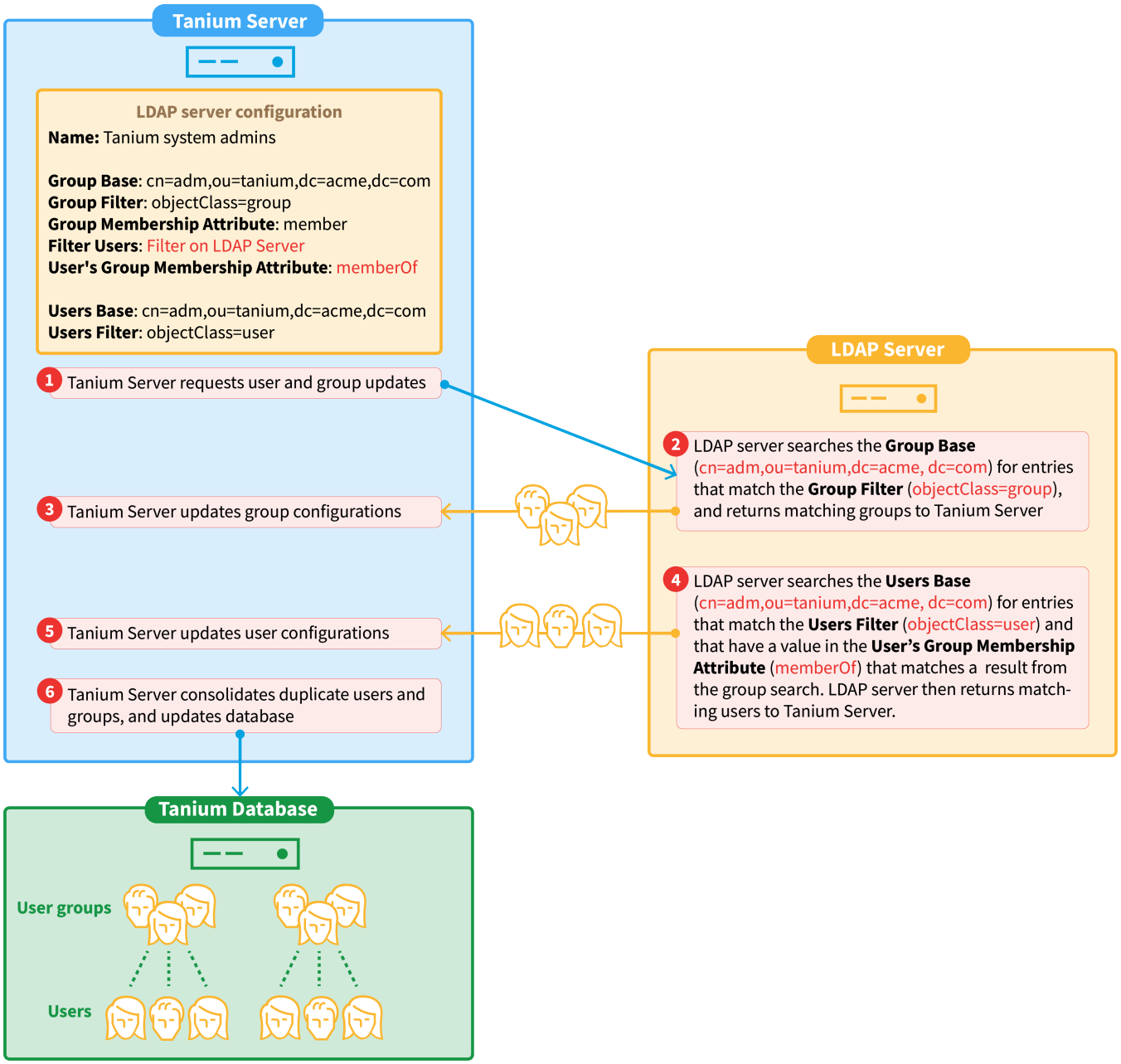
LDAP settings for user and user group filtering

LDAP setting	Filtering behavior
Group Base	When the Tanium Server sends a synchronization request (Step 1 in both figures), the LDAP server searches only for user groups that are under this base DN, such as `cn=adm,ou=tanium,dc=acme,dc=com`.
Group Filter	The LDAP server uses this field to filter the user groups in the **Group Base**. In this example, the LDAP server returns groups only if their `objectClass` attribute is set to `group` (Step 2 in both figures). The Tanium Server then synchronizes those groups (Step 3 in both figures).
Users Base	The LDAP server searches only for users that are under this base DN, such as `cn=adm,ou=tanium,dc=acme,dc=com`.
Users Filter	The LDAP server uses this field to filter the users in the **Users Base**. In this example, the LDAP server returns users only if their `objectClass` attribute is set to `user` (Step 4 in both figures).
Filter Users	If you want to exclude users who are not assigned to user groups that are synchronized with the Tanium Server, select one or both of the following options: • **Filter on LDAP Server** (figure Filtering on LDAP servers on page 670): The LDAP server returns users only if they have a value (DN) in their **User's Group Membership Attribute** (the `memberOf` attribute, in this example) that matches one of the groups from the group search (Step 4). Selecting this option is the best practice because filtering on the LDAP server is faster and results in less network traffic than filtering on the Tanium Server. Most LDAP servers support this option. Upon receiving the filtered users, the Tanium Server synchronizes them (Step 5). • **Filter on Tanium Server** (figure LDAP user and group filtering on page 671): The LDAP server returns all users to the Tanium Server if they match the **Users Filter** (Step 4); the LDAP server does not filter by the **User's Group Membership Attribute**. The Tanium Server then discards any users (Step 5) if none of the synchronized user groups have the user DN in their **Group Membership Attribute** (the `member` attribute, in this example). This option is intended as a backup in cases where the LDAP server does not support filtering by the **User's Group Membership Attribute**. After consolidating any duplicates in the synchronized users and groups, the Tanium Server updates the Tanium database (Step 6 in both figures).

The following figure illustrates user filtering on LDAP servers.

© 2026 Tanium Inc. All Rights Reserved

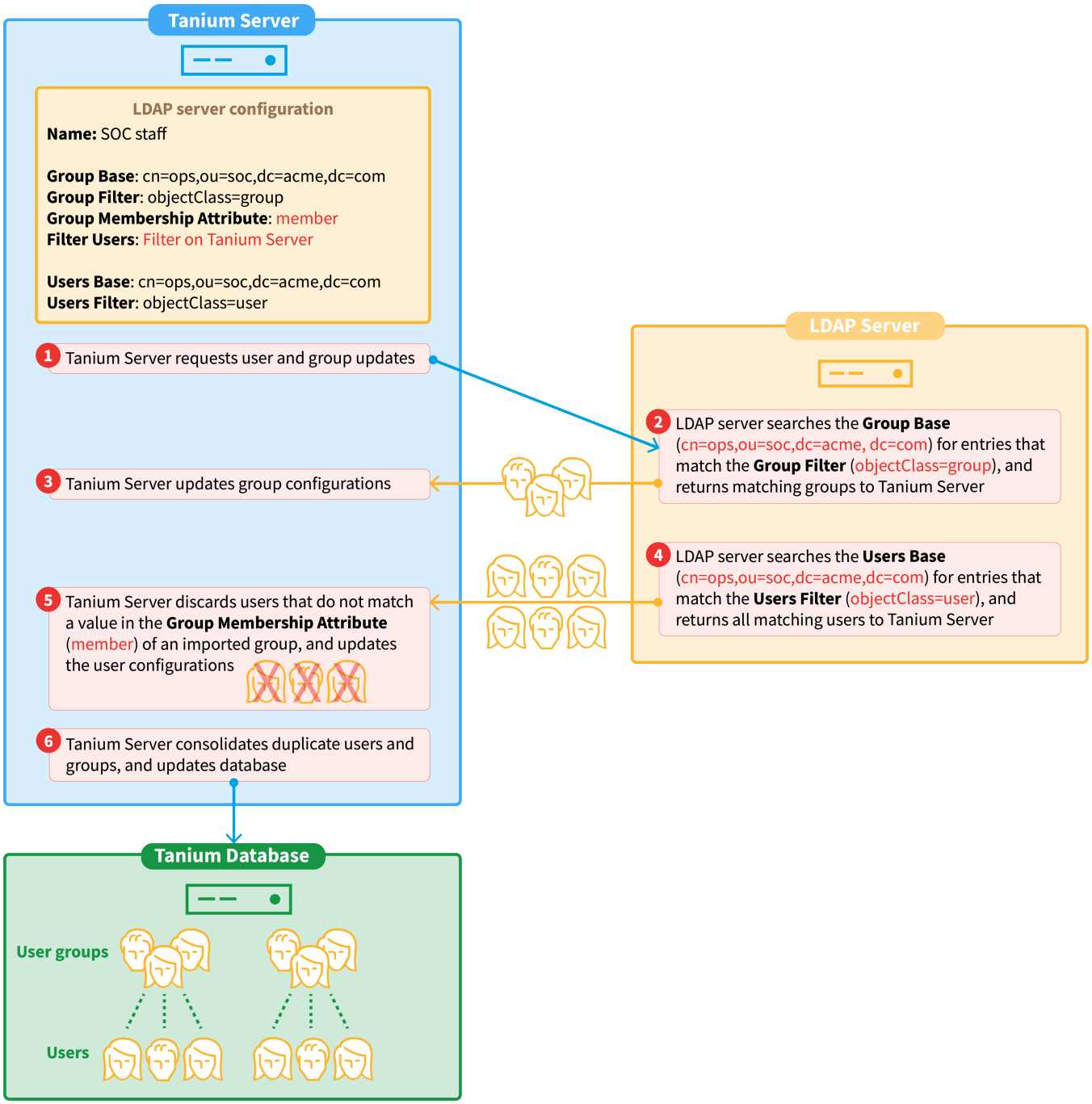
Filtering on LDAP servers



The following figure illustrates user filtering on the Tanium Server.

© 2026 Tanium Inc. All Rights Reserved

LDAP user and group filtering



Best practices for LDAP integrations

When establishing and managing the integration between Tanium Servers and LDAP servers, observe the following best practices to avoid unexpected issues.

© 2026 Tanium Inc. All Rights Reserved

CREATE USERS AND USER GROUPS ON THE LDAP SERVER

On the back-end LDAP server, create LDAP user groups that correspond with Tanium user groups, and create user accounts for the users who require access to the Tanium system.

MANAGE TANIUM ACCESS THROUGH THE LDAP SERVER

Manage Tanium access through the back-end LDAP server configuration instead of the front-end Tanium Console configuration. For example, the best way to on-board and off-board users is to modify the membership of synchronized user groups.

CONTROL LDAP SERVER ACCESS

Control access to the back-end LDAP server configuration so that LDAP administrators who are not familiar with your Tanium deployment cannot make changes that affect it.

MAINTAIN A LOCAL ADMINISTRATOR ACCOUNT

On the Tanium Server, maintain at least one account in the **Users** configuration that the Tanium Server does not import from an LDAP server. Assign the **Administrator** reserved role to this local user so that you can use the account to sign in to Tanium Console and re-configure the LDAP server connections in case they fail. Some organizations provision multiple administrator users outside of the LDAP servers for this reason. To avoid creating duplicate user configurations in cases where the account name also exists on an LDAP server, you can configure the **Users Filter** in the LDAP servers to prevent synchronization for the account. For more information, see LDAP server connection settings on page 675.

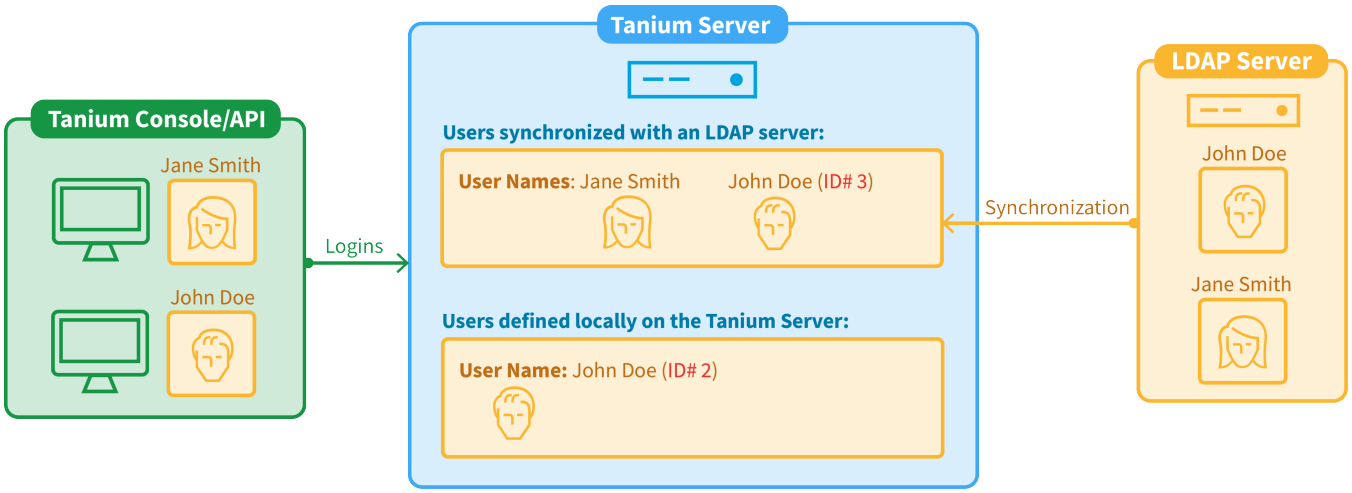
DELETING USERS

When transitioning from manually-created users to LDAP-synchronized users, you might inadvertently create multiple configuration objects for a single real user. When deleting user configurations to correct redundancies, be sure to understand the impact on associated configuration objects, such as scheduled actions, saved questions, Tanium Connect objects, solution plugins, or solution services.

For example, you might have used Tanium Console to manually create a user named john.doe and then synchronized with an LDAP server that returns the same user name. This causes the Tanium Server to have two user configurations for john.doe and automatically assign a unique object ID to each one. In the example of the figure Redundant user configurations on the Tanium Server on page 673, the objects that john.doe - ID 2 created do not also belong to john.doe - ID 3. If you delete the john.doe - ID 2 configuration, you must be ready to re-create or transfer ownership for the configuration objects that run under that ID.

© 2026 Tanium Inc. All Rights Reserved

Redundant user configurations on the Tanium Server



Before correcting user account redundancies, it is important to understand the ramifications of deleting an account based on its source:

- **Local user**

  If you delete the configuration for a user defined locally on the Tanium Server, but the user still matches the filters defined in an LDAP server, the Tanium Server retains a configuration for the user.

- **Imported user**

  If you use Tanium Console to delete a user account that was imported from an LDAP server, that user remains deleted after the next synchronization.

- **User on LDAP server**

  If you delete a user from the back-end LDAP server configuration, the Tanium Server marks that user as locked out after the next synchronization. The user cannot sign in, but the Tanium Server does not automatically delete the user account. Any scheduled questions and actions that the user owns continue to run. This gives other Tanium administrators the chance to re-create the scheduled questions and actions under a different user account or to transfer the content to another user.

For more information, see Delete, un-delete, or lock out a user on page 640 and Delete content or transfer ownership on page 637.

Configure LDAP server connections

Before you begin

Before you configure connections to LDAP servers, review the Best practices for LDAP integrations on page 671 and ensure that your environment meets the following requirements.

© 2026 Tanium Inc. All Rights Reserved

Requirements for LDAP integration

Requirement	Details
Ports	For synchronization, the Tanium Server initiates the connection with the LDAP server. The standard LDAP port is 389 (3268 for an AD global catalog) for unencrypted connections, connections that use **StartTLS**, or AD connections that use the **Sign and encrypt** option for Encryption on page 676. The standard port for **LDAPS** encryption is 636 (3269 for an AD global catalog). In the LDAP server configuration, you can specify whatever port your LDAP server listens on for its inbound LDAP traffic. Your network administrator must configure network security to allow this traffic.
Encryption (Tanium Appliance only)	If you plan to use **LDAPS** or **StartTLS** as the Encryption on page 676 option, you must first import the certificate authority (CA) certificate for the LDAP server and enable the encryption configuration on the Appliance. In an active-active deployment, upload the certificate and enable encryption on both Tanium Servers. For more information, see Tanium Appliance User Guide: Configure LDAPS or StartTLS.
Digital keys	For the minimum bit size of the keys that LDAP servers must use to communicate with the Tanium Server, see Communication with external systems on page 210.
Identifiers	You must know the base distinguished name (DN), IDs, and filter expressions for the users and user groups that you want to import. The values are case sensitive.
Query permission	The LDAP server must allow queries using the configured filter expressions.

Configure an LDAP server connection

1. From the Main menu, go to **Administration > Configuration > LDAP/AD Sync Configurations**.
2. Click **Add Server** to create a new LDAP server connection or click Edit  in the row for an existing connection to modify its settings.

© 2026 Tanium Inc. All Rights Reserved

3. Configure the following settings:

LDAP server connection settings

Setting	Description
Set Status	Set the synchronization and authentication state of the LDAP server connection: • **Enable**: Synchronization occurs every five minutes and users can authenticate through the LDAP server if you select **Use LDAP for user authentication**. • **Disable**: The Tanium Server does not synchronize with, or allow users to authenticate through, the LDAP server. You can select the disabled state only when you initially create the configuration. If you later edit the configuration, you can change its state to enabled or paused, but you cannot disable a configuration that was initially set to enabled or paused. • **Pause**: The Tanium Server does not synchronize with the LDAP server. However, authentication continues to work and the Tanium Server preserves existing RBAC assignments.
Name	Enter a name to identify this LDAP server.
Host	Enter the fully qualified domain name (FQDN) of the LDAP server. If you connect using LDAPS, the **Host** value must match the Common Name (CN) or one of the Subject Alternative Names (SANs) of the LDAP certificate.
Port	Specify the number of the port on which your LDAP server listens for its inbound LDAP traffic. The standard port depends on the protocol: • **LDAP**: The standard port is 389 (3268 for an AD global catalog). The LDAP server uses this port for unencrypted connections, connections that use **StartTLS**, and AD connections that use the **Sign and encrypt** option. • **LDAPS**: The standard port is 636 (3269 for an AD global catalog).
Referrals	**Disable** referrals if the LDAP server is a Microsoft AD server. Disabling referrals is optional for other server types.

© 2026 Tanium Inc. All Rights Reserved

LDAP server connection settings (continued)

Setting	Description
Encryption	Select an encryption option: • **None**: Do not use this option in a production environment. • **Sign and encrypt**: The LDAP connector turns on the LDAP_OPT_SIGN and LDAP_OPT_ENCRYPT session options. The session is encrypted, but it does not use Transport Layer Security (TLS). Use this option only for Tanium Server on Windows. The external LDAP server must be an AD server. • **StartTLS**: The LDAP connector calls the ldap_start_tls_s function to set up a TLS connection. You can use this option with Tanium Server on Windows or the Tanium Appliance. • **LDAP**: The LDAP connector initiates an SSL connection to the LDAPS server. You can use this option with Tanium Server on Windows or the Appliance.  (Appliance only) If you plan to use **LDAPS** or **StartTLS**, you must first import the LDAP server CA certificate and enable the encryption configuration on the Appliance. In an active-active deployment, upload the certificate and enable encryption on both Tanium Servers. For more information, see Tanium Appliance User Guide: Configure LDAPS or StartTLS.
NTLM	Select whether the Tanium Server uses Microsoft NT LAN Manager (NTLM) for the connection with the LDAP server. This option is enabled by default. If you use NTLM, the Tanium Server uses its service account to access the LDAP server, and you do not need to configure an **LDAP User Name** or **LDAP Password**. The LDAP server must allow this account to query with the configured filter expressions.  Use NTLM if the Tanium Server is installed on a Windows Server and the connection is to an AD server.
LDAP User Name and Password	If you selected **Do not use NTLM**, specify the user name and password of an account on the LDAP server that the Tanium Server can use for LDAP queries. If the account credentials ever change, be sure to update them in the LDAP server configuration on the Tanium Server.  Provision a special account for this purpose with permissions that are low but sufficient to query the LDAP server.

© 2026 Tanium Inc. All Rights Reserved

LDAP server connection settings (continued)

Setting	Description
Group Sync	Enable (**Yes**) or disable (**No**) user group synchronization. If you enable the feature, the Tanium Server synchronizes with the groups on the LDAP server based on the settings that you configure in the **Groups** section.  IMPORTANT If you disable user group synchronization, at the next synchronization time the Tanium Server deletes the groups that it previously imported. If you subsequently re-enable group synchronization, the Tanium Server re-adds the user groups but with no RBAC or computer management group assignments.
Group Base	This is the base DN for the user groups container. The Tanium Server synchronizes groups from all locations below this path. Example: `cn=Ops,ou=TaniumAdmins,dc=tam,dc=local`  NOTE If setting the **Group Base** or **Users Base** to the root of a domain produces errors, select **Disable referrals** in the **General** section.
Group Filter	The LDAP server uses this field to filter the user groups in the **Group Base**. For example, if you enter `objectCategory=group`, the LDAP server returns groups only if their `objectCategory` attribute is set to `group`.  NOTE Use a backslash (\) to escape special characters in a group name. For Windows, use one backslash (example: `name=\#myGroup`). For the Appliance (Linux), use two backslashes (example: `name=\\#myGroup`). For more information, see the LDAP server documentation for a list of special characters.
Group Unique ID Property	Enter the attribute (such as `objectGUID`) that uniquely identifies each user group.  NOTE The value is case sensitive.

© 2026 Tanium Inc. All Rights Reserved

LDAP server connection settings (continued)

Setting	Description
Group Member List Identifier	Enter the name of the user attribute that contains the identifier referenced by the membership property of the group object in LDAP. The user attribute must be a text property. For example, if the group object in LDAP has a `member` property, and the value of that property contains a list of user object `_uid` identifiers, specify `_uid`. The default user attribute is `distinguishedName` if you do not enter a value.  NOTE The value is case sensitive.
Group Name Property	Enter the attribute (such as `cn`) that identifies the name of a user group.  NOTE The value is case sensitive.
Group Membership Attribute	Enter the user group attribute (such as `member`) that indicates which users are members.  NOTE The value is case sensitive.
Filter Users	If you want to exclude users who are not assigned to user groups that are synchronized with the Tanium Server, select one or both of the following options: • **Filter on LDAP Server via User's Group Membership Attribute**: Specify an attribute in the **User's Group Membership Attribute** text box. The most common LDAP attribute is `memberOf`. You must enter an attribute name, not an expression. The LDAP server returns users only if they have a value (DN) for that attribute that matches one of the groups from the group search. Selecting this option is the best practice because filtering on the LDAP server is faster and results in less network traffic than filtering on the Tanium Server. Most LDAP servers support this option. • **Filter on Tanium Server**: The LDAP server returns all users to the Tanium Server if they match the **Users Filter**; the LDAP server does not filter by the **User's Group Membership Attribute**. The Tanium Server then discards any users if none of the synchronized user groups have the user DN in their **Group Membership Attribute**. This option is intended as a backup in cases where the LDAP server does not support filtering by the **User's Group Membership Attribute**.

© 2026 Tanium Inc. All Rights Reserved

LDAP server connection settings (continued)

Setting	Description
User Domain	Enter the domain that the Tanium Server uses to match users in the Tanium database. Specify a NetBIOS name to match users who sign in using the *<domain>**<username>* format (such as example-corp\user1) or specify a *<domain>.<top-level_domain>* name to match users who sign in using the *<username>*@*<domain.top-level_domain>* format (such as user1@example-corp.com). Either domain format matches users who sign in using only their user name.
Sync group members individually	By default, the LDAP server searches for users to synchronize based on the **Users Base** value. However, if your LDAP implementation does not allow for a base user group that lists all users, select **Sync group members individually** to skip the **Users Base** search. Instead, this option directs the LDAP server to search for the DN of each user group member based on the **Group Membership Attribute**. The users must still match the **Users Filter**, which can exclude group members that are computers or other groups.  NOTE Compared to a **Users Base** search, a search based on **Group Membership Attribute** requires more processing and can take noticeably more time if you have many users.
Users Base	This is the base DN for the users container. The Tanium Server synchronizes users from all locations below this path. Example: `cn=Users,dc=tam,dc=local`  NOTE If setting the **Group Base** or **Users Base** to the root of a domain produces errors, select **Disable referrals** in the **General** section.

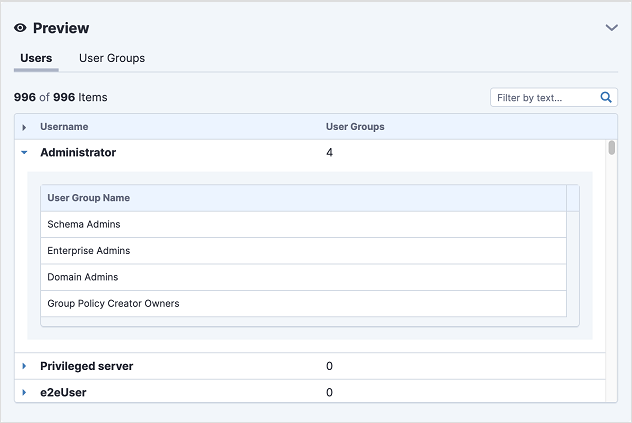
© 2026 Tanium Inc. All Rights Reserved

LDAP server connection settings (continued)

Setting	Description
Users Filter	The LDAP server uses this field to filter the users in the **Users Base**. For example, if you enter `objectCategory=user`, the LDAP server returns users only if their `objectCategory` attribute is set to `user`. You must precede special characters in the filter with a backslash \ to escape them. For more information, see the LDAP server documentation for a list of special characters. Use the following filter to exclude an account from synchronization, where *<account_name>* is the user name: `((&(objectCategory=user)(!(sAMAccountName=<account_name>))))` NOTE: If you add an LDAP server for the local authentication service of a Tanium Server running on a Tanium Appliance, you must use the following user filter: `(&(objectCategory=person)(uidNumber>=20000))`
User Unique ID Property	Enter the attribute (such as `objectGUID`) that uniquely identifies each user. NOTE: The value is case sensitive.
User Name Property	Enter the attribute that identifies the name of a user. The value that the Tanium Server imports for this field becomes the user name that users type to sign in to Tanium Console. Be sure to specify the attribute that is suitable for this purpose and be sure to communicate the expected form to your users. Use `sAMAccountName` for AD providers and `cn` for other LDAP providers. NOTE: The value is case sensitive.
User Display Name Property	Enter the attribute that identifies the display name for users (typically `displayName`).
Authentication	Select **Use LDAP for user authentication** to use the configured server as the authentication source. Otherwise, the Tanium Server uses the LDAP server only to synchronize users and user groups, and for authentication uses whatever other method you configured. For more information, see User authentication on page 626.

© 2026 Tanium Inc. All Rights Reserved

4. Click **Show Preview to Continue**, review the users and groups to import, and click **Save**.



Clone an LDAP server

Cloning an LDAP server configuration is usually easier than creating a new configuration from scratch if the clone has settings that are similar to an existing configuration. For example, you can create multiple clones in which only the domains differ .

1. From the Main menu, go to **Administration > Configuration > LDAP/AD Sync Configurations**.
2. Click Clone in the row of the LDAP server that you want to clone.
3. Click Edit in the row for the cloned configuration.
4. Edit the settings as necessary using the guidance provided in LDAP server connection settings on page 675.
5. Click **Show Preview to Continue**, review the users and user groups to import, and click **Save**.

Manually synchronize with an LDAP server

The Tanium Server automatically synchronizes with LDAP servers every five minutes. However, you can manually synchronize to make Tanium Console immediately show changes made on the LDAP servers, such as user group membership updates.

> NOTE
>
> At any given time in an active-active deployment, only one Tanium Server synchronizes with LDAP servers and records synchronization events in the LDAP logs.

1. From the Main menu, go to **Administration > Configuration > LDAP/AD Sync Configurations**.
   If the **Sync Now** button is enabled, proceed to the next step. If the button is disabled, sign in to Tanium Console on the other Tanium Server to manually synchronize.
2. Click **Sync Now**.

© 2026 Tanium Inc. All Rights Reserved

Import LDAP server connection configurations

After you use the Tanium REST API to export the configurations of LDAP server connections, perform the following steps to import the configurations through Tanium Console.

You must be assigned a role with **Import Signed Content** permission to import content files through the following steps.

1. (Non-Tanium-provided content only) Digitally sign the content file and ensure a public key is in place to validate the signature. For more information, see Authenticating content files on page 482.

   NOTE

   You do not have to generate keys or signatures for Tanium-provided solutions. Tanium signs this content before making it available, and the associated public key is distributed to the Tanium Server key store during the Server installation process.

   If you plan to import a file that another user signed, you can first perform an integrity check on the file. For more information, see Verify content file signatures on page 487.

2. From the Main menu, go to any of the following **Administration** pages:
   - **Configuration > Solutions**
   - **Permissions > Filter Groups**
   - Under **Content**, select **Sensors**, **Packages**, or **Saved Questions**
   - Under **Actions**, select **Scheduled Actions**, **All Pending Approvals**, or **Actions I Can Approve**
3. Select an **Import** option based on the source of the content:
   - **Import > Import Files**: Perform one of the following steps to select one or more files:
     - Drag and drop files from your file explorer.
     - Click **Browse for File**, select the files, and click **Open**.
   - **Import > Import URL**: Enter the URL in the **Import URL** field, and click **Import**.
4. For each file, expand the **File name**, review the content to import, and select resolutions for any conflicts with existing content. For more information, see Resolve import conflicts.
5. If you want to overwrite existing content set assignments for all imported objects with the default Tanium-defined assignments, select **Include content set overwrite**. By default, **Include content set overwrite** is cleared and the Tanium Server preserves the existing content set assignments.
6. Click **Begin Install**.

© 2026 Tanium Inc. All Rights Reserved

Pause or resume an LDAP server

If you are upgrading an LDAP server, or troubleshooting unexpected synchronization results, you can pause synchronization for a particular LDAP server. When synchronization is paused, authentication continues to work and the Tanium Server preserves existing RBAC assignments. After you finish upgrading or troubleshooting, you can resume synchronization.

1. From the Main menu, go to **Administration > Configuration > LDAP/AD Sync Configurations**.
2. Click Edit  in the row for the LDAP server.
3. Select **Pause** to pause LDAP synchronization or select **Enable** to resume synchronization.
4. Click **Show Preview to Continue**, review the affected users and user groups, and click **Save**.

Delete an LDAP server

When you delete an LDAP server configuration, the Tanium Server stops updating the users and user groups that it previously imported from that LDAP server. When the Tanium Server next performs synchronization for the remaining LDAP servers, it removes the users and groups associated with the deleted configuration. If you no longer want that information saved on the Tanium Server, perform the following steps to delete the configuration:

1. From the Main menu, go to **Administration > Configuration > LDAP/AD Sync Configurations**.
2. Click Edit  in the row for the LDAP server and click **Delete** at the top right.

© 2026 Tanium Inc. All Rights Reserved

Enabling SSO through SAML

SAML overview

Security Assertion Markup Language (SAML) is a standard for exchanging authentication requests and responses between service providers (SPs) and identity providers (IdPs). You can integrate your Tanium environment with an IdP to give users single sign-on (SSO) access to Tanium Console.

SAML enables SPs to give users access to applications across multiple security domains through an SSO authentication service that the IdP provides. Upon receiving an authentication request, the IdP responds with a SAML assertion, which is a message that indicates whether a user authenticated successfully. In the context of the Tanium Core Platform, enabling SAML means configuring the Tanium Server as an SP. You can configure the Server to support both IdP-initiated and SP-initiated SSO or only IdP-initiated SSO. You cannot configure only SP-initiated SSO.

BEST PRACTICE

Maintain at least one user account on the Tanium Server that does not require SAML authentication and assign that account the **Administrator** reserved role. You can use this account to access Tanium Console if SAML authentication stops working (for example, if the connection to the IdP goes down).

NOTE

The Tanium Server does not support user authorization (role-based access control) through SAML. To control the features, settings, and information that users are allowed to see and use after accessing Tanium Console, assign user groups, roles, personas, and computer groups to the users. For more information, see Managing users on page 625.

Only users who have the **Administrator** reserved role can see and manage the SAML configuration.

To troubleshoot cases where a user cannot sign in to Tanium Console through SAML, see User account status and user group status on page 704.

IdP-initiated SSO

In some enterprises, users are expected to access many or all applications by signing into a single SSO portal that the enterprise IdP provides. After you enable SAML on the Tanium Server, users can access Tanium Console through the IdP SSO portal. An IdP-initiated workflow has the following phases (matching the numbers in the figure IdP-initiated SAML SSO on page 685):

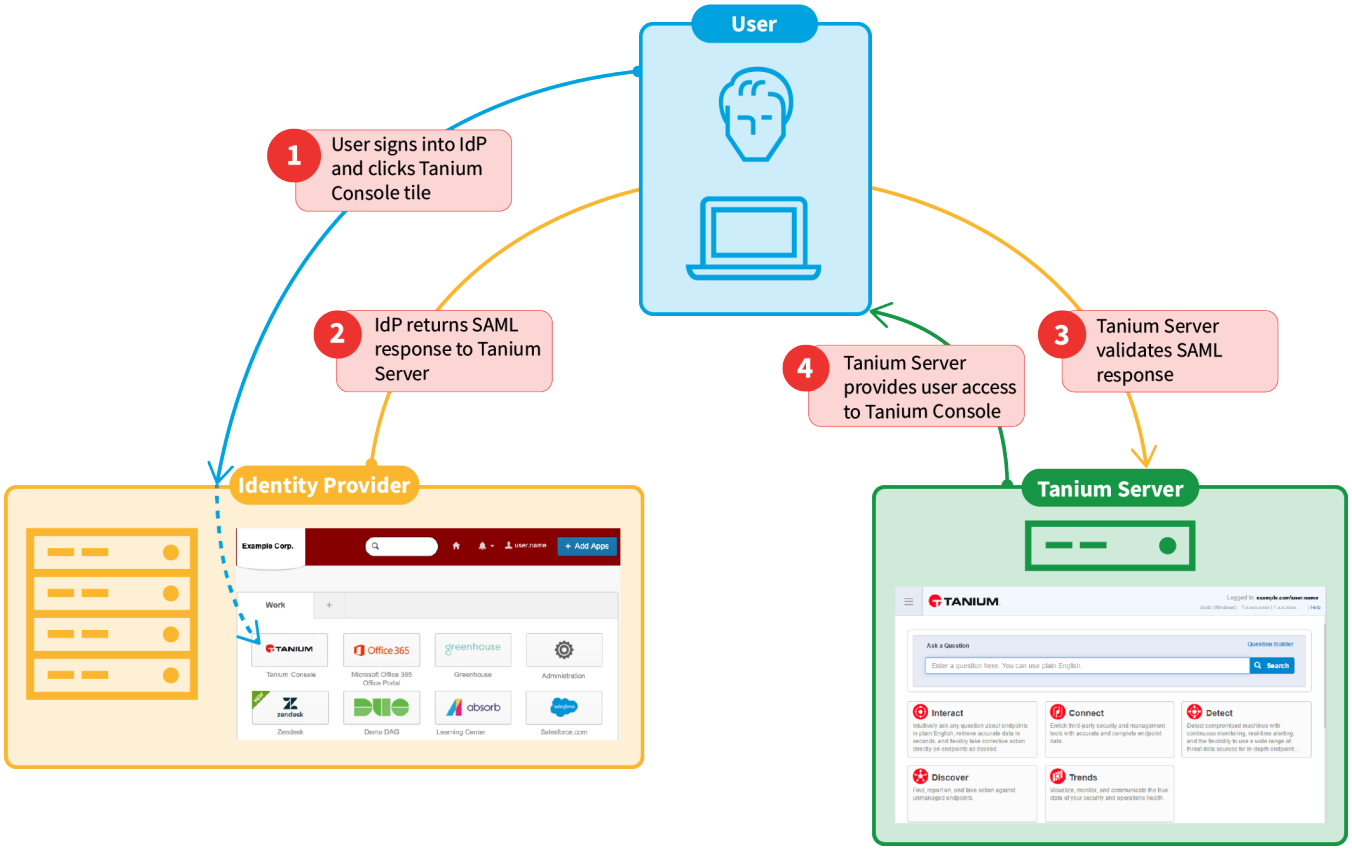
1. A user signs into the IdP SSO portal using an enterprise user name and password, and clicks an application tile (the Tanium Console tile in this case).
2. The IdP returns a signed response (which contains a SAML assertion) that indicates the user authenticated successfully. The user browser automatically forwards the response to the SP (the Tanium Server in this case).

© 2026 Tanium Inc. All Rights Reserved

3 The SP uses the IdP certificate to verify that the SAML response signature is valid.

4 The SP provides the user access to the application.

IdP-initiated SAML SSO



SP-initiated SSO

An SP-initiated workflow has the following phases (matching the numbers in the figure SP-initiated SAML SSO on page 686):

1 The user tries to access the application (Tanium Console in this case) directly through the SP (the Tanium Server in this case).

2 The SP redirects the user to authenticate through the IdP. The user browser processes the redirection automatically.

3 The user signs in to the IdP.

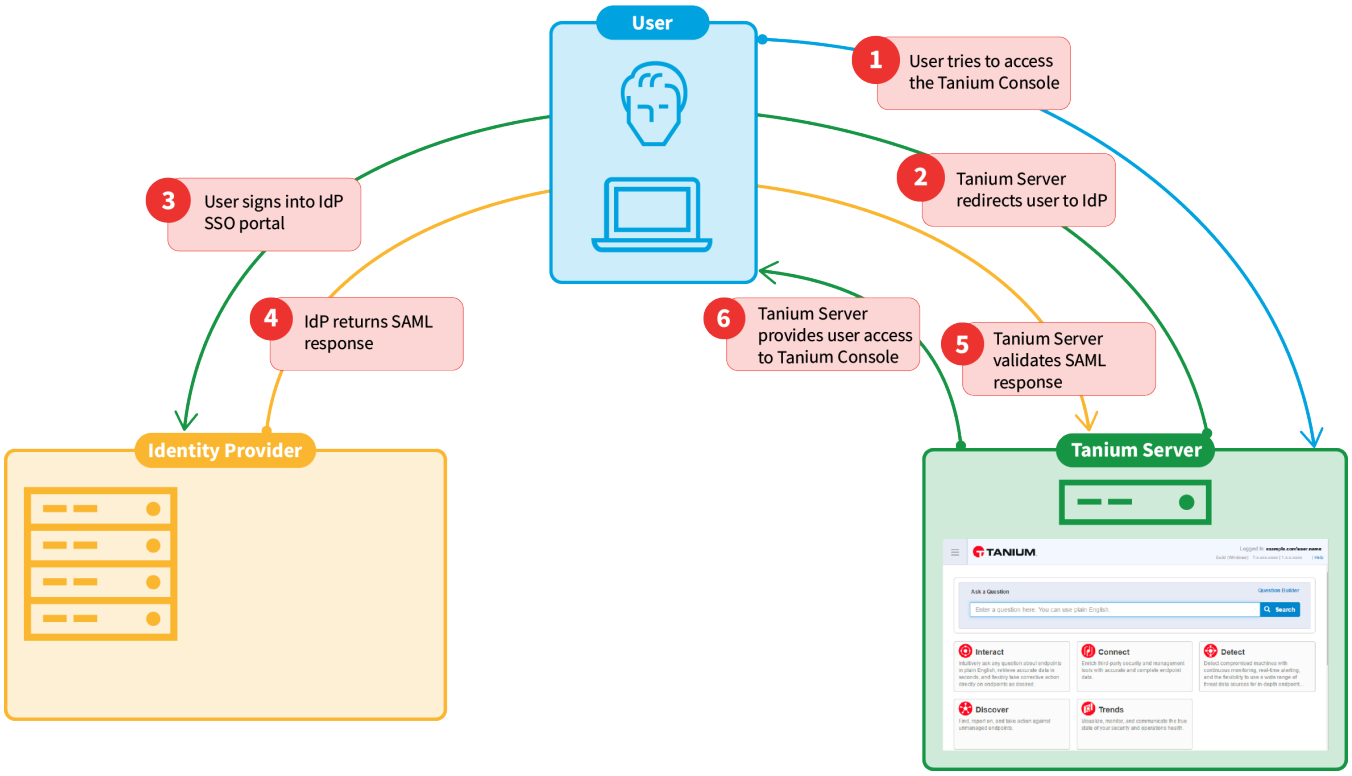
4 The IdP returns a signed response (which contains a SAML assertion) that indicates the user authenticated successfully. The user browser automatically forwards the response to the SP.

5 The SP uses the IdP certificate to verify that the SAML response signature is valid.

6 The SP provides the user access to the application.

© 2026 Tanium Inc. All Rights Reserved

SP-initiated SAML SSO



Before you begin

You must meet the following prerequisites before configuring a SAML integration:

- **Tanium Console users**

  Work with the IdP administrator to identify which users must access Console through the IdP. The IdP administrator is responsible for configuring authentication through an Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) server and managing user access through the IdP. For information about setting up an application through an IdP, see your IdP documentation.

  IMPORTANT

  An administrator must create Console users if they are local to the Tanium Server (see Create a user on page 629) or must import the users from an LDAP server (see Importing and authenticating users through LDAP on page 666).

- (Optional) **IdP metadata file**

  Obtain an IdP metadata file from the IdP administrator. This XML file specifies IdP-specific settings that enable the Tanium Server to trust the IdP. For example, the file specifies the entity ID, also known as the audience Uniform Resource Identifier (URI), which is the globally unique identifier for the IdP in SAML communications. Usually and ideally, the metadata file also

© 2026 Tanium Inc. All Rights Reserved

includes the IdP certificate, which the Server must use to validate SAML responses and assertions from the IdP. Otherwise, you must obtain the certificate from the IdP administrator separately from the metadata file. The certificate file must be Privacy Enhanced Mail (PEM)-encoded.

- **Request-signing certificate**

  Generate a certificate for signing authentication requests from the Tanium Server. Some IdPs require signed requests. For more information, see Generate a request-signing certificate on page 687.

- (IdP-initiated SSO only) **SSO portal URLs**

  If changes occur to the URLs where Console users access the IdP SSO portal, work with the IdP administrator when rolling out the changes.

Generate a request-signing certificate

Some IdPs require a digital signature on SAML requests from an SP such as the Tanium Server. To enable the IdP to authenticate requests, you must generate a request-signing certificate and private key. The Server uses the key to sign the requests and the IdP uses the certificate to validate the signature.

The request-signing certificate also supports encrypting SAML assertions from the IdP through SAML token encryption. The IdP uses the public key in the certificate to encrypt the assertions and the Tanium Server uses the private key to decrypt the assertions. A SAML integration with the Tanium Server supports the following algorithms for SAML token encryption:

Supported algorithms for SAML token encryption

Type	Name	Identifier
Key transport	RSA_OAEP	http://www.w3.org/2009/xmlenc11#rsa-oaep
	RSA_v15	http://www.w3.org/2001/04/xmlenc#rsa-1_5
Encryption	AES_256_CBC	http://www.w3.org/2001/04/xmlenc#aes256-cbc



Use RSA_OAEP as the key transport algorithm.

Generate a request-signing certificate in a Tanium Appliance deployment

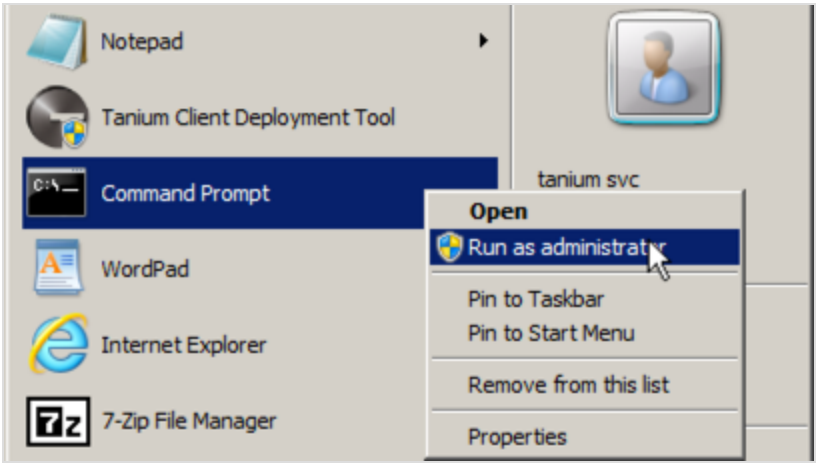
To generate a request-signing certificate in a Tanium Appliance deployment, see Tanium Appliance User Guide: Install a custom certificate. In an active-active deployment, you can use one certificate and key for both Tanium Servers.

Generate a request-signing certificate in a Windows deployment

After generating the SAML request-signing certificate and private key, you must restart the Tanium Server for it to read the certificate. Therefore, perform the following steps during a period when restarting the Server will not interrupt critical operations. In an active-active deployment, you generate the certificate and key files on one Server (either peer), copy the files to the peer Server, and restart both Servers.

© 2026 Tanium Inc. All Rights Reserved

1. Access the Tanium Server CLI. If necessary, elevate permissions to open the command prompt as the administrator user.



2. Go to the Tanium Server installation directory.

3. Run the following command to generate the certificate and private key. For the *<hostname>*, specify the FQDN of the Tanium Server. In an active-active deployment, separate the host names with a comma (such as `ts1.example.com,ts2.example.com`). You must specify `SAMLEncryption` as the certificate and key file names for the Server to use them for SAML communication. The utility automatically appends the `.crt` and `.key` suffixes to the certificate and key file names.

   ```
   KeyUtility selfsign <hostname> SAMLEncryption
   ```

   The utility generates the certificate and key at the top level of the Server installation directory.

4. (Active-active deployment only) Copy the certificate and key to the top level installation directory of the peer Server.

   IMPORTANT When you move a copy of the private key, use a secure method that prevents unauthorized access during transit and that avoids leaving the copy on any system other than the Tanium Servers.

5. Open the Windows **Services** program and restart the **Tanium Server** service. In an active-active deployment, perform this step on both Servers.

   As long as the certificate and key files remain in the top level of the Tanium Server installation directory, the Server automatically uses the key to sign SAML requests and includes the certificate in the **Tanium Metadata** file. You send the file to the IdP in the last step of Configure SAML on the Tanium Server on page 689.

   TIP Alternatively, you can add the **SAMLEncryptionCertPath** and **SAMLEncryptionKeyPath** settings on the Tanium Server to configure different file names and locations for the certificate and key. Contact Tanium Support for details. For more information, see Contact Tanium Support on page 724.

© 2026 Tanium Inc. All Rights Reserved

Configure SAML on the Tanium Server

Perform the following steps to configure SP-initiated or IdP-initiated SAML SSO.

IMPORTANT

If you previously enabled a password prompt for configuration changes, the Tanium Server automatically changes it to a **Yes/Cancel** prompt after you enable SAML authentication.

1. From the Main menu, go to **Administration > Configuration > SAML Configuration** and click one of the following buttons:
   - **Configure SAML**: This button appears if no IdP is currently configured.
   - Edit : Click this button to edit the existing configuration.

     IMPORTANT

     Specifying a new IdP removes any existing IdP configuration because the Tanium Server supports only one IdP at a time.
2. Configure the following fields:

SAML configuration settings

Settings	Guidelines
Identity Provider Metadata	If your IdP administrator provided an IdP metadata file, upload it to automatically configure the following SAML settings: • **Entity ID Configuration**: The **Validate IdP's Entity ID** setting is selected by default and the text field contains the IdP entity ID. • **Identity Provider Certificate**: The metadata usually contains the certificate. If not, you must manually upload the certificate file. • **Identity Provider SSO URL**: If the metadata specifies this URL, the **Enable SP-initiated SSO** option is automatically selected. To upload the IdP metadata file, click **Choose File**, select the file, and click **Open**.

© 2026 Tanium Inc. All Rights Reserved

SAML configuration settings (continued)

Settings	Guidelines
Entity ID Configuration	By default, **Validate IdP's Entity ID** is selected, which means that the Tanium Server validates the entity ID in SAML responses from the IdP. The text field displays the ID from the **Identity Provider Metadata** file that you imported (for example, `http://www.okta.com/gzn4gvh7dvpeDr6oG4g1`).  Enabling **Validate IdP's Entity ID** is optional but a security best practice to provide another layer of protection in addition to using the IdP certificate to validate SAML responses.
Elements which must be signed	Every **SAML Response** from the IdP requires a digital signature and therefore you cannot clear the read-only checkbox. Select **SAML Assertion** if your IdP is also configured to sign assertions. The Tanium Server uses the IdP signing certificate to validate both signatures. SAML authentication fails if a response is not signed and also fails if you selected **SAML Assertion** and the assertion is not signed.
Identity Provider Certificate	The Tanium Server uses the IdP certificate to validate SAML responses and assertions from the IdP. If the **Identity Provider Metadata** specifies the certificate, the Server automatically extracts it and populates this setting with the certificate file name. Otherwise, you must manually upload the certificate that the IdP provided separately from the metadata: click **Update File**, select the certificate, and click **Open**.
Tanium Entity ID	The entity ID of your Tanium environment. The Tanium Server automatically generates an ID, but you can replace it with any Uniform Resource Identifier (URI) that uniquely identifies your Tanium environment in SAML communications. The URI is typically a URL that contains the Tanium Server domain name (such as `https://tanium.example.com/sp`).

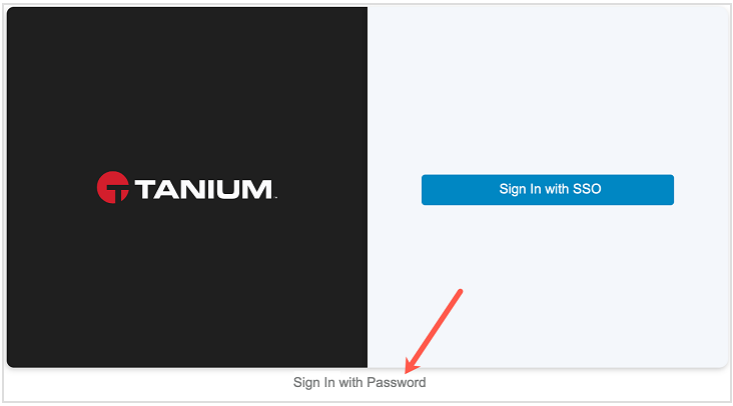
© 2026 Tanium Inc. All Rights Reserved

SAML configuration settings (continued)

Settings	Guidelines
Customize Tanium ACS URLs	Select this option if the Assertion Consumer Service (ACS) URL that the Tanium Server generates by default will not work in your deployment. The Server uses the ACS URL to receive and process SAML assertions from the IdP. The default URL is based on the actual host name or IP address of the Server, which might differ from the host name or address that users specify in their browser to access Tanium Console. Select an option: • **Use the same host name for all Tanium Servers**: Select this option if your deployment uses a load balancer that masks the presence of one or more Tanium Servers. For the **Shared Custom Hostname**, enter the host name or IP address that users specify in their browser to access Tanium Console. This option is required if your IdP supports only one ACS URL for each SP. • **Specify unique host names for each Tanium Server**: Select this option if users access Tanium Console on each active-active Tanium Server using separate host names or IP addresses. Enter the **Custom Host Name** of each Server.  NOTE In rare circumstances, one of the Tanium Servers in an active-active deployment might not be registered yet. In such cases, enter the **Custom Host Name** of each Server anyway to ensure that both can function as an SP when the unregistered Server does register.

© 2026 Tanium Inc. All Rights Reserved

SAML configuration settings (continued)

Settings	Guidelines
SP-Initiated SSO Configuration	If the **Identity Provider Metadata** specifies an **Identity Provider SSO URL**, the Tanium Server automatically populates this setting and selects **Enable SP-initiated SSO**. This is the URL where users access Tanium Console (for example, `https://company.saml-provider.com/app/companyinc_tanium/dGFuaXVtc2FtbA/sso/saml`). If you want users to access Console only through the IdP SSO portal, deselect **Enable SP-initiated SSO**. Select the sign-in options if you enable SP-initiated SSO: • **Allow users to sign in with username and password**: This setting controls whether the Tanium Console sign-in page displays a **Sign In with Password** link.  This link gives users the option to access Tanium Console by entering credentials instead of using SSO. Deselect this option if you want to force all users to authenticate through SAML SSO when they sign in to Console. The option applies only to Console access and does not control access to the Tanium Server CLI or API through any authentication method. IMPORTANT If you disable password sign ins and SP-initiated SSO later stops working (for example, the connection to the IdP goes down), no users can access Tanium Console. In such cases, you must disable SP-initiated SSO through the CLI to re-enable local or LDAP password authentication. For more information, see Disable SP-initiated SSO without Console access on page 694. NOTE To disable LDAP password-based authentication at the API level, disable the Authentication on page 680 option in the LDAP server configuration. • **Force full user re-authentication at every sign-in**: Select this option if you want to force users to enter sign-in credentials when they start a new Tanium Console session even if they already authenticated for a previous session that ended due to inactivity or a manual sign-out event. By default, this option is deselected and users can just click **Sign In with SSO** to start another Console session without entering sign-in credentials.

© 2026 Tanium Inc. All Rights Reserved

3. Click **Save**.

   You must wait up to three minutes for the Tanium Server to apply your changes. If you changed the **SP-Initiated SSO Configuration** settings for an existing SAML configuration, you must also manually refresh the sign-in page after waiting.

   > NOTE
   >
   > If the **Tanium Metadata** section displays the message `Request Signing Certificate Not Configured`, consider generating the certificate before proceeding. For more information, see Generate a request-signing certificate on page 687.

4. Perform one of the following tasks based on whether the IdP supports metadata exchange documents:

   - **Supported**: Click **Download** in the **Tanium Metadata** section to export the metadata file to the `Downloads` directory on the system that you use to access Tanium Console. The Tanium Server automatically generates the metadata based on the settings that you configured in the **SAML Configuration** page. You must send the file to the IdP. The IdP administrator then uses the file to configure the IdP with the settings that are required to communicate with the Tanium Server.
   - **Not supported**: Ask the IdP administrator to manually configure the settings in the IdP system.

   To complete these tasks on the IdP, see Before you begin on page 693 in the procedure to Configure SAML on the IdP on page 693. You must complete that procedure before users can start accessing Tanium Console through SSO.

Configure SAML on the IdP

Work with an IdP administrator to configure the IdP for integration with the Tanium Server.

> IMPORTANT
>
> To integrate Microsoft Entra with the Tanium Server, see Microsoft Learn: Azure Active Directory SSO integration with Tanium SSO. Microsoft Entra was formerly known as Microsoft Azure Active Directory (Azure AD).

Before you begin

Perform one of the following tasks based on whether the IdP supports metadata exchange documents:

- **Supported**: Import the Tanium metadata file into the IdP to automatically configure settings that you already configured on the Tanium Server. For more information, see the last step of Configure SAML on the Tanium Server on page 689.
- **Not supported**: Record the settings that you must manually enter in the IdP:

  1. Sign in to Tanium Console as a user with the **Administrator** role.
  2. From the Main menu, go to **Administration > Configuration > SAML Configuration**.
  3. Record the **Tanium Entity ID** and **Tanium ACS URLs** values and provide them to the administrator who will configure the IdP for integration with the Tanium Server.

© 2026 Tanium Inc. All Rights Reserved

Configure Tanium Server settings on the IdP

The specific steps to configure an IdP for integration with an SP (the Tanium Server in this case) vary by IdP vendor. However, all IdPs require the following settings. If you imported the Tanium metadata file, settings from that file are automatically configured in the IdP and you just have to verify them.

- **Tanium Entity ID**
- **Tanium ACS URLs**
- **NameID format**: Set to `Unspecified`. In SAML assertions, the **NameID** value must match the **User Name** (not the **Display Name**) of a user on the Tanium Server. For more information, see View user details on page 627. If the Server imports users through LDAP, the **NameID** value must match the User Name Property on page 680 value for each user.
- **RelayState**: Set to no value (blank). The Tanium Server does not process this setting.

After the administrator configures the IdP, users can start accessing Tanium Console through SSO. For more information, see Sign in to Console on page 49.

Disable or enable SAML SSO

Initially, you enable SAML SSO by performing the steps under Enabling SSO through SAML on page 684. If disabling SSO becomes necessary, such as for troubleshooting authentication issues, you can later re-enable it. While SSO is disabled, users must enter their username and password to sign in to Tanium Console.

Events might prevent SSO from working, such as if the connection to the IdP goes down. In such cases, users can access Console through sign-in credentials only if you selected **Allow users to sign in with username and password** in the SAML configuration. If you deselected that option, you must Disable SP-initiated SSO without Console access on page 694 to re-enable access through sign-in credentials.

Disable SSO through Console

1. From the Main menu, go to **Administration > Configuration > SAML Configuration**.
2. Click **Disable SAML**.

Enable SSO through Console

1. From the Main menu, go to **Administration > Configuration > SAML Configuration**.
2. Click **Enable SAML**.
3. (Optional) Select **Enable SP-initiated SSO** and edit the **SP-Initiated SSO Configuration** options if necessary.
4. Click **Save**.

Disable SP-initiated SSO without Console access

Tanium Appliance and Windows deployments have separate procedures for disabling SP-initiated SSO without accessing Tanium Console.

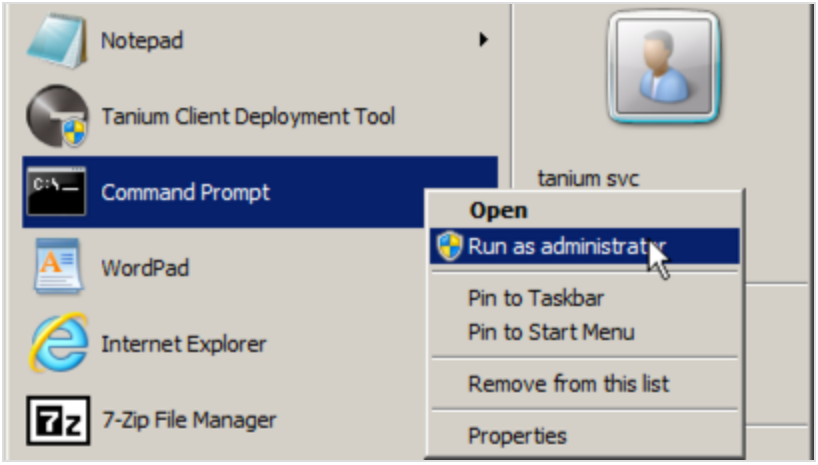
© 2026 Tanium Inc. All Rights Reserved

APPLIANCE: DISABLE SSO

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-X` (Tanium Operations > Advanced Operations).
3. Enter `7` to disable SAML SSO.

WINDOWS: DISABLE SSO

1. Access the Tanium Server CLI. If necessary, elevate permissions to open the command prompt as the administrator user.



2. Go to the Tanium Server installation folder.
3. Run the following command:

```
TaniumReceiver global-settings set console_saml_sp_enabled 0
```

Wait up to a minute for the change to apply, or restart the Tanium Server service to apply the change immediately. You can find the Tanium Server service in the Windows **Services** program.

© 2026 Tanium Inc. All Rights Reserved

Enabling long-lived Tanium sessions through API tokens

API tokens overview

Tanium™ API authentication tokens enable users to establish long-lived sessions with the Tanium Server without repeatedly re-authenticating for workflows that are long-lived but not continuously running. For example, you can add a token that enables the synchronization of patch definitions and statuses between the Tanium Patch module and the Tanium Patch Management for IT Operations application in a ServiceNow instance.

Tokens have a configurable expiration interval. To prevent interruptions to long-lived workflows, users must *rotate* tokens: request new tokens and revoke the current ones before they expire.



For the user role permissions that are required to manage API tokens, see Manage API tokens on page 106.

To troubleshoot issues with API tokens, see Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform.

Token permissions

A token can authenticate only the service account, user account, or persona that you select for the token when creating it. Each account or persona can have multiple tokens. The role permissions of a token are those of the account or persona that you select when creating the token. If the permissions of an account or persona change after the token is created, the token permissions change to match those of the account or persona.

Best practices for tokens

Observe the following best practices when you create tokens:

- **Use service accounts**

  Select a service account for every token unless the token is for workflows that a specific user account or persona must run according to the mandates of your organization. If users or personas are deleted, disabled, or locked out (such as when a user leaves your organization), their tokens produce `401 Unauthorized` errors when other accounts or personas try to use those tokens. Such errors are less likely for tokens that are bound to service accounts because those accounts are more often permanent.

- **Use one token per process**

  Do not use a single token for multiple processes. For example, do not use a single token for a ServiceNow integration and a Splunk integration, or for multiple ServiceNow instances, or for multiple connections from one ServiceNow instance to the Tanium Server. When a token rotates for any process, that token stops working for any other processes that use it.

© 2026 Tanium Inc. All Rights Reserved

View API token details

Viewing API token attributes can help you to determine if new tokens are necessary and to manage or troubleshoot existing tokens. For example, you can check if a token is about to expire and for which user the token is bound. The **API Tokens** grid shows only valid tokens and stops showing tokens that you revoke.

1. From the Main menu, go to **Administration > Permissions > API Tokens**.
   The page displays API token attributes on page 698 but not token strings.
2. (Optional) To display a token value, select the token in the grid and click **View Token**.

   The token value includes the `token-` prefix.
   You cannot view the token value in Tanium Console after:

   - The visibility timeout expires (five minutes)
   - You refresh the **API Tokens** page or grid
   - You navigate to another Console page
3. (Optional) Use the filters to find specific tokens:
   - **Filter by text**: Enter a text string in the **Filter items** field to filter the grid by any column values.
   - **Filter by attribute**: Expand the **Filters** section, select a token attribute (such as **User**), select an operator (such as **contains**), enter a text string that contains all or part of the attribute value, and click Apply. For each additional filter, click, select **Add Row**, and configure the filter. Boolean **AND** logic applies if you configure multiple filters.

© 2026 Tanium Inc. All Rights Reserved

Create an API token

1. From the Main menu, go to **Administration > Permissions > API Tokens**.
2. Click **New API Token** and configure the token settings:

API token attributes

Attribute	Description
Notes	Enter an optional description of the purpose for this token.
Expiration	Enter the expiration interval in days. By default, the maximum interval is 365 days. If you do not enter a value, the interval defaults to 7 days. To change the default interval or maximum interval, see Configure token expiration settings on page 699.
Persona	Select the user account (**Default** persona) or alternative persona to which the token is bound. The default option is the currently selected persona for your Tanium Console session.
Trusted IP addresses	Enter the external IP addresses of the systems from which you will use this token to authenticate with the Tanium Server. The addresses can be IPv4 (such as `192.0.2.0/24`) or IPv6 (such as `2001:db8::/32`). Use commas or new lines to separate multiple entries. To enable any system to use the token, enter `0.0.0.0/0`. However, for security, enable the token for all systems only in a non-production environment.

3. Click **Save** and review the token details.
4. Copy the token to your clipboard if you want to record it for future reference, and then click **Close**.



The token value includes the `token-` prefix. You cannot view the token value in Tanium Console after the visibility timeout (five minutes) expires, or you refresh the **API Tokens** page or grid, or you navigate to another Console page. If you later rotate the token, you must re-enter its value. Therefore, if you want rotation to be an option, copy the value (including `token-`) before the timeout and save it in a secure location.

Rotate an API token

To extend the expiration interval of a token without changing any of its other settings, rotate the token. Rotation deletes the existing token and creates a new one. The expiration timer of the new token is reset and has the same interval as the deleted token.

© 2026 Tanium Inc. All Rights Reserved

NOTE

You cannot rotate a token unless you saved a record of its value after creating the token. After you rotate the token, the visibility timeout for its value resets to five minutes. For more information, see View API token details on page 697.

BEST PRACTICE

If you integrate your Tanium deployment with another platform such as ServiceNow or Splunk, use the Tanium API to configure the integration to automatically rotate its tokens when their expiration is imminent. Automatic rotation reduces the maintenance workload for an integration. For more information about APIs and integrations, see APIs & Integrations. For help configuring your integrations, see Contact Tanium Support on page 724.

1. Sign in to Tanium Console as a user who has the **Token - Rotate** permission.
2. From the Main menu, go to **Administration > Permissions > API Tokens**.
3. Select the token and click **Rotate Token**.
4. Enter the **Token** value (including the `token-` prefix) and click **Confirm**.

   NOTE

   The token for which you enter a value is the token that is rotated regardless of which token you select on the **API Tokens** page in the previous step.
5. Copy the new token value to your clipboard if you want to record it for future use (such as for rotating the token again), and then click **Close**.

Enable API token authentication behind a reverse proxy

Enable the setting **authenticate_api_token_with_x_forwarded_for_ip** only if all API token access to the Tanium Server must go through a reverse proxy server.

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.
2. In the **Name** column, click **authenticate_api_token_with_x_forwarded_for_ip**.
3. Set the **Value** to `1` and click **Save**.

Configure token expiration settings

By default, API tokens expire one week after you create them if you did not specify the expiration interval during token creation. Also by default, you cannot specify an interval beyond 365 days during token creation. You can change both the default interval and maximum interval. However, changes to the default interval apply only to tokens that are created after you change the setting; you cannot change the interval for existing tokens.

Perform the following steps to change the settings that control the expiration interval:

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.
2. To change the default expiration interval, click **api_token_expiration_in_days** in the **Name** column, set the **Value** to a new interval (in days), and click **Save**.
3. To change the maximum expiration interval, click **api_token_max_expiration_in_days** in the **Name** column, set the **Value** to a new maximum (in days), and click **Save**.

Revoke API tokens

You might want to revoke an API token if you have doubts about its security or if its associated user is no longer with your organization.

1. From the Main menu, go to **Administration > Permissions > API Tokens**.
2. Select one or more API tokens, click Delete Selected , and **Confirm** the operation.

   The revoked tokens no longer appear in the **API Tokens** grid.

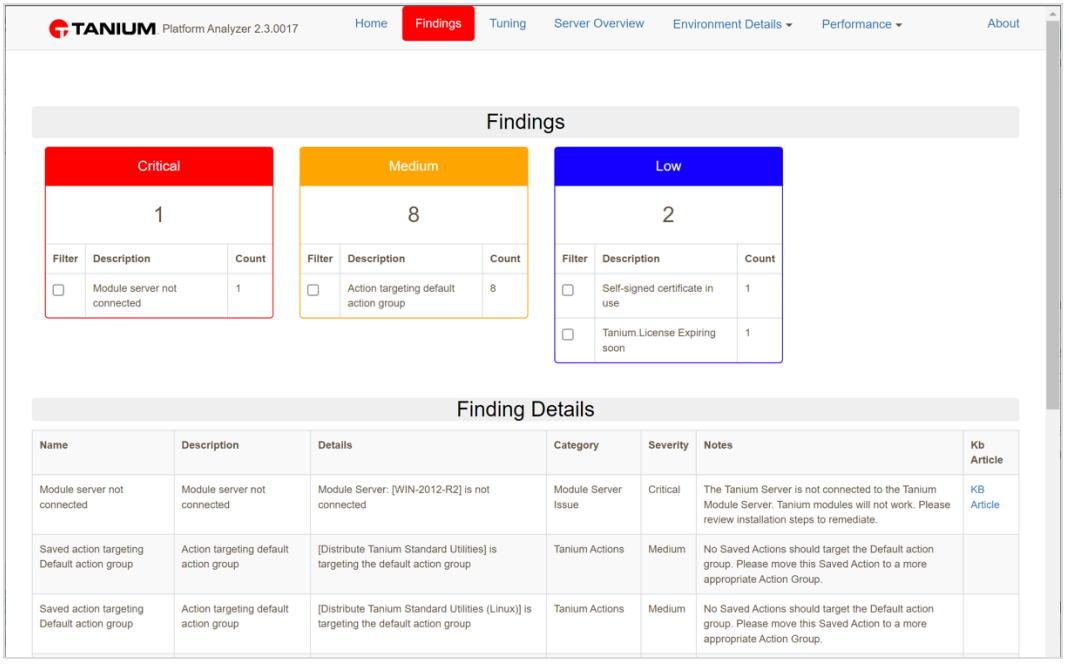
© 2026 Tanium Inc. All Rights Reserved

Part 12: Troubleshooting Console and Interact

Basic troubleshooting tips

The following features and processes can help you perform basic troubleshooting for your Tanium environment.

Tips for basic troubleshooting

Feature or process	Tip
TPAN report	Regularly run and review the the Tanium Platform Analyzer (TPAN) report. The report can facilitate future troubleshooting regardless of whether your deployment currently has issues. For more information about the best practices for TPAN settings, see: • Tanium Appliance User Guide: Troubleshooting workflow • Tanium Core Platform User Guide for Windows Deployments: Troubleshooting workflow **TPAN report findings to troubleshoot Console issues** 
Periodic maintenance	Perform recommended maintenance tasks at regular intervals to ensure that your Tanium deployment uses resources efficiently and provides the best user experience. For more information, see Tanium Maintenance User Guide.

© 2026 Tanium Inc. All Rights Reserved

Tips for basic troubleshooting (continued)

Feature or process	Tip
Solution updates	Installing later versions of Tanium solutions (modules and shared services) might resolve unexpected behavior. The Tanium Console version appears in the Console header. To check the currently installed versions of other solutions, and to update them if necessary, see Part 4: Managing Tanium solutions on page 108. BEST PRACTICE Install the most recent version of every solution.
Warning messages	If warning conditions exist, Console initially displays the warnings when you sign in. After you close the warnings, you can click the warnings icon ⚠ in the Console header to redisplay them.
Local Error Log	Review any error messages in the Tanium Console error log. For more information, see Work with the Console error log on page 705.
Other logs	If other troubleshooting tasks are insufficient for diagnosing issues, you can view logs on the Tanium Core Platform servers. For information about optimizing the logging level for troubleshooting, see: • Tanium Appliance User Guide: Logging levels • Tanium Core Platform User Guide for Windows Deployments: Logging levels The requirements for viewing log types other than the **Local Error Log** vary by infrastructure: • Tanium Appliance User Guide: Log and report types • Tanium Core Platform User Guide for Windows Deployments: Log and report types

NOTE If the browser that you use to access Tanium Console displays an HTTP response status code in the 500 to 599 range, this indicates a server error. However, the responsible server might or might not be a Tanium Core Platform server. For more information, see Troubleshoot core platform server issues on page 705.

Troubleshoot Console issues

Troubleshoot Console access

If you cannot access Tanium Console, review the following causes and troubleshooting tasks.

NOTE If you can access Console but not a particular Tanium solution or Console feature, the issue might be related to user permissions. For more information, see Troubleshoot RBAC issues on page 713.

© 2026 Tanium Inc. All Rights Reserved

CONSOLE IS UNAVAILABLE

If you cannot reach Tanium Console through your browser, review the following issues and remediation tasks.

Tanium Console availability issues and remediation tasks

Issue	Remediation
Browser requirements	Verify that your browser meets the requirements for Console access. For more information, see Web browsers on page 73.
Protocol and port	Verify that you are specifying the correct protocol and Tanium Server port for Console access: • **Protocol**: Connect through HTTPS, not HTTP. • **Port**: The standard port is 8443/443 on the Tanium Appliance and port 443 in a Windows deployment. If the Tanium Server uses a non-standard port, you must specify it in your browser in the format `https://<Tanium Server FQDN or IP address>[:<port>]`. The port is set during Server installation. To view the port setting, see: ◦ Tanium Appliance User Guide: Reference: Deployment-related Tanium Core Platform settings ◦ Tanium Core Platform User Guide for Windows Deployments: Reference: Deployment-related Tanium Core Platform settings
Tanium database status	Verify the status of the Tanium databases on the database server. For specific steps, see the documentation for the database type: Microsoft SQL (MSSQL) or PostgreSQL.
Tanium Server status	Verify the status of the **Tanium Server** service and, if necessary, restart it: • **Tanium Appliance**: For more information, see Tanium Appliance User Guide: Start, stop, and restart Tanium services. • **Windows Server**: For more information, see Tanium Core Platform User Guide for Windows Deployments: Manage Windows services for core platform servers.

CONSOLE AUTHENTICATION ERRORS

If you cannot sign in to Tanium Console, review the following issues and remediation tasks:

Tanium Console authentication issues and remediation tasks

Issue	Remediation
User configuration	Ask an administrator who has permissions for managing users to verify that your account exists in **Administration > Permissions > Users**. For the steps to view or create accounts, see Managing users on page 625.

© 2026 Tanium Inc. All Rights Reserved

Tanium Console authentication issues and remediation tasks (continued)

Issue	Remediation
User account status and user group status	Verify that your account is not renamed, deleted, disabled, or locked out. The specific steps depend on the type of authentication that is configured for your account. On the **Users** page, check the **Source** column to quickly determine which users and user groups are **Local** to your Tanium Cloud instance or are imported from an **External** identity store, such as a Security Assertion Markup Language (SAML) identity provider (IdP), Active Directory (AD) server, or Lightweight Directory Access Protocol (LDAP) server. • **Local authentication**: Verify that local user access is enabled. For more information, see Disable or enable local user access on page 642. Also check the account and authentication service that corresponds to your Tanium infrastructure: ◦ **Appliance**: For more information, see Tanium Appliance User Guide: Configure the local authentication service. ◦ **Windows**: Check the account status in the Windows user database: From the Windows menu, open the **Control Panel**, click **User Accounts**, and click **Manage another account**. • **LDAP/AD**: If your account is imported, ask your AD or LDAP administrator to check the account status. You can also review the LDAP logs. For more information, see Example: LDAP synchronization and authentication on page 667. • **SAML**: For accounts that authenticate through SAML, ask your IdP administrator to check the account status in the identity store. User accounts and user groups might fall out of sync between Tanium Cloud and the identity store over time. This might happen if accounts or groups are renamed, undeleted, or deleted and recreated. When you troubleshoot synchronization issues, the **External ID**, **Reflected ID**, and **SCIM Server Name** values in the User account attributes on page 628 and User group attributes on page 644 enable you to correlate between objects in Tanium Cloud and the identity store. To troubleshoot other issues with your SAML integration, review the authentication log. To find specific events, open the log in a text editor or use CLI commands to search for keywords such as `SAML`. For more information, see: ◦ Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform ◦ Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform
Smart Card access	To troubleshoot Console access through smart cards, see: • Tanium Appliance User Guide: Configuring smart card authentication • Tanium Core Platform User Guide for Windows Deployments: Configuring smart card authentication
Logs	Review the history of authentication events in the authentication log: • Tanium Appliance User Guide: Authentication log • Tanium Core Platform User Guide for Windows Deployments: Authentication log

© 2026 Tanium Inc. All Rights Reserved

Tanium Console authentication issues and remediation tasks (continued)

Issue	Remediation
Tanium Server upgrades	In rare cases, if the Tanium Server was upgraded since your last sign-in session, you might have to clear your browser cache or try a different browser.

Troubleshoot session termination issues

If Tanium Console user sessions terminate prematurely, review the events, user preferences, and platform settings that affect the duration of a user session. For more information, see Session validity and timeouts on page 53.

NOTE

The browser that you use to access Console might display the **401 Unauthorized** error when a session expires.

Troubleshoot license issues

To troubleshoot issues with the Tanium license, see Troubleshoot license issues on page 208.

Work with the Console error log

Tanium Console maintains an error log on the local host computer for your web browser. It includes details on the last 100 errors that were returned to the Console in response to actions that you performed through the browser. For example, the log records errors that are associated with attempting to save a configuration or import a content file. Console maintains a separate log for each browser that you use.

1. In the Console header, hover over the user icon and select **Local Error Log**.
2. (Optional) Expand a log entry and Copy the log details to the clipboard.
3. (Optional) Click **Clear Log** if you want to remove all the log entries. For example, you might want to remove the entries after you finish resolving the associated issues.

Troubleshoot core platform server issues

Unexpected behaviors that manifest in Tanium Console might result from issues in Tanium Core Platform servers. In some cases, upgrading to later server versions might resolve the issues. Use the **Solutions** page to check whether server updates are available and to install the updates. For the steps, see Part 4: Managing Tanium solutions on page 108.

The following sections describe other server troubleshooting tasks that you can perform through Console.

TIP

You can use the command-line interface (CLI) or other methods to perform additional troubleshooting and remediation tasks on the servers. For example, you can restart services, upgrade servers, or view installation logs. For more information, see:

© 2026 Tanium Inc. All Rights Reserved

TIP

- Tanium Appliance User Guide: Support and Troubleshooting
- Tanium Core Platform User Guide for Windows Deployments: Troubleshooting

NOTE

If the browser that you use to access Console displays an HTTP response status code in the 500 to 599 range, this indicates a server error. The responsible server might or might not be a Tanium Core Platform server.

Troubleshoot platform server disk space consumption

When you sign in to Console, it displays a warning if the amount of free disk space is 20% or less of the total disk capacity of a Tanium Server, Module Server, or Zone Server. If you see the warning:

1. Review the disk space requirements of the server:
   - Tanium Appliance User Guide: Reference: Tanium Appliance specifications
   - Tanium Core Platform User Guide for Windows Deployments: Reference: Host system resource guidelines
2. Contact Tanium Support for help reducing disk space usage. For more information, see Contact Tanium Support on page 724.

Troubleshoot platform server trust issues

In an active-active deployment, Tanium Servers must trust each other for synchronization. In a deployment with Tanium Zone Servers, trust is also required between Tanium Servers and Zone Server Hubs, and each Zone Server must be mapped to a Hub. To troubleshoot issues related to server trust and mapping:

1. View Tanium Server trust history on page 225 to see details about who approved or revoked trust, when, and whether the operation succeeded.
2. Review the PKI log for additional information about events that relate to server trust:
   - Tanium Appliance User Guide: PKI log
   - Tanium Core Platform User Guide for Windows Deployments: PKI log

Troubleshoot certificate and key issues

To troubleshoot errors that relate to the digital certificates and keys that secure communication among Tanium Core Platform servers and Tanium Clients, review the following issues and remediation tasks.

© 2026 Tanium Inc. All Rights Reserved

Certificate and key issues and remediation tasks

Issue	Remediation
Certificate validation	If your browser displays a certificate validation error when you access Tanium Console or the Tanium API, this might indicate that the Tanium Server is using a self-signed certificate. To replace it with a certificate that a certificate authority (CA) has issued, see Securing Console and API access through certificates on page 220.
Key rotation	If you encounter issues after rotating Tanium root keys, see: • View root key information on page 216 • Rotation intervals for subordinate keys on page 213
File downloads	If you encounter issues with the certificates that the Tanium Server uses to secure file downloads from remote sources, see Enabling authentication between platform servers and remote systems on page 173.

Tanium Client communication	If Clients connect to the Tanium Server or Zone Server but exhibit other communication issues (such as failing to answer questions):
	1. Go to **Administration > Configuration > Client Status** and verify whether the Clients are **Using TLS** and a **Valid Key**. For more information, see View the status of Tanium Client registration and communication on page 718.
	2. If Clients are not using TLS to communicate with the server, perform one of the following tasks:
	  • Redeploy the Tanium root key to Clients. For more information, see Download infrastructure configuration files (keys) on page 218.
	  • Reinstall the Tanium Client on the affected endpoints. For more information, see Tanium Client Management User Guide.

HSM integration	If Tanium keys are managed on a hardware security module, see Tanium Core Platform User Guide for Windows Deployments: Securing keys with an HSM.
Smart card access	If Tanium Console access is secured through smart cards and you encounter issues with the associated certificate, see: • Tanium Appliance User Guide: Configuring smart card authentication • Tanium Core Platform User Guide for Windows Deployments: Configuring smart card authentication

Logs	To see the history of cryptographic events on Tanium Core Platform servers, review the following logs:
	• **PKI log**: This log records events that relate to key operations, such as key generation or revocation. For more information, see:
	  ◦ Tanium Appliance User Guide: PKI log
	  ◦ Tanium Core Platform User Guide for Windows Deployments: PKI log
	• **PKI TLS log**: This log records events that relate to Transport Layer Security (TLS) connections among Tanium Core Platform servers and Tanium Clients. For more information, see:
	  ◦ Tanium Appliance User Guide: PKI TLS log
	  ◦ Tanium Core Platform User Guide for Windows Deployments: PKI TLS log

© 2026 Tanium Inc. All Rights Reserved

Troubleshoot API token access issues

To troubleshoot issues relating to the Tanium REST API authentication tokens that enable users and service accounts to establish long-lived sessions with the Tanium Server:

1. View API token details on page 697 to verify that tokens enable authentication from the correct IP addresses and have not expired.
2. Review the authentication log:
    - Tanium Appliance User Guide: Authentication log
    - Tanium Core Platform User Guide for Windows Deployments: Authentication log

Configure server logging levels

The logging level determines how much detail the Tanium Server and Tanium Module Server record in their logs. Tanium Support might instruct you to change the logging level when troubleshooting issues.



Only users who are assigned the **Administrator** reserved role can access the **Logging** page.

For more information about logging levels, best practice levels for various scenarios, and to change the level for all Tanium Core Platform components, see:

- Tanium Appliance User Guide: Logging levels
- Tanium Core Platform User Guide for Windows Deployments: Logging levels

1. From the Main menu, go to **Administration > Configuration > Logging**.
2. Set the logging level for each server and click **Save**.

Troubleshoot proxy server issues

If you observe issues that relate to Tanium Core Platform servers accessing Internet locations through a proxy server, you can test the proxy settings and update them as necessary as described under Configure proxy server settings on page 182.

Troubleshoot Interact issues

Troubleshoot question runtimes

If Tanium Clients answer a question slower than expected, the question might use sensors that take a long time to run. When you enter text in the **Ask a Question** field, Interact shows the average runtimes of sensors that you select for questions. If necessary, you can customize the thresholds that determine which icon appears for a specific runtime, as described under Assessing question impacts on endpoints through sensor runtime indicators on page 438.

On the **Question Results** page, you might initially see the answer `[current result unavailable]` from endpoints that take longer than usual to evaluate a question sensor. For more information, see Current result unavailable on page 709.

© 2026 Tanium Inc. All Rights Reserved

Complex regular expressions might increase the time that Clients take to answer a question. For more information, see Reference: Advanced question syntax in Console and Interact on page 731.

Troubleshoot question results issues

If the **Question Results** page shows errors, unavailable results, or unexpected results, review the following issues and remediation tasks.



The Tanium Console user preferences control, on a per-user basis, whether the **Question Results** page shows error results. For more information, see Hide error results from questions on page 157.

Issues and remediation for question results

Issue	Remediation
No results	The **Question Results** grid shows `[no results]` from a Tanium Client if: • The sensor returns no value. • The Client does not have a value that matches the sensor filter. This occurs if you apply a filter to the `get` clause and not the `from` clause. For example, if the question is `Get Computer Name starts with tan from all machines`, all endpoints return answers and all endpoints that do not start with `tan` in their computer name return `[no results]`.  Add the filter in the `from` clause. For example, `Get Computer Name from all machines with Computer Name starts with tan` does not return unexpected `[no results]` rows.
Current result unavailable	If an endpoint takes longer than usual to evaluate a sensor, it might initially supply the answer `[current result unavailable]` to the answer message that it passes along the linear chain and ultimately to the Tanium Server. However, the sensor process continues on the endpoint after supplying that initial answer and, upon completing the process, the endpoint sends its updated answer. The Server then updates the **Question Results** grid.
Results currently unavailable	The **Question Results** grid displays the `[results currently unavailable]` message to indicate that the Tanium Server cannot correctly parse an answer. Parsing errors can result from various conditions, such as the excessive growth of answer strings. Contact Tanium Support on page 724 if you observe this message.

© 2026 Tanium Inc. All Rights Reserved

Issues and remediation for question results (continued)

Issue	Remediation
Too many results	The **Question Results** grid displays `[too many results]` to indicate that more results are available, but the Tanium Clients will not return the additional results. The Tanium Server has certain checks to limit the network and memory impact of questions. Because of how the Server generates these messages, you cannot drill down on this response. Try the following solutions to avoid this message: • Use sensors that are more focused. • Target only a certain endpoint or computer group to limit the unique number of strings for each answer. • Use a non-counting question instead of a counting question. For more information, see Counting and non-counting questions on page 235.
TSE-Error	Messages that begin with `[TSE-Error` indicate a Tanium Client is in a state that prevents it from answering the question. Common reasons include: • Unstable operating system (OS) • Configuration issues • Lack of memory • Sensor cannot execute the script • Antivirus software blocks: To ensure that all the required exclusions are configured in your antivirus software, see Tanium Client Management Guide: Reference: Endpoint security exclusions and for Windows-based Tanium Core Platform deployments, see Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform Server security exclusions. • Corrupted Windows Management Instrumentation (WMI) repositories • Sensor quarantines: The **Question Results** page displays `TSE-Error: The sensor is quarantined` if the question uses quarantined sensors. You can remove those sensors from quarantine if appropriate. For more information, see Manage sensor quarantines on page 433. • Issues related to the roles that are assigned to your user account. For more information, see Troubleshoot RBAC issues on page 713. • Issues related to the computer groups that are assigned to your user account. For more information, see Results missing from certain endpoints on page 711.

© 2026 Tanium Inc. All Rights Reserved

Issues and remediation for question results (continued)

Issue	Remediation
Results missing from certain endpoints	You can see question results only from endpoints in computer groups that are assigned to the user account or persona that you use to issue questions. If certain endpoints to do return results, troubleshoot computer group assignments and configurations: • **Assignments**: Verify that the appropriate computer groups are assigned. If your user account inherits computer group assignments, you might have to assign a different user group: ◦ Assign computer groups on page 618 ◦ Manage user group assignments for a user on page 635 • **Configurations**: View the computer group configurations to ensure that their membership **Expression** is correct. Note that you cannot edit the membership of a computer group. If the membership does not include the correct endpoints, you must create and assign a new computer group. ◦ View computer group details on page 616 ◦ Configure a computer group on page 617
Tanium Client communication issues	View the status of Client connections and, if necessary, correct them. For more information, see Troubleshoot Tanium Client issues on page 717.

Troubleshoot action deployment issues

To ensure actions deploy as expected and to troubleshoot deployment issues, see the task for the action type:

- Simple (non-ring-based) actions: Monitor actions on page 337.
- Adaptive (ring-based) actions: Troubleshoot deployments on page 379.

Troubleshoot TDS issues

To troubleshoot issues related to Tanium Data Service (TDS), see Tanium Interact User Guide: Troubleshoot Tanium Data Service issues.

Manage the package file repository

By default, the Tanium Server uses its `<Tanium Server installation directory>/Downloads` directory to store action package files that it downloads to Tanium Clients. When you are troubleshooting download issues, Tanium Support might instruct you to monitor usage for this repository and to free space in it if necessary.



Only users who have the **Administrator** reserved role can see the **Package File Repository** page.

© 2026 Tanium Inc. All Rights Reserved

As additional troubleshooting for download issues on the Tanium Server, review the following logs:

- Tanium Downloader log
- Download catalog cleaner log
- Package cache cleaner log
- Package download log

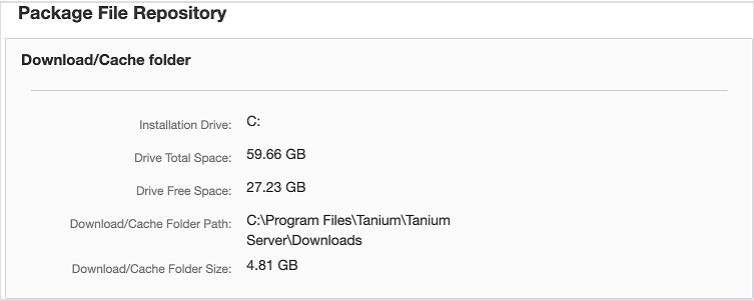
For more information about these logs and how to access them, see:

- Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform
- Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform

View package file repository usage

From the Main menu, go to **Administration > Configuration > Package File Repository** and review the information about the respository for action package files.

Usage metrics for the repository of action package files



Clean the package file repository (Windows infrastructure only)

By default, the Tanium Server automatically cleans the respository for action package files (deletes unused files) every Sunday at 2 AM. However, if you see symptoms of low disk space on the Server (see Troubleshoot platform server disk space consumption on page 706), you can manually clean the repository before then if the Server is deployed on a Windows host. For example, when space is low, users might not be able to access the Tanium Console sign-in page or they might experience sign-in failures.

To manually clean the repository:

© 2026 Tanium Inc. All Rights Reserved

1. Sign in to the Tanium Server host as the **Administrator** user.
2. Open the Windows **Command Prompt** to access the CLI.

   TIP

   For information about using the CLI, see:

   - Tanium Appliance User Guide: Reference: Tanium Core Platform command-line interface
   - Tanium Core Platform User Guide for Windows Deployments: Reference: Command-line interface
3. Navigate to the Tanium Server <*installation directory*>:

   ```
   cd <installation directory>
   ```
4. Run the following command to clear the repository:

   ```
   TaniumReceiver clean-downloads
   ```

Relocate the package file repository (Windows infrastructure only)

Optionally, you can relocate the repository for action package files if another drive on the Tanium Server host has better resources for storing package downloads. For more information, see Tanium Core Platform User Guide for Windows Deployments: Relocate the package file repository.

Troubleshoot RBAC issues

Troubleshoot permission issues

If you see permission errors when trying to access certain Tanium Console pages or features, perform the following tasks.

NOTE

If you cannot access Tanium Console, see Troubleshoot Console access on page 702.

The browser that you use to access Console might display the **403 Forbidden** error for permission issues.

1. Determine which permissions are required to access specific pages and features. For more information, see User role requirements on page 76.
2. Verify that the required permissions are assigned to the user account or persona that you used when trying to access those pages and features:
   - View effective role permissions for a user on page 631
   - View effective role permissions for a persona on page 658

© 2026 Tanium Inc. All Rights Reserved

3. If the effective permissions of the user or persona are insufficient, update the role assignments or role configurations. If the user inherits permissions, you might have to assign that user to a different user group.

    - Configure a custom role on page 586
    - Manage user and user group assignments for a role on page 587
    - Configure role assignments for a persona on page 662
    - Manage user and user group assignments for a role on page 587
    - Manage user group assignments for a user on page 635

4. Review the following logs for additional information about RBAC issues:

    - RBAC log

    The Console error log might record an entry such as the following to identify permission errors: `ERROR: 400 Bad Request RBAC Exception (Ref# 1f14e8215610cf72): RBACInsufficientPrivilege`

    You can use the `Ref#` value to find the corresponding entry in the RBAC log, which provides additional details about the error. For more information, see Work with the Console error log on page 705.

    - Module-provided privileges logs

    For more information, see:

    - Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform
    - Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform

5. Verify that user accounts and user groups are not out of sync between Tanium Cloud and your IdP. For more information, see User account status and user group status on page 704.

Troubleshoot service account lockouts

If passwords change for service accounts, lockout errors might occur for those accounts until you update the account configurations:

- Service accounts for Tanium Core Platform servers, modules, and shared services: For more information, see Manage service accounts for solutions on page 144.
- Service account for LDAP synchronization: For more information, see LDAP User Name and Password on page 676.

© 2026 Tanium Inc. All Rights Reserved

Troubleshoot solution issues

Verify and update solution versions

Installing a later release of Tanium solutions might resolve unexpected behavior. To check the currently installed release and update it if necessary, see Tanium releases on page 111.

BEST PRACTICE

Install the most recent Tanium release.

Troubleshoot installation, update, or uninstallation issues

If errors occur when you install, update, or uninstall Tanium modules, shared services, or content-only solutions, review the following issues and remediation tasks:

Issues and remediation for solution installations, uninstallations, and updates

Issue	Remediation
Active-active synchronization errors	In active-active deployments, if module operations succeed on one Tanium Server but fail to synchronize on the peer, see Resolve Tanium Server synchronization errors on page 142.
Version incompatibility	If any installed solutions are incompatible with the current Tanium Console version, a warning banner lists those solutions. Clicking **Uninstall** in the banner uninstalls those solutions. For more information, see Uninstall solutions on page 138.
Installed Version Newer Than Manifest Version	If the **Solutions** page shows this warning in a module tile, you cannot import the solution version that the Tanium manifest on page 113 specifies because the currently installed version is later than the manifest version, and downgrading to an earlier version is not supported. This condition might occur if you installed the solution through the Import content files on page 134 option. Contact Tanium Support on page 724 for assistance with this issue.
Update errors	For more information about the status of a semiannual or maintenance release update, see Release status on page 116. If errors occur during the update, see Troubleshoot release update issues on page 131.
Workbench installation or uninstallation	If a solution workbench did not install or uninstall correctly, see: • Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform • Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform.
404 Not Found	If the browser that you use to access Console displays the **404 Not Found** error, solution files might be missing due to an incomplete installation. However, this error might also occur for other reasons, such as browser extension issues. Contact Tanium Support on page 724 for assistance with this issue.

© 2026 Tanium Inc. All Rights Reserved

Troubleshoot plugin issues

A *plugin* is an extension to a Tanium Core Platform component, module, or shared service. Tanium modules and shared services run scheduled plugins as background processes at intervals. Plugin operations are usually transparent to users. However, Tanium Support might instruct you to review plugin details when troubleshooting unexpected behavior.



Only users who are assigned the **Administrator** reserved role can access the **Configuration** pages for viewing plugin information.

To see details about installed plugins and scheduled plugins, from the Main menu go to **Administration > Configuration > Plugins**. The **Plugins** page displays separate grids for installed plugins and scheduled plugins.

Perform the following tasks to troubleshoot plugin errors:

1. Verify that passwords are up-to-date for the service accounts that Tanium solutions use to create plugins. Solutions might create new plugins during version upgrades or other events. For more information, see Manage service accounts for solutions on page 144.
2. Review the module plugin history logs:
    - Tanium Appliance User Guide: Module plugin history log
    - Tanium Core Platform User Guide for Windows Deployments: Module plugin history log
3. Contact Tanium Support on page 724

Troubleshoot solution-specific issues

To troubleshoot issues with a specific solution, see the associated user guide:

- Asset
- Automate
- Benchmark
- Certificate Manager
- Client Management
- Comply
- Connect
- Criticality
- Deploy
- Direct Connect
- Directory Query
- Discover

© 2026 Tanium Inc. All Rights Reserved

- Endpoint Configuration
- Endpoint Management for Operational Technology
- End-User Notifications
- Enforce
- Engage
- Gateway
- Guide
- Health Check
- Impact
- Integrations Gallery
- Integrity Monitor
- Investigate
- Jump Gate
- Patch
- Performance
- Provision
- Reporting
- Reputation
- Reveal
- Threat Response
- Trends
- Zero Trust

Troubleshoot Tanium Client issues

The following subsections describe diagnostic and remediation tasks for Tanium Client connectivity, registration, and licensing issues. For other Client troubleshooting tasks, see Tanium Client Management User Guide: Troubleshooting Tanium Clients and Client Management.

The **Client Status** page shows information about the state of Tanium Client registration and connectivity, and enables you to deploy actions to remediate issues.

© 2026 Tanium Inc. All Rights Reserved

NOTE

Client Status read permission is required to see the **Client Status** page. The **Administrator** reserved role has this permission.

The **Client Status** page shows information for all Clients that meet the specified filter criteria, regardless of whether those Clients are in computer groups that are assigned to your user account or persona. However, computer group assignments still determine to which Clients you can deploy actions.

The **Client Status** page does not show information for endpoints managed using entity providers. For more information, see Part 1: Tanium Console and Interact overview on page 42.

View the status of Tanium Client registration and communication

1. From the Main menu, go to **Administration > Configuration > Client Status**.
2. (Optional) Edit the default filter settings to view details only for specific Clients. You can also enter text in the **Filter items** field to filter the grid by host name, computer ID, network location, send/receive state, status, or version.
3. (Optional) Select **Hide Duplicate Host Names** (it is selected by default) to show only one row for each **Host Name**, containing only the information from the last time the Client registered. If you clear the checkbox, the grid shows a separate row for each registration in which the Tanium Server assigned a different Computer ID on page 719 to the host.

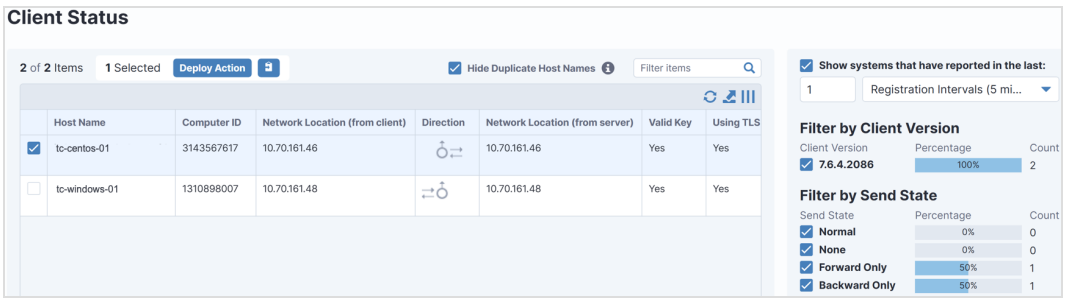
NOTE

In the **<#> of <#> Items** count, the first number shows the number of grid rows, which changes based on the filters that you specify. The second number shows the unfiltered number of registered Clients, which changes based on whether you select **Hide Duplicate Host Names**.

TIP

To check if the count of managed endpoints is within the limit of your Tanium license, select **Hide Duplicate Host Names** and set the filter **Show systems that have reported in the last** to `30 Days`. To see the most accurate count for purposes other than license usage, go to the Tanium **Home** page, **Environment Status** section, and check the **Total Endpoints**. For more information, see View environment status.

Client Status page in Tanium Console



© 2026 Tanium Inc. All Rights Reserved

The following table lists the information that the **Client Status** page displays for each Tanium Client.

Certain columns are hidden by default. To show or hide columns, click Customize Columns and select (show) or clear (hide) column names.

Client Status columns

Column	Description
Host Name	Endpoint host name.
Computer ID	The computer ID uniquely identifies each managed endpoint that connects to the Tanium Server at any given moment. The Server assigns the ID when the Tanium Client registers. The computer ID might change when a Client re-registers after certain events, such as: • The endpoint is re-imaged or cloned. • A new OS is installed on the endpoint. • The endpoint is a virtual machine (VM) that is reverted to a previous state. The Client records every computer ID that the Server has assigned over the history of registrations for that Client. NOTE: The **Computer ID** column shows the same value as the **Computer ID** sensor. If you issue a question with the sensor, the Client returns all the computer IDs that the Tanium Server has assigned to the host. For more information about how the Server assigns the ID, see Tanium Client Management User Guide: Information about registration and ComputerID.
Network Location (from Client)	Client IP address returned from a sensor on the Client.
Network Location (from Server)	Client IP address recorded on the Tanium Server or Zone Server during the last registration.
Direction	A circle represents the Client and arrows represent its connections. For a list of possible connection states, see the table Tanium Client peer connection states on page 721.
Valid Key	`No` indicates an issue with the public key that the Tanium Client uses to secure communication with other Tanium Core Platform components. Perform one of the following tasks to resolve the issue: • Reinstall the Tanium Client. For more information, see Tanium Client Management User Guide. • Redeploy the key. For more information, see Download infrastructure configuration files (keys).

© 2026 Tanium Inc. All Rights Reserved

Client Status columns (continued)

Column	Description
Using TLS	This column indicates whether Clients are (`Yes`) or are not (`No`) using Transport Layer Security (TLS) for communication with the Tanium Server or Zone Server.
Send State	• **Normal**: The Client is sending data to its backward and forward peers. • **None**: The Client is not sending data to its forward or backward peers. • **Forward Only**: The Client is sending data to its forward peer but not to its backward peer. • **Backward Only**: The Client is sending data to its backward peer but not to its forward peer.
Receive State	• **Normal**: The Client is receiving data from its backward and forward peers. • **None**: The Client is not receiving data from its forward or backward peers. • **Next Only**: The Client is receiving data from its forward peer but not from its backward peer. • **Previous Only**: The Client is receiving data from its backward peer but not from its forward peer.
Status	• **Normal**: The Client is communicating normally. • **Slow Link**: The Client has connections with abnormally slow throughput. • **Leader**: The Client is communicating with the Tanium Server or Zone Server because it is a backward leader, a forward leader, a neighborhood leader, or a Client with no peer connections (such as a Client in an isolated subnet). • **Blocked**: The Client is not communicating reliably.
Last Registration	Date and time when the Tanium Client last registered with the Tanium Server or Zone Server.
Protocol Version (hidden by default)	Tanium Protocol version. For more information about the protocol, see TLS communication.
Version	Tanium Client version.

The **Direction** column displays icons that use the following conventions to depict Tanium Client connection states:

- An up arrow indicates a connection with the Tanium Server or Zone Server.
- Side arrows pointing away from the Client indicate outbound connections to peers.
- Side arrows pointing at the Client indicate inbound connections from peers.
- Side arrows on the right side of Clients indicate the state of connections to forward peers.
- Side arrows on the left side of Clients indicate the state of connections to backward peers.
- Side arrows with dashed lines indicate slow connections.

You can use the **Direction** column to understand why a Tanium Client is a leader and to identify connection issues. The following table lists the possible connection states:

© 2026 Tanium Inc. All Rights Reserved

Tanium Client peer connection states

Attribute	Value	Description
Leader	Backward 	The Client is a backward leader that terminates one end of a linear chain. It typically has the lowest IP address in its linear chain.
	Forward 	The Client is a forward leader that terminates one end of a linear chain. It typically has the highest IP address in its linear chain.
	Neighborhood 	The Client is designated as a neighborhood leader because its linear chain has reached the maximum number of Clients.
	Isolated 	The Client is an isolated leader that connects only to the Tanium Server or Zone Server, and has no connections to other Clients. The Client might be isolated because its IP address falls within the range of an isolated subnet or because it has no peers in its local subnet with which to connect.
Neighbor	No side arrows 	This is the same as an isolated leader.
	Single side arrow 	The Client has a neighborhood list of peers but has not established a peer connection. This state generally results from a misconfiguration, such as when a host-based firewall on the endpoint does not allow inbound connections to the Client.
	Double side arrows 	The Client has a neighborhood list of peers and has connected with peers.
Client state	Normal 	A Client represented by an empty circle is communicating normally. Any of the above neighbor or leader arrows might apply.
	Blocked 	A Client represented by a circle with an X is not communicating reliably with connected peers (when the Client displays neighbor arrows) or with the Tanium Server or Zone Server (when the Client displays a leader arrow). Unreliable communication might result from a network issue or host resource issue, such as an anti-virus program that slows the Client.

Export Tanium Client status details

Export information in the **Client Status** page as a CSV file or, if you have the **Administrator** reserved role, as a JSON file.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Configuration > Client Status**.
2. Edit the default filter settings to show only the Clients for which you want to export information. You can also enter text in the **Filter items** field to filter the grid by host name, computer ID, network location, send/receive state, status, or version. Skip this step if you want to export information for all Clients.
3. Select rows in the grid to export information for specific Tanium Clients. Skip this step if you want to export information for all Clients.
4. Click Export.
5. (Optional) Edit the default export **File Name**.

   NOTE: The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.
6. Select an **Export Data** option:
   - **All**: Export information for all Clients that have registered, regardless of whether the grid is filtered to exclude them
   - **Selected**: Export information only for the Clients that you selected in the grid
   - **Filtered**: Export information only for the Clients that the grid filters include
7. Select the file **Format**:
   - **List of Clients**: Export the information as a CSV file.
   - **Client Definitions** (**Administrator** reserved role only): Export the information as a JSON file.
8. Click **Export**.
   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

Copy Tanium Client status details

Copy information from the **Client Status** page to your clipboard to paste the information into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string.

1. From the Main menu, go to **Administration > Configuration > Client Status**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy.
   - **Copy cell information**: Hover over the cell, click Options, and click Copy.

Deploy actions to remediate Client registration or connectivity issues

You can deploy actions to Tanium Clients to remediate issues that you observe in the **Client Status** page. For example, if you want certain Clients to register with a Tanium Zone Server instead of the Tanium Server, you can deploy the **Set Tanium Server Name List** package to change the **ServerNameList** setting on those Clients.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration > Configuration > Client Status**.
2. Select the Tanium Clients (up to 100) to which you want to deploy actions and click **Deploy Action**.
3. Deploy the action.
4. Review the **Client Status** grid to verify that the action produced the expected result.

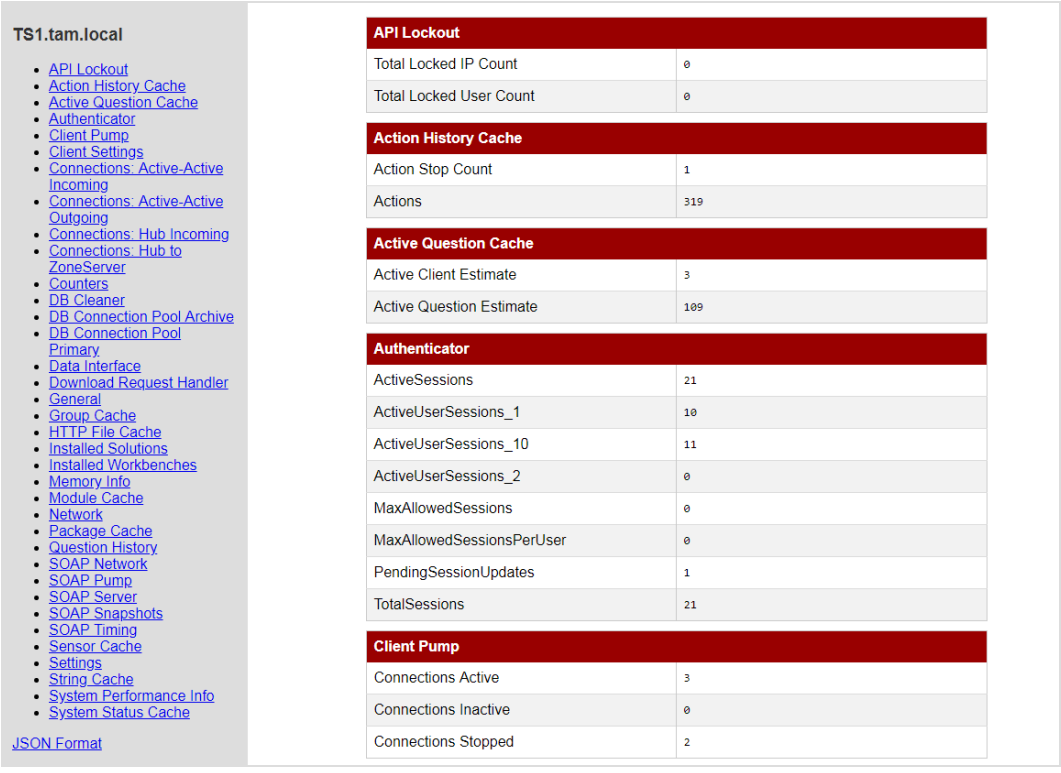
View the Tanium Server info page

If you consult Tanium Support for troubleshooting, Support might instruct you to review settings or counters on the info page.

> **NOTE** You require a role with **Server Status read** permission to view the info page.

1. Open a browser and go to `https://<Tanium Server>/info`, where `<Tanium Server>` is the FQDN or IP address of the Tanium Server.
2. Sign in as a user who is assigned the **Administrator** reserved role.

Tanium Server info page



© 2026 Tanium Inc. All Rights Reserved

Contact Tanium Support

Tanium Support is your first contact for assistance with preparing for and performing a solution installation or upgrade, as well as verifying and troubleshooting the initial deployment. If you require further assistance from Tanium Support, include version information for Tanium Core Platform components and specific details on dependencies, such as the host system hardware and OS details and database server version. You can also send Tanium Support a collection of logs and other information as a ZIP file. For more information, see Part 12: Troubleshooting Console and Interact on page 701.

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

For more information about how to submit a support case, see Case Submission Form.

© 2026 Tanium Inc. All Rights Reserved

Reference: Example questions in Console and Interact

Review the following examples to learn about the kinds of questions that Tanium Interact enables you to issue to endpoints.

Example questions

The following examples show common questions. You can add filters to the `from` clause of these questions in cases where not all endpoints return useful results and you want to see fewer rows in the **Question Results** grid to make it easier to scan. Common reasons for filtering include:

- **Endpoint-specific results**

  Targeting a specific endpoint is useful if the `get` clause of a question includes sensors that return many rows in the **Question Results** grid. For example, the question `Get IP Address and Logged In Users from all machines` produces as many rows as there are endpoints managed using Tanium Client in your network. To view results only from a specific endpoint, add a target filter that identifies the endpoint, such as `from all machines with Computer Name equals "<hostname>"`, where `<hostname>` is the computer name.

- **OS-specific results**

  If the sensors in a question are intended only for endpoints that run a specific operating system (OS), you can use the `Is <OS> equals true` filter to return results only from those endpoints. For example, the **Registry Value Data** sensor applies only to Windows endpoints, and non-Windows endpoints would return results that are not useful, such as `N/A on Linux`. In this case, you can specify `from all machines with Is Windows equals true` to return results only from Windows endpoints.

How can I get a list of running services on endpoints?

On the **Question Results** page, the following question returns one row for each unique service that is running on any Tanium Client managed endpoint in your environment. For each row, the **Running Service** column shows the service name and the **Count** column shows the number of endpoints where the service is running.

```
Get Running Service from all machines
```

The following question returns additional details about each service, such as its status and startup mode:

```
Get Service Details from all machines
```

How can I get a list of running processes on endpoints?

On the **Question Results** page, the following question returns one row for each unique process that is running on any endpoint managed using Tanium Client in your environment. For each row, the **Running Processes** column shows the process name and the **Count** column shows the number of endpoints where the process is running.

© 2026 Tanium Inc. All Rights Reserved

```
Get Running Processes from all machines
```

The following question returns additional details about each process, such as its path and ID. The `get` clause uses a parameterized sensor that requires you to enter two parameters: **Hashing Algorithm** and **Hostname or IP** address. In this example, the parameter values are `SHA256` and `192.168.0.1`.

```
Get Process Details[SHA256, 192.168.0.1] from all machines
```

How can I see Windows Registry keys and values?

The following questions use sensors that apply only to Windows endpoints.

To view registry values, issue a question with the parameterized sensor **Registry Value Data**, which requires the `<registry key path>` and `<value-name>` parameters in the following format:

```
Get Registry Value Data[<registry key path>, <value-name>] from all machines
```

The following example shows the question after you enter specific parameter values and add a targeting filter for Windows endpoints.

```
Get Registry Value Data[HKEY_LOCAL_
MACHINE\Software\Microsoft\Windows\CurrentVersion, CommonFilesDir] from all
machines with Is Windows equals true
```

You use similar question syntax to determine if a registry key value exists on endpoints:

```
Get Registry Key Exists[HKEY_LOCAL_
MACHINE\Software\Microsoft\Windows\CurrentVersion, CommonFilesDir] from all
machines with Is Windows equals true
```

How can I get a list of open ports?

The following question returns the open ports on each Tanium Client managed endpoint:

```
Get Computer Name and Open Port from all machines
```

How can I get user authentication information?

The following question returns users who are signed in to Tanium Client managed endpoints and who have the string `Administrator` in their user name:

```
Get Logged In Users contains Administrator from all machines
```

© 2026 Tanium Inc. All Rights Reserved

The following question identifies each endpoint and the user who is signed in to the Tanium Client managed endpoint:

```
Get Computer Name and Logged In Users from all machines
```

The following question returns users who are signed in to Windows endpoints and the dates when they signed in. For endpoints where no user is signed in, the **Local User Login Dates** sensor returns the last user who signed in.

```
Get Local User Login Dates from all machines with Is Windows equals true
```

The following question returns users who are signed in to Tanium Client managed endpoints that run any OS and returns the current date on the endpoints:

```
Get Logged In Users and Client Date from all machines
```

The following question returns the same information as the preceding question except that, for Tanium Client managed endpoints where no user is signed in, the **Last Logged In User** sensor returns the last user who signed in.

```
Get Last Logged In User and Client Date from all machines
```

The following question returns users who are signed in to Tanium Client managed endpoints and returns other session information, such as session states. The **User Sessions** sensor applies only to Windows and macOS endpoints.

```
Get User Sessions from all machines
```

The following question returns users and groups who are considered administrators on non-Windows endpoints that have Tanium Client installed:

```
Get Local Administrators from all machines
```

The following question returns users and groups that are members of the local Administrators group on Windows endpoints.



The **AD Query - Local Administrators** sensor is part of the Core AD Query Content solution and returns results only from endpoints where you deployed an action with the **Collect Active Directory Info** package.

```
Get AD Query - Local Administrators from all machines with Is Windows equals true
```

How can I get sign-in information for service accounts?

The following question returns the names of accounts under which services are configured to run, but excludes the default accounts, including LocalSystem, LocalService, and NetworkService.

© 2026 Tanium Inc. All Rights Reserved

```
Get Service Login Names from all machines
```

How can I get certificate information?

The following questions use the sensor **Certificate Details**, which is supplied by Tanium Certificate Manager. The sensor returns information about all scanned certificates, including the source, location, subject, issuer, validity dates, expiration status, key and signature algorithms, and thumbprints. The **Not Before** and **Not After** values are in UTC.

The following question returns information about all scanned certificates on all endpoints:

```
Get Certificate Details from all machines
```

The following question returns information about certificates on Windows endpoints:

```
Get Certificate Details from all machines with Is Windows equals true
```

The following question returns information about certificates on Linux endpoints:

```
Get Certificate Details from all machines with Is Linux equals true
```

The following question returns information about certificates on Tanium-managed endpoints:

```
Get Certificate Details from all machines with Is Managed equals true
```

The following question returns the certification records for certificates that have expired:

```
Get Certificate Details having Certificate Details:Expiration Status equals
Expired from all machines
```

The following question uses the **Computer Name** and **Certificate Expiry** sensors to return only the computer name, source, location, and status about certificates that have expired:

```
Get Computer Name and Certificate Expiry having Certificate Expiry:Expiration
Status equals Expired from all machines
```

How can I detect all running Oracle instances within a Linux environment?

The following question includes `Running Processes contains ora_pmon` in the `from` clause to ensure that you see results only from endpoints that are running Oracle instances. Without that filter, the **Question Results** page would return results for every endpoint because the question includes the **Computer Name** sensor.

© 2026 Tanium Inc. All Rights Reserved

```
Get Computer Name and Running Processes contains ora_pmon from all machines with
Running Processes contains ora_pmon
```

How can I get asset information?

The following question returns identification and architecture details for Tanium Client managed endpoints.

```
Get Computer Name and "Computer Serial Number" and IP Address and MAC Address and
BIOS Name and CPU Details and Chassis Type from all machines
```

Example dashboard questions

Reviewing the list of predefined saved questions in categories and dashboards is a good way to learn how to use questions and get meaningful results. The following examples show a few predefined questions that are organized by ***<category> > <dashboard>***.

Security > Data Leakage

The questions in the **Data Leakage** dashboard return information about established connections that a prohibited process opened or that connect to a prohibited destination:

```
Get Computer Name and Non-Approved Established Connections from all machines with
Non-Approved Established Connections matches ".*:.*"
```

```
Get Non-Approved Established Connections from all machines with Non-Approved
Established Connections matches ".*:.*"
```

Security > Proactive Network Security

The questions in the **Proactive Network Security** dashboard return information that you can use to assess the security of your network:

```
Get Computer Name and IP Address and MAC Address from all machines with "DHCP
Enabled?" contains True
```

```
Get Firewall Status contains disabled from all machines with Firewall Status
contains disabled
```

```
Get DNS Server from all machines
```

© 2026 Tanium Inc. All Rights Reserved

```
Get Computer Name and Open Share Details from all machines with all Open Share Details not contains No shares
```

Security > Wireless Network Security

The questions in the **Wireless Network Security** dashboard return information that you can use to assess the security of wireless networks in your environment:

```
Get Computer Name and Username and Wireless Network Connected SSID from all machines with all Wireless Network Connected SSID not matches ".*:No Connection:.*"
```

```
Get Wireless Networks Visible from all machines
```

```
Get Wireless Network Details from all machines
```

```
Get Hosted Wireless Ad-Hoc Networks from all machines with Hosted Wireless Ad-Hoc Networks contains started
```

```
Get Wireless Networks Using WEP from all machines with Wireless Networks Using WEP contains wep
```

```
Get Unencrypted Wireless Networks from all machines with Unencrypted Wireless Networks contains open
```

Security > Workstation USB Write Protection

The questions in the **Workstation USB Write Protection** dashboard return information about which workstations have USB storage devices that are in write-protected mode. That mode prevents users from copying data from the workstation to a USB device.

```
Get Computer Name and Username from all machines with ( Operating System not containing "server" and USB Write Protected containing "False" )
```

```
Get Computer Name and Username from all machines with ( Operating System not containing "server" and USB Write Protected containing "True" )
```

© 2026 Tanium Inc. All Rights Reserved

Reference: Advanced question syntax in Console and Interact

You can issue complex questions in natural language without understanding the precise associated syntax. When you start typing a free-form question in one of the Tanium Console or Interact question fields, the Tanium natural language parser evaluates your entry and proposes a question in valid syntax, as described in Issue a free-form question on page 241. However, understanding the syntax is useful if you want to edit the proposed question, add filters or options, reuse the question in other contexts, or learn more about the question results. For example, you can issue a question with the **Computer Name** sensor filtered to return results only from endpoints that match a case-sensitive character string.

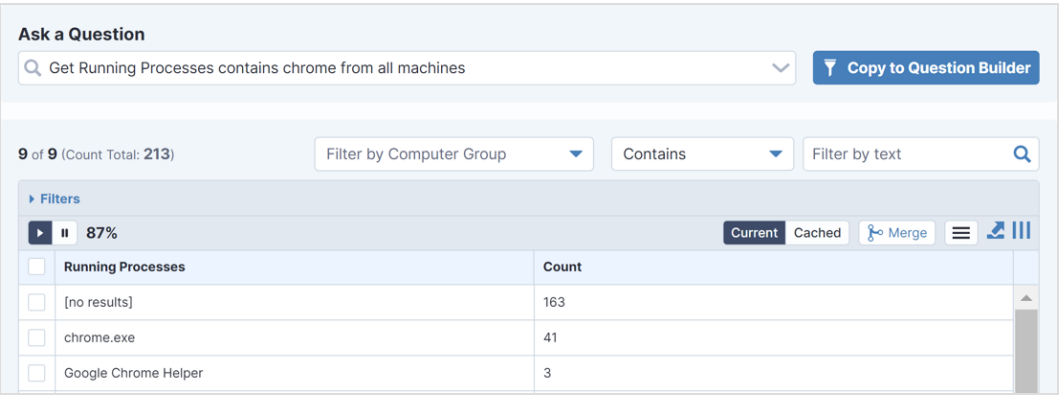
Use question filters

Each Tanium question has a `get` clause that specifies the information to retrieve and a `from` clause that specifies the target endpoints. You can add filters to both clauses when you issue a question.

Filters in get clause

In a Tanium question, the `get` clause specifies the sensors that Tanium Clients run to answer the question. Clients apply any filters to the sensor results and return the filtered results to the Tanium Server. Interact then shows the filtered results in the **Question Results** page. For example, if the `get` clause specifies `Get Running Processes contains chrome`, Clients filter the **Running Processes** sensor to show processes with names that contain the string `chrome`. Clients return the answer `[no results]` if no results match the filter. In this example, Clients return `[no results]` if they have no running processes that contain `chrome`.

Filter in Get clause of question



Filters in from clause

In a Tanium question, the `from` clause specifies whether the question targets all Tanium Client (`from all machines`) or only Tanium Clients that evaluate the filtering sensor to a Boolean true. For example, the question `Get Running Processes from all machines with CPU Consumption > 80%` returns the names of all running processes on endpoints managed using Tanium Client where CPU consumption exceeds 80%.

© 2026 Tanium Inc. All Rights Reserved

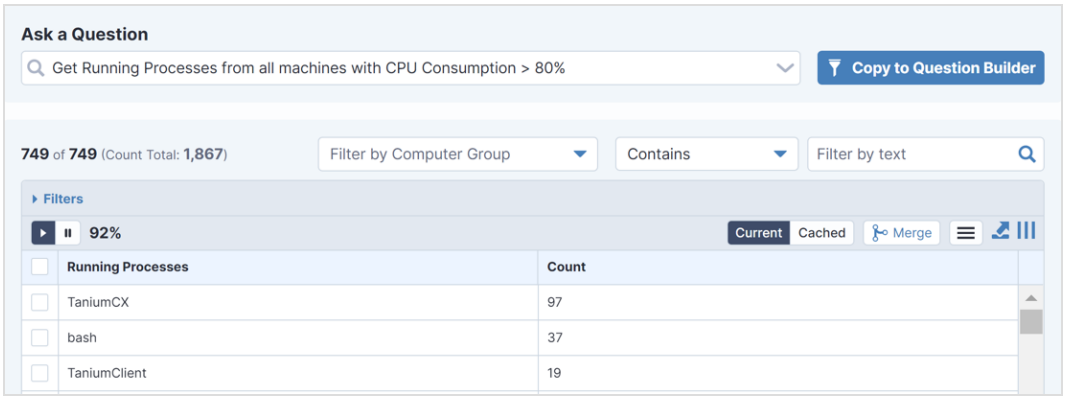
NOTE

Regardless of targeting filters, you can see question results only from endpoints that are in computer management groups that are assigned to the user account or alternative persona that you use for the current Console session. For more information, see Computer groups in questions on page 612.

You also use filters to define the dynamic membership of computer management groups and filter groups. For more information, see Computer group membership on page 614.

For more information about `from` clause filters, see Questions with target filters on page 240.

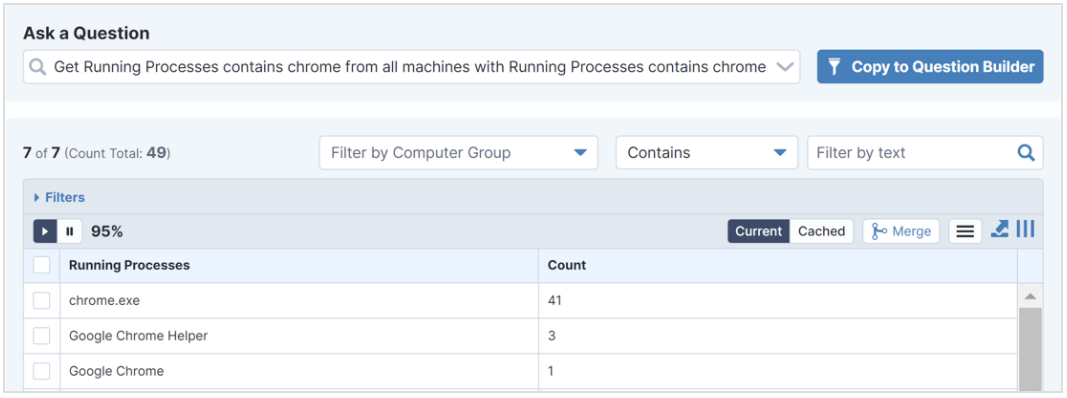
Filter in From clause of question



Exclude [no results]

Use a combination of `get` and `from` filters in a question if you want the **Question Results** page to exclude Clients that return `[no results]`. For example, the following question shows processes with names that contain the string `chrome` but only on Clients that have at least one process name with that string.

Filter to exclude [no results]



© 2026 Tanium Inc. All Rights Reserved

Filter operators

Filter expressions in questions can match strings or regular expressions. The following table describes the supported filter operators as they appear when you use the Interact **Question Builder**. The table also describes how some operators are normalized after you enter the expressions in the **Ask a Question** field or issue a question from the **Question Builder**.

NOTE

If you use operators that evaluate integer results from sensors and a Tanium Client returns a string result instead (such as `true`, `false`, or an error), Interact interprets the error string as the value 0. For example, if a Client returns `TSE-Error` for a question with the filter `installed application version[chrome] <= 12`, the filter evaluates to true for that Client because Interact interprets `TSE-Error` as a 0 value. Adding the filter `and <sensor> not equals 0` causes Interact to evaluate strings to false in such cases, but also evaluates non-string 0 values to false.

If you use operator words as string literals instead of as filters in question text, you must enclose the words in quotation marks. For more information, see Use reserved words or characters on page 735.

Filter operators

Filter operator	Usage
contains	The sensor value contains the specified string. Example: `running processes contains "chrome"`
does not contain	The sensor value does not contain the specified string.
starts with	The sensor value starts with the specified string. Example: `starts with "chrome"` When you issue the question, the expression is translated to a regular expression using the `matches` operator.
does not start with	The sensor value does not start with the specified string.
ends with	The sensor value ends with the specified string. Example: `ends with "chrome.exe"` When you issue the question, the expression is translated to a regular expression using the `matches` operator.
does not end with	The sensor value does not end with the specified string.

© 2026 Tanium Inc. All Rights Reserved

Filter operators (continued)

Filter operator	Usage
matches	The sensor value matches the specified regular expression. For more information, see Use regular expression filters on page 739. For sensors in the `get` clause of a question, use the `matches` operator to match any value in a list. In the **Ask a Question** field, enclose the values in quotation marks and parentheses `"( )"`, and use the pipe character `|` as a separator. In the **Question Builder**, you can skip the quotation marks; Interact adds them automatically when you issue the question. For example, the following question matches the user names `root` or `reboot`: `Get Last Logged In User matches "(root|reboot)" from all machines` In the `from` clause of a question, you can also use the `in` operator to match values in a list.
does not match	The sensor value does not match the specified regular expression. When you issue the question, the expression shown in the question field uses `not matches` in place of `does not match`.
in (`from` clause only)	The sensor value is equal to one of the specified strings. Enclose the values in parentheses and use commas as separators. When you issue the question, the question field shows the expression with `equals` in place of `in` and with `or` in place of commas. Example: the filter `with Chassis Type in (Virtual,Physical)` in the **Ask a Question** field becomes `with (Chassis Type equals Virtual or Chassis Type equals Physical)` when you issue the question. For more information, see Use the "in" operator for filtering on page 743. NOTE In the `get` clause of a question, the `in` operator is not available but you can use the `matches` operator instead.
is equal to	The sensor value is equal to the specified value or string. When you issue the question, the expression shown in the question field uses `equals` in place of `is equal to`.
is not equal to	The sensor value is not equal to the specified value or string. When you issue the question, the expression shown in the question field uses `not equals` in place of `is not equal to`.
is less than	The sensor value is less than the specified value. When you issue the question, the expression shown in the question field uses a symbol (`<`) in place of the operator words. Example: `installed application version[chrome] < 12`

© 2026 Tanium Inc. All Rights Reserved

Filter operators (continued)

Filter operator	Usage
is less than or equal to	The sensor value is less than or equal to the specified string. When you issue the question, the expression shown in the question field uses symbols (`<=`) in place of the operator words. Example: `installed application version[chrome] <= 12`
is greater than	The sensor value is greater than the specified value. When you issue the question, the expression shown in the question field uses a symbol (`>`) in place of the operator words. Example: `installed application version[chrome] > 12`
is greater than or equal to	The sensor value is greater than or equal to the specified string. When you issue the question, the expression shown in the question field uses symbols (`>=`) in place of the operator words. Example: `installed application version[chrome] >= 12`

Use reserved words or characters

Reserved words or characters in question text

The Tanium™ parser uses certain words and characters to interpret the question text that you enter as valid query syntax. For example, the parser uses the bracket characters `[` and `]` to enclose the values of parameterized sensors and uses variations of the word `match` to support regular expressions. You must enclose these reserved words and characters in quotation marks when you use them as string literals in questions. For example, to see all endpoints that have computer names containing the letter combination `in`, issue the question `Get Computer Name from all machines with Computer Name contains "in"`.

- "
  Use double quotation marks as an escape-character sequence for each instance of quotation marks in a text string. For example, to see which endpoints have a computer name that contains the string `"test"`, issue the question:
  `Get Computer Name from all machines with Computer Name contains """test"""`
- .
- ,
- :
- ?
- $

© 2026 Tanium Inc. All Rights Reserved

- White spaces

  For example, to see which endpoints have a computer name that has a blank space before and after the string `DBserver`, issue the question:

  ```
  Get Computer Name from all machines with Computer Name contains " DBserver "
  ```

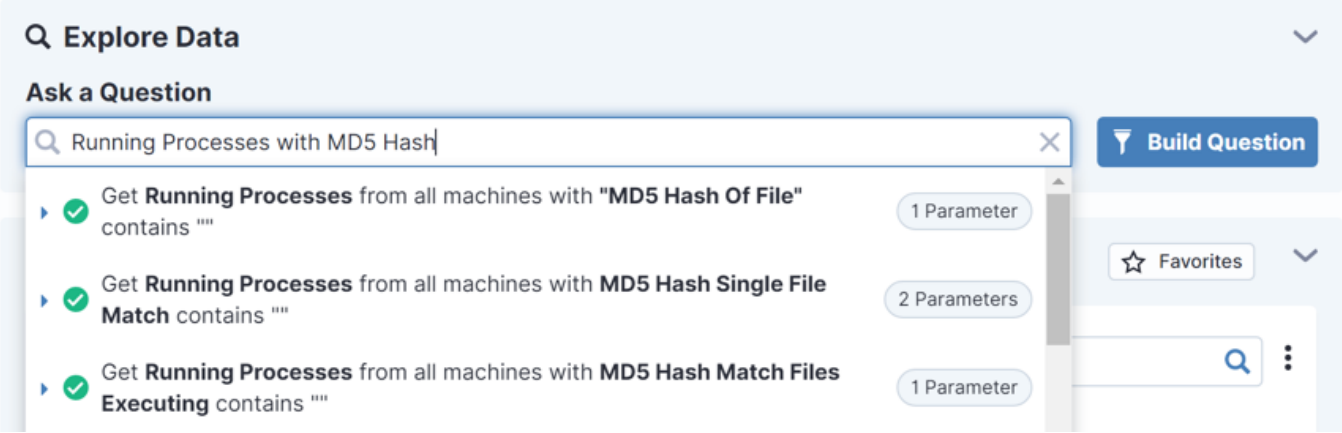
- all
- and
- any
- contain
- containing
- contains
- does match
- does not match
- ending
- ends
- equals
- get
- having
- in
- matches
- matching
- not
- or
- with
- starting
- starts

Reserved words in sensor names

Sensors with names that use reserved words require quotation marks when you use them as string literals in the Interact **Ask a Question** field. Otherwise, the dropdown list that displays suggested questions cannot accurately match your entry. For example, if you enter the **Running Processes with MD5 Hash** sensor without quotation marks, the dropdown list displays suggestions that confuse your entry with other sensors that contain the words `MD5 Hash`:

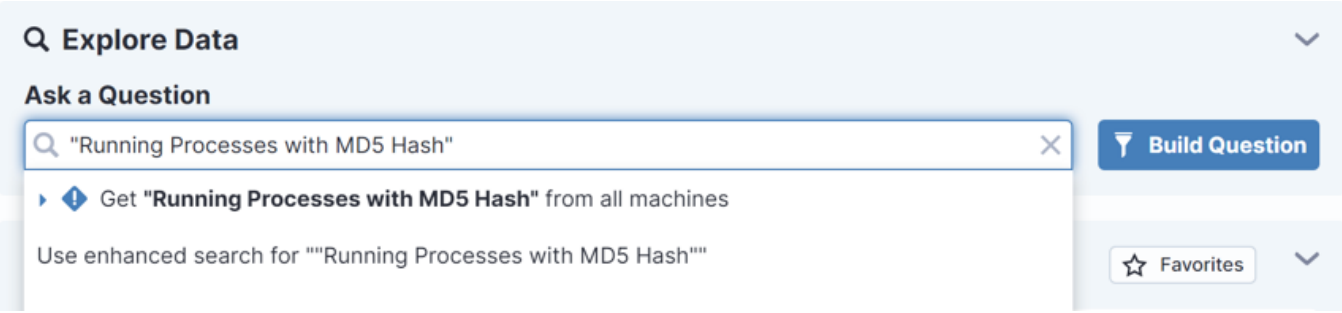
© 2026 Tanium Inc. All Rights Reserved

Sensor name without quotations



If you use quotation marks around the sensor name, the dropdown list displays the correct question:

Sensor name with quotations



- $serverNames
- $serverIDs
- $substring
- $unescape
- all
- All
- ALL
- and
- any
- computers
- Computers
- COMPUTERS
- contains

© 2026 Tanium Inc. All Rights Reserved

- containing
- equals
- from
- From
- FROM
- get
- Get
- GET
- having
- Having
- HAVING
- in
- machines
- Machines
- MACHINES
- matches
- matching
- not
- number
- Number
- NUMBER
- of
- Of
- OF
- or
- where
- Where
- WHERE
- with
- With

© 2026 Tanium Inc. All Rights Reserved

- WITH

Use regular expression filters

Tanium questions support regular expression (regex) matching in both the `get` statement and `from` clause. Regex filters provide great flexibility for specifying the exact information to retrieve and the specific endpoints to query.

> NOTE
>
> You can also use regular expressions to define the membership of computer groups. For more information, see Computer group membership on page 614.

Processing limits for regular expressions

The Tanium Core Platform stops processing regular expressions that run for an excessive amount of time to protect against the misuse of platform resources. For example, if complex regular expressions in a question cause it to exceed the limit for processing resources, the Tanium Client stops processing that question and returns `[no results]` for it.

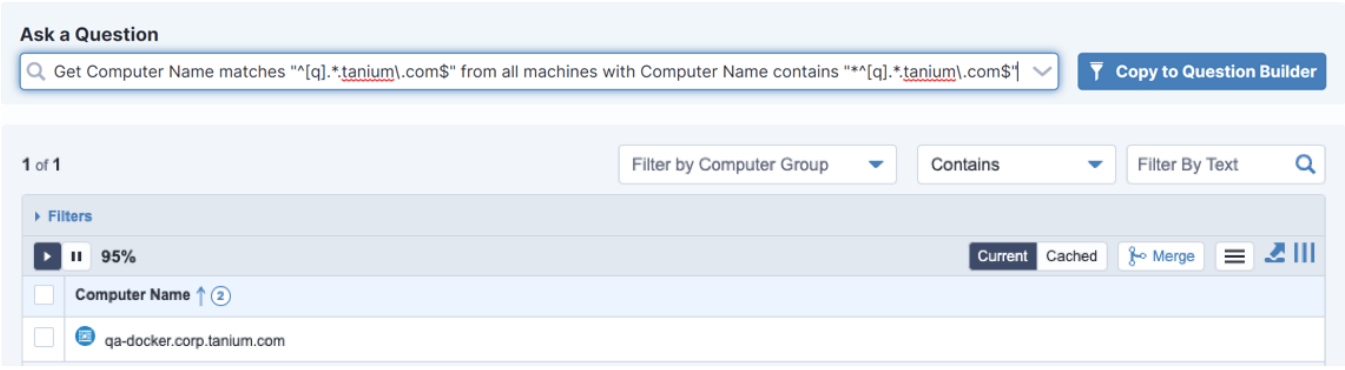
The following types of regular expressions might exceed the resource limit:

- Negative lookaheads (`?!` syntax), such as `(?!tool)ai.*`
- Positive lookaheads (`?=` syntax), such as `(?=tool)ai.*`
- Named capture groups (`?<group-name>` syntax), such as `?<year>` in the expression `/(?<year>\d{4})-\d{2}|\d{2}-(?<year>\d{4})/`

Example: Match a starting character

The following regular expression matches computer names that start with the letter `q` in the domain `tanium.com`.

Regular expression to match initial character

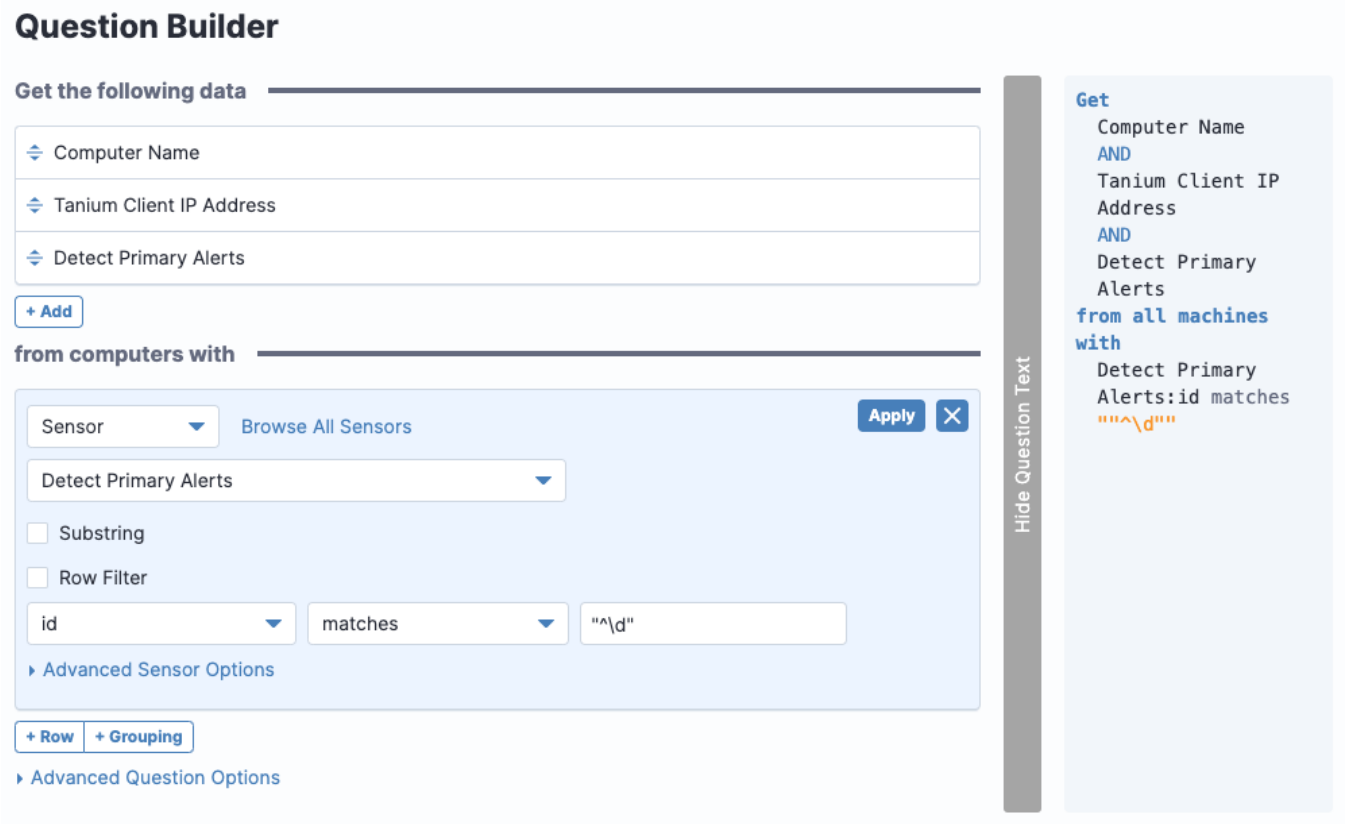


Example: Match any digit

The **Detect Primary Alerts** sensor uses a regular expression to collect results that match any digit in the range 0 to 9. Because alerts have numeric IDs, this expression excludes empty results.

© 2026 Tanium Inc. All Rights Reserved

Regular expression to match any digit

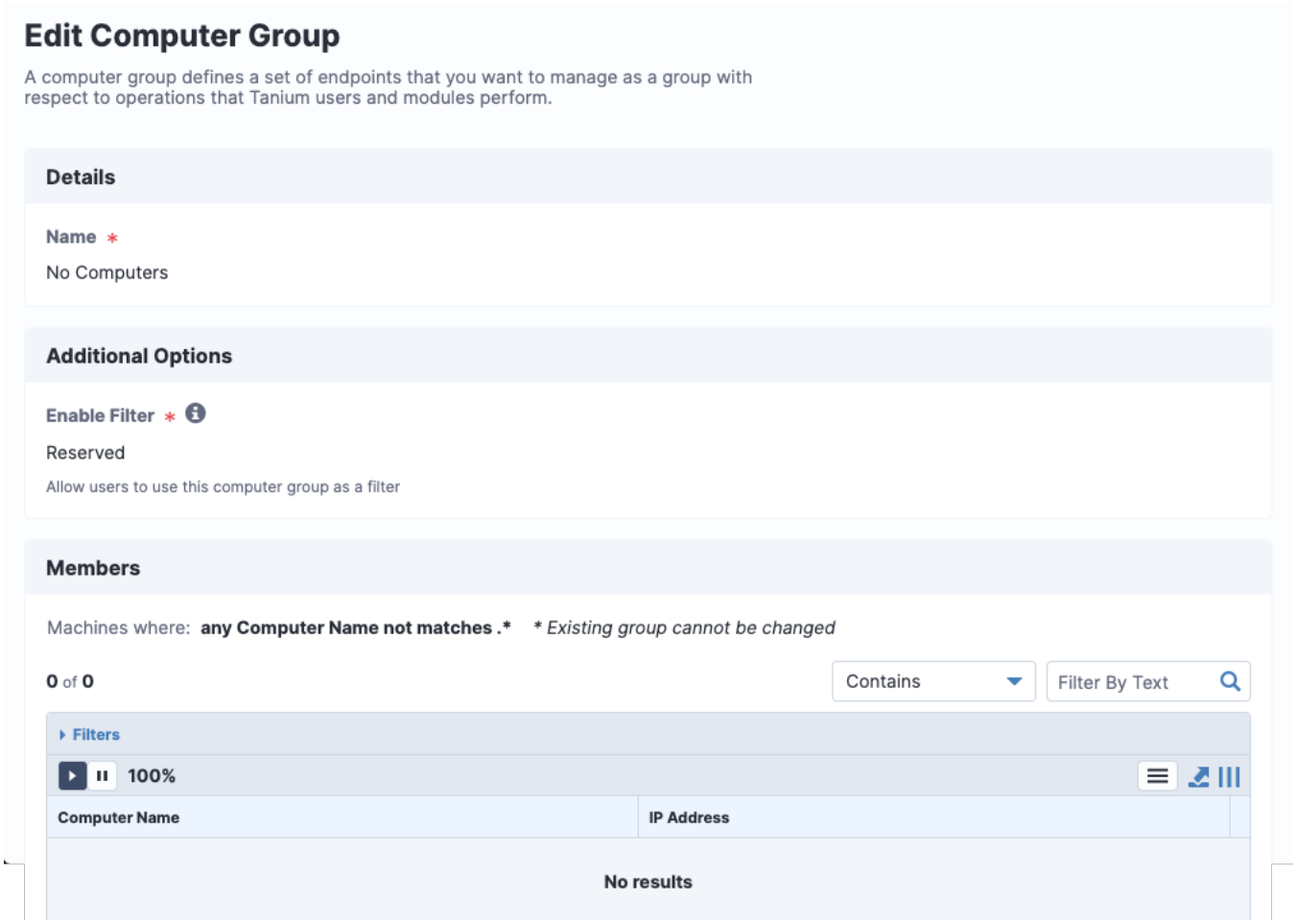


Example: Negation

You can also use a combination of negation and regular expressions to build filter expressions. For example, the predefined computer group **No Computers** has a membership definition that uses a question with the `not matches` expression and a regular expression (`.*`) to match empty results. Because the **Computer Name** sensor always returns a string, this combination provides a way to prevent action deployment. To stop the Tanium Server from deploying certain actions to any endpoints, configure those actions to target the **Default** action group, which includes only the **No Computers** computer group.

© 2026 Tanium Inc. All Rights Reserved

Regular expression with negation



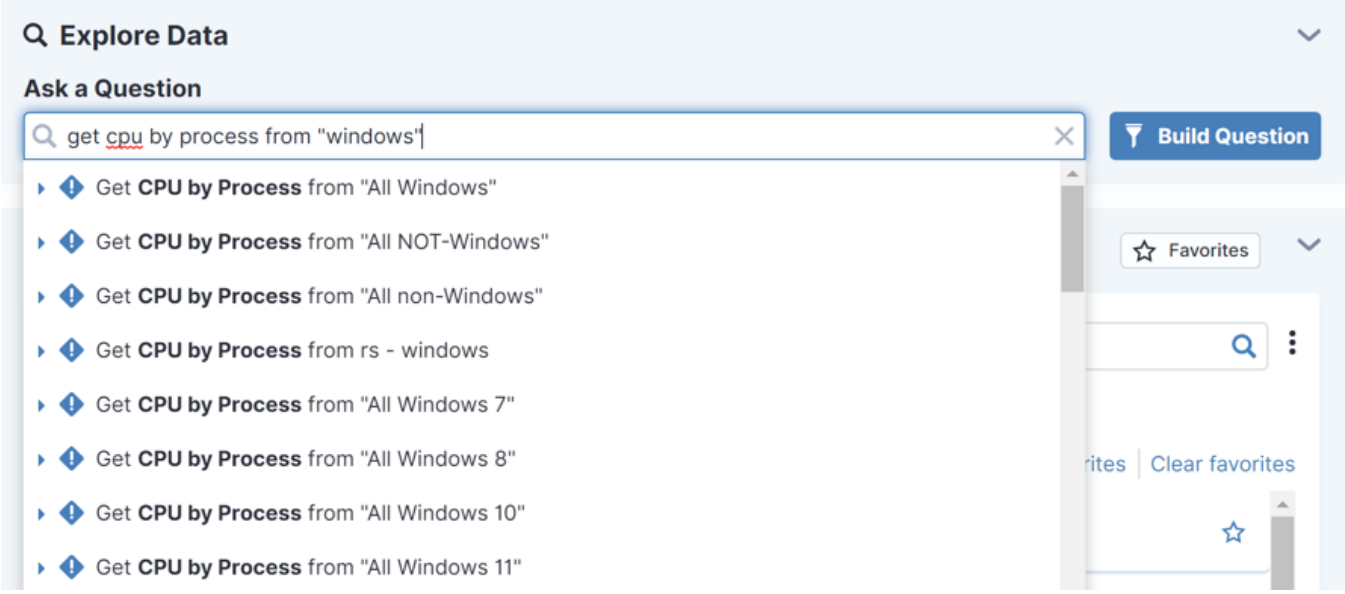
Use computer group filters

You can issue questions with a computer group filter in the `from` clause to ensure that only endpoints in the group respond. The computer group can be a management group or filter group. For more information about these types, see Controlling endpoint management rights through computer groups on page 610.

Use quotation marks around the computer group name when you enter it in the `from` clause. For groups with dynamic (filter-defined) membership, the question parser converts the specified group name into a question that determines membership. For more information, see Computer group membership on page 614.

© 2026 Tanium Inc. All Rights Reserved

Question with computer group in From clause



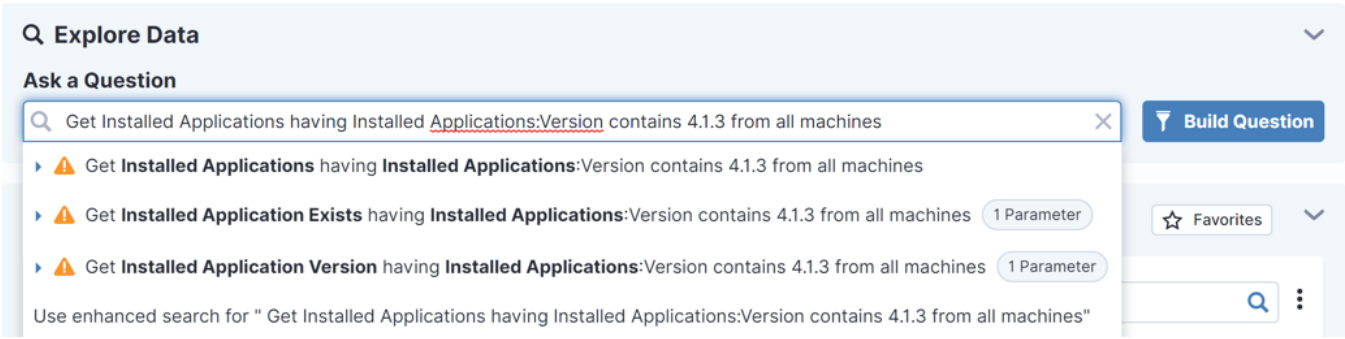
Use sensor column filters

Multi-column sensors are designed to collect multiple pieces of related information in a single answer. For example, the **Installed Applications** sensor returns four columns of information, as shown in the figure Sensor column filter in the Get and From clauses of a question on page 743. Using the regular expression `starts with`, `ends with`, or `contains` in a question to filter results for a multi-column sensor can be tricky because the sensor result string is actually a single string with column delimiters. If you enter the filter incorrectly, you might match a string in an unexpected column or unknowingly match a string in a hidden column. To avoid unintended results, you can specify a particular column for results matching. The syntax is `get <sensor> having <sensor>:<column> contains <value>`. The column name is case sensitive.

Single-column filtering works only if the sensor configuration specifies column delimiters with a single character (such as `|`), not multiple characters (such as `|:`). For more information, see Split into multiple columns on page 428. To match results from all the columns, the syntax is `get <sensor> contains <value>`.

The following example shows a sensor column filter in the `get` clause of a question.

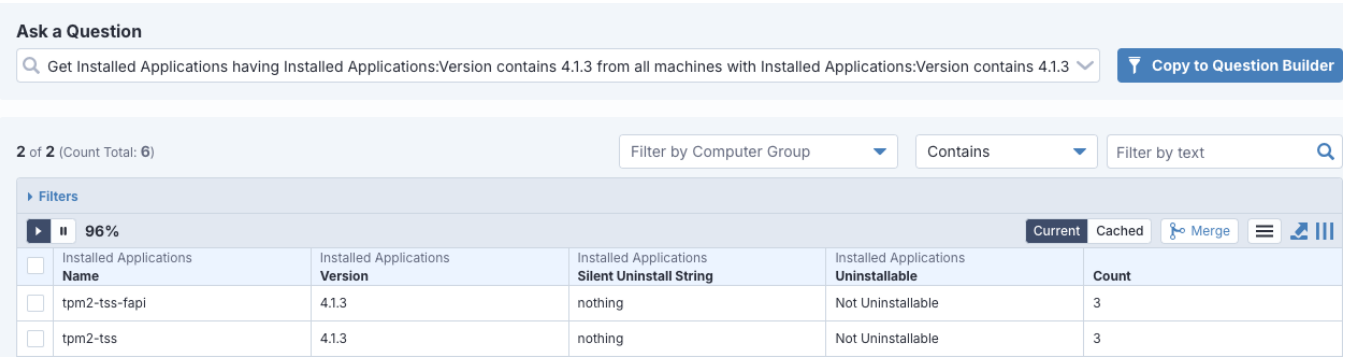
Sensor column filter in the Get clause of a question



The following example shows a sensor column filter in both the `get` clause and the `from` clause of a question and shows the results.

© 2026 Tanium Inc. All Rights Reserved

Sensor column filter in the Get and From clauses of a question

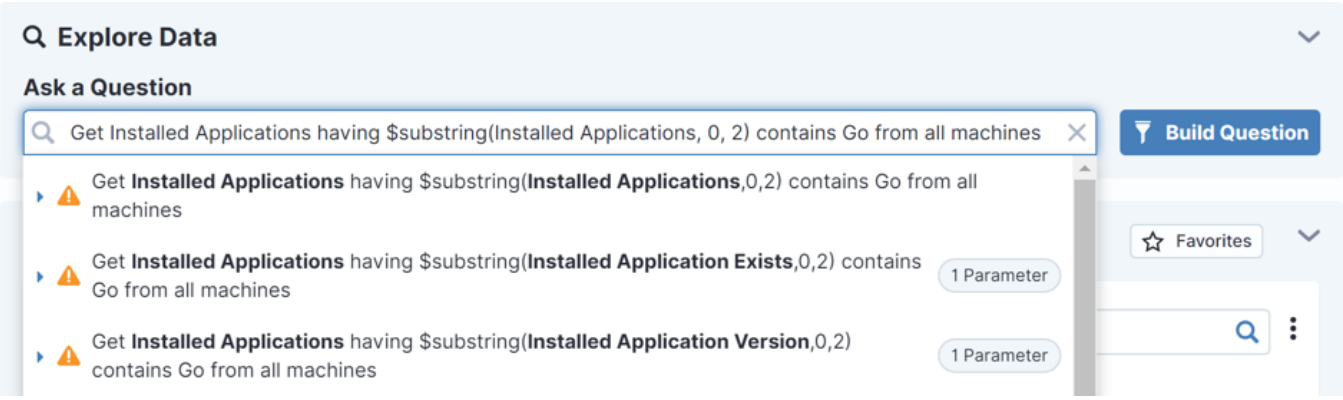


Use $substring() filters

You can use `$substring()` filters in questions to match result string patterns. The `$substring()` function takes the following arguments: sensor name, starting position (where 0 is the first position), number of characters.

The following example matches results from the **Installed Applications** sensor where the first two characters match the string `Go`.

$substring() filter in a question



NOTE

In a multi-column sensor, the `$substring()` filter applies across all the columns. You cannot apply the `$substring()` filter to a specific column.

Use the "in" operator for filtering

In the `from` clause of a question, use the `in` operator to specify a collection of matching sensor results. The `in` operator applies the is equal to on page 734 operator to any value in a comma-separated list that you enclose in parentheses. After you issue the question, the question field shows the expression with `equals` in place of `in` and with a Boolean `or` in place of commas.

© 2026 Tanium Inc. All Rights Reserved

NOTE

In the `get` clause of a question, the `in` operator is not available but you can use the matches on page 734 operator instead.

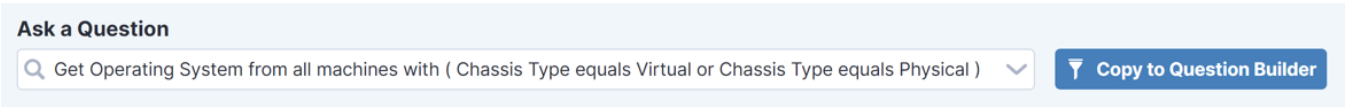
The following example shows the `in` operator applied to results containing `Virtual` or `Physical`.

Question with "in" operator



The following example shows the question syntax after you issue the question.

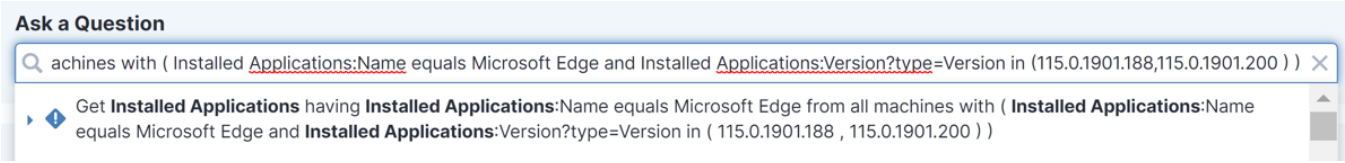
Issued question with "in" operator



The following question applies the `in` operator to values (`115.0.1901.188` or `115.0.1901.200`) in a specific column (`Version`) of the multi-column sensor (`Installed Applications`):

```
Get Installed Applications having Installed Applications:Name equals Microsoft Edge from all machines with ( Installed Applications:Name equals Microsoft Edge and Installed Applications:Version?type=Version in (115.0.1901.188,115.0.1901.200 ) )
```

Question with "in" operator applied to a sensor column filter



After you issue the question, its syntax changes to:

```
Get Installed Applications having Installed Applications:Name equals Microsoft Edge from all machines with ( Installed Applications:Name equals Microsoft Edge and ( Installed Applications:Version?type=Version equals 115.0.1901.188 or Installed Applications:Version?type=Version equals 115.0.1901.200 ) )
```

Use nested filters

In the `from` clause of a question, you can configure multiple filters, including nested filters.

The following example shows nested filters in the **Question Builder**. The example combines one matching expression with either one of the nested expressions.

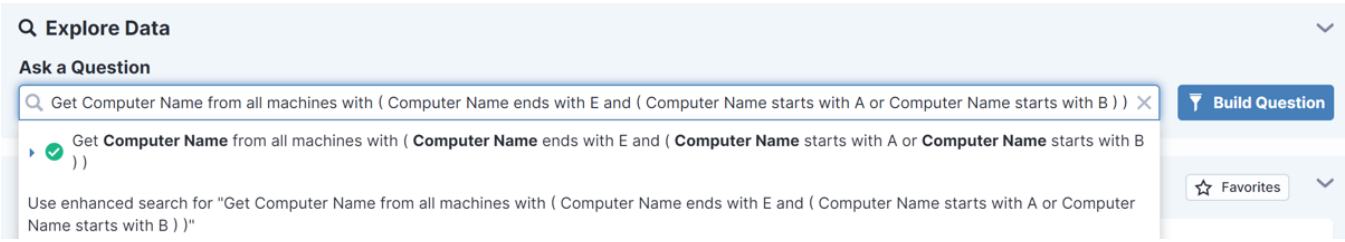
© 2026 Tanium Inc. All Rights Reserved

Nested filters in the Question Builder



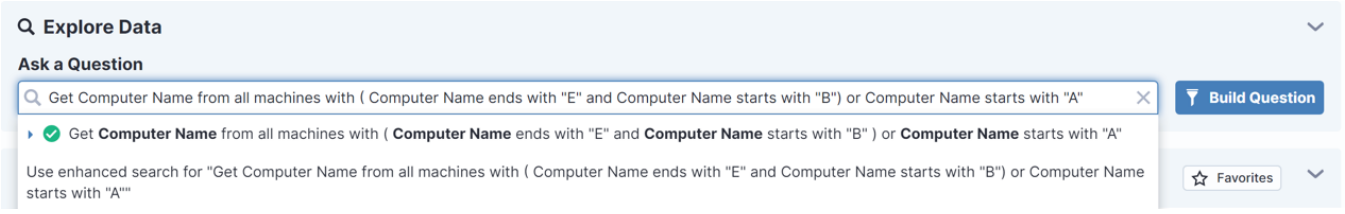
You can also specify nested filters in the **Ask a Question** field.

Nested filters in the Ask a Question field to match either of two results



The following example shows different Boolean logic: match both of these or this one.

Nested filters in the Ask a Question field to match both results or one result



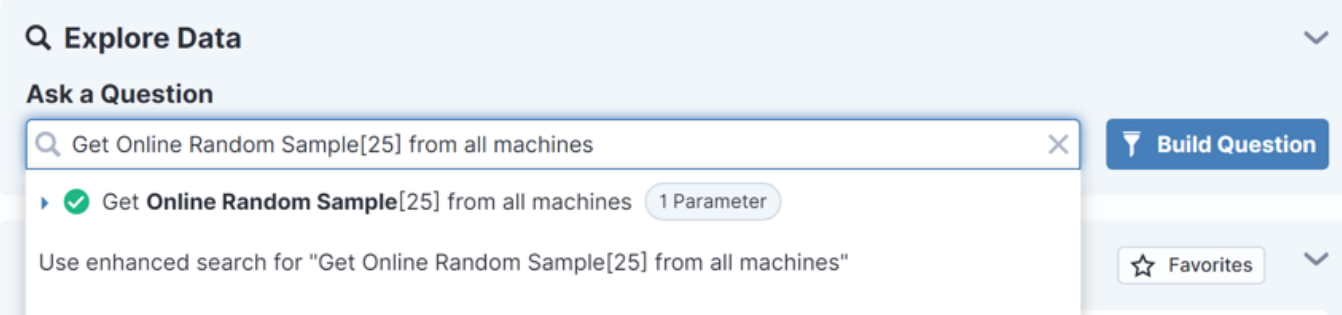
Target random endpoints

Use the **Online Random Sample** sensor to identify a random subset of online endpoints managed using Tanium Client from all targeted endpoints. You might want to target random endpoints when you test a new package or configuration on a random subset of endpoints, or to check a random set of endpoints to ensure they have proper configurations prior to an audit. The **Online Random Sample** sensor is included in the content-only solution Default Content.

© 2026 Tanium Inc. All Rights Reserved

The **Online Random Sample** sensor retrieves `True` and `False` results from all targeted endpoints. The sensor accepts a **Sample %** parameter from 0-100 to determine the rough percentage of endpoints that answer with True. For example, if you pass 25 as a parameter and target `from all machines`, approximately 25% of endpoints in the environment will return a True response. Because each endpoint evaluates the sensor and generates a random True or False answer according to the percentage that you specify, the number of endpoints that return True can vary. The default value for **Sample %** is 5.

Online Random Sample sensor

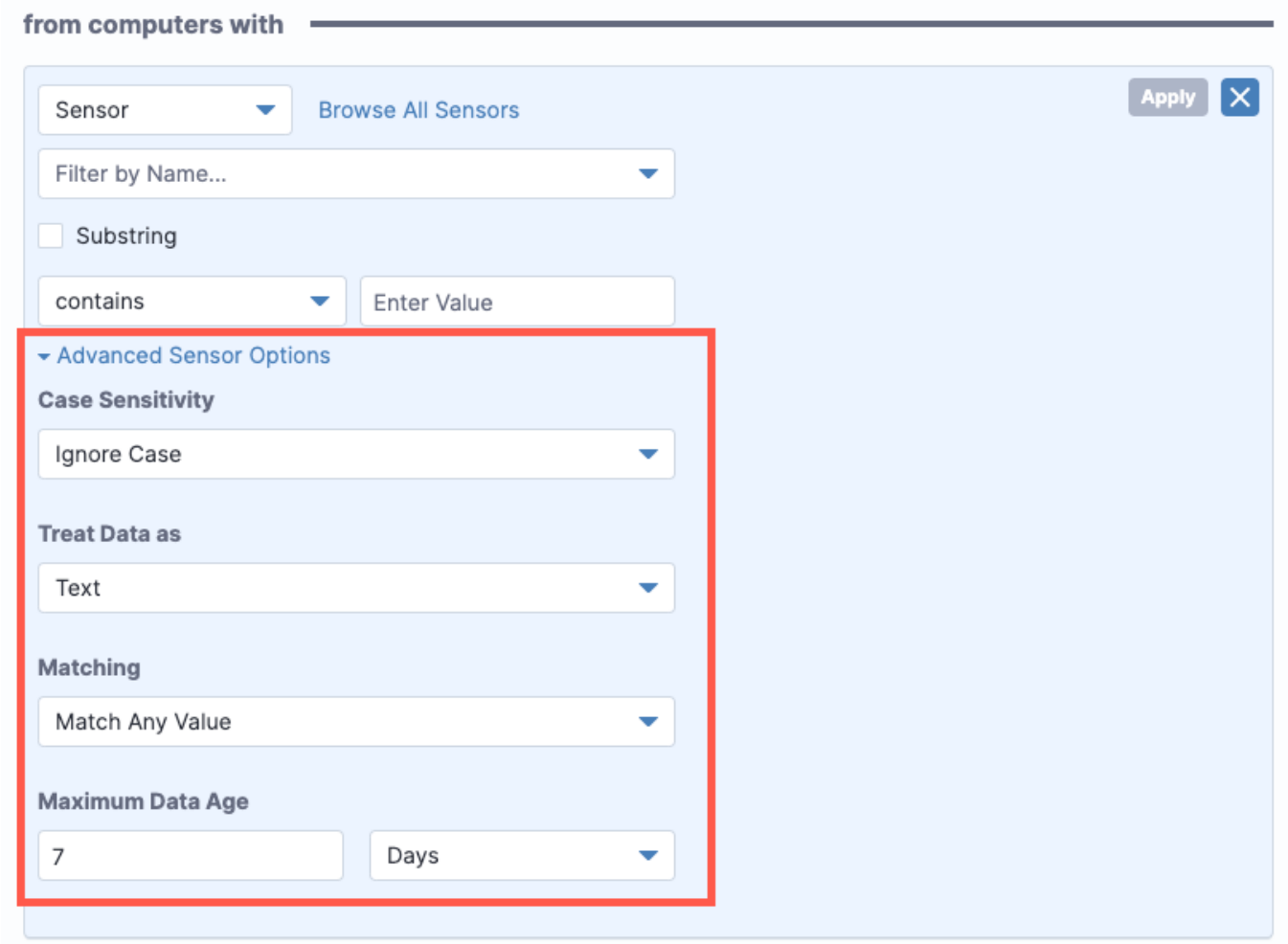


Use advanced sensor options

Question results from Tanium Clients must conform with any advanced options that you specify for sensors in the question. You can configure advanced sensor options in the **Question Builder** (see Question Builder: Advanced sensor options on page 747) or the **Ask a Question** field.

© 2026 Tanium Inc. All Rights Reserved

Question Builder: Advanced sensor options



In the **Ask a Question** field, all sensor options use the syntax format `<sensor>?<option>=<value>`. To specify multiple advanced options for a sensor, separate each option with an ampersand `&`: `<sensor>?<option 1>=<value>&<option 2>=<value>...&<option N>=<value>`. The following example shows a question with two options for the **Installed Applications** sensor.

```
Get Installed Applications?ignoreCase=0&maxAge=120 contains A from all machines
```

The following sections describe the advanced sensor options and provide examples of their syntax in the **Ask a Question** field.

Case Sensitivity

Select whether Interact accounts for upper-case and lower-case characters when grouping and counting question results that contain letters.

In the **Question Builder**, the options are:

- **Ignore case**
- **Match case**

© 2026 Tanium Inc. All Rights Reserved

In the **Ask a Question** field, the syntax is `<sensor>?ignoreCase=[0|1]`. The value `0` means match the case and the value `1` means ignore the case. The following example specifies the **Case Sensitivity** option with a value set to **Match Case**.

```
Get Installed Applications having Installed Applications:Name?ignoreCase=0 contains A from all machines
```



If you omit **Case Sensitivity**, the **Ignore case in result values** setting in the sensor configuration controls case sensitivity for grouping and counting results. For more information, see Ignore case in result values on page 428.

Matching

If the Tanium Client computes multiple results for certain sensors, you can use the **Matching** option as a filter such that the Client answers the question only if its results conform to your selection. For example, a Client with multiple interfaces returns multiple results for the **IP Address** sensor. You can specify matching to return results only from Clients on which all the interfaces have an IP address that contains the string `192`.

In the **Question Builder**, this option is available only in the **from computers with** section, and the options are:

- **Match Any Value**: The Client returns results if any of its results match the sensor value.
- **Match All Values**: The Client returns results only if all its results match the sensor value.

In the **Ask a Question** field, this option is available only in the `from` clause. The syntax is `with [all] <sensor> contains <value>`, where omitting the `all` option specifies **Match Any Value**. In the following example, the **Matching** option is set to **Match All Values** (`with all`) for the **IP Address** sensor.

```
Get IP Address from all machines with all IP Address?type=String contains 192
```

Treat Data As

Interact treats sensor values as the type of data that you specify. For descriptions of the data types that you can select in the **Question Builder**, see Result Type on page 428.

In the **Ask a Question** field, the syntax for filtering by data type is `<sensor>?type=<type>`. The following example specifies **Numeric** as the type.

```
Get Free Memory?type=Numeric > 300 from all machines
```

The **File Size** data type in the **Question Builder** corresponds to the `DataSize` type in the **Ask a Question** field, where the syntax is `<sensor>?type=DataSize`. The following example returns results from endpoints where the installation folder of the Tanium Client is at least 10 GB.

```
Get Tanium Client Folder Size?type=DataSize >= 10 GB from all machines
```



Use the **Treat Data As** option only with comparison operators, such as `>` and `>=` in the preceding examples.

© 2026 Tanium Inc. All Rights Reserved

Maximum Data Age

Specify the maximum time for which the Tanium Client can use a cached result for the sensor, instead of re-running it for a fresh result, when answering questions. For example, you might specify 15 minutes for the **File Size** sensor. When a Client receives a question that runs the **File Size** sensor, it caches the result. Over the next 15 minutes, if the Client receives another question with the **File Size** sensor, it returns the cached result. After 15 minutes, if the Client receives a question with the **File Size** sensor, it re-runs the sensor script to return a fresh result.

To improve the accuracy of results, use shorter ages for sensors with values that change frequently, such as status and usage sensors. To reduce unnecessary resource consumption on endpoints, use longer ages only for sensors with values that typically do not change frequently, such as the chassis type or Active Directory domain membership.

In the **Question Builder**, you can specify the **Maximum Data Age** units (**minutes**, **hours**, **days**). In the **Ask a Question** field, the syntax is `<sensor>?maxAge=<value>` and the units are always seconds. The following example specifies a maximum age of `3600` seconds.

```
Get Computer Name?maxAge=3600 from all machines
```



If you omit the **Maximum Data Age**, the **Max Sensor Age** setting in the sensor configuration determines the maximum time for cached results. For more information, see Max Sensor Age on page 428.



Specify a **Maximum Data Age** only when issuing dynamic questions, not when creating saved questions that periodically reissue or when configuring endpoint membership in computer management groups and filter groups. Setting a **Maximum Data Age** that is lower than the **Max Sensor Age** increases CPU usage on endpoints.

Use advanced question options

Enable the **Force Computer ID** option to convert a single-sensor, counting question into a non-counting question by forcing Tanium Clients to include the computer ID in their answers. Note that the **Question Results** page does not include the computer ID results when you select this option. Converting to a non-counting question is a workaround that resolves cases where a counting question returns the `too many results` answer. For more information, see Too many results on page 710. You can enable the option in the **Ask a Question** field by using the `Get?forceComputerIdFlag=1` statement. You can also enable the option in the **Question Builder**, under **Advanced Question Options**.

© 2026 Tanium Inc. All Rights Reserved

Reference: User-specific saved questions

Overview of user-specific saved questions

Multiple users can work with the same saved questions during activities such as collecting information from endpoints. However, each user might see different settings for the same question based on the role permissions of that user and changes that the user makes to the question. To ensure that users can work productively with shared questions, it is important to understand and manage the properties that control question visibility:

- **User role permissions**

  To view and edit a saved question, a user must have the required role permissions for the content set to which the question is assigned. Additionally, the **Visibility** setting in the question determines whether the question is visible only to the owner (question creator) or to any user who has the required role permissions. For more information about the role permissions, see Manage saved questions on page 99.

- **User-specific configuration changes**

  When a user saves changes to the question configuration, the Tanium Server saves a copy of the question. When users sign in to Tanium Console, the users see only the copy with their own changes.

- **Computer group management rights**

  The computer groups assigned to users, user groups, and personas determine the visibility of the saved question **Reissue** interval and recent question results. For more information about assigning computer groups, see Assign computer groups on page 618.

Example: Saved question shared among multiple users

The following sections use an example scenario to describe how various factors determine the visibility of a question and its settings and results. All users in the example have permissions to read, create, and edit the **Installed Applications on Windows Workstation** question.

To see the question settings described in the following sections:

1. From the Main menu, go to **Administration > Content > Saved Questions**.
2. Click the title of a saved question to preview and edit the saved question.

For the example, the following table lists the users in the order that they made changes to the question configuration.

© 2026 Tanium Inc. All Rights Reserved

Example user role permissions and computer group assignments

User name	Role permissions	Computer group management rights	Question configuration edits
Admin1	Administrator reserved role	Unrestricted management rights	Created and saved the question with the **Display this question in the list of questions that are available for drilling down** and **Display this question in the list of questions that are available to merge** options disabled, and the **Reissue** interval set to one day.
User1	Read, create, and edit the saved question	All Windows (endpoints that run any Windows OS)	Resaved the question with **Display this question in the list of questions that are available to merge** enabled.
Admin2	Content Administrator reserved role	Unrestricted management rights	Resaved the question with **Display this question in the list of questions that are available to merge** reverted to disabled *after* User1 enabled it.
User2	Read, create, and edit the saved question	All Windows desktops (endpoints that run the Windows desktop OS)	Resaved the question with **Display this question in the list of questions that are available for drilling down** enabled.
User3	Read, create, and edit the saved question	All Windows	Made no changes.

Role permissions

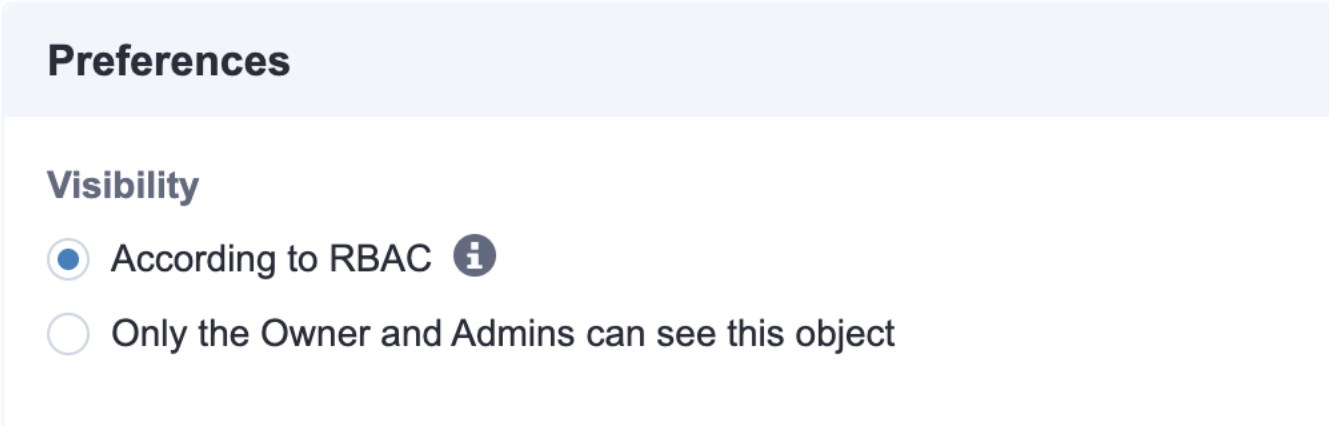
Visibility

Whether a saved question is visible to users depends on their role permissions and the **Visibility** option in the question configuration:

- **According to RBAC**
  All users who have the necessary role permissions can see the question. In this example, all users have the role permissions required to read and edit saved questions in the content set that contains this question. Therefore, this option enables all users to see the question.
- **Only the Owner and Admins can see this object**
  Only users with the **Administrator** or **Content Administrator** reserved role, and the question owner (creator), can see the question. In this example, this option enables only Admin1 and Admin2 to see the question.

© 2026 Tanium Inc. All Rights Reserved

Saved question visibility options



User settings

The **User Settings** in a saved question configuration vary based on the role permissions and any default settings. In addition to the merge and drilldown settings, administrators can see and set default settings. The default settings are useful when you want a question to initially have the same **User Settings** for all users until the users edit those settings. In this context, administrators are users who have the **Administrator** reserved role (Admin1 in this example) or **Content Administrator** reserved role (Admin2 in this example). The default settings differ based on whether the administrator creates a new question or edits an existing question.

For information about all saved question settings, see Create a saved question on page 463.

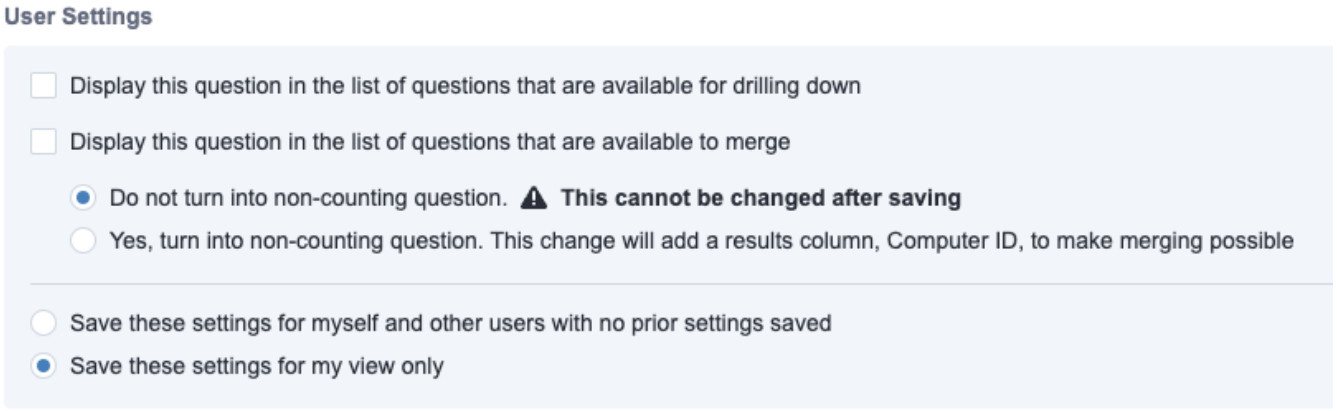
NOTE

The figures in the following sections show the **User Settings** for counting questions. Non-counting questions have fewer options.

USER SETTINGS FOR A NEW SAVED QUESTION

The following figure shows the **User Settings** in a saved question configuration for an administrator who creates the question.

User Settings for a new saved question



The default settings include:

© 2026 Tanium Inc. All Rights Reserved

- **Save these settings for myself and other users with no prior settings saved**: For each non-administrator user, the Tanium Server applies the **User Settings** according to the changes that the user made to these settings. For non-administrator users who never changed the settings, the Server applies the settings according to whichever administrator was the last to save changes. For administrators, the latest changes that an administrator makes override any earlier changes that other administrators made.
  For all the users in this example, the Server applies the settings that Admin1 configured when creating the saved question, with the following exceptions:

  Example: Settings for a new saved question that apply to the current user and other users

User	Settings
User1	Merging is enabled for this user because the user made that change.
User2	Drilldown is enabled for this user because the user made that change.
User3	The settings are as Admin2 configured them because Admin2 was the last administrator user to save changes to the settings and User3 made no subsequent changes.

- **Save these settings for my view only**: For each user, the Tanium Server applies the user settings according to the changes that the user made to these settings.
  For all the users in this example, the Server applies the settings that Admin1 configured when creating the saved question, except as follows:

  Example: Settings for a new saved question that apply only to the current user

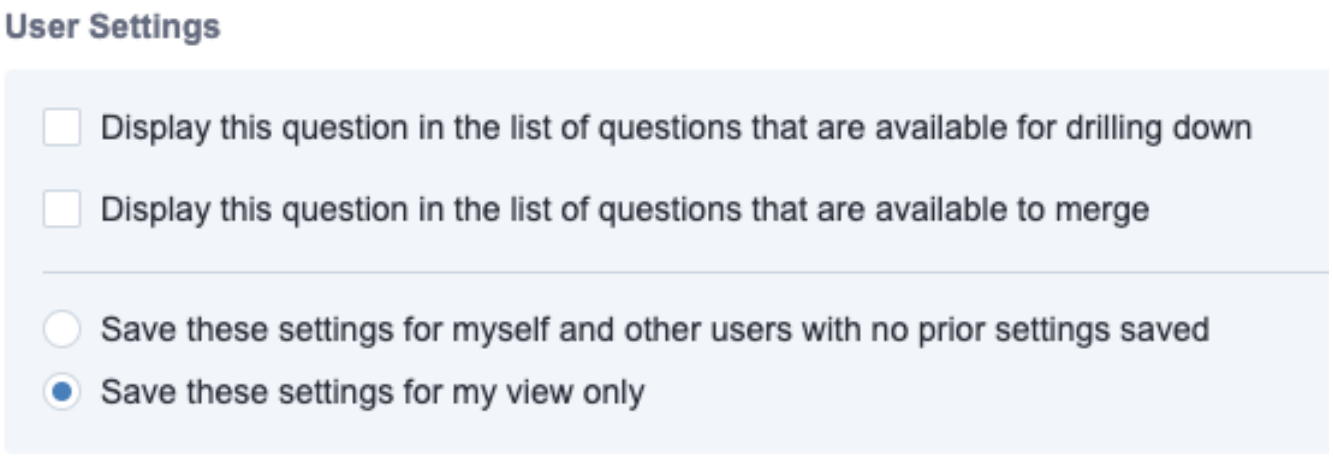
User	Settings
User1	Merging is enabled for this user because the user made the change.
User2	Drilldown is enabled for this user because the user made that change.
User3	The settings are as Admin1 configured them because User3 made no changes.

USER SETTINGS FOR AN EXISTING SAVED QUESTION

The following figure shows the **User Settings** in a saved question configuration for an administrator who is editing the question.

© 2026 Tanium Inc. All Rights Reserved

User Settings for an existing saved question



The options are as follows:

- **Save these settings for my view only**: For each user, the Tanium Server applies the **User Settings** according to the changes that the user made to these settings.
  For all the users in this example, the Server applies the settings that Admin1 configured when creating the saved question except for the changes that each user saved, as follows:

  Example: Settings for an existing saved question that apply only to the current user

User	Settings
User1	Merging is enabled for this user because the user made that change.
User2	Drilldown is enabled for this user because the user made that change.
User3	The settings are as Admin1 configured them because User3 made no changes.

- **Save these settings for myself and other users with no prior settings saved**: For each user, the Tanium Server applies the **User Settings** according to the changes that the user made to these settings. For a user who never edited the settings, the Server applies the settings according to whichever user was the last to save changes.
  For all the users in this example, the Server applies the settings that Admin1 configured when creating the saved question, except as follows:

  Example: Settings for an existing saved question that apply to the current user and other users

User	Settings
User1	Merging is enabled for this user because the user made that change.
User2	Drilldown is enabled for this user because the user made that change.
User3	Drilldown is enabled for this user because User2 was the last user to set the values and User3 made no subsequent changes.

© 2026 Tanium Inc. All Rights Reserved

Saved question configuration copies

The Tanium Server maintains a copy of a saved question configuration for each user who saves changes to it. Users who make no changes share the same configuration as the question creator.

In this example, the Server maintains the original configuration that Admin1 created and adds a copy for Admin2, User1, and User2 because those users made changes. The Server does not add a copy for User3 because that user made no changes. Upon signing in to the Server, User3 sees the saved question that Admin1 created, whereas the other users each see their own copy.

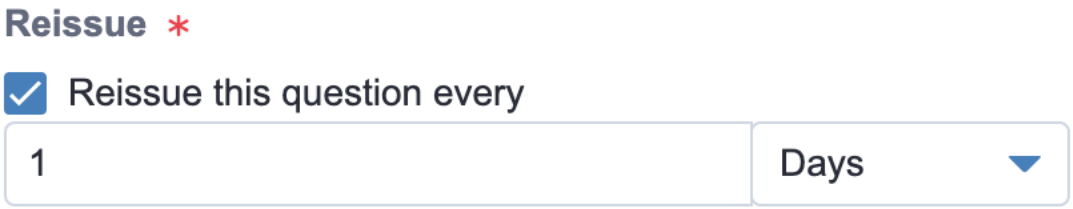


The visibility of the saved question **Reissue** interval and recent question results depends on computer group assignments, even among users who share the same saved question configuration as the creator. The following sections explain this in detail.

Recent results and computer group assignments

The Tanium Server creates a management rights identifier (computer management group ID) for each identical set of computer group assignments, and associates that identifier with each user who has the set. If a user specifies a **Reissue** interval when creating a saved question, other users who subsequently sign in to Tanium Console can see that setting only if they have the same computer management group ID as the creator. Otherwise, users must set their own **Reissue** interval, at which point the Server creates user-specific copies of the question configuration.

Saved question reissue interval



In this example, Admin1 creates the saved question **Installed Applications on Windows Workstation** and sets the **Reissue** interval to one day. Admin1 and Admin2 have the same computer group assignments (**Unrestricted management rights**), so Admin2 can see the **Reissue** interval that Admin1 configured. However, because User1, User2, and User3 have different computer group assignments than Admin1, they cannot see the **Reissue** interval that Admin1 configured.

The computer management group ID that controls **Reissue** visibility requires exact matching for computer group assignments. For example, if User2 creates a question, User1 and User3 cannot see its **Reissue** interval even though their computer group **All Windows** includes all the endpoints in the **All Windows desktops** computer group that is assigned to User2. As another example, consider what happens when an administrator assigns two computer groups to User1 (**All Windows** and **All macOS**), but assigns only one computer group to User3 (**All Windows**). User1 and User3 will have different computer management group IDs because the combination of computer groups assigned to each user differs. Therefore, if User1 then creates a saved question, User3 cannot see its **Reissue** interval.

© 2026 Tanium Inc. All Rights Reserved

The Tanium Server issues a saved question at the interval specified in each user-specific configuration. However, if multiple users have the same computer management group ID, the Server consolidates the redundant traffic. For example, consider what happens when User1, User2, and User3 keep the **Reissue** interval at one day and User3 enables drilldown. Because User3 changed a setting, the Server adds a User3-specific copy of the question. Nevertheless, User1 and User3 have the same computer group assignments (**All Windows**), so the Server issues the question once per day for both users instead of twice per day. The Server also has a User2-specific copy of the question. However, even though the User2 copy has the same **Reissue** interval as the User1 and User3 copies, User2 has a different computer group assignment (**All Windows desktops**), so the Server issues the User2 question separately from the other users. Ultimately, the Server issues the same question twice per day: once to the **All Windows** computer group (for User1 and User3) and once to the **All Windows desktops** computer group (for User2).

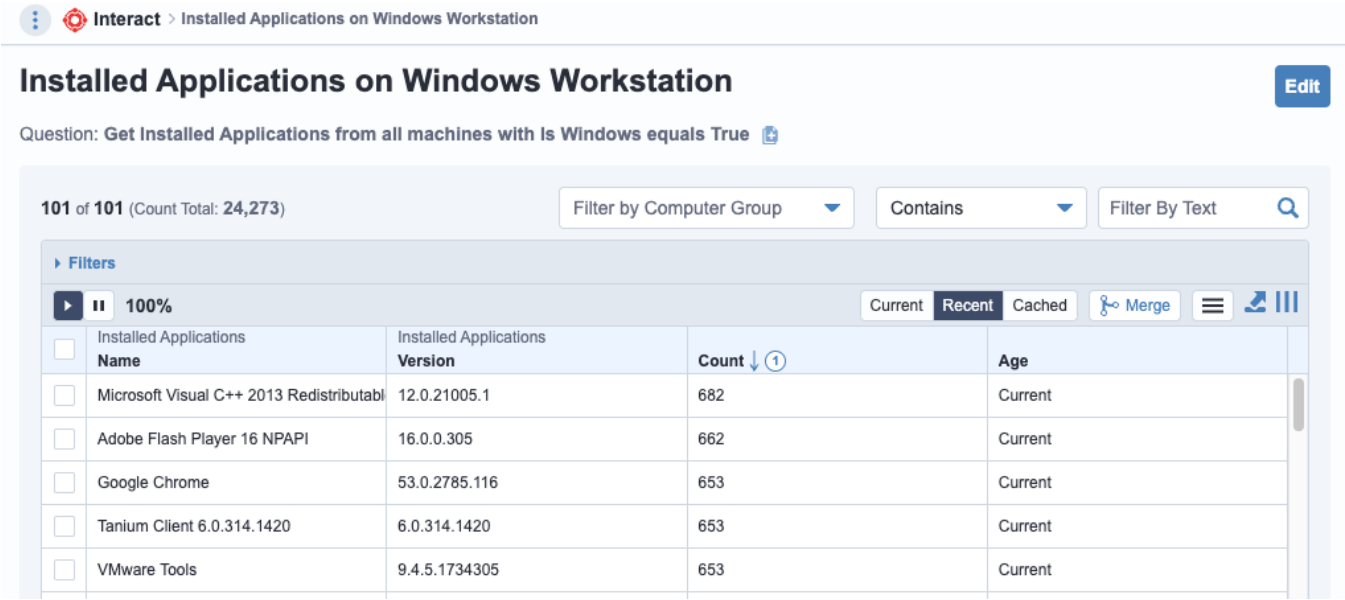
Recent results and computer group assignments

When you view the results of a saved question in Tanium Console, the results grid provides the option to show **Current**, **Recent**, or **Cached** data. Current data includes results only from endpoints that are currently online. In addition to data from online endpoints, **Recent** data includes results from offline endpoints if those results still reside in the Tanium Server cache. The Server stores results for seven days by default. If an endpoint is offline when the Server issues a question, the Server passes any cached result for that endpoint to the results grid.

NOTE

Cached data includes data retrieved by Tanium Data Service (TDS). For more information, see Display results for online and offline endpoints on page 258.

Saved question recent results



When caching results for a question, the Tanium Server maintains a separate cache for each set of results that is associated with a distinct computer management group ID. Consequently, users with different computer management group IDs might see different recent results for the same endpoints.

© 2026 Tanium Inc. All Rights Reserved

To understand how recent results might differ for each user, consider an example where the Tanium Server reissues the question **Installed Applications on Windows Workstation** twice per day: once for each computer management group ID. For offline endpoints, the Server caches one set of results for the computer management group ID associated with **All Windows** (results are visible to User1 and User3) and one set for the computer management group ID associated with **All Windows desktops** (results are visible to User2). User1 and User2 then show the results in the **Saved Question Results** grid and set the **Zoom** setting to **Recent**. However, say a different set of endpoints were offline when the Server issued the question to **All Windows** than when issuing the question to **All Windows desktops**. As a result, the Server saved different updates to the separate results caches. User1 and User2 then see different recent (cached) results for the same endpoints that are offline while they are viewing the results grid.

© 2026 Tanium Inc. All Rights Reserved

Reference: Manage sensor string growth

When you issue a question to endpoints, Tanium Clients return answers in the form of strings for each sensor in the question. The Tanium Server stores the strings in the `<Tanium Server installation folder>/strings` directory and loads them into memory (the string cache) when it uses them. You can mitigate the impact that question results have on Tanium Server memory and disk usage by setting, for each sensor, a maximum age for the strings in storage.

Sensor string cleaning

To prevent sensor string growth from consuming too much space, the Tanium Server clears a portion of the strings for all sensors when the total strings exceed a default threshold. However, the default string-cleaning settings do not distinguish among sensors in terms of how likely they are to generate strings that are unique and that are used only once. This matters because unique strings consume more space and clearing single-use strings has less impact on Server processing and traffic; the Server does not have to reissue questions to regenerate the strings for future use. For example, the **Detect Primary Alerts** sensor often generates many unique, single-use strings. To account for these factors, you can configure string cleaning for individual sensors based on their **Max String Age** setting. The Server bases string ages on when it last used the strings or received them from Tanium Clients and discards strings that exceed the maximum.

Maximum string age

In a sensor configuration, the **Max String Age** setting controls the maximum age that answer strings for the sensor can reach before the Tanium Server removes them. The string age is based on the number of minutes since the Server last used the string or received it from Tanium Clients. When you create a custom sensor, the setting is disabled by default and the Server does not apply sensor-specific, age-based string removal for this sensor. If you enable the setting, it defaults to 7 days, which is the best practice value.



The **Max String Age** does not apply to the results cache that Tanium Data Service (TDS) stores on the Tanium Server. For more information, see Tanium Interact User Guide: Managing Tanium Data Service.

Maximum strings per sensor



When limiting string growth, set the **Max Strings Age** instead of the **Max Strings**. Contact Tanium Support on page 724 before setting the **Max Strings** in extreme cases that might require a string count limit for individual sensors.

In a sensor configuration, the **Max Strings** setting controls the maximum number of answer strings that the Tanium Server stores for the sensor before removing the oldest strings. The Server includes the string count for temporary sensors (associated with Parameterized sensors on page 422) when calculating the string count for their source sensors. When you create a custom sensor, the default is 0, which specifies no limit. The string age is based on when the Server last used the string or received it from Tanium Clients.

© 2026 Tanium Inc. All Rights Reserved

NOTE

The **Max Strings** does not apply to the results cache that TDS stores on the Tanium Server. For more information, see Tanium Interact User Guide: Managing Tanium Data Service.

Check sensor string growth

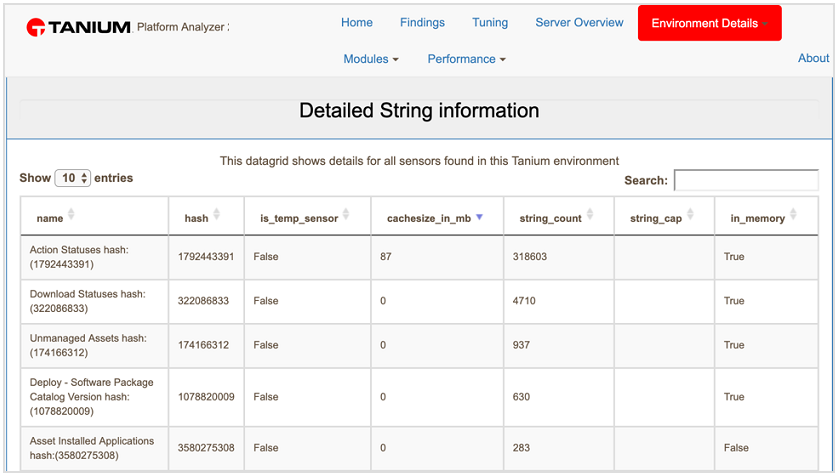
You can determine which sensors produce the most string growth through Tanium™ Health Check or Tanium Console. Health Check enables you to view the top sensors by both string count and memory usage. Console displays only the string count.

Check string growth through Health Check

If Health Check is not installed, install it before performing the following steps. For more information, see Tanium Health Check User Guide: Installing Health Check.

1. From the Main menu, select **Shared Services > Health Check**.
2. Under **Manual Report Generation**, click **Run TPAN Report Now**.
3. Under **Reports** click the **HTML** link for the **Full Report** that you just ran.
4. At the top of the report, select **Environmental Details > String Details**.
5. Review the grids that list the top sensors by string count and memory usage to determine which sensors produce the most string growth.

TPAN report showing details about sensor strings



name	hash	is_temp_sensor	cachesize_in_mb	string_count	string_cap	in_memory
Action Statuses hash: (1792443391)	1792443391	False	87	318603		True
Download Statuses hash: (322086833)	322086833	False	0	4710		True
Unmanaged Assets hash: (174166312)	174166312	False	0	937		True
Deploy - Software Package Catalog Version hash: (1078820009)	1078820009	False	0	630		True
Asset Installed Applications hash:(3580275308)	3580275308	False	0	283		False

Check string growth through Console

Check the string count of sensors to determine which are producing the most string growth.

© 2026 Tanium Inc. All Rights Reserved

NOTE **Sensor read** permission is required to see string counts.

1. From the Main menu, select **Administration > Content > Sensors**.
2. Click Customize Columns and select **String Count**.

   TIP On the **Sensors** page, you might have to navigate horizontally to match string count values to the associated sensors. To avoid the navigation step, drag the **String Count** column beside the **Name** column when you Customize Columns.

3. Click the **String Count** column header twice to sort the grid by string count in descending order (from highest to lowest).

Set the maximum string age

Not all sensors require a **Max String Age**, and the setting is disabled by default when you create a new sensor. If you enable the setting, the best practice is to set the value to seven days. Setting a lower maximum is required only in rare cases, such as for sensors that produce results containing date or time stamps. When you create a sensor, the best practice is to avoid including date and time stamps in string results because they tend to produce unusually large string growth. However, if such sensors are necessary, you can set the maximum as low as one day for sensors that use date stamps and as low as six hours for sensors that use time stamps. Contact Tanium Support if you are considering setting the **Max String Age** to lower than six hours; only exceptional cases require such limits. For more information, see Contact Tanium Support on page 724.

NOTE **Sensor write** permission is required to change the maximum string age.

1. From the Main menu, select **Administration > Content > Sensors**.
   Perform the remaining steps for each sensor that you determine requires a string age limit.
2. Select the sensor and click **Edit**.
3. Enable and set the **Max String Age**, and then click **Save**.

   NOTE For almost all sensors, setting the **Max String Age** reduces string growth to a manageable level and setting the **Max Strings** (string count limit) is unnecessary. Contact Tanium Support before setting the **Max Strings** in extreme cases that might require a string count limit for individual sensors. For more information, see Contact Tanium Support on page 724.

4. Over the next two days, repeat the steps to verify that string counts and memory usage are reduced as expected for the sensors that have string limits: see Check sensor string growth on page 759. If necessary, set a lower **Max String Age** for sensors that still produce too much string growth.

© 2026 Tanium Inc. All Rights Reserved

Reference: Language support

You can select one of the Supported languages on page 764 that is most comfortable for you when reading user interface (UI) text in Tanium solution workbenches and the text in Tanium user documentation. Your language selection also determines the date and time format that solution workbenches use. For example, if you select English (United States), dates appear in the format `month/day/year` and times appear in the format `hour:minute:second [AM|PM] <time zone>`.

Language selection for solution workbenches



Tanium generates workbench text for non-English languages through a combination of machine translation from English and post-editing. Contact Tanium Support on page 724 to request changes to workbench text.

Browser default for language

By default, Tanium solutions show text in the language that you select for the browser through which you access solution workbenches. For Solutions that support multiple languages on page 764, you can Select the language and date format on page 762 through a Console setting that overrides the browser.

Language selection for users and personas

The language selection applies to the default persona of your user account and any alternative persona that you select for a Tanium session. The selection does not affect the language that other users see in solution workbenches.

Language selection for solution workbenches

The language selection applies to all the solutions that support the language. You cannot select a different language for different solutions.

Translation inclusions and exclusions

Your language selection for solutions applies to workbench UI elements, such as field labels, dropdown list options, and page titles. The language selection does not apply to the following elements:

Workbench text that is not translated

Element	Description
Endpoint data	When a user or Tanium solution issues a question, the results that Tanium Clients return for the question sensors are not translated. Interact, Reporting, and other solutions show endpoint data in the original language of that data.
Tanium products	Product names, such as Interact or the Tanium Server, are not translated.

© 2026 Tanium Inc. All Rights Reserved

Workbench text that is not translated (continued)

Element	Description
Content names	The names and associated metadata of content objects are not translated. For example, the **Sensors** page lists Tanium-managed sensors with names and descriptions in English regardless of your language selection. The names and metadata of user-defined content appear in the language that the content authors used when creating the content.
Messages	Some error, warning, and informational messages that workbenches show during user or system activities are not translated.

Select the language and date format

1. In the Console header, click  and select **Preferences**.
2. Select a **Language** and click **Save**. The change applies immediately.



If you select a non-English language and then access the workbench of a solution that does not support multiple languages, the workbench appears in English.

Language selection for Tanium documentation

By default, Tanium documentation that you access through the Tanium Resource Center (TRC) is in English. When you Select the documentation language on page 763, a browser cookie saves your selection and applies it for all subsequent TRC visits. Selecting the language again is necessary only if you clear the browser cookies.



Tanium generates documentation text for non-English languages through machine translation.

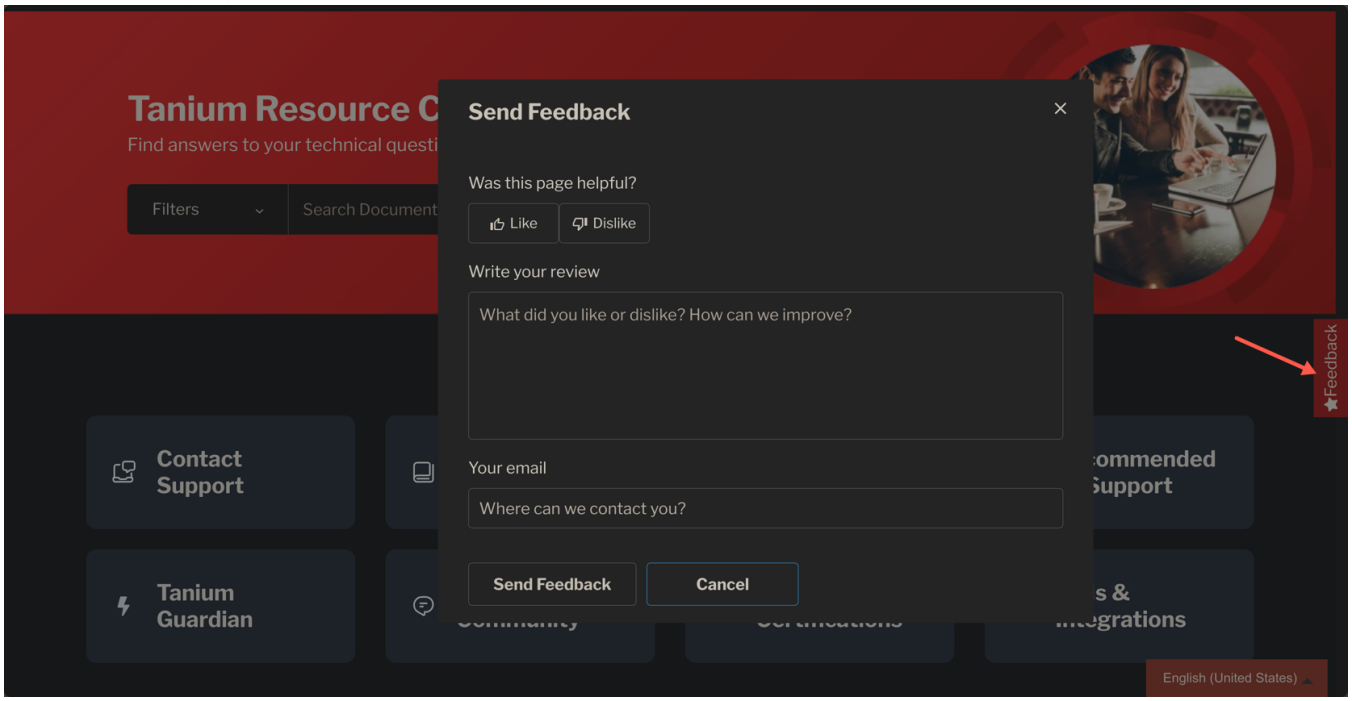
Translation inclusions, exclusions, and feedback

Your language selection for Tanium documentation applies to the text in all user guides and in most Tanium Community articles, Tanium Knowledge Base articles, TRC pages, and workflow maps. The language selection does not apply to images in the documentation, including screen captures and associated text labels.

To provide feedback on documentation translation, click  **Feedback** on any TRC page, complete the form, and click **Send Feedback**.

© 2026 Tanium Inc. All Rights Reserved

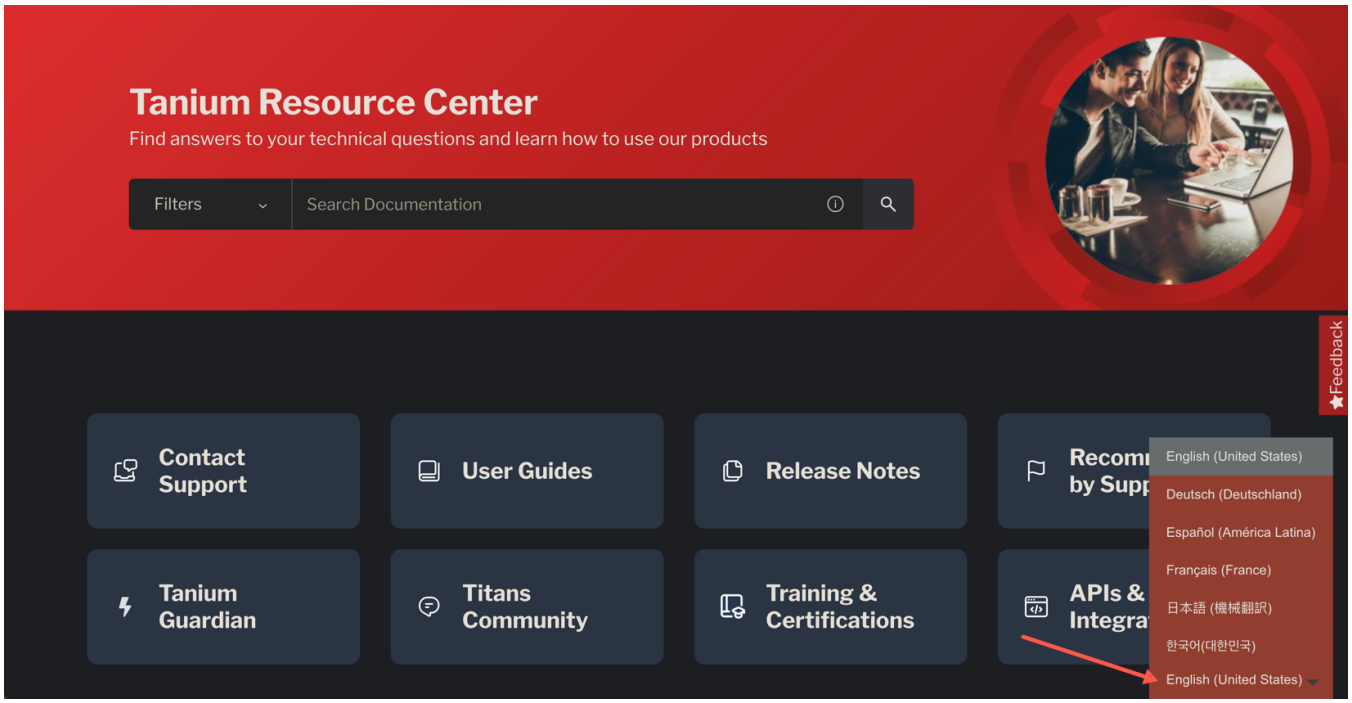
Feedback for language translation in the Tanium Resource Center



Select the documentation language

Go to any page in the Tanium Resource Center and select a language in the ***<Current Language>* (*<Country>*)** dropdown list.

Language selection in the Tanium Resource Center



© 2026 Tanium Inc. All Rights Reserved

Solutions that support multiple languages

You can select any of the Supported languages on page 764 for the workbench text of the following Tanium solutions.

- Asset
- Automate
- Console
- Deploy
- Interact
- Patch
- Reporting
- Threat Response



If you select a non-English language and then access the workbench of a solution that does not support multiple languages, the workbench appears in English.

Supported languages

You can select one of the languages in the following table for Tanium solution workbenches and Tanium documentation. The language selection also sets the date and time format for workbenches.

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

Supported languages and the corresponding date and time formats

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

© 2026 Tanium Inc. All Rights Reserved

Reference: Tanium Core Platform settings

You can use Tanium Console to configure the settings that are listed in the table Tanium Core Platform settings on page 766. These settings control the behaviors of Tanium Core Platform servers, Tanium Clients, Console, and other Tanium solutions. For example, you might configure the max_console_idle_seconds setting to specify the maximum time that Console users can specify in their user preferences for the inactivity timeout.



Before you add or edit settings through Tanium Console, see Manage advanced settings on page 164 for information about the types of settings and how to configure them.

The table Tanium Core Platform settings on page 766 indicates which Tanium Server settings are local and therefore must be configured on each peer in an active-active deployment.

To configure settings that you must set on individual platform servers, see:

- Tanium Appliance User Guide: Reference: Tanium Core Platform command-line interface
- Tanium Core Platform User Guide for Windows Deployments: Reference: Command-line interface

You can configure Client settings locally if you want specific Clients to override the values that the Tanium Server propagates. For more information, see Tanium Client Management User Guide: Managing Client settings and Index configurations.

For more information about Client peering settings that you do not customize, see Tanium Client Management User Guide: Peering settings reference.



The following table describes only the settings that are most commonly configured or viewed when you set up or customize a Tanium deployment. Contact Tanium Support on page 724 for more information about additional settings.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings

Settings	Infrastructure	Platform components	Guidelines
access_control_origin_servers	Appliance Windows	Tanium Server	In most deployments, Tanium Servers automatically enable Cross-Origin Resource Sharing (CORS). However, in an active-active deployment, if module synchronization fails during module import, update, or uninstallation operations, manually add this Server setting to enable CORS. Enter a comma-separated list of the fully qualified domain names (FQDNs) or IP addresses that you use to access Tanium Console on each Server, such as `ts1.example.com,ts2.example.com` or `192.0.2.1,192.0.2.2`. This setting is hidden by default. For more information, see Resolve Tanium Server synchronization errors on page 142.
action_target_estimate_min_percent	Appliance Windows	Tanium Server	Specify the estimated percentage of endpoints that must answer the target question before users can deploy an action based on the question results. Raising the value forces users to wait longer before deploying an action but provides a more accurate estimate of the number of targeted endpoints. The default is `20` percent. For more information, see Administrative setup for actions on page 328.
AddressMask	Appliance Windows	Tanium Server (local)	Enter the hexadecimal value of a subnet CIDR that defines the boundaries of a Tanium linear chain of IPv4 Tanium Clients. Contact Tanium Support on page 724 for guidance before configuring this setting. For more information, see Tanium Client User Guide: AddressMask.
AddressPrefixIPv6	Appliance Windows	Tanium Server (local)	Enter a decimal number from 0 to 128 to represent the IPv6 prefix that defines the boundaries of a linear chain of IPv6 Tanium Clients. By default, this setting is hidden and has a value of `0`, which specifies no peering. Contact Tanium Support on page 724 to determine the optimum value for peering in IPv6 networks. Do not add or change the setting without direction from Support. For more information, see Tanium Client User Guide: AddressPrefixIPv6.
allow_multiple_action_approval	Appliance Windows	Tanium Server	Enable (`1`) or disable (default `0`) the ability to approve actions in bulk for users who have approval permissions. Users must preview each action before approving it. For more information, see Enable or disable action approval on page 412.
allow_process_group_flag_edit	Appliance Windows	Tanium Server	Enable (`1`) or disable (default `0`) the ability to control whether package commands run within a process group. For more information, see Launch this package in a process group on page 448.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
AllowedHubs	Appliance Windows	Tanium Server (local) Zone Server	Configure this setting based on the infrastructure and server type: • **Tanium Appliance**: ◦ **Tanium Server**: Specify the Zone Server Hub that is allowed to connect to the Tanium Server. This setting has the value `127.0.0.1` because the Zone Server Hub is collocated on the Tanium Server in an Appliance deployment. ◦ **Zone Server**: Enter a comma-separated list of IP addresses of Zone Server Hubs that are authorized to communicate with the Zone Server. • **Windows**: ◦ **Tanium Server**: Enter a comma-separated list of Zone Server Hubs that are authorized to communicate with the Tanium Server. Specify the Hubs by FQDN or IP address. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). Note that you can configure exceptions to the AllowedHubs list in the AllowedLocalHubs on page 767 setting. ◦ **Zone Server**: Enter a comma-separated list of Zone Server Hubs that are authorized to communicate with the Zone Server. Specify the Hubs by FQDN or IP address. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). If the Zone Server Hub resides on a different host than the Tanium Server, see Tanium Core Platform User Guide for Windows Deployments: Install the Zone Server Hub.
AllowedLocalHubs	Windows	Tanium Server	By default, this setting is hidden and has a value of `1`, which enables any local Zone Server Hub to communicate with the Tanium Server regardless of the AllowedHubs on page 767 setting. Setting the value to `0` allows local Zone Server Hubs to communicate with the Tanium Server only if they are listed in AllowedHubs. You must add this setting manually if you need it. Contact Tanium Support on page 724 for guidance before adding this setting.
api_token_expiration_in_days	Appliance Windows	Tanium Server	Enter the default expiration interval (in days) for Tanium API tokens. The default is `7`, but users can enter a different value when creating a token. For more information, see Configure token expiration settings on page 699.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
api_token_max_expiration_in_days	Appliance Windows	Tanium Server	Enter the maximum expiration interval (in days) that users can specify when creating Tanium API tokens. The default is `365`. For more information, see Configure token expiration settings on page 699.
api_token_trusted_ip_address_list	Appliance Windows	Tanium Server	Specify from which systems users are allowed to use API tokens to access the Tanium Server. Enter the value as a comma-separated list of external IP addresses. By default, the Tanium Server allows token requests from the Tanium Module Server, so you do not have to add the Module Server to the allow list. For more information, see Enable API token authentication behind a reverse proxy on page 699.
authenticate_api_token_with_x_forwarded_for_ip	Appliance Windows	Tanium Server	Enable this setting (set the value to `1`) only if all API token access to the Tanium Server must go through a reverse proxy server. If the setting is disabled (value is `0`) in such deployments, the api_token_trusted_ip_address_list on page 768 setting cannot restrict which systems are allowed access. For more information, see Enable API token authentication behind a reverse proxy on page 699.
BypassCRLCheckHostList	Appliance Windows	Tanium Server Module Server TDownloader	List the servers that the Tanium Server or Module Server can trust without checking a certificate revocation list (CRL). The Tanium Server and Module Server perform a CRL check on all servers that are not in this list, and do not download files from a server that fails the check. Specify the servers by FQDN or IP address. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). Configure BypassCRLCheckHostList according to the infrastructure and server type: • **Tanium Appliance**: Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. • **Windows**: Configure this setting in the Tanium Server and Module Server configurations. If you configure the Tanium Server and Module Server to access Internet sites through a proxy server, you can configure BypassCRLCheckHostList through Tanium Console. For more information, see Configuring Internet access through proxy servers on page 181.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
BypassProxyHostList	Appliance Windows	Tanium Server Module Server TDownloader	If you configure the Tanium Core Platform to access Internet sites through a proxy server, enter a comma-separated list of FQDNs or IP addresses for the hosts that do not go through the proxy server. You do not have to enter `127.0.0.1`, `localhost`, or the Module Server, but enter active-active Tanium Servers if necessary. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). Specify literal values. All supported Tanium Core Platform versions allow wildcards. Configure BypassProxyHostList according to the infrastructure and server type: • **Tanium Appliance**: Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. • **Windows**: Configure this setting in the Tanium Server and Module Server configurations. For more information, see Configuring Internet access through proxy servers on page 181.
ClientCacheLimitInMB	Appliance Windows	Tanium Client	Enter the absolute amount of disk space that a Client can use for caching chunks. The value is in megabytes (MB) and the default is 2048. For more information about chunk caching, see Tanium Client Management User Guide: Chunk caching. For more information about how this setting affects action deployment, see Administrative setup for actions on page 328.
ComputerID	Appliance Windows	Tanium Client	Do not edit this setting, which exists only on the Tanium Client. The Tanium Server assigns a value to each Client to uniquely identify and track each managed endpoint. For more information, see Tanium Client Management User Guide: Registration and ComputerID.
console_confirmation_prompt_type	Appliance Windows	Tanium Server	Specify the confirmation type to display when a user is making a critical change that requires a confirmation prompt: • `0` (default): Show a password prompt • `1`: Show a prompt with **Yes** and **Cancel** buttons For more information, see Select the task confirmation prompt on page 153.
console_consoleColor	Appliance Windows	Tanium Server	Specify the color of the top border and the Tanium Console version text background in the Main menu of Tanium Console. For more information, see Select the Console color on page 151.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
console_disable_ha_workbench_install	Appliance Windows	Tanium Server	In an active-active deployment of Tanium Servers, disable (`1`) or enable (`0`) module synchronization for solution import, update, and uninstallation operations. If synchronization is enabled when you manually perform an operation on one Server, the other Server automatically attempts the same operation. Disabling synchronization might be necessary in a deployment where no access_control_origin_servers on page 766 value can enable CORS to work. By default, console_disable_ha_workbench_install is a hidden setting and its value is `0`. For more information, see Resolve Tanium Server synchronization errors on page 142.
console_headerText	Appliance Windows	Tanium Server	Enter custom text to appear above the Console version text in the Main menu of Tanium Console. For more information, see Configure Console header text on page 152.
console_PreLoginBannerHTML	Appliance Windows	Tanium Server	Add this setting to enable a pre-login banner that provides information or warnings to users before they sign in to Tanium Console. This setting supports HTML with images, links, and complex text formatting, but requires you to copy the HTML file to the Tanium Server. For more information, see Configure a pre-login banner on page 147.
console_ PreLoginBannerHTMLText	Appliance Windows	Tanium Server	Configure this setting to enable a pre-login banner that provides information or warnings to users before they sign in to Tanium Console. This setting supports HTML with only text and basic formatting. For more information, see Configure a pre-login banner on page 147.
DatabaseEpoch	Appliance Windows	Tanium Client	Do not edit this setting, which exists only on the Tanium Client and indicates the date and time when the Tanium Server was deployed.
DBUserDomain	Windows	Tanium Server	This is the domain for the Tanium Server service account that connects to the Tanium database server. You configure DBUserDomain when completing the installation wizard for the Tanium Server. For more information, see Tanium Core Platform User Guide for Windows Deployments: Install the Tanium Server.
DBUserName	Windows	Tanium Server	This is the user name for the Tanium Server service account that connects to the Tanium database server. You configure DBUserName when completing the installation wizard for the Tanium Server. For more information, see Tanium Core Platform User Guide for Windows Deployments: Install the Tanium Server.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
enable_protocol_314_flag	Appliance Windows	Tanium Server	This setting applies only to Tanium Client 7.2, which Tanium release 2026H1 or later does not support. Upgrade any Client 7.2 installations to a new Client version and then set **enable_protocol_314_flag** to `0`, as described in Tanium Client Management User Guide: Upgrading Tanium Clients. The value `0` disables the legacy Tanium™ Protocol version that Client 7.2 uses to encrypt communication with the Tanium Server and other Tanium Core Platform components. For any Clients 7.2 that you have not finished upgrading, the value `1` enables the legacy Tanium Protocol version.
EnableFileCache	Windows	Zone Server	If the Zone Server Hub is installed on a dedicated host instead of on the Tanium Server host, set the value to `1` to enable file caching. You must configure this setting through the Hub CLI. For more information, see Tanium Core Platform User Guide for Windows Deployments: Manage caching on the Zone Server and Zone Server Hub.
EnableRandomListeningPort	Appliance Windows	Tanium Client	Enable (`1`) or disable (`0`) the randomized selection of a new listening port at intervals. The Client uses the port for communications from peer Clients. If another application is already using the selected port, the Client selects another port immediately instead of at the next interval. By default, EnableRandomListeningPort is disabled and the Client uses a fixed listening port (default is 17472). For more information, see Tanium Client Management User Guide: Randomize listening ports. BEST PRACTICE Randomize listening ports only if it is required by rules in your organization. Using randomized listening ports requires more complex firewall rules to allow Client communication, and it makes troubleshooting issues with Client communication more difficult.
EnableSensorQuarantine	Appliance Windows	Tanium Client	Enable (`1`) or disable (`0`) the enforcement of quarantined sensors. If you enable quarantine enforcement, Tanium Clients do not answer questions that use quarantined sensors and those sensors do not run for actions. If you disable enforcement, Clients still quarantine sensors and log quarantine events, but do not prevent those sensors from running. By default, EnableSensorQuarantine is hidden and set to `0` until you manually add it and change its value. For more information, see Enable or disable enforcement of quarantined sensors on page 435.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
EnforceAllowedHubs	Appliance Windows	Tanium Server (local) Zone Server	Configure this setting to enable (`1`) or disable (`0`) enforcement of the AllowedHubs on page 767 setting: • **Tanium Appliance**: EnforceAllowedHubs is a Zone Server setting. The default value is `1` and you must not change it. • **Windows**: EnforceAllowedHubs is a setting on the Tanium Server and Zone Server. If the Zone Server Hub resides on a different host than the Tanium Server, the best practice is to set the value to the default `1` on both servers. ◦ **Tanium Server**: The value `1` specifies that only Hubs listed in AllowedHubs can communicate with the Tanium Server. The value `0` specifies that any Hub can communicate with the Tanium Server regardless of the AllowedHubs setting. ◦ **Zone Server**: The value `1` specifies that only Hubs listed in AllowedHubs can communicate with the Zone Server. The value `0` specifies that any Hub can communicate with the Zone Server regardless of the AllowedHubs setting. For more information, see Tanium Core Platform User Guide for Windows Deployments: Install the Zone Server Hub.
FirstInstall	Appliance Windows	Tanium Client	Do not edit this setting, which exists only on the Tanium Client and indicates the date and time of the initial Client installation.
ForceIPV6	Appliance Windows	Tanium Server Module Server TDownloader	In deployments where traffic between Tanium Core Platform servers and the Internet traverses a proxy server, TDownloader resolves the proxy address as an IPv4 address by default. If the proxy server has an IPv6 address, add ForceIPV6 with a value of `1`. ForceIPV6 is a TDownloader setting on the Tanium Server and Module Server in both Tanium Appliance and Windows deployments. The setting is hidden by default and its default value is `0`. Contact Tanium Support on page 724 for guidance before adding this setting. For more information about proxy server settings, see Tanium Appliance User Guide: Configuring proxy server settings or Tanium Core Platform User Guide for Windows Deployments: Configuring proxy server settings.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
HostDomainName	Appliance Windows	Tanium Client (non-Windows)	Configure this setting only for Clients that do not return the domain name correctly in question results. The value that you specify overrides the data that the Client operating system (OS) would otherwise return. Specify just the domain portion of the FQDN. For example, if the FQDN is `host.example.com`, specify `example.com`.
HostFQDN	Appliance Windows	Tanium Client (non-Windows)	Configure this setting as an alternative to HostDomainName on page 773 if the Clients do not return the host name and domain name correctly in question results. The value that you specify for this setting overrides the data that the Client OS would otherwise return. Specify the complete FQDN, including host name, such as `host.example.com`.
HSMModulePath	Windows	Tanium Server (local)	Add this setting if you use a hardware security module (HSM) to manage the Tanium root keys and message-signing keys. The value must be the directory path of the HSM vendor-specific PKCS #11 module, such as `C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll`. For more information, see Tanium Core Platform User Guide for Windows Deployments: Securing keys with an HSM.
hub_hot_cache_limit_in_MB	Appliance Windows	Zone Server Hub	Specify the maximum storage space in megabytes for the Zone Server Hub cache. The default is 0 (20% of disk space). This setting applies only if the Hub is installed on a dedicated host instead of on the Tanium Server host and you enabled file caching on the Hub (set the EnableFileCache on page 771 setting value to `1`). On Console, add this setting with the **Type** set to **Server**. For more information, see Tanium Core Platform User Guide for Windows Deployments: Manage Zone Server caching.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
HubPriorityList	Appliance Windows	Zone Server	Add this setting on the Zone Server to specify the FQDN or IP address of the preferred Zone Server Hub for sending Tanium Client content (such as sensor definitions, configuration information, and action package files) to the Zone Server. As long as that Hub is available, the Zone Server does not receive content from any other Hub. If the preferred Hub goes down, the Zone Server fails over to receiving content from any other available Hub. Typically you use this setting for active-active deployments that have pairs of Zone Servers and Hubs, where each Hub connects to each Zone Server.  BEST PRACTICE In active-active deployments, add HubPriorityList to ensure that each Zone Server receives content from its closest Hub. Configuring this setting also optimizes Hub usage by ensuring that each Hub serves one Zone Server instead of one Hub servicing both Zone Servers. For more information, see Tanium Core Platform User Guide for Windows Deployments: Zone Server High Availability.
Keys.<*key*>.HSMPassword	Windows	Tanium Server (local)	If you use an HSM to manage the Tanium root keys and message-signing keys, add this setting for each key that the HSM manages. The value must be the PIN that is associated with the token that contains the key. Replace the <*key*> variable with the Tanium key that the HSM manages: `Root` or `MessageSigning`. When the Tanium Server performs key operations, it uses HSMPassword to authenticate to the token that contains the key. For more information, see Tanium Core Platform User Guide for Windows Deployments: Securing keys with an HSM.
Keys.<*key*>.HSMTokenID	Windows	Tanium Server (local)	If you use an HSM to manage the Tanium root keys and message-signing keys, add this setting for each key that the HSM manages. Enter the token ID and replace the <*key*> variable with the Tanium key that the HSM manages: `Root` or `MessageSigning`. The Tanium Server uses HSMTokenID to identify the token that contains the key. Alternatively, you can configure the Keys.<key>.HSMTokenName on page 775. For more information, see Tanium Core Platform User Guide for Windows Deployments: Securing keys with an HSM.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
Keys.<*key*>.HSMTokenName	Windows	Tanium Server (local)	If you use an HSM to manage the Tanium root keys and message-signing keys, add this setting for each key that the HSM manages. Enter the token name and replace the <*key*> variable with the Tanium key that the HSM manages: `Root` or `MessageSigning`. The Tanium Server uses HSMTokenName to identify the token that contains the key. Alternatively, you can configure the Keys.<key>.HSMTokenID on page 774. For more information, see Tanium Core Platform User Guide for Windows Deployments: Securing keys with an HSM.
Keys.<*key*>.UseHSM	Windows	Tanium Server (local)	If you use an HSM to manage the Tanium root keys and message-signing keys, add this setting for each key that the HSM manages. Replace the <*key*> variable with the Tanium key that the HSM manages: `Root` or `MessageSigning`. Setting the value to `1` forces the Tanium Server to generate the keys on the HSM instead of locally. Setting the value to `0` disables the integration between the Server and HSM. For more information, see Tanium Core Platform User Guide for Windows Deployments: Securing keys with an HSM.
LastGoodServerName	Appliance Windows	Tanium Client	This setting exists only on the Tanium Client and indicates the name of the Tanium Server or Zone Server with which the Client last connected successfully. If the Client cannot reach a server that the ServerNameList on page 790 or ServerName on page 789 setting specifies, the Client tries to connect to the server that LastGoodServerName specifies. You do not configure LastGoodServerName; the Client configures it automatically. For more information, see Tanium Client Management User Guide: LastGoodServerName. TIP To avoid this fallback behavior during testing, troubleshooting, or migration scenarios, delete the LastGoodServerName value.
LastInstall	Appliance Windows	Tanium Client	Do not edit this setting, which exists only on the Tanium Client and indicates the date and time of the latest Client installation.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
ldap_page_size	Appliance Windows	Tanium Server	Specify the number of objects that the Tanium Server requests per page when it retrieves users and groups from an LDAP server during synchronization. This setting applies only to Active Directory connections. Paged queries enable synchronization to return more objects than the Active Directory per-search limit (1000 objects by default) allows in a single search. The value `0` disables paging. On the Tanium Appliance, the default is `0`. Specify a value lower than `1000`. IMPORTANT If you change this setting, you must restart the Tanium Server: • **Tanium Appliance**: For more information, see Tanium Appliance User Guide: Start, stop, and restart Tanium services. • **Windows Server**: For more information, see Tanium Core Platform User Guide for Windows Deployments: Manage Windows services for core platform servers.
ListenPort	Appliance Windows	Tanium Client	Specify the port on which the Client listens for communications from peer Clients. The default is `17472`. However, if you install the Client on the Tanium Server or Zone Server (Windows deployment only), the default port is `17473`. If you enable the EnableRandomListeningPort on page 771 setting, do not configure ListenPort because the Client overwrites the value whenever it selects a new port. NOTE Changes to ListenPort automatically affect the Tanium Client API port, which is one port number higher. For example, if you set ListenPort to `17473`, the Client API port becomes `17474`. ListenPort overrides the ServerPort on page 791 setting for Client-Client communication.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
LogFileSize	Appliance Windows	Tanium Client	Specify the size threshold in bytes that Tanium Client logs must reach before the Client rotates them. For more information, see Tanium Client Management User Guide: Review Tanium Client logs to troubleshoot connections and other Client issues.
LogVerbosityLevel	Appliance Windows	Tanium Server (local) Module Server Zone Server TDownloader Tanium Client	Specify the logging level as a decimal value on the Tanium Client, Tanium Server, Module Server, or Zone Server. On the Tanium Server and Module Server, you can configure the logging level separately for TDownloader. For best practices and configuration, see Tanium Appliance User Guide: Reviewing logs and troubleshooting Tanium Core Platform or Tanium Core Platform User Guide for Windows Deployments: Reviewing logs and troubleshooting Tanium Core Platform. NOTE By default, this setting is not present on Tanium Clients unless you set the logging level when deploying Clients. TIP If you deploy an action to configure this setting on Tanium Clients, use the **Set Windows Tanium Client Logging Level** or **Set Tanium Client Logging Level [Non-Windows]** package. BEST PRACTICE On Tanium Clients that run on virtual desktop infrastructure (VDI) endpoints or endpoints with limited resources, leave this setting at the default value of 1 to minimize disk writes. Do not disable logging. For more information, see Tanium Client Management User Guide: Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
Logs.extensions.LogVerbosityLevel	Appliance Windows	Tanium Client	Specify the logging level for client extensions (such as the Tanium™ Client Recorder Extension and Tanium™ Index) on an endpoint. For more information, see • Tanium Appliance User Guide: Logging levels • Tanium Core Platform User Guide for Windows Deployments: Logging levels. BEST PRACTICE On VDI endpoints or endpoints with limited resources, leave this setting at the default value of 11 to minimize disk writes. Do not disable logging. For more information, see Tanium Client Management User Guide: Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources.
max_console_idle_seconds	Appliance Windows	Tanium Server	Specify the maximum time that Tanium Console users can specify in their user preferences for the inactivity timeout. When a user is inactive on Console for longer than the timeout period, Console ends the user session. The default maximum is 3,600 seconds (60 minutes). If the user preference is less than the platform setting, the Tanium Server applies the user preference. For more information, see Suspend console automatically if no activity detected for on page 156.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
MaxAgeMultiplier	Appliance Windows	Tanium Client	Each sensor has a Max Sensor Age on page 428 attribute that determines how long the Tanium Client caches sensor results for subsequent questions that include the same sensor. MaxAgeMultiplier multiplies the maximum age that is configured for each sensor by the specified value. The default value is `1`, which specifies the unmodified age value of the **Max Sensor Age** attribute.  On Tanium Clients that run on VDI endpoints or endpoints with limited resources, set the value to `2` to double the duration for caching the results of each sensor and thereby reduce sensor executions. For more information, see Tanium Client Management User Guide: Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources.
MinDistributeOverTimeInSeconds	Appliance Windows	Tanium Client	Each action has a Distribute Over on page 396 attribute that randomizes the distribution of that action to Clients over the specified time. MinDistributeOverTimeInSeconds forces all actions to distribute over a minimum time period. The default `0` specifies no minimum, and therefore some actions might distribute immediately.  On Tanium Clients that run on VDI endpoints or endpoints with limited resources, set the value to `60` to force all actions to distribute over at least 1 minute. For more information, see Tanium Client Management User Guide: Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources.
ModuleServer	Appliance Windows	Tanium Server (local)	This setting specifies the IP address or FQDN of the Module Server. It is set automatically when the Module Server registers with the Tanium Server during installation. Contact Tanium Support on page 724 before editing this setting.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
ModuleServerPort	Appliance Windows	Tanium Server (local)	This setting specifies the Module Server port (default `17477`) for traffic from the Tanium Server. The port is set automatically when the Module Server registers with the Tanium Server during installation. Contact Tanium Support on page 724 before editing this setting.
Path	Windows	All Tanium Core Platform servers Tanium Client (Windows)	This setting indicates the installation directory of the platform server or Tanium Client: • **Servers**: You configure the path when completing the server installation wizard. For more information, see Tanium Core Platform Deployment Guide for Windows. • **Clients**: If you do not specify a path, the Client assumes the default path for the OS. TIP For Linux, Solaris, and AIX Clients, you can use symbolic links. For more information, see the following tasks in the Tanium Client Management User Guide: • Move an existing installation of the Tanium Client on Linux • Move an existing installation of the Tanium Client on Solaris • Move an existing installation of the Tanium Client on AIX
PeerNeighborhood	Appliance Windows	Tanium Client	Specify Clients that are allowed to peer with one another regardless of the NAT IP of each Client. For more information, see Tanium Client Management User Guide: Define intentional subnets using the PeerNeighborhood Client setting.
PGDLLPath	Windows	Tanium Server	This setting indicates the directory path of the PostgreSQL Server libraries. The path is set automatically during Tanium Server installation. Contact Tanium Support on page 724 before editing this setting.
PGRoot	Windows	Tanium Server	This setting indicates the directory path of the PostgreSQL installation. The path is set automatically during Tanium Server installation. Contact Tanium Support on page 724 before editing this setting.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
pki_client_tls_ca_key_duration_days	Appliance Windows	Tanium Server	Enter the validity period for the key pair that the Zone Server or Tanium Server uses to provide digital signatures for Tanium Clients when they generate new TLS key pairs. The default is 180 days. For more information, see Securing Tanium connections and operations through digital keys on page 209.
pki_client_tls_ca_key_renewal_window_hours	Appliance Windows	Tanium Server	Enter the renewal window for the key pair that the Zone Server or Tanium Server uses to provide digital signatures for Tanium Clients when they generate new TLS key pairs. The default is 168 hours (7 days). For more information, see Securing Tanium connections and operations through digital keys on page 209.
pki_client_tls_key_duration_days	Appliance Windows	Tanium Server	Enter the validity period for the key pairs that Tanium Clients use for TLS communication with each other and with the Zone Server or Tanium Server. The default is 7 days. For more information, see Securing Tanium connections and operations through digital keys on page 209.
pki_hub_tls_key_duration_days	Appliance Windows	Tanium Server	Enter the validity period for the key pair that the Zone Server Hub uses for TLS communication with the Tanium Server and Zone Server. The default is 60 days. For more information, see Securing Tanium connections and operations through digital keys on page 209.
pki_hub_tls_key_renewal_window_hours	Appliance Windows	Tanium Server	Enter the renewal window for the key pair that the Zone Server Hub uses for TLS communication with the Tanium Server and Zone Server. The default is 4 hours. For more information, see Securing Tanium connections and operations through digital keys on page 209.
pki_message_signing_key_duration_days	Appliance Windows	Tanium Server	Enter the validity period for the key pair that the Tanium Server uses to sign messages (such as for action packages) that it sends to Tanium Clients. The default is 180 days. For more information, see Securing Tanium connections and operations through digital keys on page 209.
pki_message_signing_key_renewal_window_hours	Appliance Windows	Tanium Server	Enter the renewal window for the key pair that the Tanium Server uses to sign messages (such as for action packages) that it sends to Tanium Clients. The default is 4 hours. For more information, see Securing Tanium connections and operations through digital keys on page 209.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
pki_server_tls_key_duration_days	Appliance Windows	Tanium Server	Enter the validity period for the key pair that the Tanium Server uses for TLS communication with another Tanium Server (in an active-active deployment), the Zone Server Hub, or Tanium Clients. The default is 60 days. For more information, see Securing Tanium connections and operations through digital keys on page 209.
pki_server_tls_key_renewal_window_hours	Appliance Windows	Tanium Server	Enter the renewal window for the key pair that the Tanium Server uses for TLS communication with another Tanium Server (in an active-active deployment), the Zone Server Hub, or Tanium Clients. The default is 4 hours. For more information, see Securing Tanium connections and operations through digital keys on page 209.
pki_zoneserver_tls_key_duration_days	Appliance Windows	Tanium Server	Enter the validity period for the key pair that the Zone Server uses for TLS communication with the Zone Server Hub and Tanium Clients. The default is 60 days. For more information, see Securing Tanium connections and operations through digital keys on page 209.
pki_zoneserver_tls_key_renewal_window_hours	Appliance Windows	Tanium Server	Enter the renewal window for the key pair that the Zone Server uses for TLS communication with the Zone Server Hub and Tanium Clients. The default is 4 hours. For more information, see Securing Tanium connections and operations through digital keys on page 209.
PKIClientTLSKeyRenewalWindowHours		Tanium Server	Enter the renewal window for the key pairs that Tanium Clients use for TLS communication with each other and with the Zone Server or Tanium Server. The default is 4 hours. For more information, see Securing Tanium connections and operations through digital keys on page 209.
PKIDatabasePassword	Appliance Windows	Tanium Server (local)	Specify a password to encrypt the root keys that the Tanium Server stores in the `pki.db` file. For more information, see Encrypt the root keys database on page 217.
prompt_estimate_threshold	Appliance Windows	Tanium Server	Action deployment and approval workflows prompt users to enter the estimated number of targeted endpoints when the estimate exceeds the threshold. The default threshold is `100` endpoints. The value `0` specifies that action issuers and approvers must enter the estimate for all actions regardless of the estimate count. For more information, see Administrative setup for actions on page 328.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
ProxyAutoConfigAddress	Appliance Windows	Tanium Client (Windows)	Specify the URL and file name of a proxy auto configuration (PAC) file that the Tanium Client can access. The format `http[s]://<PAC file URL>/<PAC file name>.pac`. The PAC file defines how Clients connect to the Tanium Server or Zone Server: directly or through a Hypertext Transfer Protocol Secure (HTTPS) proxy server. The Client downloads the file from the URL that you specify and runs a script that the file contains to select the correct proxy for connecting to a particular server. If no proxy is available, the Client falls back to connecting directly with the Tanium Server or Zone Server. For more information, see Tanium Client Management User Guide: Configure proxy connections with a PAC file.
ProxyPassword	Appliance Windows	Tanium Server Module Server TDownloader	For a proxy server that requires authentication, enter the password of the ProxyUserid on page 785 user that establishes a connection with the proxy server. Configure this setting according to the Tanium infrastructure and Tanium Core Platform server type: • **Tanium Appliance**: ProxyPassword is a TDownloader setting on the Tanium Server and Module Server. • **Windows**: ProxyPassword is a Tanium Server and Module Server setting. For more information, see Configuring Internet access through proxy servers on page 181.
ProxyPort	Appliance Windows	Tanium Server Module Server TDownloader	Configure the proxy server listening port according to the Tanium infrastructure and Tanium Core Platform server type: • **Tanium Appliance**: ProxyPort is a TDownloader setting on the Tanium Server and Module Server. • **Windows**: ProxyPort is a Tanium Server and Module Server setting. For more information, see Configuring Internet access through proxy servers on page 181.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
ProxyServer	Appliance Windows	Tanium Server Module Server TDownloader	Configure the IP address of the proxy server according to the Tanium infrastructure and Tanium Core Platform server type: • **Tanium Appliance**: ProxyServer is a TDownloader setting on the Tanium Server and Module Server. • **Windows**: ProxyServer is a Tanium Server and Module Server setting. For more information, see Configuring Internet access through proxy servers on page 181. NOTE By default, the proxy server address is resolved as an IPv4 address. If the proxy server has an IPv6 address, you must enter it within brackets (for example, `[2001:db8::1]`) and configure the TDownloader setting ForceIPV6 on page 772 to `1`.
ProxyServers	Appliance Windows	Tanium Client	If Clients connect to the Tanium Server or Zone Server through an HTTPS proxy server, specify the IP address or FQDN, and port number, of the proxy server. You can specify multiple proxies as a comma-separated list in the format `"<proxy1>:<port>,...,<proxyN>:<port>"`. The Client tries to connect to the proxies in the order that you list them. After any single connection succeeds, the Client stops trying to connect with more proxies. If no proxy is available, the Client falls back to connecting directly with the Tanium Server or Zone Server. For more information, see Tanium Client Management User Guide: Configure specific proxy servers during Client deployment.
ProxyType	Appliance Windows	Tanium Server Module Server TDownloader	Specify the type of proxy server authentication according to the Tanium infrastructure and Tanium Core Platform server type: • **Tanium Appliance**: ProxyType is a TDownloader setting on the Tanium Server and Module Server. The possible values are `Basic`, `NTLM`, or `None`. • **Windows**: ProxyType is a Tanium Server and Module Server setting. The possible values are `Basic` or `NTLM`. For more information, see Configuring Internet access through proxy servers on page 181.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
ProxyUserid	Appliance Windows	Tanium Server Module Server TDownloader	For a proxy server that requires authentication, specify the user ID of the account that establishes a connection with the proxy server. Configure this setting according to the Tanium infrastructure and Tanium Core Platform server type: • **Tanium Appliance**: ProxyUserid is a TDownloader setting on the Tanium Server and Module Server. • **Windows**: ProxyUserid is a Tanium Server and Module Server setting. For more information, see Configuring Internet access through proxy servers on page 181.
RandomListeningPortExclusions	Appliance Windows	Tanium Client	Specify the ports that the Client never selects as a listening port if you enable the EnableRandomListeningPort on page 771 setting. For example, to prevent port competition conflicts, you might specify ports that other applications use. If you specify multiple exclusions, use a comma to separate each port. By default, the Client does not exclude any ports that are within the range that the RandomListeningPortMin on page 785 and RandomListeningPortMax on page 785 settings define.
RandomListeningPortMax	Appliance Windows	Tanium Client	Specify the high end of the range of ports from which the Client randomly selects a listening port if you enabled the EnableRandomListeningPort on page 771 setting. The default is port `64000`.
RandomListeningPortMin	Appliance Windows	Tanium Client	Specify the low end of the range of ports from which the Client randomly selects a listening port if you enabled the EnableRandomListeningPort on page 771 setting. The default is port `32000`.
RandomListeningPortTTLInHours	Appliance Windows	Tanium Client	Specify the interval in hours at which the Client selects a new listening port if you enabled the EnableRandomListeningPort on page 771 setting. The default is `24` hours. Do not set the value lower than the Client reset interval, which is a random interval typically in the range of 2 to 6 hours.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
RandomSensorDelayInSeconds	Appliance Windows	Tanium Client	This setting delays the execution of any sensor by a random time up to the specified value in seconds. The delay reduces concurrent execution of sensors and packages. The default value `0` specifies that sensors run immediately.  On Tanium Clients that run on VDI endpoints or endpoints with limited resources, set the delay to `5` seconds. If these endpoints experience poor performance, you can increase this value incrementally up to `20`. For more information, see Tanium Client Management User Guide: Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources.
RegistrationCount	Appliance Windows	Tanium Client	Do not edit this setting, which exists only on the Tanium Client and indicates the number of completed registrations. RegistrationCount, in conjunction with the ComputerID on page 769 setting, enables the Tanium Server to detect duplicate Computer IDs. If the RegistrationCount value that the Server maintains does not match the value that the Client reports, the Server assigns a new, unique ComputerID to the endpoint to resolve the apparent ComputerID duplication. For more information, see Tanium Client Management User Guide: Registration and ComputerID.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
ReportingTLSMode	Appliance	Tanium Server Tanium Client 7.2	This setting applies only to Client 7.2, which Tanium release 2026H1 or later does not support. Upgrade any Client 7.2 installations to a new Client version as described in Tanium Client Management User Guide: Upgrading Tanium Clients. For any Clients 7.2 that you have not finished upgrading, the setting sets the mode for TLS connections from the Tanium Client to the Tanium Server or Zone Server. The values are: • `0` (TLS not used): TLS is disabled. This is the default value. • `1` (TLS required): If a TLS handshake fails, the Client cannot register or communicate with the Tanium Server or Zone Server. • `2` (TLS optional): The Client tries to connect over TLS. If the TLS connection fails, the Client tries a non-TLS connection.  BEST PRACTICE If you will use TLS, initially setting the value to `2` is a best practice. After you confirm that Clients establish TLS connections reliably, setting the value to `1` will enforce the best security. For more information, see Tanium Appliance User Guide: Securing Tanium Server, Zone Server, and Tanium Client access or Tanium Core Platform User Guide for Windows Deployments: Securing Tanium Server, Zone Server, and Tanium Client access.
require_action_approval	Appliance Windows	Tanium Server	Enable (`1`) or disable (default `0`) the requirement for action approval. If you enable the setting, a user other than the action issuer must approve the action before the Tanium Server deploys it. For more information, see Enable or disable action approval on page 412.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
require_client_tls_314_flag	Appliance Windows	Tanium Server	This setting applies only to Client 7.2, which Tanium release 2026H1 or later does not support. Upgrade any Client 7.2 installations to a new Client version as described in Tanium Client Management User Guide: Upgrading Tanium Clients. For any Clients 7.2 that you have not finished upgrading, the setting values are: • `0` (default): The Tanium Server allows both TLS and non-TLS connections from endpoints with Tanium Client 7.2. • `1`: The Tanium Server allows connections from endpoints with Tanium Client 7.2 only if TLS is used. Do not set the value to `1` until you are sure that all 7.2 Clients that have been deployed are configured to use TLS and you are ready to deploy the 7.2 Client to new endpoints with TLS configured before initial registration.
require_client_tls_315_flag	Appliance Windows	Tanium Server	Specify one of the following values: • `1` (default): The Tanium Server allows connections from endpoints with Tanium Client 7.6 or later only if TLS is used. Tanium strongly recommends that you leave the value at `1`. • `0`: The Tanium Server allows both TLS and non-TLS connections from endpoints with Tanium Client 7.6 or later. Contact Tanium Support on page 724 before setting the value to `0`. For more information, see Tanium Appliance User Guide: Securing Tanium Server, Zone Server, and Tanium Client access or Tanium Core Platform User Guide for Windows Deployments: Securing Tanium Server, Zone Server, and Tanium Client access.
Resolver	Appliance Windows	Tanium Client (non-Windows)	Specify the program to invoke for resolving the IP address of the Tanium Server. The default is `getent`. For AIX and Solaris, set this to `nslookup`. The options are `getent`, `getenta`, `host`, `nslookup`, `dig`, and `res_search`.
restricted_targeting_recommended_configs	Appliance Windows	Tanium Server	Set the value to `1` to make action groups target the **No Computers** computer group during initial configuration of Tanium solutions. The default is `0`, which specifies that action groups target the computer groups that are specified in their default configuration. Changes to this setting affect only solutions that you subsequently add, not solutions that are already configured. For more information, see Tools deployment and restricted targeting on page 121.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
SaveClientStateIntervalInSeconds	Appliance Windows	Tanium Client	Specify the interval (in seconds) at which Client state is written to disk. The default is `300`, which is every 5 minutes. BEST PRACTICE On Tanium Clients that run on VDI endpoints or endpoints with limited resources, set the value to `1800` (every 30 minutes) to reduce disk writes. For more information, see Tanium Client Management User Guide: Tuning Tanium Client settings for VDI endpoints and other endpoints with limited resources.
ServerName	Appliance Windows	Tanium Server Module Server Tanium Client	On the Tanium Server or Module Server, specify the network adapter binding that the server uses to listen for IPv4 Client registrations. By default, this setting is hidden and has a value of `0.0.0.0`, which specifies binding to all network adapters. Contact Tanium Support on page 724 for guidance before changing this setting. NOTE Do not specify a value for this setting on the Zone Server, where the setting is deprecated. On the Tanium Client, specify the FQDN or IP address of the Tanium Server or Zone Server with which the Client tries to connect. For more information, see Tanium Client Management User Guide: ServerName. TIP If you deploy an action to configure this setting on the Client, use the **Set Tanium Server Name** or **Set Tanium Server Name [Non-Windows]** package.
ServerNameIPv6	Appliance Windows	Tanium Server Module Server	By default, this setting is hidden and has a value of `[::]`, which specifies that the server binds to all network adapters to listen for IPv6 Client registrations. To bind to a specific network adapter, add the setting and enter the IPv6 address of the adapter within square brackets (for example, `[2001:db8::1]`). Contact Tanium Support on page 724 for guidance before adding this setting.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
ServerNameList	Appliance Windows	Tanium Client	Specify a comma-separated list of Tanium Server and Zone Server FQDNs or IP addresses with which the Client can try to connect. For more information, see Tanium Client Management User Guide: ServerNameList. TIP If you deploy an action to configure this setting on the Client, use the **Set Tanium Server Name List** or **Set Tanium Server Name List [Non-Windows]** package.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
ServerPort	Appliance Windows	Tanium Server (local) Module Server Zone Server Tanium Client	On Tanium Core Platform servers, the ServerPort is set during server installation. Update this setting if necessary according to the Tanium infrastructure: • **Tanium Appliance**: For the steps to update the port on an Appliance, see Tanium Appliance User Guide: Manage Tanium Core Platform settings. You can update the following ports: ◦ **Tanium Server**: Specify the port on which the Server listens for Tanium Clients. The default is `17472`. Do not change ServerPort in the `TaniumServer.ini` configuration file. ◦ **Module Server**: Specify the port for traffic from the Tanium Server. The default is `17477`. ◦ **Zone Server Hub**: Specify the inbound port for traffic from the Tanium Server and Zone Server. The default is `17472`. • **Windows**: ◦ **Tanium Server**: This is the port on which the Server listens for Tanium Clients. The default is `17472`. You configure ServerPort when completing the Server installation wizard. For more information, see Tanium Core Platform User Guide for Windows Deployments: Install the Tanium Server. ◦ **Module Server**: Specify the port for traffic from the Tanium Server. The default is `17477`. You configure ServerPort when completing the Module Server installation wizard. For more information, see Tanium Core Platform User Guide for Windows Deployments: Installing the Module Server. ◦ **Zone Server Hub**: Specify the inbound port for traffic from the Tanium Server and Zone Server. The default is `17472`. You configure ServerPort when completing the Hub installation wizard. For more information, see Tanium Core Platform User Guide for Windows Deployments: Installing the Zone Server. NOTE For more information, see ZoneServerPort on page 798 and ZoneServerPortForHub on page 798. On the Tanium Client, the ServerPort is set during Client installation. It specifies the port to use for communication between Clients and between Clients and Tanium Core Platform servers. The default is 17472. If you need to update the port, see Tanium Client Management User Guide: ServerPort.

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
ServerSOAPPort	Appliance Windows	Tanium Server (local)	Specify the port for Tanium Console and the SOAP API. The default value depends on your Tanium infrastructure: • **Appliance**: The default is `8443`. Port `443` redirects to this `8443`. • **Windows**: The default is `443`. You specify the port when completing the Tanium Server installation wizard. For more information, see Tanium Core Platform User Guide for Windows Deployments: Install the Tanium Server.
ServiceUserDomain	Windows	Zone Server Zone Server Hub	This is a setting on the Zone Server and Zone Server Hub. The Windows service for the Zone Server or Hub runs in the context of a service account. You configure the domain when completing the installation wizard. For more information, see Tanium Core Platform User Guide for Windows Deployments: Installing the Zone Server.
ServiceUserName	Windows	Zone Server Zone Server Hub	This is a setting on the Zone Server and Zone Server Hub. The Windows service for the Zone Server or Hub runs in the context of a service account. You configure the user name when completing the installation wizard. For more information, see Tanium Core Platform User Guide for Windows Deployments: Installing the Zone Server.
site_throttles_use_local_ip	Appliance Windows	Tanium Server	If you define sites for bandwidth throttling, specify how Tanium Servers and Zone Servers treat the IP addresses: • `0` (default): Network Address Translation (NAT) IP addresses • `1`: Local IP addresses For more information, see Base throttles on local or NAT IP addresses on page 192.
soap_enable_local_auth	Windows	Tanium Server	Enable (`1`) or disable (`0`) Tanium Console access for user accounts that are local to the Tanium Server. For more information, see Local users on a Windows server on page 642.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
SQLConnectionString	Appliance Windows	Tanium Server (local)	Specify connection information for the Tanium database server, such as in the following examples: • **Appliance**: `postgres:<server IP address>@user=postgres dbname=tanium sslmode=require sslcert=/opt/Tanium/.postgresql/postgresql.crt sslkey=/opt/Tanium/.postgresql/postgresql.key sslcompression=1` • **Windows**: ◦ **MSSQL**: `SQL1\SQLEXPRESS@tanium` ◦ **PostgreSQL**: `postgres:<server IP address>@user=postgres dbname=tanium sslmode=require sslcert=/Program Files/Tanium/.postgresql/postgresql.crt sslkey=/Program Files/Tanium/.postgresql/postgresql.key sslcompression=1` For more information, see the PostgreSQL documentation for the supported PostgreSQL keywords, such as `dbname`, `port`, and `user`. IMPORTANT If you change this setting, you must restart the Tanium Server: • **Tanium Appliance**: For more information, see Tanium Appliance User Guide: Start, stop, and restart Tanium services. • **Windows Server**: For more information, see Tanium Core Platform User Guide for Windows Deployments: Manage Windows services for core platform servers.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
SSLCipherSuite	Appliance Windows	Tanium Server (local)	Specify the cipher suites to use for TLS connections to the Tanium Server from the Module Server or the systems of Tanium Console users. The default is: `TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384` For more information, see: • Tanium Appliance User Guide: Securing Tanium Server, Zone Server, and Tanium Client access • Tanium Core Platform User Guide for Windows Deployments: Securing Tanium Server, Zone Server, and Tanium Client access.
SSLHonorCipherOrder	Appliance Windows	Tanium Server (local)	When the Tanium Server and Tanium Client determine a mutual set of supported ciphers, the Client normally selects which cipher to use. However, if you set SSLHonorCipherOrder to `1`, the Server selects a mutually supported cipher based on the SSLCipherSuite on page 794 setting. The Server applies an order of preference from left to right when selecting from the ciphers that SSLCipherSuite lists . For more information, see Tanium Appliance User Guide: Securing Tanium Server, Zone Server, and Tanium Client access or Tanium Core Platform User Guide for Windows Deployments: Securing Tanium Server, Zone Server, and Tanium Client access.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
StateProtectedFlag	Appliance Windows	Tanium Client	Enable (`1`) or disable (`0`) encryption of the Client state and sensor queries that are stored on the Client. NOTE By default, read access to the Tanium Client installation directory is restricted for non-Administrators. However, encrypting the Client state and sensor queries can provide additional protection. For more information, see Tanium Client Management User Guide: Harden the Tanium Client on Windows.
tds_disable_registration_check	Appliance Windows	Tanium Server	When you register a sensor with Tanium Data Service (TDS), the Service checks the cardinality of the sensor results, in terms of the typical number of unique values versus duplicate values in the results from a set of endpoints. After the service checks the cardinality, a message indicates if you can register the sensor or if the service blocks registration due to high cardinality. Tanium recommends that you do not disable the cardinality check because high cardinality sensors can negatively impact Tanium Server performance. Contact Tanium Support on page 724 for guidance before you set tds_disable_registration_check to `1` to disable the cardinality check. The default value `0` specifies that the cardinality check is enabled. For more information, see Tanium Interact User Guide: Resource consumption for registered sensors.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
TrustedHostList	Appliance Windows	Tanium Server (local) Module Server TDownloader	By default, the Tanium Server and Module Server validate the SSL/TLS certificate of remote servers when establishing connections to them (such as for downloading files). To bypass certificate validation for specific servers, enter their FQDN or IP address. You do not have to enter 127.0.0.1, localhost, the Tanium Module Server, or Tanium Servers (standalone or active-active). Wildcards are supported. You must enter IPv6 addresses within square brackets (for example, `[2001:db8::1]`). Configure this setting according to the Tanium infrastructure: • **Tanium Appliance**: TrustedHostList is a TDownloader setting on the Tanium Server and Module Server. • **Windows**: TrustedHostList is a Tanium Server and Module Server setting. For more information, see Configuring Internet access through proxy servers on page 181.
user_auto_provision_group_id	Appliance Windows	Tanium Server	Specify a user group to automatically assign to new users in your remote identity store. Changes to the setting do not apply to existing users. The default user group applies only to users who authenticate through SAML and are not synchronized with an LDAP server. By default, no default user group is selected. For more information, see Set the default user group on page 652.
Version	Appliance Windows	Tanium Server (local) Module Server Zone Server Zone Server Hub Tanium Client	Do not edit this setting, which indicates the server, Hub, or Client version.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
zs_address_mask	Appliance Windows	Tanium Server Zone Server	In IPv4 subnets where Tanium Clients register with a Zone Server, this setting governs the network proximity of Client peers to prevent suboptimal peer connections. The Zone Server receives the setting from the Tanium Server with a default value that limits peering to neighbors that share the same 24-bit address mask. If necessary, you can override the platform setting by configuring the AddressMask on page 766 setting locally on each Zone Server. When each Client registers with the Zone Server, the Server sends the Client a neighborhood list that adheres to the zs_address_mask (or local AddressMask) boundary. This setting uses the same values as the AddressMask setting.
zs_address_prefix_ipv6	Appliance Windows	Tanium Server Zone Server	In IPv6 subnets where Tanium Clients register with a Zone Server, this setting governs the network proximity of Client peers to prevent suboptimal peer connections. The Zone Server receives the setting from the Tanium Server. The default value is 0, which specifies no peering. If necessary, you can override the platform setting by configuring the AddressPrefixIPv6 on page 766 setting locally on each Zone Server. When each Client registers with the Zone Server, the Zone Server sends the Client a neighborhood list that adheres to the zs_address_prefix_ipv6 (or local AddressPrefixIPv6) boundary. Contact Tanium Support on page 724 to determine the optimum value for peering in IPv6 networks.
ZoneHubFlag	Appliance Windows	Zone Server Zone Server Hub	On the host where you install an instance of the Zone Server or Zone Server Hub, this setting indicates whether the current instance is (`1`) or is not (`0`) a Hub. View this setting according to the Tanium infrastructure: • **Tanium Appliance**: View the setting through the TanOS console. For more information, see Tanium Appliance User Guide: Reference: Deployment-related Tanium Core Platform settings or Tanium Core Platform User Guide for Windows Deployments: Reference: Deployment-related Tanium Core Platform settings. • **Windows**: View the setting through the CLI. For more information, see Tanium Appliance User Guide: Reference: Tanium Core Platform command-line interface or Tanium Core Platform User Guide for Windows Deployments: Reference: Command-line interface.

© 2026 Tanium Inc. All Rights Reserved

Tanium Core Platform settings (continued)

Settings	Infrastructure	Platform components	Guidelines
zs_hot_cache_limit_in_MB	Windows	Zone Server	This setting applies only if the Zone Server Hub is installed on a dedicated host instead of on the Tanium Server host and file caching is enabled on the Hub through the EnableFileCache on page 771 setting. You can configure zs_hot_cache_limit_in_MB to specify the maximum storage space in megabytes for the Hub cache. By default, zs_hot_cache_limit_in_MB is hidden and has a value of `0` (20% of disk space). On Tanium Console, manually add zs_hot_cache_limit_in_MB as a server setting. For more information, see Tanium Core Platform User Guide for Windows Deployments: Manage caching on the Zone Server and Zone Server Hub.
ZoneServerPort	Windows	Zone Server	On the Zone Server, configure the incoming port (default `17472`) for traffic from Tanium Clients. For more information, see Tanium Core Platform User Guide for Windows Deployments: Configure ports for traffic from Zone Server Hubs and Tanium Clients.
ZoneServerPortForHub	Windows	Zone Server	On the Zone Server, configure the incoming port (default `17472`) for traffic from Zone Server Hubs. For more information, see Tanium Core Platform User Guide for Windows Deployments: Configure ports for traffic from Zone Server Hubs and Tanium Clients.

© 2026 Tanium Inc. All Rights Reserved