Tanium Appliance User Guide

2026H2 Semiannual Release

Version 1.9.1

November 17, 2026



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

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

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

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

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

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

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

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

©2026 Tanium Inc. All Rights Reserved

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

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

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

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

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

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

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

© 2026 Tanium Inc. All rights reserved.

Table of contents

Overview 24
- Tanium Appliance types 25
- Appliance roles 25
- Topology 26
- TanOS menus 27

Requirements 28
- Tanium Appliance specifications 28
- Compatibility among components in a Tanium release 28
  - Tanium Appliance software versions 28
  - Tanium™ Semiannual Release 2026H2 28
  - Maintenance releases 29
  - Upgrade process 29
    - Upgrading the Tanium Endpoint Configuration Toolset and Tanium Client 30
- SSL certificates 31
- Tanium Appliance Array 31
- Network connectivity and firewall 32
- Internet access (direct or by proxy) 39
  - Internet URLs 39
    - Solution-specific internet URLs 39
  - Proxies 40
  - Air gap 40

Getting started 41
- Step 1: Prepare your environment 41
  - (Physical Tanium Appliance) Install and configure the Appliance 41
  - (cloud-based Tanium Appliance) Set up the environment for the Appliance 41
- Step 2: Complete the initial setup 41
- Step 3: Set up an Appliance Array 42
- Step 4: Verify the installation 42

©2026 Tanium Inc. All Rights Reserved

Step 5: Configure monitoring 42

Installing a physical Tanium Appliance in a datacenter 43
Contents of the box 43
What you need to provide 44
Information tag 44
Physical connections 45
Small/Medium (v4) 45
Small/medium (v3) 46
Large/extra-large (v4) 46
Large/extra-large (v3) 48
Installation and bootstrap configuration 49
Install and connect the Tanium Appliance 49
Power on the Appliance and configure the iDRAC interface 50
(Optional) Configure the Appliance IP address 54

Performing initial configuration of Tanium Appliances 60
Initial setup (physical Tanium Appliance) 60
Install and configure physical Tanium Appliances 60
(FIPS-compliant organizations) Enable FIPSStandard mode before initial setup 61
Configuration options 62
Configure iDRAC 62
Before you begin 62
Configure the iDRAC 62
Configure IP address only 66
Perform full initial configuration 71
Before you begin 71
Complete the initial configuration 71
Access TanOS remotely 77
Configure SSH keys 78
Before you begin 79
Add and test an SSH key for the tancopy user 79
Add the SSH key for the tancopy user 79
Test the SFTP connection with the SSH key 81
Add SSH keys for other TanOS users 84
Add TanOS system users 88

©2026 Tanium Inc. All Rights Reserved

Export the Disk Encryption Key 89
Export the GRUB key 91
What to do next 93
Initial setup (virtual Tanium Appliance) 93
Requirements 93
Hypervisors and image formats 93
Virtual CPU 94
Deploy the virtual image to the hypervisor 94
(Optional) Change keyboard mapping for virtual console 96
(FIPS-compliant organizations) Enable FIPSStandard mode before initial setup 105
Configuration options 106
Perform full initial configuration 107
Before you begin 107
Complete the initial configuration 107
Configure IP address only 113
Before you begin 113
Configure the IP address settings 113
Access TanOS remotely 117
Add TanOS system users 118
Configure SSH keys 119
Before you begin 120
Add and test an SSH key for the tancopy user 120
Add the SSH key for the tancopy user 120
Test the SFTP connection with the SSH key 122
Add SSH keys for other TanOS users 125
Export the GRUB key 129
What to do next 130
Initial setup (cloud-based Tanium Appliance) 130
Requirements 130
Set up the environment for the Appliance 131
Deploy the virtual image to the cloud provider 131
Considerations for specific cloud providers 132
Microsoft Azure 132
Google Cloud Platform 132
(FIPS-compliant organizations) Enable FIPSStandard mode before initial setup 133

©2026 Tanium Inc. All Rights Reserved

Perform full initial configuration 134
Access TanOS remotely 137
Add TanOS system users 137
Configure SSH keys 139
Before you begin 139
Add and test an SSH key for the tancopy user 140
Add the SSH key for the tancopy user 140
Test the SFTP connection with the SSH key 142
Add SSH keys for other TanOS users 145
Export the GRUB key 149
What to do next 150
Configuring proxy server settings 150
Overview of proxy server connections 150
TDownloader user context 152
Tanium Console: Configure proxy settings 152
Configure proxy settings 152
Installing and managing an Appliance Array 158
Before you begin 159
(Optional) Import keys 160
Create the Array 161
Add members to the Array 162
Assign roles 165
Configuring a Tanium cluster 168
Tanium cluster requirements and limitations 169
Configuring a standby Module Server 170
Install Tanium roles 170
Before you begin 170
Install roles 171
What to do next 171
Additional management tasks for an Appliance Array 172
Promote a Tanium Server to Array Manager 172
Remove an Appliance from an Appliance Array 173
Refresh an Appliance Array 174
Reset an Appliance Array 175
Measure the data transfer rate between an Array Manager and an Array member 176

©2026 Tanium Inc. All Rights Reserved

Configuring optional components 176
Installing individual Zone Servers 176
Before you begin 177
Install the Zone Server role 178
Import the Tanium Server public key file to the Zone Server 178
Install the Zone Server hub 179
Set up AllowedHubs on the Zone Server Appliance 179
Configure trust mappings 181
Approve trust for the Zone Server Hub 181
Map the Zone Server to the Zone Server Hub 181
What to do next 182
Installing and managing a Direct Connect Zone Proxy 183
About Direct Connect Zone Proxies 183
Import and configure Direct Connect 183
Obtain the Direct Connect Zone Proxy Installer file 183
Install the Direct Connect Zone Proxy on each Zone Server Appliance 183
Check installed versions of the Direct Connect Zone Proxy 185
Upgrade the Direct Connect Zone Proxy on all Zone Server Appliances 186
Remove the Direct Connect Zone Proxy 187
Installing a Tanium All-in-One for demos 187
Before you begin 188
Install the Tanium All-in-One role 189
Before you begin 189
Install the All-in-One role 190
What to do next 191
Installing and managing a Tanium Cloud Access Point 191
Before you begin 192
Install the Tanium Cloud Access Point role 193
What to do next 194
Manage the Cloud Access Point service 194
Reconfigure a Tanium Cloud Access Point 194
Review the Cloud Access Point log 195
Verifying the installation 196
Sign in to Tanium Console 196
Upload the Tanium license 198

©2026 Tanium Inc. All Rights Reserved

Deploy the Tanium Client to your lab computers 198
Verify Tanium components in the deployment 198
Verify the basic deployment 198
Verify the Zone Server deployment 198
Verify a Tanium Cluster deployment 199

Working in an air-gapped environment 201
Overview 201
Perform initial setup of an air-gapped environment 203
Before you begin 203
Prepare a TanOS installation for an air-gapped environment 204
Complete initial setup 205
Supply a Tanium license 205
Install an Appliance Array and Tanium roles 205
Update the TrustedHostList settings on each Tanium Server 206
Update the TrustedHostList settings on each Module Server 206
Install a full update 207
Before you begin 207
Download the ZIP file 208
Install the update 208
Sign in to Tanium Console and let the Server complete the initial import 210
Import recommended content 210
Import content packs and modules 211
Update an existing air gap installation 212
Types of air gap updates 212
When to perform an update 212
Customer lab 212
Customer production 213
Before you begin 213
Install a full update to update an existing air-gapped installation 214
Install an individual update 214
Before you begin 214
Download the update file 215
Install the update 216
What to do next 218

©2026 Tanium Inc. All Rights Reserved

Update external files for individual modules ... 218
Update the Tanium Comply engine packages ... 218
Configure an alternate location for the Predefined Package Gallery in Tanium Deploy ... 219
Update Tanium Patch files ... 219
Install or update Tanium Threat Response Signals ... 219
Download the Tanium Signals file ... 220
Install or update the Tanium Signals file ... 220
View the air gap usage report ... 221
View the air gap installation log ... 222
Prune unused air gap content ... 222
Manage web server content ... 223
Before you begin ... 223
Install content ... 223
Delete content by list ... 223
Change the air gap manifest URLs ... 223
Managing TanOS users ... 225
Change the current user password ... 225
Manage SSH keys ... 227
Before you begin ... 227
Generate keys ... 228
Add authorized keys ... 229
View public keys ... 231
Configure TanOS system users ... 233
Add a system user ... 234
Disable password access ... 235
Reset a user password or enable password access ... 237
Enable or disable a system user account ... 238
Protect or unprotect a user account with the tanadmin role ... 239
Delete a system user ... 239
Edit known hosts ... 240
View history of sign in attempts ... 242
Configure global authentication requirements and MFA ... 242
Require key authentication globally ... 243
Make key authentication optional globally ... 244

©2026 Tanium Inc. All Rights Reserved

Require password authentication globally 244
Make password authentication optional globally 244
Enable global multifactor authentication 244
Disable global multifactor authentication 245
Configure individual multi-factor authentication 245
Exempt a user from global multifactor requirements 245
Configure Google Authenticator for a user 247
View user multifactor settings 249
Reset user multifactor settings 251
Configure LDAP for TanOS users 252
Manage the authentication certificate for the LDAP server 253
Option 1: Paste the LDAP server root CA certificate Contents 254
Option 2: Import the LDAP server root CA certificate file 255
Manage the imported LDAP server root CA certificate 255
Configure the LDAP server connection settings 256
Complete the walk-through configuration 256
Configure specific LDAP connection settings 257
View the LDAP connection status and query results 262
Verify that the LDAP query returns a specific user 263
Verify that the LDAP query returns a specific group 264
Export the LDAP configuration for use on another TanOS Appliance 264
Import an LDAP configuration that was exported from another TanOS Appliance 265
Enable or disable LDAP authentication 265

Managing the Tanium Core Platform 266
Secure Tanium Console, API, and Module Server access 266
Overview of certificates and keys 266
Tanium Console and API 267
Signed and encrypted SAML authentication on the Tanium Server 268
Module Server communication 269
SSL/TLS connection processes and setup tasks 270
CA-issued Tanium Server SOAP certificates 272
Certificate requirements 273
Install a custom certificate 278
Install the SOAP or SAML certificate file on a Tanium Server or the SSL certificate file on a Module Server 279

©2026 Tanium Inc. All Rights Reserved

Manually register the remote Module Server with each Tanium Server 282
Configure the Module Server on the Tanium Server 283
Enable the remote Module Server 284
Restart Tanium Server and Module Server services 287
(Optional) Enable HTTP Strict Transport Security for Tanium Console access 287
Secure Tanium Server, Zone Server, and Tanium Client access 288
Overview of TLS in the Tanium Core Platform 288
TLS communication process 290
Supported cipher suites 291
TLS options, and defaults 292
HSM integration 292
(Optional) Configure the TLS requirement for Tanium Client connections 292
Configure TLS on Tanium Clients 293
Verify the TLS connections 293
Update the TLS configuration when you make changes to key pair 294
Configure the local authentication service for Tanium Console users 294
Add a local user 295
Set a user password 296
Delete a user 298
Disable the local authentication service 298
Modify the local authentication service security policy 299
Configure smart card authentication for Tanium Console users 300
Requirements 300
Create a certificate 301
Extract the certificates 302
Create a new certificate file 304
Configure CAC 306
Step 1: Install the certificate 306
Step 2: Add the required Tanium Server configuration settings 307
Troubleshoot smart card authentication 312
Start, stop, and restart Tanium services 313
Manage Tanium Core Platform settings 314
Manage the TDownloader configuration 315
Add an authentication user for TDownloader 315
Edit TDownloader settings 316

©2026 Tanium Inc. All Rights Reserved

Add an authentication certificate for TDownloader 321
Manage additional authentication certificates 323
Zone Server isolated or separated subnets 324
Enable import of user-created content 325
Manage a Tanium cluster 328
Manually configure a Tanium cluster 328
Perform database failover 328
Check replication status 328
Reinitialize replication 329
Manage the standby Module Server 329
Schedule sync jobs 329
View detailed status for Module Server sync 330
Promote the standby Module Server 332
Change the Tanium content manifest URL 332
Configure solution module file share mounts 333
Add a file share mount 333
List a file share mount 334
Test a file share mount 334
Manage advanced features 335
Enable UseTBBAllocatorStats 335
Upload an HTML banner 336

Configuring Appliance connections 337
Modify the host name and DNS configuration 337
Modify the host name 337
Modify the DNS server 338
Modify the hosts file 339
Enable or disable a network interface, change the IP address, or modify the MTU size 340
Modify advertised Ethernet speeds (physical Tanium Appliance only) 343
Reset a network interface 345
Set up an IPsec tunnel 345
View the IPSEC configuration for an Appliance 348
Modify the routing configuration 349
Configure NIC teaming (physical Tanium Appliance only) 350
Create NIC team 350

©2026 Tanium Inc. All Rights Reserved

Manage NIC team 350
Modify the NTP configuration 351
Change from a static IP address to DHCP (virtual Tanium Appliance only) 353

Configuring Appliance security 354
Manage inbound SSH access rules 354
Configure SSH banner text 354
View SSH fingerprints 355
Manage inbound HTTPS access rules 355
Configure LDAPS or StartTLS 356
Paste the LDAP server root CA contents 356
Import the LDAP server root CA certificate files 358
Enable/Disable the LDAPS or StartTLS configuration 358
Enable/Disable TLS certificate validation 358
View and manage LDAPS certificates 359
Copy the LDAPS configuration and certificates to another Tanium Server in a Cluster 360
Configure security policy rules 361
Enable FIPS 140-3 mode 362
Use AIDE reporting 365
Enable AIDE 366
Run an AIDE check report 367
Disable the weekly AIDE check report 367
Enable the weekly AIDE check report 368
Export the weekly AIDE check report 368
Toggle SELinux mode 370
Set menu timeout 370
Manage the Disk Encryption Key 372
Export the Disk Encryption Key (physical Tanium Appliance only) 372
Change the Disk Encryption Key (physical Tanium Appliance only) 373
Before you begin 374
Change the key with the decrypted previous key 374
Manage the GRUB key (physical Tanium Appliance or virtual Tanium Appliance only) 375
Export the GRUB key 375
Change the GRUB key password 377

Redundancy, backup, and recovery 379

©2026 Tanium Inc. All Rights Reserved

Tanium Appliance redundancy and backup best practices and considerations 379
Use multiple layers of redundancy and backup for Tanium Appliances 379
Define a disaster recovery plan 381
Additional best practices 382
Considerations after a recovery 382
Use a Tanium Server cluster for redundancy 383
Testing a planned Tanium Server failover 383
Recover a failed member of a redundant TS cluster 384
Prerequisites 384
(Primary Server failure only) Initiate the Database server failover 384
Restore a secondary Tanium Server 385
Use a standby Module Server for redundancy 386
Test a planned Module Server failover or recover a failed Module Server with a standby Module Server 386
Prerequisites 386
Prepare for promotion of the standby Module Server 386
Promote the standby Module Server to active 387
Make sure plugin schedules are in place and perform standard checkout steps 388
(Testing or Planned Failover only) Reassign sync roles 388
(Failed Module Server only) Replace failed Module Server 389
Schedule Module Server Sync and optionally perform a failback 390
Use image-based backups for backup and restoration (cloud-based Tanium Appliance or virtual Tanium Appliance only) 390
Restore TanOS using a VM image (cloud-based Tanium Appliance or virtual Tanium Appliance only) 390
Prerequisites 390
Steps 391
Use partition sync for backup and restoration (physical Tanium Appliance and test-environment virtual Tanium Appliance only) 391
Manage partitions 392
Enable alternate partitions (test-environment virtual Tanium Appliance only) 392
Disable alternate partitions (virtual Tanium Appliance only) 393
Boot from the active or inactive partition 395
Perform a partition sync 395
Perform a partition swap to restore TanOS from a partition sync 396
Prerequisites 397

©2026 Tanium Inc. All Rights Reserved

Steps 397
Use core and comprehensive backups for backup and restoration 397
Items excluded from backups 399
Sample contents of a core recovery bundle 400
Sample contents of a comprehensive recovery bundle 402
Configure automatic core or comprehensive backups 405
Add encryption key for the backups 406
Configure an automatic backup 408
Test an automatic backup 409
Schedule an automatic backup 410
View log files after a backup 411
Manually run a core or comprehensive backup 412
Review the TanOS log file 413
Use a comprehensive recovery bundle to perform a full restoration of the TanOS or Tanium environment 413
Prepare a new installation for restoration 414
Restore the Module Server 415
Restore the Tanium Server and register the restored Module Server 415
Restore the remaining Array members 416
View the log for the backup restoration 416

Monitoring and maintaining the Tanium Appliance 417
Configure monitoring and perform routine maintenance 417
Configure Tanium Appliance monitoring 417
Configure TanOS alerts 417
Configure syslog forwarding 418
Configure SNMP 418
Perform monthly maintenance 418
Review the Health Check report 418
Monitor Appliance performance (optional) 418
Perform quarterly maintenance 419
Verify the GRUB key backup 419
Review and update TanOS user accounts 419
Backup overview 420
Manage iDRAC 420

©2026 Tanium Inc. All Rights Reserved

Before you begin 421
Configure the iDRAC interface 421
Set password for the tanremote user 421
Enable the tanremote user 422
Disable the tanremote user 422
Close all iDRAC sessions 422
Reset iDRAC 422
Import a custom certificate for the iDRAC interface 423
Extract a certificate and key from a PFX file 424
Access the iDRAC virtual console 425
Troubleshoot the Lifecycle Controller job queue 426
Clear queued firmware updates 426
Clear the Lifecycle Controller job queue 427
View the iDRAC log 427
Configure syslog forwarding or alerts 427
Syslog alerts versus forwarding 428
Check the syslog status 428
Configure syslog forwarding 429
Access the syslog configuration menu 429
Manage the syslog server trust certificate 429
Manage the key pair for certificate authentication 430
Import a key pair 430
View or remove the previously imported key pair 430
Configure syslog forwarding destinations 430
(Optional) Force the full FQDN to appear in syslog messages 434
(Optional) Forward entries from other log files 434
Configure syslog alerts 436
Enable or disable all alerts 436
Set the alert severity level 436
Configure a syslog server destination for alerts 437
Configure an SMTP destination for alerts 438
Configuring SNMP 439
Set password and start the SNMP service 441
Change the SNMP user name, location, or contact 443
Change the SNMP authentication or privacy type 443

©2026 Tanium Inc. All Rights Reserved

View SNMP service status 443
Stop the SNMP service 443
Clean directories 444
Reboot or shut down 444
Reboot 444
Shut down 444
Increase storage 445
Manage OS services 446
View status 448
View OS status and partition information 448
View OS status and partition information with the tanadmin role 448
tanuser: View OS status and partition information with the tanuser role 448
View network status 448
View network status with the tanadmin role 449
tanuser: View network status with the tanuser role 449
View Tanium component status 449
View Tanium status with the tanadmin role 449
View Tanium status with the tanuser role 449
View Appliance status 449
View Appliance status with the tanadmin role 449
View Appliance status with the tanuser role 450
Perform database operations 450
View the Postgres log file 450
View Postgres configuration files 451
View Postgres control data 451
Enable full Postgres audit log 452
Manage the database memory plan 453
Run the Postgres top command 453
Query the tanium database 454
View database replication status and history 455
Initiate database server failover 457
Collect database replication statistics (Module Server only) 457
Monitor performance 458
Run a SAR command 458
Export a SAR snapshot 459

©2026 Tanium Inc. All Rights Reserved

Export a SAR performance data 459
Export all SAR files 460
Run the iotop command 460
Run the perf top command 461
Run the htop command 461
Perform advanced maintenance 461
Install a firmware update 461
Perform a TanOS reset 463
Re-install ACLs 464
Overwrite Module ACLs (Module Server only) 464
View the TanOS partition sync log 464

Upgrading TanOS and Tanium Core Platform 465
Upgrading to a new semiannual release or maintenance release 465
Tanium™ Semiannual Release 2026H2 466
Maintenance releases 467
Upgrade process 467
Upgrading the Tanium Endpoint Configuration Toolset and Tanium Client 468
Upgrade TanOS on Tanium Appliances 469
Before you begin 470
Understand the upgrade process 472
Upgrade paths 473
Perform the upgrade 474
Provide the Tanium Core Platform installation package 474
Use a downloaded installation package 475
Use a tokens download 475
(Internet-connect environments) Upgrade from the TanOS manifest 476
(Air-gapped environments) Upgrade by manually uploading an RPM file 479
What to do next 480
View the TanOS upgrade log 481
Upgrade Tanium Core Platform in an Appliance deployment 481
Before you begin 482
Upgrade the Tanium Core Platform 483
Install solution updates and verify the upgrade 485
Sign in to Tanium Console and update solutions 485

©2026 Tanium Inc. All Rights Reserved

Verify the basic deployment 485
Verify the Zone Server deployment 485
Verify a Tanium Cluster deployment 486

Tanium Appliance support and troubleshooting 487
View version information 487
Run the Health Check 488
Overview of Tanium Appliance logs, reports, and troubleshooting features 493
Restart services or networking 495
Restart services 495
Restart networking 495
Exit maintenance mode after an error 496
Reinitialize replication 496
Reindex databases 496
Review TanOS Appliance logs 497
Review Tanium Core Platform logs 497
Review Tanium solution module logs 499
Review the configuration 499
Run Tanium Support Gatherer 500
Copy core files 501
Run tcpdump 501
Run network diagnostics 503
Ping a remote system 503
Test a connection using a remote port 503
Trace the connection path to a destination 503
Resolve a host name 504
Check IPSEC 504
Listening ports 504
Show firewall 504
View network latency between Array members 505
View current network latency 505
View network latency history 505
Measure the data transfer rate between an Array Manager and an Array member 505
Examine Tanium and TanOS files 506
Open read-only restricted shell 506

©2026 Tanium Inc. All Rights Reserved

Request read-write restricted shell or full shell access 507
Security of Tanium Appliances 509
Security scanners and antivirus tools are not allowed on Tanium Appliances 510
Support for Tanium Appliances 510
Contact Tanium Support 510
TanOS support lifecycle 510
Support information for physical Tanium Appliances 511

Tanium Core Platform troubleshooting and logs 512
Logging levels 512
Troubleshooting workflow 514
Troubleshoot issues during Server deployment or solution operations 515
Log and report types 516
Action scheduler log 518
Authentication log 519
Console local error log 519
Database upgrade log 519
Download catalog cleaner log 519
HTTP connection log 520
LDAP log 520
Module plugin history log 521
Module-provided privileges log 521
Package cache cleaner log 522
Package download log 522
PKI log 523
PKI TLS log 523
PostgreSQL installation log 524
RBAC log 524
Server logs 525
Solution logs and support packages 526
TDownloader log 528
TPAN report 529
Workbenches manager log 530
Log rollover 530
Rollover for plain text logs 532

©2026 Tanium Inc. All Rights Reserved

Rollover for ZIP logs 532
Create a custom log for Tanium Core Platform Servers 532

Reference: TanOS health check results 538

Reference: TanOS menu map 559

Reference: TanOS CLI 587

Reference: Transfer files to and from the Appliance 621

Reference: Tanium Core Platform CLI 627
CLI examples 628
Display help 628
Display config help 629
Example: List configuration settings 629
Example: Set configuration values 630
Example: Set configuration values 630
Example: Configure global settings 630
Example: Add an administrator user 630

Reference: Deployment-related settings 632
Deployment-related settings reference 633

Reference: Tanium Appliance specifications 644
Tanium Appliance options and sizing 644
Physical Tanium Appliance specifications 646
Physical Tanium Appliance component specifications 646
Physical Tanium Appliance environmental specifications 647
Physical Tanium Appliance dimensions 647
Cloud-based Tanium Appliance and virtual Tanium Appliance specifications 648
Cloud-based Tanium Appliance deployment 648
Virtual Tanium Appliance deployment 648
Recommended resources for cloud-based Tanium Appliances and virtual Tanium Appliances 650
Up to 10,000 endpoints 651
10,001 to 35,000 endpoints 652
35,001 to 50,000 endpoints 652

©2026 Tanium Inc. All Rights Reserved

50,001 to 200,000 endpoints 652
200,001 to 500,000 endpoints (cloud-based Tanium Appliances only) 653
Over 500,000 endpoints (cloud-based Tanium Appliances only) 653

Reference: Default installation directory for the Tanium Client 654

Export Commodity Classification 655

©2026 Tanium Inc. All Rights Reserved

Tanium Appliance overview

This guide describes how to deploy Tanium Appliances with Tanium™ Core Platform roles and how to use the Tanium™ Operating System (TanOS) menus.

For information about physical Appliance support and the support lifecycle of TanOS, see Support for Tanium Appliances on page 510.

The Tanium Appliance is designed for the low-latency and high-throughput needs of the Tanium Core Platform. The Tanium Appliance runs a tuned, hardened Linux-based operating system (OS). Deploying a Tanium Appliance provides the following advantages:

- Built and tested with specified hardware components that are proven to support the indicated deployment sizes.
- Easy-to-use TanOS menus to quickly configure and deploy Tanium Core Platform roles.
- Eliminates challenges or side-effects of OS patch deployments. Tanium tests updates to the OS and provides RPM updates that are simple to install.
- Eliminates adverse interactions with third-party tools or drivers.
- Eliminates issues when provisioning service accounts needed by Tanium Core Platform components and solution modules.
- Eliminates difficulty troubleshooting across components that were designed by multiple vendors. Tanium is the single point of contact for hardware (physical Tanium Appliance), OS, and application support.
- Reduces additional licensing costs for OS and database products. TanOS is based on a Linux OS and the Tanium Server role is integrated with a limited access database.
- Saves time. A controlled and consistent Tanium platform environment means high reliability. Your teams can focus on maximizing Tanium value instead of OS and hardware issues.

©2026 Tanium Inc. All Rights Reserved

Note: Tanium prohibits installation of third-party software on Tanium Appliances to preserve the security, supportability, and performance of the Appliance. Access to the underlying operating system is restricted. For more information, see Security of Tanium Appliances on page 509.

Tanium Appliance types

There are three Tanium Appliance options for deploying the Tanium Core Platform:

- Physical Tanium Appliance
- Virtual Tanium Appliance
- Cloud-based Tanium Appliance

For application of Tanium Appliance types and sizing based on managed endpoint count, see Tanium Appliance options and sizing on page 644.

Physical Tanium Appliance

The Tanium Physical Appliance is a purpose-built, hardened system that provides performance at scale, with rapid diagnostics and response in the event of a hardware failure.

Virtual Tanium Appliance and cloud-based Tanium Appliance

The virtual Tanium Appliance and cloud-based Tanium Appliance are software versions of the Appliance, running on customer-provided hypervisor infrastructure or customer-purchased cloud-provider infrastructure, which provides a hardened, rapidly deployed, and easily managed system to run the Tanium Core Platform.

Note: Tanium does not offer on-premises virtualization infrastructure or cloud hosting for cloud-based Tanium Appliances. You must purchases these services separately.

Appliance roles

You can deploy a Tanium Appliance in any of the following Tanium Core Platform roles:

©2026 Tanium Inc. All Rights Reserved

Tanium™ Server

The core server that communicates with Tanium™ Clients. The Tanium Server also runs Tanium™ Console and Tanium™ API services and communicates with all other platform and solution components, as well as the content.tanium.com servers that host Tanium content packs and Tanium solutions. The Tanium Server depends on a database server that is installed when the Tanium Server role is installed.

Tanium™ Module Server

A dedicated server to run application services and store files for Tanium solution modules. It is installed on a separate Tanium Appliance to prevent intentional or accidental scripts from having a direct impact on the Tanium Server.

Tanium™ Zone Server

A server typically deployed in an enterprise DMZ network or another separate network with limited access to proxy traffic between Tanium Clients that reside there and a Tanium Server that resides on the trusted core network.

All-in-One

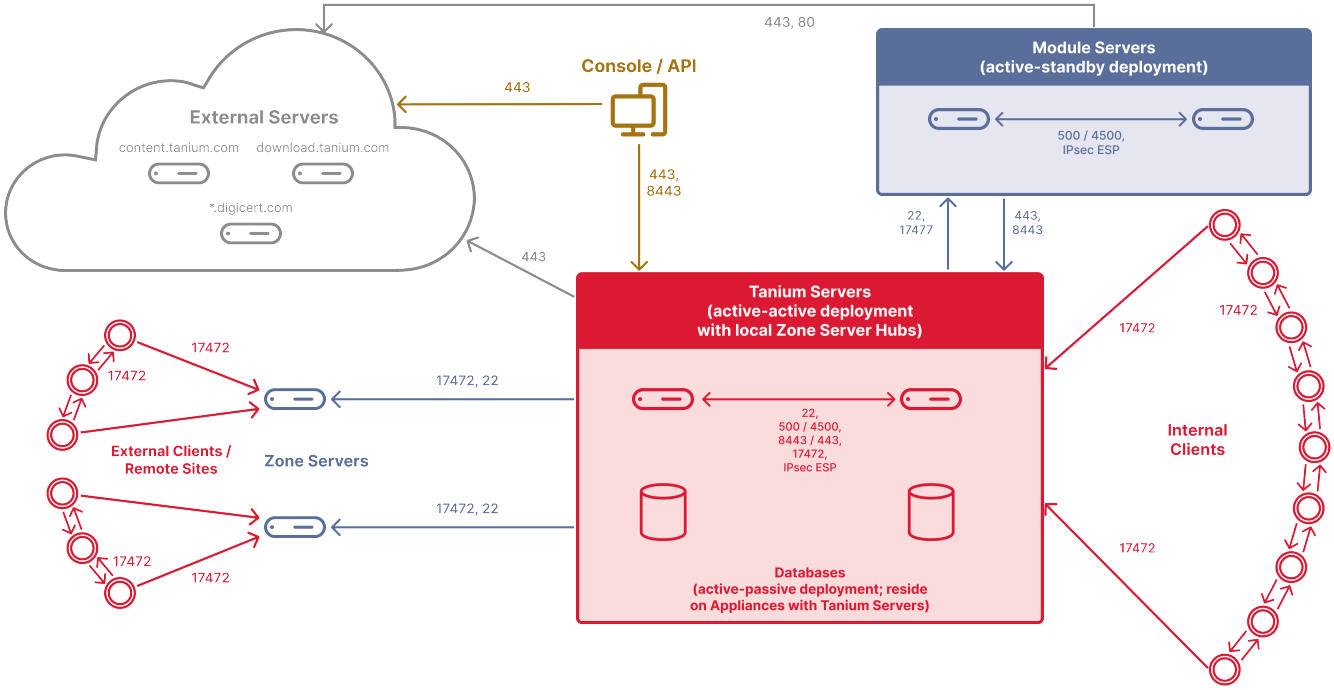
A Tanium Server, Tanium Module Server, and database server on the same Appliance. You can optionally use separate Zone Servers with an All-in-One Tanium Appliance, but you cannot use additional Tanium Servers or Module Servers. Use Tanium Appliances configured with the All-in-One role only for evaluation purposes. Tanium does not support All-in-One deployments in production environments.

Topology

In an enterprise production deployment, the Tanium Server and Tanium Module Server reside on separate Tanium Appliances.

Figure 1. Enterprise production or enterprise lab deployment

©2026 Tanium Inc. All Rights Reserved



TanOS menus

TanOS includes a menu interface to guide you through installation, configuration, and maintenance tasks.

For a reference of TanOS menus, see Reference: TanOS menu map on page 559. Entries are linked to associated topics elsewhere in this guide.

©2026 Tanium Inc. All Rights Reserved

Tanium Appliance requirements

Review the requirements before you set up and use a Tanium Appliance.

> **Note:** Any modification to the Licensed Software by Customer or any third-party or failure by Customer to implement any Enhancements to the Licensed Software may void Tanium's obligation to provide Support Services and Tanium's warranties.

Contact Tanium Support for the official security attestation for Tanium™ Appliance. To contact Tanium Support, sign in to https://support.tanium.com.

Tanium Appliance specifications

Review the Tanium Appliance specifications to ensure support for your environment and to determine appropriate sizing. For more information, see Reference: Tanium Appliance sizing and specifications on page 644.

Compatibility among components in a Tanium release

Tanium Appliance software versions

The *TanOS version* is the version of the Appliance operating system and menus. The Appliance operating system software is updated periodically to support new features and to support new Tanium Core Platform features.

The *Tanium version* is the version of the Tanium Core Platform Server component installed on an Appliance. All components must run the Tanium version provided in the same semiannual release bundle with the current TanOS version.

For more information, see the TanOS release notes for your release.

Tanium™ Semiannual Release 2026H2

©2026 Tanium Inc. All Rights Reserved

Tanium™ Semiannual Release 2026H2 includes new versions of the following components:

- Tanium Operating System (TanOS): The operating system that runs on each Appliance
- Tanium Core Platform: The software that runs on Tanium Core Platform Servers, including the Tanium Server, Tanium Module Server, Tanium Zone Server, and Tanium Zone Server Hub
- Tanium solutions: The solutions that you have licensed to provide specific functionality in your Tanium environment, including modules, shared services, and content-only solutions
- Tanium Client: The service that runs on endpoints to discover and report data in the Tanium environment
- Tanium™ Endpoint Configuration Toolset: A collection of tools, such as Tanium™ Client Extensions, that are deployed to endpoints to enable functionality for Tanium solutions

For version and support information, see 2026H2 release notes.

For more information about Tanium releases, see Tanium releases.

Maintenance releases

Maintenance releases provide security and bug fixes for currently supported semiannual releases. These upgrades are typically released monthly, and the support window remains based on the semiannual release. The maintenance release provides new versions only for the components that have fixes since the last update and might or might not contain upgrades for

Tanium Core Platform, Tanium solutions, Tanium Client, and the Tanium Endpoint Configuration Toolset.

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

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

Upgrade process

©2026 Tanium Inc. All Rights Reserved

Upgrading TanOS, Tanium Core Platform, and Tanium solutions

You must use the versions of TanOS, Tanium Core Platform, and Tanium solutions that are provided in a semiannual release together, or the later versions of each component that are provided in maintenance releases that upgrade the semiannual release. When upgrading to a new semiannual release, you must upgrade these components at the same time, beginning with TanOS. To begin the upgrade, see Upgrade TanOS on Tanium Appliances.

Important:

- After you start the upgrade process for a new semiannual release, you cannot access Tanium solutions until you finish upgrading both the platform and solutions. Make sure to plan a maintenance window with enough time to complete all upgrades.
- As a best practice, upgrade to the latest maintenance release available for semiannual release 2026H2. Do not upgrade to a maintenance release that has an earlier release date than the currently installed maintenance release. For example, if you have a maintenance release from February 1 currently installed, install a maintenance release of the 2026H2 semiannual release from February 1 or later.

Note: If you are installing a maintenance release that does not include a TanOS upgrade, begin the upgrade process with Tanium Core Platform. For more information, see Upgrade Tanium Core Platform in an Appliance deployment.

UPGRADING THE TANIUM ENDPOINT CONFIGURATION TOOLSET AND TANIUM CLIENT

You deploy the Tanium Endpoint Configuration Toolset and, optionally, the Tanium Client to endpoints using the change management feature of Tanium Endpoint Configuration. For more information, see Managing endpoint tool upgrade rollouts. If you do not enable Client upgrades in the change management feature, or if you need to upgrade the Tanium Client in upgrade rings for which Client upgrades are not yet enabled, you must upgrade the Tanium Client on endpoints using Client Management or other means to maintain a supported configuration. For more information, see Upgrading Tanium Clients. Tanium Semiannual Release 2026H2 supports all Tanium Client versions that the Tanium Core Platform supports. Each semiannual release supports the current endpoint

©2026 Tanium Inc. All Rights Reserved

configuration toolset and the two previous toolset releases.

Best Practice:

To ensure that all the features and fixes are available to endpoints, upgrade the Tanium Client to the version provided in the release, and deploy the Endpoint Configuration Toolset to all endpoints as soon as possible.

Note:

You cannot install the Tanium Client on a Tanium Appliance.

SSL certificates

The connections to Tanium Console or the SOAP and REST APIs, the connections between the Tanium Server and the Tanium Module Server, and connections to the Module Server are secured with SSL/TLS certificate and key exchanges. The installation process uses self-signed certificates. For best results, verify the installation with the self-signed certificates before you replace them with your commercial or enterprise certificates signed by a Certificate Authority. Doing this facilitates troubleshooting by separating potential installation issues and SSL issues.

For more information about SSL certificate requirements, see the Secure Tanium Console, API, and Module Server access on Tanium Appliances on page 266.

Tanium Appliance Array

An *Appliance Array* manages the connections and establishes trust between the Tanium Appliances that contain the components of a Tanium deployment. The Appliance Array makes it easy to set up and manage the Appliances.

A typical Appliance Array contains the following Appliances:

- A primary Tanium Server Appliance with an active database

©2026 Tanium Inc. All Rights Reserved

- A secondary Tanium Server Appliance with a passive database
- A Tanium Module Server Appliance
- An optional standby Tanium Module Server Appliance
- One or more Tanium Zone Server Appliances

Important: An Appliance Array is required to manage Tanium Servers and Tanium Module Servers in a Tanium Appliance deployment. For more information about how to install an Appliance Array, see Installing and managing an Appliance Array on page 158.

Best Practice: Use the Appliance Array to manage Tanium Zone Servers as well. Install and configure a Zone Server separately from the Appliance Array only if the network in which the Zone Server is installed does not allow SSH communication.

Network connectivity and firewall

Tanium components use TCP/IP to communicate. You must work with your network administrator to ensure that the Tanium components are provisioned IP addresses and that DNS can be used to resolve host names.

The Tanium Server must be able to connect to the Module Server. In a redundant cluster, the Tanium Servers must be able to connect to each other over a reliable Ethernet connection. These connections require a minimum throughput of 1 Gbps and a maximum round-trip latency of 30 ms.

The following table summarizes the Tanium processes and default values for ports used in Tanium core platform communication. You might need to configure network firewalls to allow the specified processes to send/receive TCP packets through the ports listed.

Network communication ports used by Tanium Appliances and Tanium Core Platform components

Source	Destination	Port	Protocol	Purpose
All Tanium Appliances	content.tanium.com download.tanium.com	443	TCP	Tanium Server (TaniumReceiver.exe) or Module Server (TaniumModuleServer.exe) communication with

©2026 Tanium Inc. All Rights Reserved

Source	Destination	Port	Protocol	Purpose
	*.digicert.com			content.tanium.com to import updates to Tanium Core Platform components and modules; communication from all Tanium Appliances to download TanOS upgrades
All Tanium Appliances	LDAP servers	389	TCP	(Optional) External LDAP communications for TanOS authentication
All Tanium Appliances	NTP servers	123	UDP	NTP time synchronization
All Tanium Appliances	Syslog servers	514	TCP, UDP	(Optional) Syslog monitoring
All Tanium Appliances	*.digicert.com	80	TCP	Certificate revocation checks (CRL/OCSP) against DigiCert for the DigiCert-signed Tanium binaries and certificates used by content.tanium.com and download.tanium.com. DigiCert serves these checks over HTTP rather than HTTPS, so this port is separate from the port 443 content and download traffic above.
Console/API users	content.tanium.com *.digicert.com	443	TCP	Download and install solutions to the Tanium Core Platform
Console/API users	Tanium Servers	443, 8443	TCP	Tanium Console/API user workstation (browser) communication with Tanium Servers
Module Servers	Module Servers	500, 4500	UDP	IPsec IKE for setting up a secure channel during Module Server synchronization
Module Servers	Module Servers	Not applicable	IPsec ESP [2]	Protocol for data confidentiality and authentication during Module Server synchronization
Module Servers	Tanium Servers	443, 8443	TCP	Module Server communication with Tanium Servers
Module Servers	Zone Servers [1]	17487	TCP	Used by Zone Servers for Module Server connections using Direct Connect.

©2026 Tanium Inc. All Rights Reserved

Source	Destination	Port	Protocol	Purpose
				The default port number is `17487`. If needed, you can specify a different port number when you configure the zone proxy.
		17488	TCP	Used by the Module Server to provision the Zone Proxy on the Zone Server. After the Zone Proxy is provisioned, used for connection status and diagnostics. The Direct Connect Zone Proxy installer automatically configures the firewall on the Zone Server to open port 17488. This port number is not configurable.
SNMP servers	All Tanium Appliances	161	UDP	(Optional) SNMP monitoring
Tanium Clients	Tanium Clients Tanium Servers Zone Servers	17472	TCP	Communication between Tanium Clients (TaniumClient.exe), communication between the Clients and the Tanium Servers or Zone Servers
Tanium Clients (external)	Zone Servers [1]	17486	TCP	Used by Zone Servers for endpoint connections to external Clients using Direct Connect. The default port number is `17486`. If needed, you can specify a different port number when you configure the zone proxy.
Tanium Clients (internal)	Module Servers	17475	TCP	Used by the Module Server for endpoint connections to internal Clients using Direct Connect.
Tanium Servers	All Tanium Appliances	22	TCP	SSH, SCP, SFTP communication for Appliance Array management
Tanium Servers	LDAP servers	389, 636	TCP	(Optional) External LDAP communications for Tanium Console authentication
Tanium Servers	Module Servers	17477	TCP	Tanium Server communication with Module Servers
Tanium	Tanium Servers	443,	TCP	Communication between active-active Tanium Servers

©2026 Tanium Inc. All Rights Reserved

Source	Destination	Port	Protocol	Purpose
Servers		17472		
Tanium Servers	Tanium Servers	500, 4500	UDP	IPsec Internet Key Exchange (IKE) protocol for setting up a secure channel in Tanium Server cluster communications
Tanium Servers	Tanium Servers	Not applicable	IPsec ESP [2]	IP protocol 50, which is used for data confidentiality and authentication in Tanium Server cluster communications
Tanium Servers, Module Servers	content.tanium.com *.digicert.com	443	TCP	Tanium Server (TaniumReceiver.exe) or Module Server (TaniumModuleServer.exe) communication with content.tanium.com to import updates to Tanium Core Platform components and modules
Tanium Servers Module Servers	DNS servers	53	UDP, TCP	DNS resolution for Tanium Servers and Module Servers
Tanium Servers Module Servers	SMB file servers	445	TCP	(Optional) SMB file share access used by Tanium Connect SMB File Share destinations, remote package file sources for TDownloader, and Patch air-gap alternate file locations
Tanium Servers Module Servers	Active Directory domain controllers	88	TCP, UDP	(Optional unless FIPS mode is enabled) Kerberos authentication for SMB file share access. FIPS mode disables NTLM, so the Appliance must reach the domain controllers (KDCs) of the Active Directory realm to obtain Kerberos tickets.
TanOS administrator workstations	All Tanium Appliances	22	TCP	SSH, SCP, SFTP communication for Appliance management
TanOS administrator workstations	All Tanium Appliances	443, 5900	TCP	(Physical Appliances only) iDRAC communications [3]

©2026 Tanium Inc. All Rights Reserved

Source	Destination	Port	Protocol	Purpose
Zone Server Hub	Zone Servers [1]	17472	TCP	Zone Server Hub (TaniumZoneServer.exe) communication with Zone Servers (TaniumZoneServer.exe)

[1] These ports are required only when you use a Zone Server.

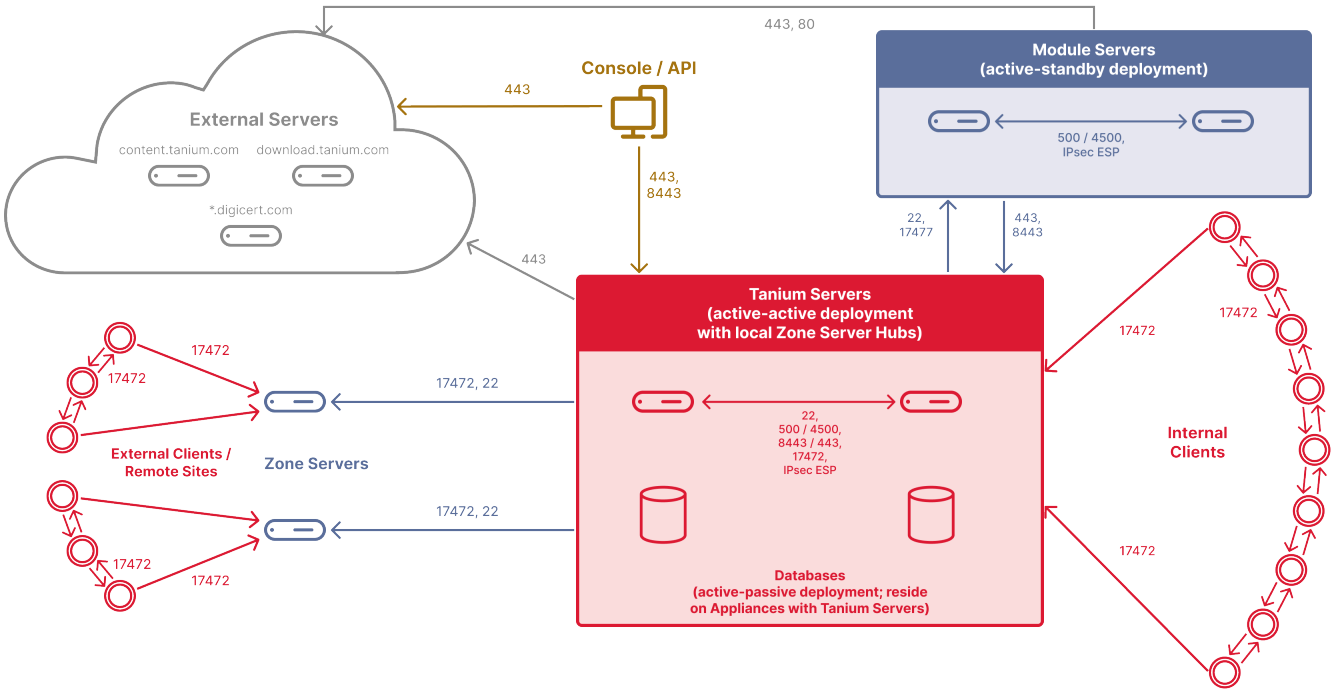
[2] IPSec Encapsulating Security Payload (ESP) is IP protocol 50 and does not use ports. For IPSec to work properly, you must add custom exceptions to your firewall rules.

[3] These ports need to be open only for the IP address of the dedicated iDRAC port (if applicable). The iDRAC port has an IP address that is different from the TanOS network interfaces. For more information, see the Configure the iDRAC interface .

Note: Do not allow a Tanium Server, a Module Server, or a Zone Server Hub to accept inbound connections from the internet. On a Zone Server, allow only the Tanium Client port to accept inbound connections from the internet.

The following figure illustrates how the Tanium Core Platform uses ports in an active-active deployment with Appliance infrastructure.

Figure 2. Network communication ports



©2026 Tanium Inc. All Rights Reserved

Note:

- For the topology of deployments that use a proxy server between Tanium Core Platform Servers and external servers, see Overview of proxy servers.
- Tanium™ Direct Connect uses additional ports for communication between Tanium Clients and the Module Server. For more information, see Host and network security requirements.
- For the ports that Tanium Client Management requires for deployment of Tanium Client, see Network connectivity, ports, and firewalls.

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

To see additional port requirements that are specific to Tanium™ modules and shared services, click the following links to access the associated user guides:

- Tanium™ Asset
- Tanium™ Automate: No additional port requirements
- Tanium™ Benchmark
- Tanium™ Certificate Manager: No additional port requirements
- Tanium™ Client Management
- Tanium™ Cloud Workloads: No additional port requirements
- Tanium™ Comply
- Tanium™ Connect
- Tanium™ Criticality
- Tanium™ Deploy

©2026 Tanium Inc. All Rights Reserved

- Tanium™ Direct Connect
- Tanium™ Directory Query
- Tanium™ Discover
- Tanium™ Endpoint Configuration
- Tanium™ End-User Notifications
- Tanium™ Enforce
- Tanium™ Engage
- Tanium™ Gateway
- Tanium™ Guide
- Tanium™ Health Check
- Tanium™ Impact
- Tanium™ Integrations Gallery
- Tanium™ Integrity Monitor
- Tanium™ Interact
- Tanium™ Investigate
- Tanium™ Jump Gate: No additional port requirements
- Tanium™ Patch
- Tanium™ Performance
- Tanium™ Provision
- Tanium™ Reporting
- Tanium™ Reputation
- Tanium™ Reveal

©2026 Tanium Inc. All Rights Reserved

- Tanium™ Threat Response
- Tanium™ Trends
- Tanium™ Zero Trust

Internet access (direct or by proxy)

Internet URLs

During installation and ongoing operations, the Tanium Server and the web browser that you use to access Tanium Console must connect to the following URLs to import updates to Tanium Core Platform components and modules:

- https://content.tanium.com
- https://download.tanium.com

  This URL is required for Tanium Server upgrades.

- http://*.digicert.com

  Module imports fails if the Certificate Revocation List is blocked or inaccessible.

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 Tanium Server and Tanium Module Server from downloading files from these locations.

If your enterprise security policy does not allow the Tanium Server to access these locations directly, you can use proxy servers. For more information, see Configuring proxy server settings on page 150.



Note: You must also enable Tanium Clients to download files from Internet URLs to run certain sensors and packages. For more information, see Managing allowed URLs.

SOLUTION-SPECIFIC INTERNET URLS

The Tanium Server might need to connect to additional URLs based on the solutions you import. For

©2026 Tanium Inc. All Rights Reserved

the required URLs for each solution, see the following links:

- Asset
- Deploy
- Discover
- Direct Connect
- Enforce
- Health Check
- Patch
- Provision
- Reputation

Proxies

If your enterprise network environment requires outbound Internet connections to traverse a proxy server, you can configure settings used to traverse the proxy server. For guidelines on proxy settings, see Configuring proxy server settings for Tanium Appliances on page 150.

Air gap

If you plan to deploy Tanium into an air-gapped environment, see Working with Appliances in an air-gapped environment on page 201.

©2026 Tanium Inc. All Rights Reserved

Getting started with the Tanium Appliance

Tip: To view a graphical, interactive checklist to track your progress with Tanium Appliance deployment, see Tanium Appliance Deployment Workflow.

Step 1: Prepare your environment

(Physical Tanium Appliance) Install and configure the Appliance

If you have one or more physical Tanium Appliances, install the Appliances into a machine room and configure bootstrap network settings.

For more information, see Installing a physical Tanium Appliance in a datacenter on page 43.

(Cloud-based Tanium Appliance) Set up the environment for the Appliance

Configure your environment to host cloud-based Tanium Appliances.

Deploy Tanium Server and Tanium Module Server Appliances into your private subnets and the Tanium Zone Server Appliances into public subnets.

Best Practice: For better resiliency in a cloud-based environment, separate Tanium Server, Tanium Module Server, and Tanium Zone Server Appliances between two zones so that each zone contains each Appliance type.

Step 2: Complete the initial setup

Connect to the TanOS console to configure network settings and initial users.

©2026 Tanium Inc. All Rights Reserved

- For physical Tanium Appliances, see Completing the initial setup (physical Tanium Appliance) on page 60.
- For virtual Tanium Appliances, see Completing the initial setup (virtual Tanium Appliance) on page 93.
- For cloud-based Tanium Appliances, see Completing the initial setup (cloud-based Tanium Appliance) on page 130.

Step 3: Set up an Appliance Array

Use the TanOS console to set up communication between the Appliances and install the components of the Tanium Core Platform from a single Appliance.

For more information, see Installing and managing an Appliance Array on page 158.

Step 4: Verify the installation

Make sure the components of the Tanium Core Platform installed correctly and that Tanium Clients can report to the Tanium Server.

For more information, see Completing and verifying the Tanium Core Platform installation on Tanium Appliances on page 196.

Step 5: Configure monitoring

Select and configure a method to monitor the health of your Tanium deployment and Appliance infrastructure. For example, if your organization has a syslog server or SNMP manager, you can integrate it with the Appliance for monitoring.

For more information, see Configure Tanium Appliance monitoring on page 417.

©2026 Tanium Inc. All Rights Reserved

Installing a physical Tanium Appliance in a datacenter

Follow the steps in this topic to rack a physical Tanium Appliance and configure its iDRAC interface and IP address.

Tip: This topic is also available as a separate download in PDF format if you or your datacenter team need it for use during installation of the Tanium Appliance in the datacenter. For more information, see the Tanium Appliance Datacenter Guide.

Before you begin, review Physical Tanium Appliance specifications on page 646, particularly the environmental requirements and physical characteristics, to ensure that the location you selected in your datacenter supports the requirements of the Appliance.

Contents of the box

- Ready Rails mounting kit
- Power cords:
    - **Small or Medium:** C13 to either NEMA 5-15P or C14 plugs
    - **Large or Extra-Large:** C19 to C20
- Hardware manual
- Tanium Hardware Addendum
- Optical transceivers (if the Tanium Appliance was purchased with the fiber network option):
    - **Small or Medium:** Short-range SFP+
    - **Large or Extra-Large (v3):** Short-range SFP+

©2026 Tanium Inc. All Rights Reserved

- **Large or Extra-Large (v4):** Short-range SFP28

What you need to provide

- Server rack or cabinet
- Two power outlets:
    - **Small or Medium:** NEMA 5-15P wall receptacles or C13 PDU receptacles
    - **Large or Extra-Large:** C19 PDU receptacles
- Two Ethernet cables with appropriate switch connections:
    - **Copper option:** RJ45 Ethernet cables adequate to support 10GbE
    - **Fiber option**—one of the following:
        - Duplex LC fiber optic cables ((supports 10GbE with included SFP+

          short-range optics for Small or Medium; supports 25GbE with included SFP28 short-range optics for Large or Extra-Large)
        - SFP28 twinax DAC (Large or Extra-Large v4 only; supports 25GbE)
        - SFP+ twinax DAC (supports 10GbE)

  Note: Additional cables and connections might be required for more advanced network configurations. Tanium Support provides guidance if that is necessary.

- • One RJ45 Ethernet cable adequate to support 1GbE for iDRAC
- • KVM console
- • Network settings (fixed IPv4 addresses, subnet mask, and default gateway for NICs and iDRAC interface)

Information tag

©2026 Tanium Inc. All Rights Reserved

The information tag is a slide-out label panel on the front of the chassis. This panel contains identifying information, such as the SKU and serial number (service tag).

Figure 3. Information tag slide-out panel



Physical connections

Small/Medium (v4)

Figure 4. Rear panel of a Small/Medium v4 Appliance



The small/medium (v4) Appliance has the following ports for use with deployment:

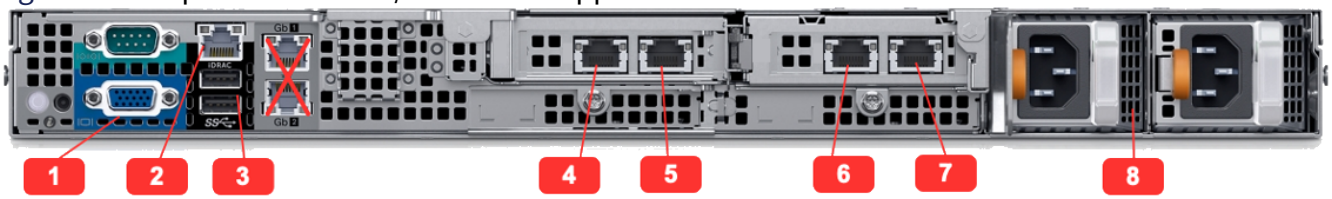
1	Network interface A1
2	Network interface A2
3	iDRAC network port
4	USB ports for KVM

©2026 Tanium Inc. All Rights Reserved

5	Network interface B1
6	Network interface B2
7	VGA for KVM
8	Power 1 and Power 2 C14 inlets (support locking C13 plugs)

Small/medium (v3)

Figure 5. Rear panel of a Small/Medium v3 Appliance



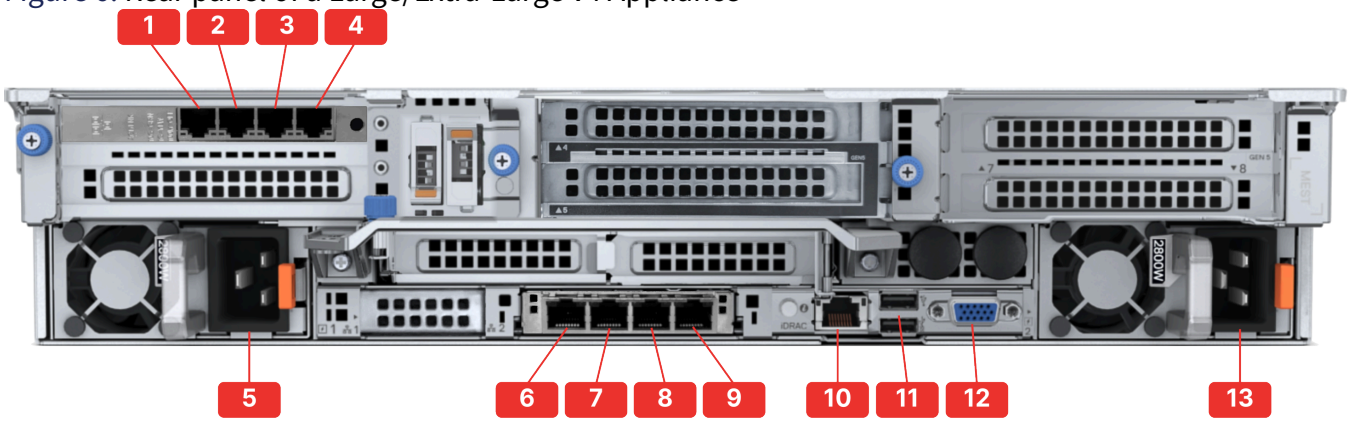
The small/medium (v3) Appliance has the following ports for use with deployment:

1	VGA for KVM
2	iDRAC network port
3	USB ports for KVM
4	Network interface A1
5	Network interface A2
6	Network interface B1
7	Network interface B2
8	Power 1 and Power 2 C14 inlets (support locking C13 plugs)

Large/extra-large (v4)

©2026 Tanium Inc. All Rights Reserved

Figure 6. Rear panel of a Large/Extra-Large v4 Appliance



The large/extra-large (v4) Appliance has the following ports for use with deployment:

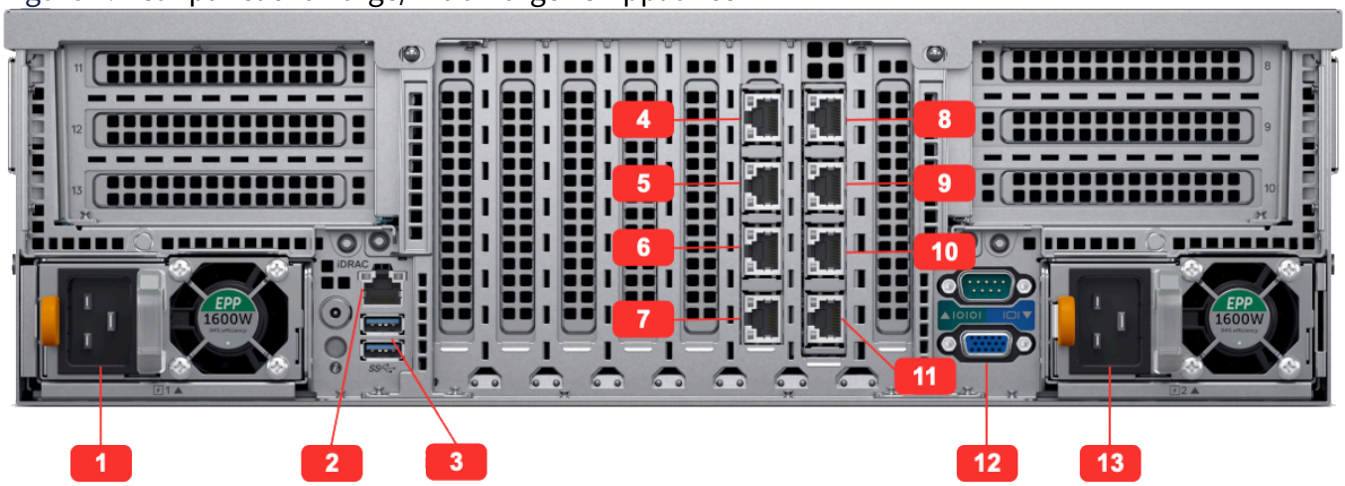
1	Network interface A1
2	Network interface A2
3	Network interface A3
4	Network interface A4
5	Power 1 C20 inlet (supports locking C19 plug)
6	Network interface B1
7	Network interface B2
8	Network interface B3
9	Network interface B4
10	iDRAC network port
11	USB ports for KVM
12	VGA for KVM

©2026 Tanium Inc. All Rights Reserved

13	Power 2 C20 inlet (supports locking C19 plug)

Large/extra-large (v3)

Figure 7. Rear panel of a Large/Extra-Large v3 Appliance



The large/extra-large (v3) Appliance has the following ports for use with deployment:

1	Power 1 C20 inlet (supports locking C19 plug)
2	iDRAC network port
3	USB ports for KVM
4	Network interface A1 (fiber option only; copper option has only two interfaces on this card)
5	Network interface A2
6	Network interface A3
7	Network interface A4 (fiber option only; copper option has only two interfaces on this card)
8	Network interface B1
9	Network interface B2

©2026 Tanium Inc. All Rights Reserved

10	Network interface B3
11	Network interface B4
12	VGA for KVM
13	Power 2 C20 inlet (supports locking C19 plug)

Installation and bootstrap configuration

Install and connect the Tanium Appliance

1. Install the Tanium Appliance into a rack using the Ready Rails kit.
   Install in a location where the Appliance is level, required power receptacles are available, and airflow is adequate for sufficient cooling. For environmental specifications, see Physical Tanium Appliance specifications on page 646.

   Use standard 19” rackmount rails. The Appliance measures approximately 26–33” deep, depending upon the specific model. Small and medium Appliances are 1U; large and extra-large are 2U (3U for the previous version).

   Tip: For an overview of installation, see the Dell Quick Resource Locator video.

2. Connect the Appliance to a power source. Connect both power supplies to power receptacles. Ensure the power supplies are connected to appropriate circuits and protective devices in accordance with your organizational best practices for fault tolerance.

   Tip: Two power cords are supplied to connect both fully redundant power supplies.

3. Connect the Appliance to the network.
   - The Tanium Appliance includes two separate network interface cards for redundancy, with fiber or copper connections. (This option was selected when the Appliances were ordered.) Connect the appropriate cables to at least one connection on each NIC and to the appropriate network switch.

©2026 Tanium Inc. All Rights Reserved

Important: Use the Ethernet ports on the PCIe network cards for Tanium Core Platform traffic. On models that include Ethernet ports on the motherboard, do not use the ports on the motherboard.

Best Practice: Ensure each NIC is connected to a separate switch configured in accordance with your organizational best practices for fault tolerance.

- Connect the appropriate cable to the iDRAC interface and to the appropriate network switch. The iDRAC interface is labeled on the I/O shield and is a copper connection regardless of whether the Appliance uses fiber connections for other network interfaces.

Note:

- The Tanium Appliance does not support LACP or respond to LACP packets. If LACP is configured on the network switch, either disable LACP or configure the switch to enable LACP only on ports where an LACP device is detected. A user with the tanadmin role can configure NIC teaming after full initial configuration is complete.
- In rare circumstances, a Tanium Physical Appliance might fail to boot and hang at the TanOS boot screen. In this situation, disable LLDP at the switch or in the Appliance BIOS. LLDP is not supported or required by TanOS. Contact Tanium Support for more information.

Best Practice: For reference in case of future troubleshooting, take photos of the Appliance cabling after everything is connected, and provide these photos to the Tanium Appliance administrator (the user with the tanadmin role).

4. Connect a physical or IP-based KVM console to the USB and VGA ports.

Power on the Appliance and configure the iDRAC interface

Use these steps to configure the iDRAC interface. With these steps, you set up the `tanremote` user account, which can be used to complete the initial configuration later.

©2026 Tanium Inc. All Rights Reserved

Best Practice: For the best results, configure the iDRAC interface for access to the physical Tanium Appliance. This significantly reduces the need to re-enter the data center for Tanium Appliance maintenance in the future.

Note: This configuration might have been completed during physical installation in the datacenter. If so, ask your datacenter team for the password of the `tanremote` user.

You must use a cable to connect the iDRAC interface to your network.

Note: A static IP address is required. DHCP is not supported.

1. Power on the Appliance.

   The boot and start-up processes take a few minutes.

2. When prompted to sign in, specify the user name `tanadmin` and the default password `Tanium1`.`Tanium1` or the password set by your data center team when the Tanium Appliance was racked.

```
--------------------------------------------------------


>>> Initial Configuration <<<


Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.


Keymap:     us
IP Address:
Hostname:   initial-tanos-347587.localdomain
FIPS 140-3: disabled


         M: Toggle FIPS 140-3 Mode


         P: Set Password                   (INCOMPLETE)
```

©2026 Tanium Inc. All Rights Reserved

```
         I: Configure iDRAC
            Set the password to continue configuration

         F: [DISABLED] Finish Initial Configuration
         S: Shutdown

         Z: Log out

-----------------------------------------------------

TanOS Version:        1.9.1

Please select:
```

3. Enter `I` (Manage iDRAC).
4. Enter `N` to go to the **Configure iDRAC Network** screen.
5. Follow the prompts to configure the iDRAC network.

```
           >>> Initial Config -> Manage iDRAC - > Configure iDRAC Network <<< >


These configuration settings will be applied to the iDRAC interface.
iDRAC user configuration can be performed in the user administration
menu.

Current iDRAC settings:
  IPv4 Address:
  IPv4 Gateway:
  IPv6 Address: ::/64
  IPv6 Gateway:

Would you like to continue with iDRAC IP configuration? [Yes|No]: yes

Enter the IPv4 address/prefix (e.g. 10.2.3.4/24): 10.10.10.65/24
```

©2026 Tanium Inc. All Rights Reserved

```
Enter the IPv4 gateway address (e.g. 10.2.3.1): 10.10.10.2
Would you like to accept default IPv6 settings? [Yes|No]: yes

New settings:
  IPv4 Address: 10.10.10.65/24
  Default IPv4 Gateway: 10.10.10.2
  Manual IPv6 settings:  No

Are these settings correct? [Yes|No]: yes
Configuring iDRAC interface, can take a minute or two ...
Press enter to continue
```

6. Enter `P` and follow the prompts to change the password of the `tanremote` user.

```
           >>> Appliance Configuration -> Manage iDRAC -> Set iDRAC Password <<<

This will change the iDRAC user tanremote password.
Access to the iDRAC is via the specific iDRAC IP.

Would you like to change the tanremote password? [YES/NO]: yes


The password policy requires meeting these rules:
 - Minimum 10 characters long
 - Maximum 20 characters long
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
 - At least 1 other character
 - Must not be based on a dictionary word
 - Must not contain part of the username

Please enter password (will not be displayed):
```

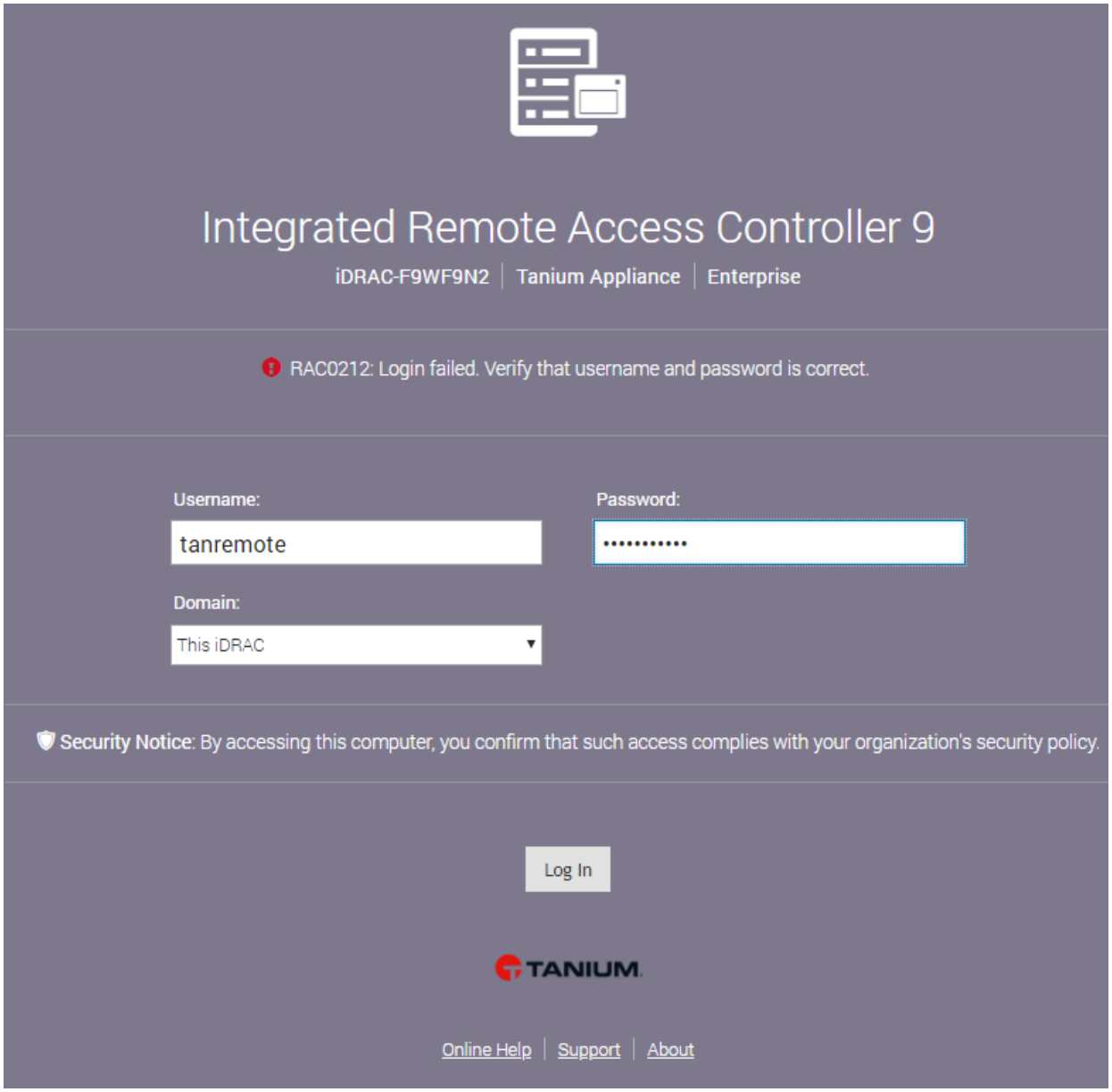
7. Ensure you can access the iDRAC virtual console at `http://<iDRAC interface IP`

©2026 Tanium Inc. All Rights Reserved

`address>`.

8. Ensure you can sign in with user name `tanremote` and the password that was set with this procedure and then provide the password for the `tanremote` user to your TanOS administrator so that user can complete the initial configuration.

Figure 8. iDRAC virtual console sign-in



(Optional) Configure the Appliance IP address

About this task

Use these steps to assign only an IP address to the Appliance. After performing these steps, you can

©2026 Tanium Inc. All Rights Reserved

sign out of the TanOS console and a TanOS administrator can connect through SSH later to resume the full initial configuration.

Note: This configuration might have been completed during physical installation in the datacenter. If so, ask your datacenter team for the IP address of the Appliance and the password for the `tanadmin` user.

1. Power on the Appliance.
   The boot and start-up processes take a few minutes.

2. When prompted to sign in, specify the user name `tanadmin` and the default password `Tanium1`.`Tanium1` or the password set by your data center team when the Tanium Appliance was racked.

```
-------------------------------------------------------


>>> Initial Configuration <<<


Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.


Keymap:     us
IP Address:
Hostname:   initial-tanos-347587.localdomain
FIPS 140-3: disabled


         M: Toggle FIPS 140-3 Mode


         P: Set Password                   (INCOMPLETE)
         I: Configure iDRAC
            Set the password to continue configuration


         F: [DISABLED] Finish Initial Configuration
         S: Shutdown


         Z: Log out
```

©2026 Tanium Inc. All Rights Reserved

```
------------------------------------------------------

TanOS Version:        1.9.1

Please select:
```

3. Enter `P` and then follow the prompts to change the password.

```
------------------------------------------------------

>>> Initial Config -> Set Password <<<

Preparing to change the password for tanadmin

The password policy requires meeting these rules:
 - Minimum of 10 characters long
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
 - At least 1 other character
 - Must not match any of recent 4 passwords
 - Must not be based on a dictionary word
 - Must not contain part of the username

Please enter password (will not be displayed):
Password score: 55 out of 100 (strong)
Please enter password again:

The password change was successful.

Press enter to continue
```


Tip: Follow the password policy guidelines closely. Note the password score that appears and aim for a strong password.

©2026 Tanium Inc. All Rights Reserved

4. Press **Enter** to return to the **Initial Configuration** menu.

```
-----------------------------------------------------

>>> Initial Configuration <<<

Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.

Keymap:     us
IP Address:
Hostname:   initial-tanos-347587.localdomain
FIPS 140-3: disabled

         M: Toggle FIPS 140-3 Mode

         P: Set Password                   (complete)
         A: Set IP Address                 (INCOMPLETE)
         N: Set FQDN (hostname)            (INCOMPLETE)
         D: Set DNS Nameservers            (INCOMPLETE)
         T: Set NTP (time)                 (INCOMPLETE)
         E: View and Accept EULA           (INCOMPLETE)

         F: [DISABLED] Finish Initial Configuration
         S: Shutdown

         Z: Log out

-----------------------------------------------------

TanOS Version:        1.9.1

Please select:
```

5. Enter `A`, and then follow the prompts to set the static IP address, IPv6 settings, gateway, and advertised Ethernet speeds. The TanOS console confirms that the settings are applied.

©2026 Tanium Inc. All Rights Reserved

```
          >>> Network Configuration <<< >

Note: any existing IP address listed below is NOT persistent/DHCP assigned.

Please provide a static IP address below regardless of the current
configuration. At the end of the initial configuration routine you will be
logged out. If the IP address is changed then you will need to modify your
connection settings to reach the TanOS menu.

Available interfaces:

        #: Interface  State  Link    MAC                IP                  Location
        1: ens160     UP      UP     00:0c:29:35:f4:fa  10.10.10.60/24      virtual

Please select: 1
Current settings:
  Interface: ens160
  IPv4 Address: 10.10.10.60/24
  Default IPv4 Gateway: 10.10.10.2
  IPv6 Address: fe80::20c:29ff:fec3:4afa/64
  IPv6 Gateway:
  Advertised Speeds: 1Gbps 10Gbps 25Gbps

Enter the IPv4 address/prefix (e.g. 10.2.3.4/24): 10.10.10.60/24
Enter the IPv4 gateway address (e.g. 10.2.3.1): 10.10.10.2
Would you like to accept default IPv6 settings? [Yes|No]: yes
Would you like to accept the current Ethernet advertised speeds? [Yes|No]: yes

New settings:
  Interface: ens160
  IPv4 Address: 10.10.10.60/24
  Default IPv4 Gateway: 10.10.10.2
  Manual IPv6:  No
  IPv6 Address: fe80::20c:29ff:fec3:4afa/64
  IPv6 Gateway:
```

©2026 Tanium Inc. All Rights Reserved

```
  Advertised Speeds: 1Gbps 10Gbps 25Gbps


Are these settings correct? [Yes|No]: yes
```

The IP address setting changes from incomplete to complete.

6. When ready, follow the steps in Perform full initial configuration. Provide the IP address and the password for the `tanadmin` user to your TanOS administrator so that user can access the Appliance using SSH and complete the initial configuration.

©2026 Tanium Inc. All Rights Reserved

Performing initial configuration of Tanium Appliances

The first step in deployment of Tanium Appliances is installing physical Tanium Appliances or deploying images to a hypervisor or cloud provider. After Appliances are installed, perform initial configuration of basic network, host, and user settings.

After initial configuration, you configure proxy servers if necessary, install the Appliance Array, and install roles.

The subsequent topics in this section detail the steps to perform initial configuration for physical Tanium Appliances, virtual Tanium Appliances, and cloud-based Tanium Appliances and perform the subsequent setup.

Completing the initial setup (physical Tanium Appliance)

To begin deployment of Tanium Appliances, install and configure physical Tanium Appliances, and then configure basic network, host, and user settings.

Install and configure physical Tanium Appliances

If you have one or more physical Tanium Appliances, install the Appliances into a machine room and configure bootstrap network settings.

For more information, see Installing a physical Tanium Appliance in a datacenter on page 43.

Important: The Tanium Appliance does not support LACP or respond to LACP packets. On a switch that is connected to a Tanium Appliance, either disable LACP or configure the switch to enable LACP only on ports where an LACP device is detected. After initial configuration is complete, a user with the `tanadmin` role can configure static NIC teaming on the Appliance to provide link redundancy.

©2026 Tanium Inc. All Rights Reserved

Important: In rare circumstances, a physical Tanium Appliance might fail to boot and hang at the TanOS boot screen. In this situation, it is best to disable LLDP at the switch or in the Appliance BIOS. LLDP is not supported or required by TanOS. Contact Tanium Support on page 510 for more information.

(FIPS-compliant organizations) Enable FIPS 140-3 mode before initial setup

About this task

Enabling Federal Information Processing Standards (FIPS) mode causes the Appliance to use a FIPS-validated cryptographic module for all cryptographic operations. It also ensures that services like SSH use only cryptographic algorithms that FIPS 140-3 allows.

If FIPS mode is required for your organization, you can enable it before you continue with initial setup so that the password and keys that you configure during setup are FIPS-compliant.

Best Practice: Enable FIPS mode only if you are required to do so for your organization.

Important: To use FIPS mode, the VM on which the virtual Tanium Appliance is installed must use a CPU type that supports the RDSEED instruction.

Note:

- Enabling FIPS mode in TanOS also puts the Tanium Platform in FIPS mode.
- You can later disable FIPS mode if it is not required and it was inadvertently enabled during setup. For more information, see Enable FIPS 140-3 mode on page 362.

1. Sign in to the TanOS console as the `tanadmin` user.
2. Enter `M` and follow the prompt to enable FIPS 140-3 mode and reboot the Appliance, and then continue initial setup.

©2026 Tanium Inc. All Rights Reserved

Configuration options

- Configure iDRAC on page 62 if you want to configure the `tanremote` user account and then continue from the iDRAC interface with initial configuration.
- Configure IP address only on page 66 if you want to complete the network configuration from the console and then later resume initial configuration elsewhere (for example, in a different location through an SSH connection).
- Perform full initial configuration on page 71 if you want to configure the `tanadmin` account and then complete all of the initial configuration steps at once from the console.

Configure iDRAC

Use these steps to configure the iDRAC interface. With these steps, you set up the `tanremote` user account, which can be used to complete the initial configuration later.

Best Practice: For the best results, configure the iDRAC interface for access to the physical Tanium Appliance. This significantly reduces the need to re-enter the data center for Tanium Appliance maintenance in the future.

Note: This configuration might have been completed during physical installation in the datacenter. If so, ask your datacenter team for the password of the `tanremote` user.

BEFORE YOU BEGIN

You must use a cable to connect the iDRAC interface to your network.

Note: A static IP address is required. DHCP is not supported.

CONFIGURE THE IDRAC

©2026 Tanium Inc. All Rights Reserved

1. Power on the Appliance.
   The boot and start-up processes take a few minutes.

2. When prompted to sign in, specify the user name `tanadmin` and the default password `Tanium1.Tanium1` or the password set by your data center team when the Tanium Appliance was racked.

```
-------------------------------------------------------

>>> Initial Configuration <<<

Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.

Keymap:     us
IP Address:
Hostname:   initial-tanos-347587.localdomain
FIPS 140-3: disabled

         M: Toggle FIPS 140-3 Mode

         P: Set Password                   (INCOMPLETE)
         I: Configure iDRAC
            Set the password to continue configuration

         F: [DISABLED] Finish Initial Configuration
         S: Shutdown

         Z: Log out

-------------------------------------------------------

TanOS Version:        1.9.1

Please select:
```

3. Enter `I` (Manage iDRAC).

©2026 Tanium Inc. All Rights Reserved

4. Enter `N` to go to the **Configure iDRAC Network** screen.
5. Follow the prompts to configure the iDRAC network.

```
           >>> Initial Config -> Manage iDRAC - > Configure iDRAC Network <<< >


These configuration settings will be applied to the iDRAC interface.
iDRAC user configuration can be performed in the user administration
menu.

Current iDRAC settings:
  IPv4 Address:
  IPv4 Gateway:
  IPv6 Address: ::/64
  IPv6 Gateway:

Would you like to continue with iDRAC IP configuration? [Yes|No]: yes

Enter the IPv4 address/prefix (e.g. 10.2.3.4/24): 10.10.10.65/24
Enter the IPv4 gateway address (e.g. 10.2.3.1): 10.10.10.2
Would you like to accept default IPv6 settings? [Yes|No]: yes

New settings:
  IPv4 Address: 10.10.10.65/24
  Default IPv4 Gateway: 10.10.10.2
  Manual IPv6 settings:  No

Are these settings correct? [Yes|No]: yes
Configuring iDRAC interface, can take a minute or two ...
Press enter to continue
```

6. Enter `P` and follow the prompts to change the password of the `tanremote` user.

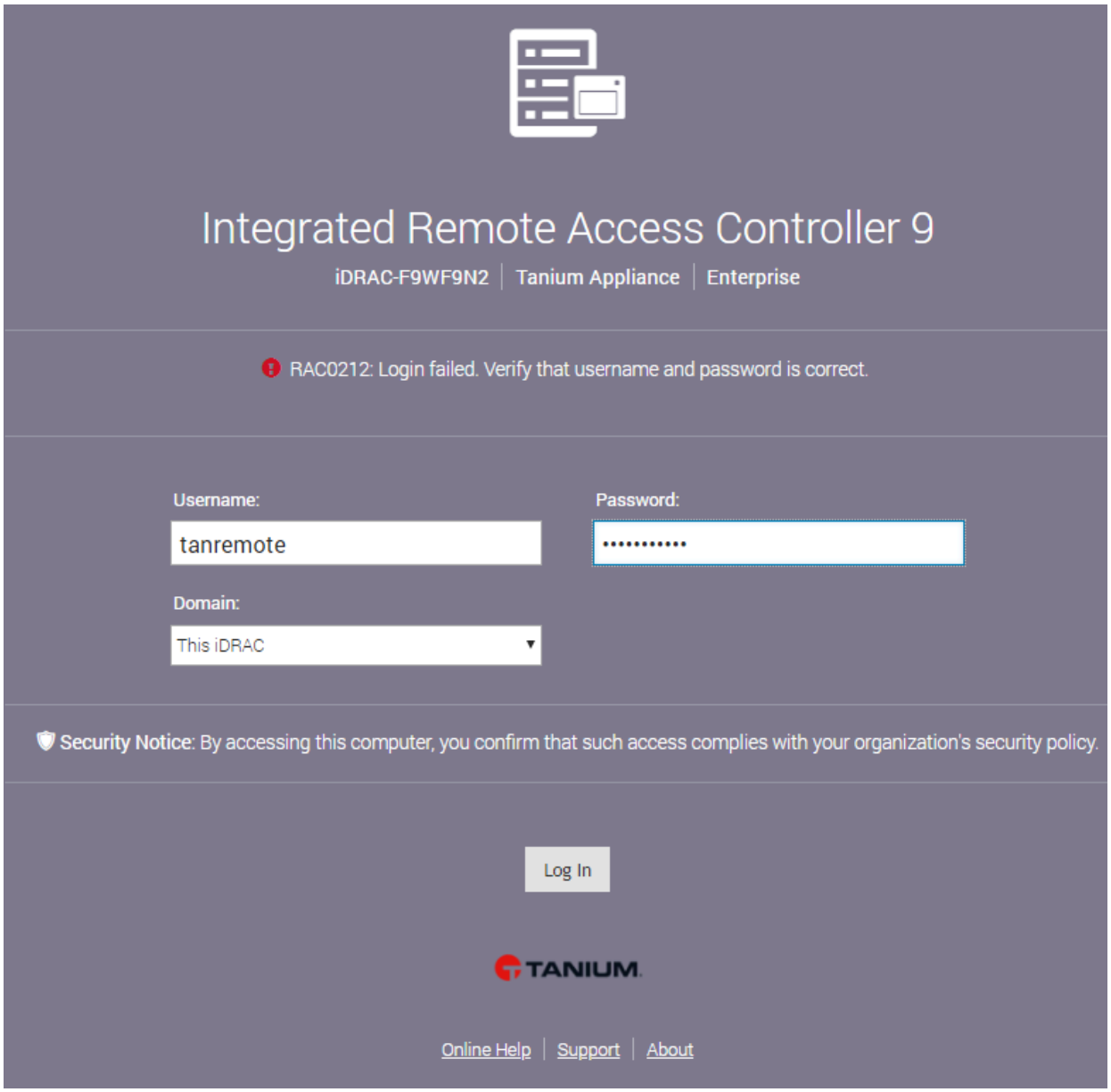
```
           >>> Appliance Configuration -> Manage iDRAC -> Set iDRAC Password <<<
```

©2026 Tanium Inc. All Rights Reserved

```
 This will change the iDRAC user tanremote password.
 Access to the iDRAC is via the specific iDRAC IP.

Would you like to change the tanremote password? [YES/NO]: yes



The password policy requires meeting these rules:
 - Minimum 10 characters long
 - Maximum 20 characters long
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
 - At least 1 other character
 - Must not be based on a dictionary word
 - Must not contain part of the username

 Please enter password (will not be displayed):
```

7. Access the iDRAC virtual console at `http://<iDRAC interface IP address>`.
8. Sign in with user name `tanremote` and the password that was set with this procedure and then proceed with the initial configuration. For more information, see Perform full initial configuration on page 71.
   Figure 9. iDRAC virtual console sign-in

©2026 Tanium Inc. All Rights Reserved



Configure IP address only

About this task

Use these steps to assign only an IP address to the Appliance. After performing these steps, you can sign out of the TanOS console and a TanOS administrator can connect through SSH later to resume the full initial configuration.

©2026 Tanium Inc. All Rights Reserved

Note: This configuration might have been completed during physical installation in the datacenter. If so, ask your datacenter team for the IP address of the Appliance and the password for the `tanadmin` user.

1. Power on the Appliance.
   The boot and start-up processes take a few minutes.

2. When prompted to sign in, specify the user name `tanadmin` and the default password `Tanium1`.`Tanium1` or the password set by your data center team when the Tanium Appliance was racked.

```
------------------------------------------------------


>>> Initial Configuration <<<


Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.


Keymap:     us
IP Address:
Hostname:   initial-tanos-347587.localdomain
FIPS 140-3: disabled


         M: Toggle FIPS 140-3 Mode


         P: Set Password                   (INCOMPLETE)
         I: Configure iDRAC
            Set the password to continue configuration


         F: [DISABLED] Finish Initial Configuration
         S: Shutdown


         Z: Log out


------------------------------------------------------


TanOS Version:        1.9.1
```

©2026 Tanium Inc. All Rights Reserved

```
Please select:
```

3. Enter `P` and then follow the prompts to change the password.

```
-----------------------------------------------------

>>> Initial Config -> Set Password <<<

Preparing to change the password for tanadmin

The password policy requires meeting these rules:
 - Minimum of 10 characters long
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
 - At least 1 other character
 - Must not match any of recent 4 passwords
 - Must not be based on a dictionary word
 - Must not contain part of the username

Please enter password (will not be displayed):
Password score: 55 out of 100 (strong)
Please enter password again:

The password change was successful.

Press enter to continue
```


Tip: Follow the password policy guidelines closely. Note the password score that appears and aim for a strong password.

4. Press **Enter** to return to the **Initial Configuration** menu.

```
-----------------------------------------------------
```

©2026 Tanium Inc. All Rights Reserved

```
>>> Initial Configuration <<<

Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.

Keymap:     us
IP Address:
Hostname:   initial-tanos-347587.localdomain
FIPS 140-3: disabled

         M: Toggle FIPS 140-3 Mode

         P: Set Password                   (complete)
         A: Set IP Address                 (INCOMPLETE)
         N: Set FQDN (hostname)            (INCOMPLETE)
         D: Set DNS Nameservers            (INCOMPLETE)
         T: Set NTP (time)                 (INCOMPLETE)
         E: View and Accept EULA           (INCOMPLETE)

         F: [DISABLED] Finish Initial Configuration
         S: Shutdown

         Z: Log out

-----------------------------------------------------

TanOS Version:        1.9.1

Please select:
```

5. Enter `A`, and then follow the prompts to set the static IP address, IPv6 settings, gateway, and advertised Ethernet speeds. The TanOS console confirms that the settings are applied.

```
          >>> Network Configuration <<< >
```

©2026 Tanium Inc. All Rights Reserved

```
Note: any existing IP address listed below is NOT persistent/DHCP assigned.

Please provide a static IP address below regardless of the current
configuration. At the end of the initial configuration routine you will be
logged out. If the IP address is changed then you will need to modify your
connection settings to reach the TanOS menu.

Available interfaces:

        #: Interface  State  Link    MAC               IP                  Location
        1: ens160     UP      UP     00:0c:29:35:f4:fa  10.10.10.60/24      virtual

Please select: 1
Current settings:
  Interface: ens160
  IPv4 Address: 10.10.10.60/24
  Default IPv4 Gateway: 10.10.10.2
  IPv6 Address: fe80::20c:29ff:fec3:4afa/64
  IPv6 Gateway:
  Advertised Speeds: 1Gbps 10Gbps 25Gbps

Enter the IPv4 address/prefix (e.g. 10.2.3.4/24): 10.10.10.60/24
Enter the IPv4 gateway address (e.g. 10.2.3.1): 10.10.10.2
Would you like to accept default IPv6 settings? [Yes|No]: yes
Would you like to accept the current Ethernet advertised speeds? [Yes|No]: yes

New settings:
  Interface: ens160
  IPv4 Address: 10.10.10.60/24
  Default IPv4 Gateway: 10.10.10.2
  Manual IPv6:  No
  IPv6 Address: fe80::20c:29ff:fec3:4afa/64
  IPv6 Gateway:
  Advertised Speeds: 1Gbps 10Gbps 25Gbps

Are these settings correct? [Yes|No]: yes
```

©2026 Tanium Inc. All Rights Reserved

The IP address setting changes from incomplete to complete.

6. When ready, follow the steps in Perform full initial configuration on page 71. Provide the IP address and the password for the `tanadmin` user to your TanOS administrator so that user can access the Appliance using SSH and complete the initial configuration.

Perform full initial configuration

You can perform initial configuration in the order that you prefer. As you finish configuring settings, the status changes from incomplete to complete.

Note: You may have already completed some of these steps from the data center.

BEFORE YOU BEGIN

Connect a keyboard, video, and mouse (KVM) to the console port.

COMPLETE THE INITIAL CONFIGURATION

1. Power on the Appliance.
   The boot and start-up processes take a few minutes.

2. When prompted to sign in, specify the user name `tanadmin` and the default password `Tanium1` or the password set by your data center team when the Tanium Appliance was racked.

```
------------------------------------------------------


>>> Initial Configuration <<<


Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.


Keymap:     us
```

©2026 Tanium Inc. All Rights Reserved

```
IP Address:
Hostname:   initial-tanos-347587.localdomain
FIPS 140-3: disabled

         M: Toggle FIPS 140-3 Mode

         P: Set Password                   (INCOMPLETE)
         I: Configure iDRAC
            Set the password to continue configuration

         F: [DISABLED] Finish Initial Configuration
         S: Shutdown

         Z: Log out

-----------------------------------------------------

TanOS Version:        1.9.1

Please select:
```

3. Enter `P` and then follow the prompts to change the password.

```
-----------------------------------------------------

>>> Initial Config -> Set Password <<<

Preparing to change the password for tanadmin

The password policy requires meeting these rules:
 - Minimum of 10 characters long
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
 - At least 1 other character
 - Must not match any of recent 4 passwords
 - Must not be based on a dictionary word
```

©2026 Tanium Inc. All Rights Reserved

```
 - Must not contain part of the username


 Please enter password (will not be displayed):
Password score: 55 out of 100 (strong)
 Please enter password again:


 The password change was successful.


 Press enter to continue
```


Tip: Follow the password policy guidelines closely. Note the password score that appears and aim for a strong password.



Important: Remember this password and, if possible, store it in a password vault approved by your organization. If you have not created a second privileged user with the tanadmin role, this password cannot be recovered.

4. Press **Enter** to return to the **Initial Configuration** menu.

```
-----------------------------------------------------


>>> Initial Configuration <<<


Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.


Keymap:     us
IP Address:
Hostname:   initial-tanos-347587.localdomain
FIPS 140-3: disabled


         M: Toggle FIPS 140-3 Mode


         P: Set Password                  (complete)
         A: Set IP Address                (INCOMPLETE)
```

©2026 Tanium Inc. All Rights Reserved

```
         N: Set FQDN (hostname)            (INCOMPLETE)
         D: Set DNS Nameservers            (INCOMPLETE)
         T: Set NTP (time)                 (INCOMPLETE)
         E: View and Accept EULA           (INCOMPLETE)

         F: [DISABLED] Finish Initial Configuration
         S: Shutdown

         Z: Log out

------------------------------------------------------

TanOS Version:        1.9.1

Please select:
```

5. If necessary, enter `A`, and then follow the prompts to set the static IP address, IPv6 settings, gateway, and advertised Ethernet speeds.

```
           >>> Network Configuration <<< >

Note: any existing IP address listed below is NOT persistent/DHCP assigned.

Please provide a static IP address below regardless of the current
configuration. At the end of the initial configuration routine you will be
logged out. If the IP address is changed then you will need to modify your
connection settings to reach the TanOS menu.

Available interfaces:

        #: Interface  State  Link    MAC               IP                  Location
        1: ens160     UP      UP     00:0c:29:35:f4:fa  10.10.10.60/24      virtual

Please select: 1
Current settings:
```

©2026 Tanium Inc. All Rights Reserved

```
  Interface: ens160
  IPv4 Address: 10.10.10.60/24
  Default IPv4 Gateway: 10.10.10.2
  IPv6 Address: fe80::20c:29ff:fec3:4afa/64
  IPv6 Gateway:
  Advertised Speeds: 1Gbps 10Gbps 25Gbps

Enter the IPv4 address/prefix (e.g. 10.2.3.4/24): 10.10.10.60/24
Enter the IPv4 gateway address (e.g. 10.2.3.1): 10.10.10.2
Would you like to accept default IPv6 settings? [Yes|No]: yes
Would you like to accept the current Ethernet advertised speeds? [Yes|No]: yes

New settings:
  Interface: ens160
  IPv4 Address: 10.10.10.60/24
  Default IPv4 Gateway: 10.10.10.2
  Manual IPv6:  No
  IPv6 Address: fe80::20c:29ff:fec3:4afa/64
  IPv6 Gateway:
  Advertised Speeds: 1Gbps 10Gbps 25Gbps

Are these settings correct? [Yes|No]: yes
```

6. After the initial configuration screen appears with the updated IP address configuration, enter `N` and then follow the prompts to configure the fully qualified domain name (FQDN).

```
>>> Initial Config -> Set FQDN <<<

Current hostname (FQDN):

New FQDN: fqdn.example.com



Setting new hostname (FQDN):
fqdn.example.com
```

©2026 Tanium Inc. All Rights Reserved

```
Do you want to continue? [Yes|No]: Yes
```



Important: Use an FQDN that is accessible from any computer from which a user will access Tanium Console.

7. After the initial configuration screen appears with the updated FQDN configuration, enter `D` and then follow the prompts to set the DNS name servers.

```
>>> Initial Config -> Set Nameservers <<<

Currently configured nameserver(s):



Enter the first DNS server address: 10.10.10.10
Enter the second DNS server address:

Setting nameserver 1: 10.10.10.10
Setting nameserver 2:

Do you want to continue? [Yes|No]: Yes
```

8. After the initial configuration screen appears with the updated DNS configuration, enter `T` and then follow the prompts to set the NTP servers.

```
>>> NTP Configuration <<<

Timezone will be automatically set to UTC.

Enter the NTP server information for up to two NTP servers. Each entry consist
of a server name or IP address.
Optionally each server may indicate authentication information using
colons as a separator: >server<:>key-id<:>SHA1|MD5<:key



1.2.3.4
pool.ntp.org
ntp.secret.corp:999:SHA1:0123456789abcdef0123456789abcdef01234567
```

©2026 Tanium Inc. All Rights Reserved

```
Please provide the NTP server address: pool.ntp.org
Please provide the second NTP server address (enter blank value for none):

The following settings will be used:

    NTP Server 1: pool.ntp.org
    NTP Server 2:

Are these settings correct? [Yes|No]: Yes
```

9. After the initial configuration screen appears with the updated NTP configuration, enter `E` and then use the spacebar to page through the end-user license agreement (EULA). When complete, press the **Q** key, enter your email address, and enter YES to accept.
   The email address is stored locally only. It is not used externally for any reason.

10. (Optional) Configure the iDRAC. This can also be done later from the TanOS menus.

11. Enter `F` to finish initial configuration.
    The Appliance reboots, and when you sign in, the initial configuration menu is replaced by the `tanadmin` menu.

> **Note:** Before you can finish initial configuration, you must have changed the `tanadmin` password, set the host name and DNS server, configured an NTP server, and accepted the EULA. If any requirement is unmet, TanOS reports which steps remain and exits without completing the configuration.

Access TanOS remotely

To access your Tanium Appliances remotely, note the following requirements.

- Your local management computer must be connected to a subnet that can reach the Appliance IP address.
- Your management computer must have an SSH client application or terminal emulator that can make a Client connection to the Appliance.
- You must have an SSH client such as PuTTY to sign in to the TanOS console. For PuTTY, use

©2026 Tanium Inc. All Rights Reserved

version 0.71 or later.

- You must have an SSH key generator such as ssh-keygen to generate keys for the tancopy user.
- You must have an SFTP client such as WinSCP to copy files to and from the Appliance. For WinSCP, use version 5.15.2 or later.

Tip: Watch the tutorial about how to configure WinSCP for the Tanium Appliance.

Configure SSH keys

TanOS has built-in and customer-created user accounts to access the Appliance operating system and perform tasks.

Before you install a Tanium Appliance role, you must add SSH keys to authenticate access for the `tancopy` built-in user. `tancopy` can make an SFTP connection with SSH key authentication to TanOS and copy files to and from the /incoming and /outgoing directories. For Google Cloud Platform, you must also set up an SSH key for the `tanadmin` user account, even if you primarily plan to use other user accounts with the `tanadmin` role.



Best Practice: Set up SSH key authentication for all TanOS user accounts.



Important: TanOS does not support self-service password reset methods. If you forget your password, you must ask a user with the tanadmin role to reset it for you. You can avoid this risk by setting up SSH key authentication.

Tip: Watch the tutorial about how to configure SSH key authentication for the Tanium Appliance.

©2026 Tanium Inc. All Rights Reserved

BEFORE YOU BEGIN

- You must have an SSH client to sign in to the TanOS console, and an SFTP client to copy files to and from the Appliance.
- You must have an SSH key generator to generate keys for the `tancopy` user.

ADD AND TEST AN SSH KEY FOR THE TANCOPY USER

Add an SSH key for the `tancopy` user, and then test the SFTP connection to confirm that the key works.

Add the SSH key for the tancopy user

1. Use an SSH key generator such as ssh-keygen to generate a public/private key pair. Note:
   - Specify an RSA key with 2048 bits (such as ssh-keygen -t rsa -b 2048).
   - Specify a passphrase that is easy to remember.
   - Save the private key to a location that you can access when you set up your SFTP client.
2. Copy the text in the public key file to the clipboard. If you use ssh-keygen, copy the contents of the .pub file that you created.

   Important: In an SSH key exchange, the keys must match exactly, including line endings.
3. Sign in to the TanOS console as a user with the `tanadmin` role.
4. Enter `C-U` (User Administration > TanOS User Management).
5. Enter the line number for the `tancopy` user to go to the user administration menu for this user.

```
          >>> User Administration -> TanOS -> tancopy <<<

Username:         tancopy
Account Enabled:  Yes
Authentication:   SSH Key Only
```

©2026 Tanium Inc. All Rights Reserved

```
Password Expires: N/A
SSH Lockout:      No (0)
Multifactor:      Not configured
Protected:        No

Notes:
  * This user account cannot be deleted
  * This user account cannot have a password
  * This user account cannot use multifactor

         A: Manage SSH Authorized Keys
         P: Manage SSH Key Pair
         L: Reset SSH Lockout
         C: [DISABLED] Change Password
         N: [DISABLED] Disable Password Access
         M: [DISABLED] Multifactor Authentication

         E: Enable Account
         D: Disable Account
         T: [DISABLED] Manage Account Protection
         X: [DISABLED] Delete User

         F: Edit known hosts file

         R: Return to previous menu  RR: Return to top

--------------------------------------------------------
```

6. Enter `A` (Authorized Keys).
7. Enter `A` and follow the prompts to add the contents of the public key generated in Step 1.

```
           >>> User Administration -> TanOS -> tancopy -> Authorized Keys -> Add
<<<

Account: tancopy
Please paste the public key and press enter:
```

©2026 Tanium Inc. All Rights Reserved

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA1ClmgkMrbbxB7jND/Y4/
Giupck35xAuGNKfZWqVLM5F0CNXuTScf6v2z
MDxW5TO5tm/U8P9sqh19RDEzTn2RayXzsoZmXyB8abCCpHG4+03Zv05RHiX4i5QomAMBnbZejdA9/
fGTxO1rPo1rdtTq
Z+KCgzbEhHLWUD44+If5RtG+U4kgyzlYsyjgwhfho+BrRY6e7QYBsXVbuBQ9ROGV6PCTB80jXZVAKrAbsTQ1D
VkpuBue
mftv7vOn3b8MKzJ/IY/
LLL1tIgpSGvgvjr2mOJJ+JoZF2XnPVUFmYiDSCkPAzhCyFHILHfOVAfws9n1G6p3fwILqNhvB
oPeaCFaApQ== rsa-key-20200123
 Validating input
 Adding key to authorized keys after validation
 Finished adding authorized keys for tancopy



 Press enter to continue
```

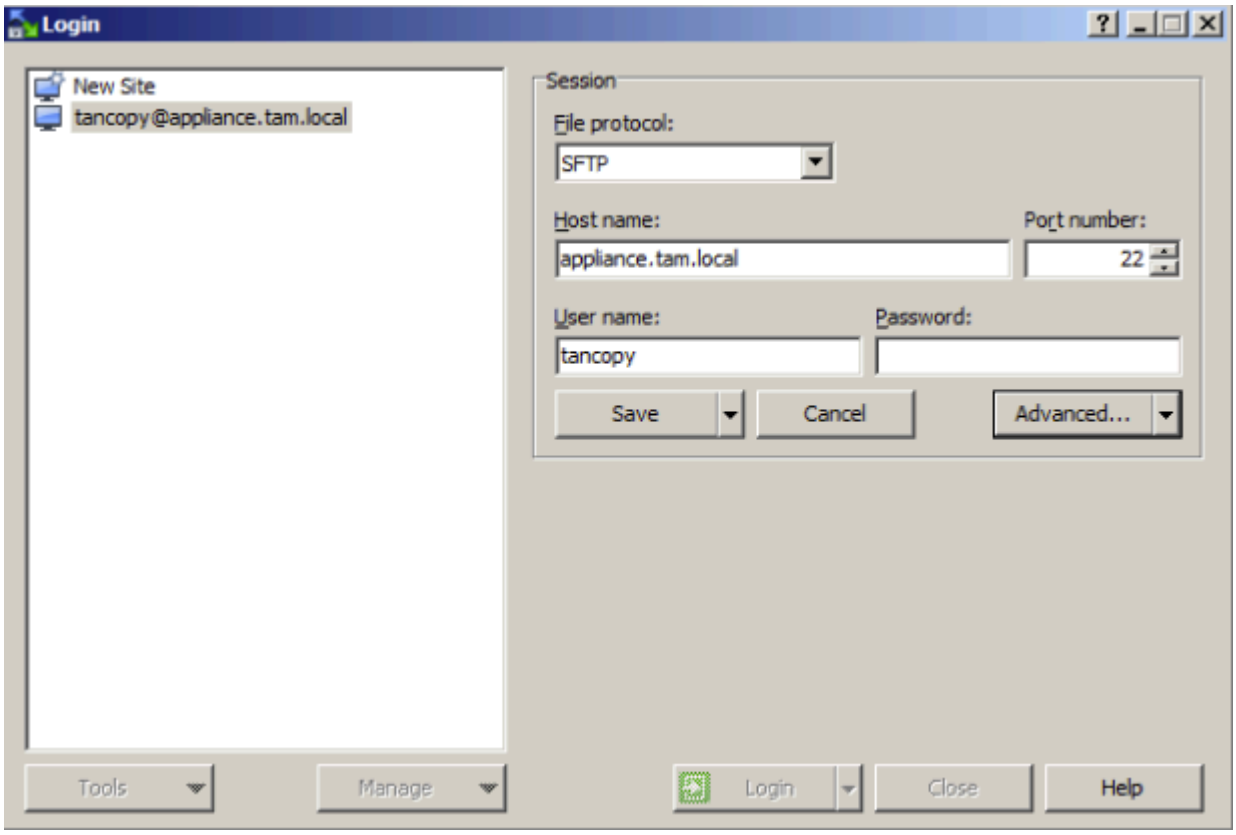
Test the SFTP connection with the SSH key

About this task

Use an SFTP client on your management computer, such as WinSCP in Windows or the sftp utility in macOS or Linux, to connect to the Tanium Server Appliance. The following steps demonstrate configuring the connection in WinSCP:

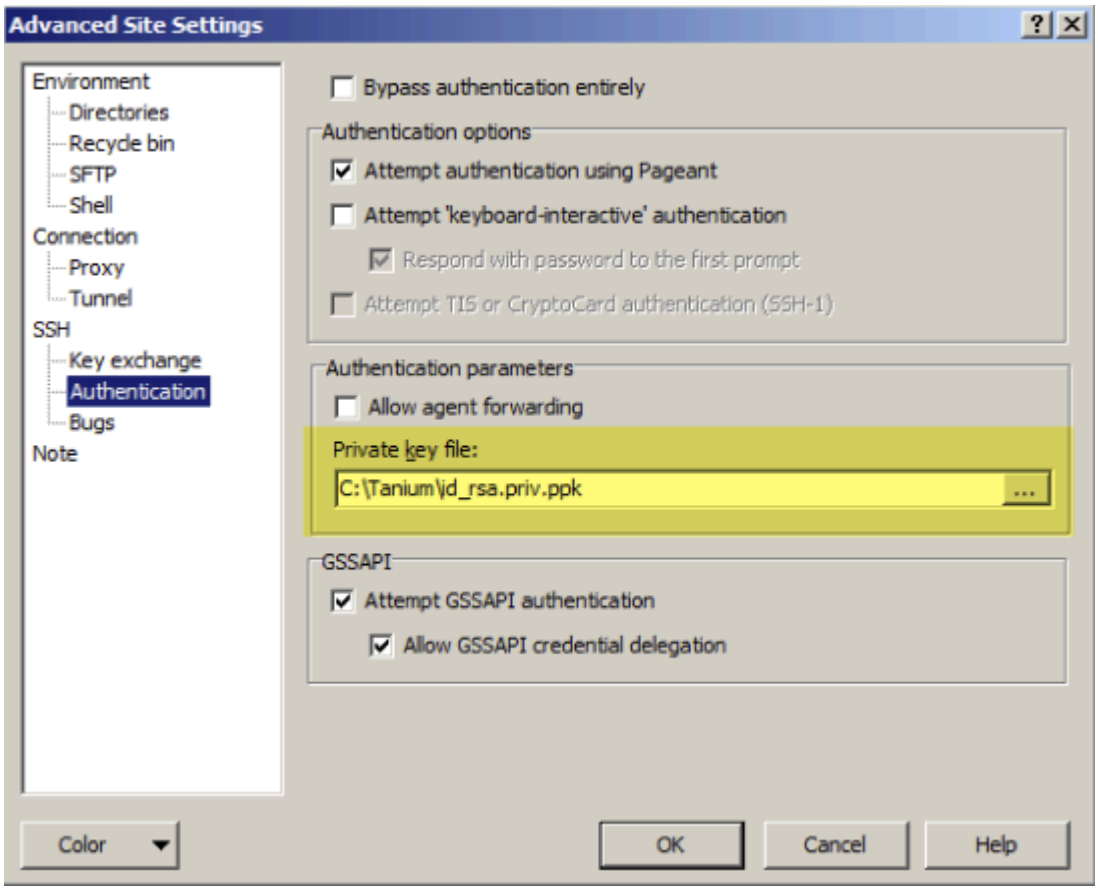
1. Specify `tancopy` for user name.
   Figure 10. WinSCP user name set to tancopy

©2026 Tanium Inc. All Rights Reserved



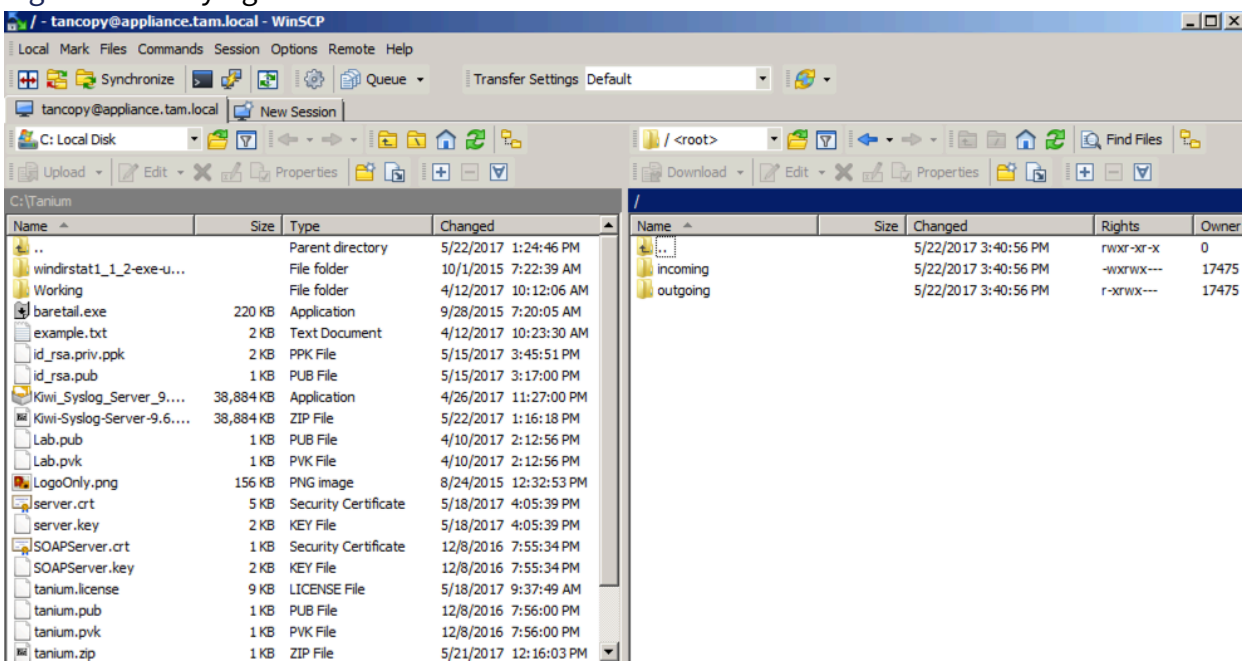
2. Click **Advanced**.
3. Under SSH, browse and select the private key that pairs with the public key uploaded to the Appliance.
   Figure 11. Selecting the private key in WinSCP

©2026 Tanium Inc. All Rights Reserved



4. Save the configuration and click **Login** to initiate the connection.
   Connect to the Appliance and make sure you can access the /incoming and /outgoing directories.

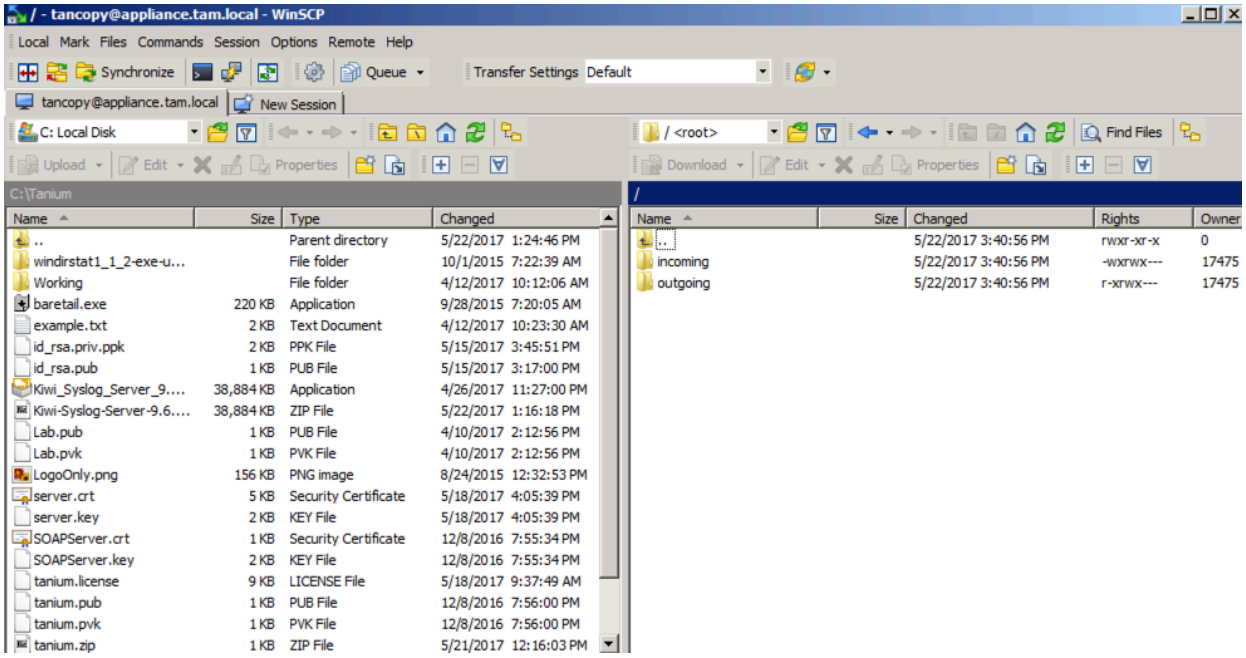
Figure 12. Verifying the SFTP connection in WinSCP



©2026 Tanium Inc. All Rights Reserved

After you connect to the Appliance, upload files to the /incoming directory, and download files from the /outgoing directory.

Figure 13. Testing file transfer in WinSCP



ADD SSH KEYS FOR OTHER TANOS USERS

About this task

It is a best practice to also set up SSH key authentication for TanOS user accounts.

Important: For Google Cloud Platform, you must set up an SSH key for the `tanadmin` user account, even if you primarily plan to use other user accounts with the `tanadmin` role.

Tip: As an alternative to the following procedure, you can use ssh-copy-id to add an SSH public key to any TanOS user with the `tanadmin` profile.

1. Use an SSH key generator such as ssh-keygen to generate a public/private key pair. Note:
   - Specify an RSA key with 2048 bits (such as ssh-keygen -t rsa -b 2048).
   - Specify a passphrase that is easy to remember.
   - Save the private key to a location that you can access when you set up your SFTP

©2026 Tanium Inc. All Rights Reserved

client.

2. Copy all of the text in the public key file to the clipboard. If you use ssh-keygen, copy the contents of the .pub file that you created.

   Important: In an SSH key exchange, the keys must match exactly, including line endings.

3. Sign in to the TanOS console as a user with the `tanadmin` role.
4. Enter `C-U` (User Administration > TanOS User Management).
5. Enter the line number of the user account that you want to manage.

```
>>> User Administration -> TanOS -> tanadmin <<<

 Username:         tanadmin
 Account Enabled:  Yes
 Authentication:   SSH Key or Password
 Password Expires: 2027-01-14 00:00:00 UTC
 SSH Lockout:      No (0)
 Multifactor:      Not configured
 Protected:        No

 Notes:
   * This user account must always have a password
   * This user account cannot be deleted
   * This user account cannot be disabled

          A: Manage SSH Authorized Keys
          P: Manage SSH Key Pair
          L: Reset SSH Lockout
          C: Change/Enable Password (Chosen)
          N: [DISABLED] Disable Password Access
          M: Multifactor Authentication

          E: [DISABLED] Enable Account
          D: [DISABLED] Disable Account
```

©2026 Tanium Inc. All Rights Reserved

```
         T: Manage Account Protection
         X: [DISABLED] Delete User


         F: Edit known hosts file


         R: Return to previous menu  RR: Return to top
```

6. Enter `A` (Authorized Keys).
7. Enter `A` and follow the prompts to paste the public key generated in Step 1.

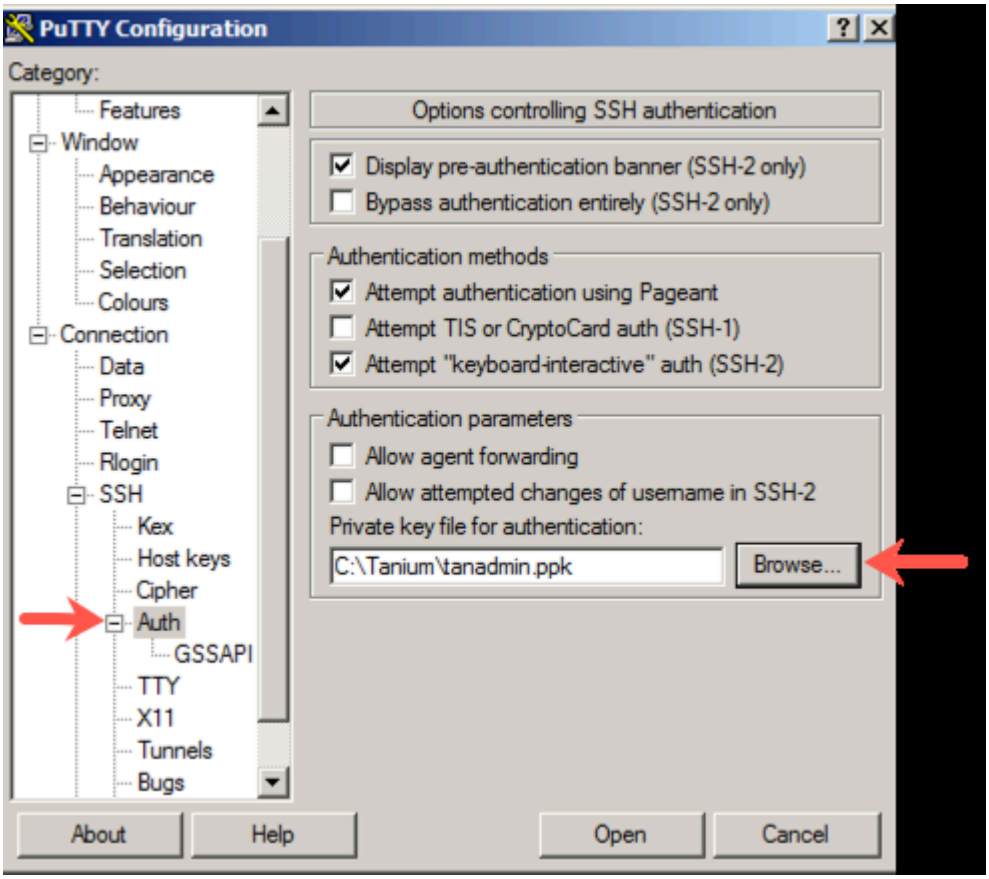
```
            >>> User Administration -> TanOS -> tanadmin -> Authorized Keys -> Add
<<<


 Account: tanadmin
 Please paste the public key and press enter:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCqXUnoyrg4opYQp4DGZoasYy8ud5oJEar9BqRr2RVHMm/
Sxcl4T1sthsN
WS0ECo0j32mCSM3ynYZn2AdJTU6HbKnFM30gtQL7+tpmGrgbkaVEJ9OXoA47JP0o5hbI16UUpuEKJrEBOYovI
srN2gtwKbz
YdOVCxVq5amzqg7/
UrQyUO3rmt54qStiqNIiHI3UjzPWYJwUxz90vU7LWsXYz1CAWBTXnh51kg0lBPFgbRmUZJb0DwLb4Sw
lFZAe5P0RO4RwdmZVgTfsqy+MVuyzaBzGD1z4MlIZ83R6sW+nXtipbzqhFTLykLRLIXobuHjuf0Yy1H7/
ZDJh/qlojce4TC
g/+5e2h1RQ8ZKgECZDJoCdrkAM6y9arHCoZwqEP9MXugQXCO6EMrP39vXajnV3YrDKKLYP1pxWZGOA4ylNqY5
mG1+AofVdG
vAUBztjXfXgC3bgL0Qgp+d3E8JvLRHXfkmRijppvj+BCJUawXJfkMtBEgrxQP9PoDwHrqJj6ey80v8P7DgojQ
w83JumsG3S
+7l0e0Ia02q/
05s2EpOv9jE9aJiLRGKbb4WkjvUSpK1VmDK54qfeSKj6yp3IIt13GBKmkVqKbbZS6gaZ3UTpzq3dj+53YeP
eOe8XMECuxl6aH4nLT4u3CqrCqxTfTa5y1Fi3/e9zI5/AKJlTXWF3ISCQ==
tanadmin@appliance-156.tam.local
 Validating input
 Adding key to authorized keys after validation
 Finished adding authorized keys for tanadmin
```

©2026 Tanium Inc. All Rights Reserved

```
Press enter to continue
```

8. To test, on your management computer, set up an SSH client such as PuTTY to connect to the Tanium Server Appliance:
    a. Specify the Tanium Server IP address, port 22, and SSH connection type.
    b. Under SSH, browse and select the private key that pairs with the public key uploaded to the Appliance.

    Figure 14. Selecting the private key for SSH authentication



    c. Open the SSH session and enter the `tanadmin` user name.
    d. You are prompted for the SSH key passphrase instead of the `tanadmin` password.

```
login as: tanadmin

######################## WARNING ########################

       Unauthorized access is strictly prohibited.

#########################################################

Authenticating with public key "rsa-key-20200119"
```

©2026 Tanium Inc. All Rights Reserved

```
Passphrase for key "rsa-key-20200119":
```

Add TanOS system users

About this task

Create additional TanOS system users based on `tanadmin` (privileged) and `tanuser` (restricted) profiles.

Best Practice: Create more than one privileged user with the `tanadmin` role in case you forget the password for the built-in `tanadmin` user.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter `A` and follow the prompts to add a system user.

```
           >>> User Administration -> System Users -> Add System User <<<

Adding a system user requires first name, last name, user name and user role.

Attention:
TanUser Role:  Monitor/Check the status of the appliance, no changes are allowed
TanAdmin Role: Full administrative role to manage the appliance

A temporary password will be generated and the new user is required to change
their password upon first login!

The password policy requires meeting these rules:
- Minimum of 10 characters long
- At least 1 upper case character
- At least 1 lower case character
- At least 1 numeric character
- At least 1 other character
- Must not match any of recent 4 passwords
```

©2026 Tanium Inc. All Rights Reserved

```
- Must not be based on a dictionary word
- Must not contain part of the username

Please enter first name: John
Please enter last name: Doe
Please enter desired user name (max 30 chars): john.doe
Which role should be assigned to john.doe?

1: TanUser (Monitoring)
2: TanAdmin (Administrative)

Please select: 2

The temporary password for john.doe is: proudbrownwildfowl

Adding local user john doe ...
Successfully added user john doe (username: john.doe) with role tanadmin.

Press enter to continue
```

Export the Disk Encryption Key

About this task

During initial startup, TanOS automatically creates a Disk Encryption Key with a randomly generated password and uses it to encrypt the disks; export this key and store it in a safe location immediately because it is required for recovery after a hardware failure.

The Disk Encryption Key is used by the Appliance to lock and unlock access to the encrypted disks. You can export the key and store it in a safe location. You must provide the key to recover data after a hardware failure. When you run a Health Check, you might see messages alerting you to export the Disk Encryption Key.

```
Boot Check: Pass (EFI Boot)
Active partition: pass (VolGroup1-root)

>>> Hardware health (will take 1-12 seconds) <<<
hardware type: pass (TV-220)
RAID controller RAID.Integrated.1-1 Security Key: pass
disk encryption: pass
```

©2026 Tanium Inc. All Rights Reserved

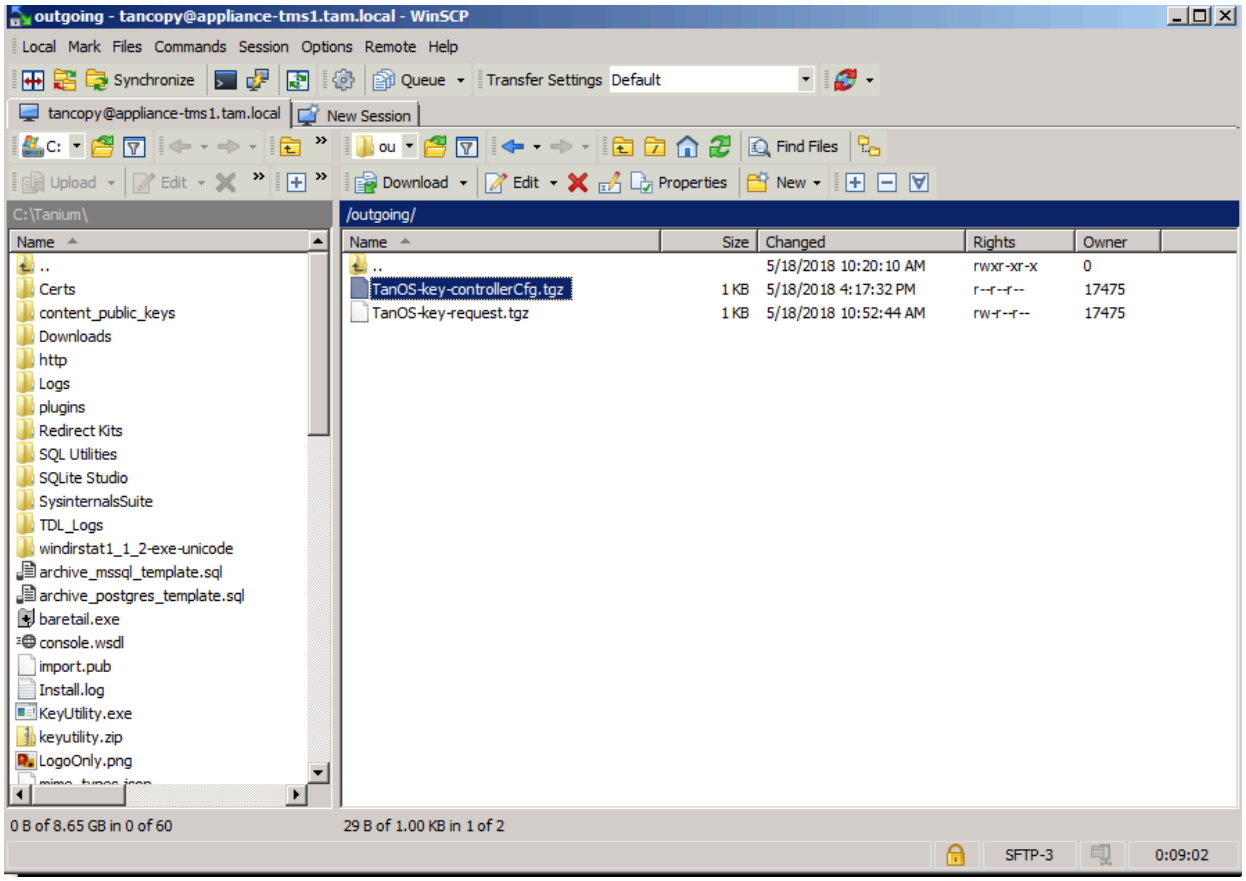
```
>>> Disk Encryption Key <<<

Disk Encryption Key check: fail (key has NOT been exported)  <--------

>>> Tanium Application file Permissions <<<

executed checks: 48
failed checks: 4
new health status setting: warning
```

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A`-`X`-`5` (Appliance Configuration > Advanced Configuration > Export Disk Encryption Key).
3. Follow the prompts to export the Disk Encryption Key to the /outgoing directory.

```
            >>> Appliance Configuration -> Advanced Menu -> Export Security Key <<<


Once the security key has been placed in the outgoing directory it
will remain until the nightly cleanup job is run. After this time it
will be deleted and must be exported again.
Please be sure to download it and save in a secure location.


Would you like to export the security key? [Yes|No]: yes


The security key has been placed in the sftp outgoing directory.
This location will be cleaned daily at 02:00am appliance time!


Press enter to continue
```

4. Use SFTP to copy the file from the /outgoing directory to your local computer.
   Figure 15. Copying the Disk Encryption Key file over SFTP

©2026 Tanium Inc. All Rights Reserved



Next steps

Important: Files copied to the /outgoing directory that are older than 24 hours are deleted every day at 02:00 AM UTC. You should copy the Disk Encryption Key file from the /outgoing directory to your local computer **immediately** after you have used the TanOS menu to export it and save it in a protected location. If you lose the Disk Encryption Key file, you can return to the Advanced Menu and export the key file again.

Tip: The default name of the Disk Encryption Key file is TanOS-key-controllerCfg.tgz. It is recommended to change the name to include the host name or serial number of the Appliance it came from before you store it. You likely have more than one Appliance, so a name based on a unique host name or serial number is useful if you later need to locate the correct file.

Export the GRUB key

About this task

©2026 Tanium Inc. All Rights Reserved

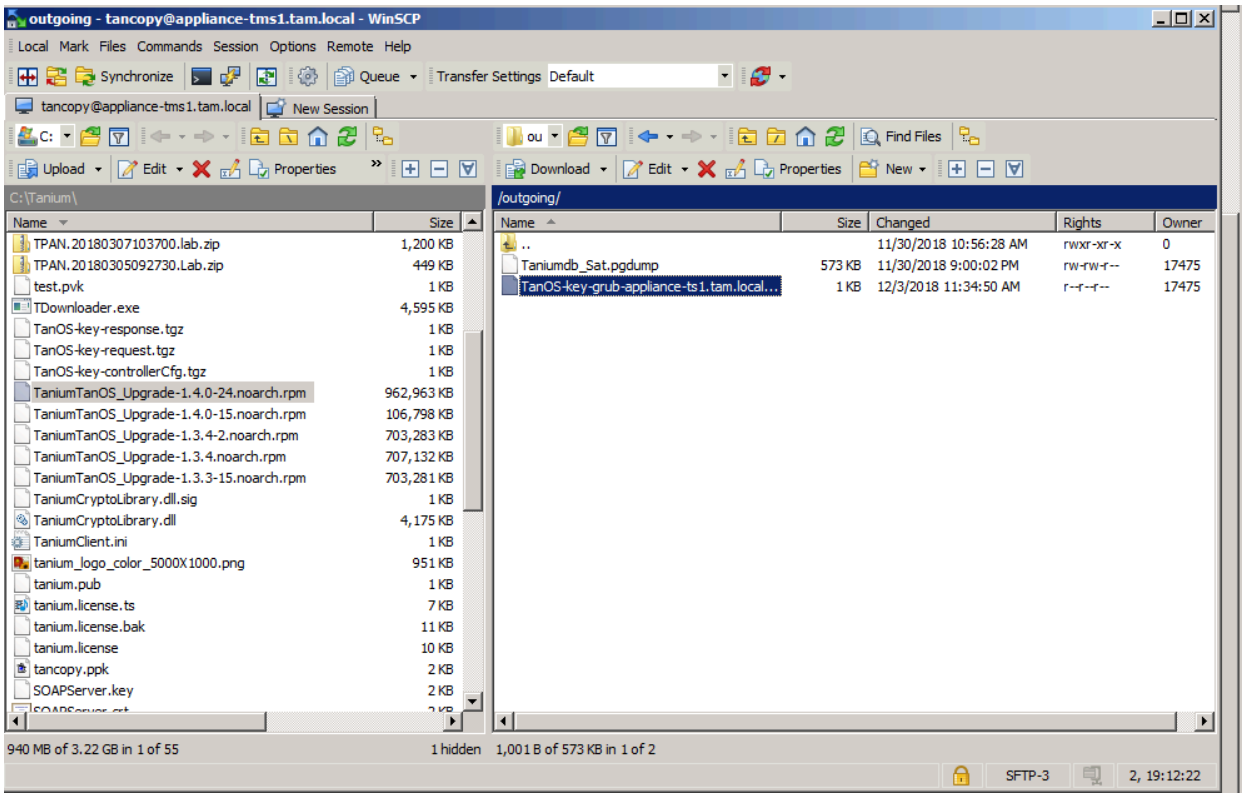
TanOS automatically generates the GRUB key during initial startup. The GRUB key can be used during the boot sequence to diagnose and recover from failure conditions. You can export the key and store it in a safe location. During recovery, you need to provide the key to Tanium Support for a technician to extract the GRUB password.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A`-`X` (Appliance Configuration > Advanced Configuration).
3. Enter `6` and follow the prompts to export the GRUB key to the /outgoing folder.

```
            >>> Appliance Configuration -> Advanced Menu -> Export Security Key <<<

Once the security key has been placed in the outgoing directory it
will remain until the nightly cleanup job is run. After this time it
will be deleted and must be exported again.
Please be sure to download it and save in a secure location.

Would you like to export the security key? [Yes|No]: yes

The security key has been placed in the sftp outgoing directory.
This location will be cleaned daily at 02:00am appliance time!

Press enter to continue
```

4. Use SFTP to copy the file from the /outgoing directory to your local computer.
   Figure 16. Copying the GRUB key file over SFTP

©2026 Tanium Inc. All Rights Reserved



What to do next

- It is a best practice to complete iDRAC configuration before you install Tanium Core Platform Servers. For more information, see Manage the iDRAC interface (physical Tanium Appliances only) on page 420.
- When these steps are completed, you can continue with the installation of an Appliance Array.

Completing the initial setup (virtual Tanium Appliance)

To begin deployment of Tanium Appliances, deploy images to your hypervisor, and then configure basic network, host, and user settings.

Requirements

HYPERVISORS AND IMAGE FORMATS

Tanium provides virtual Tanium Appliance images for the following hypervisors:

©2026 Tanium Inc. All Rights Reserved

Hypervisor	Virtual image format	Boot type
KVM	QCOW2	BIOS
VMware ESXi	OVA	UEFI
Microsoft Hyper-V	VHD	UEFI

Download the appropriate virtual image from the **Artifacts** section of your Tanium Account. For more information, see View Tanium artifacts.

Each virtual Tanium Appliance image contains the following default settings:

- 16GB RAM
- 4 CPU cores
- 1 NIC
- 500GB disk

Before you start the virtual Appliance for the first time, you might need to use the VM settings utility on the hypervisor to make changes to support the recommended specifications for your deployment size. For more information about sizing, see Cloud-based Tanium Appliance and virtual Tanium Appliance specifications on page 648.

VIRTUAL CPU

The VM on which the virtual Tanium Appliance is installed must use a CPU type that supports the x86-64-v2 architecture. You cannot upgrade to TanOS 1.9.0 or later if the CPU does not support x86-64-v2.

When using FIPS mode on the Appliance, the VM on which the virtual Tanium Appliance is installed must also use a CPU type that supports the RDSEED instruction. For more information about FIPS mode, see (FIPS-compliant organizations) Enable FIPS 140-3 mode before initial setup on page 133.

Deploy the virtual image to the hypervisor

About this task

©2026 Tanium Inc. All Rights Reserved

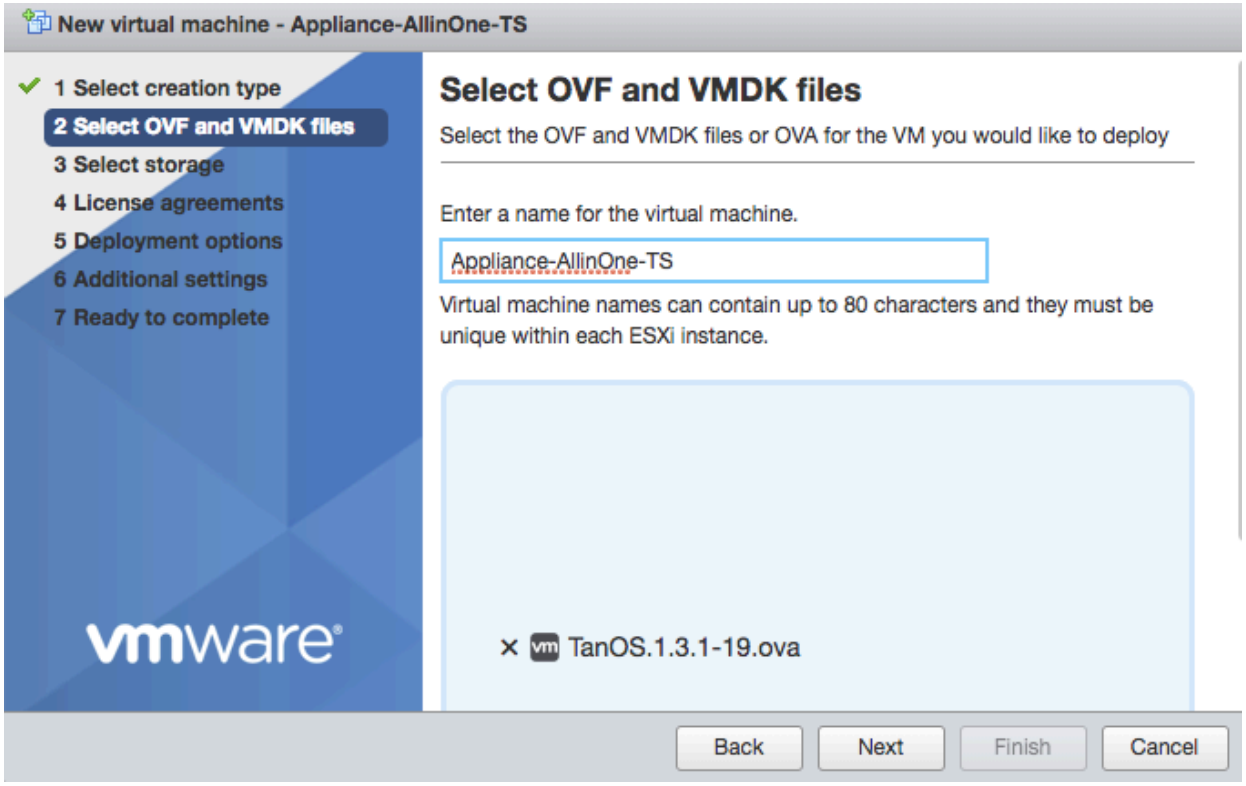
The steps in this section demonstrate a deployment of the virtual image through VMware ESXi. Perform the corresponding steps for your hypervisor.

Important:

- Virtual images must be deployed individually to ensure the serial numbers are unique; do not clone virtual images.
- Hyper-V requires the following options when you set up the VM:
  - Create the VM as a **Generation 2** VM.
  - Select the **Enable Secure Boot** option and the **Microsoft UEFI Certificate Authority** template.

1. Add the virtual image to vSphere or vCenter Server:
   - In vSphere, right-click the resource pool and select **Deploy OVF Template**
   - In vCenter Server, right-click **Virtual Machines** and select **Create/Register VM**.
2. Select the virtual image file and enter a unique name for the virtual machine.
   Figure 17. Naming the virtual machine during OVA deployment

©2026 Tanium Inc. All Rights Reserved



3. (Optional) Some environments might require changes to network adapter settings or other changes to the virtual image template settings. You might need to increase the settings from the default Cloud-based Tanium Appliance and virtual Tanium Appliance specifications on page 648. If necessary, make the changes before starting the virtual machine.
4. Start the virtual machine.
5. The boot prompt has an option to load the active or inactive partition. Load the active partition (selected by default).

   Best Practice: The TanOS QCOW2 image includes the QEMU guest agent. If you are using a KVM hypervisor, configure a VirtIO serial port in the virtual machine hardware settings to establish a dedicated communication channel between the KVM hypervisor and the QEMU guest agent, which supports graceful shutdowns and snapshot quiescing. TanOS disables operations that allow the hypervisor to access or transfer files, execute commands, or change user passwords inside the guest.

(Optional) Change keyboard mapping for virtual console

About this task

If you want to change the keyboard mapping from the default (**us**) to a different layout, you can

©2026 Tanium Inc. All Rights Reserved

change this setting before you create a new password for the `tanadmin` user account and start initial configuration.

1. Open the VM host console for the Tanium Appliance and then sign in as the `tanadmin` user with the default password `Tanium1`.

```
------------------------------------------------------


>>> Initial Configuration <<<


Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.


Keymap:     us
IP Address:
Hostname:   initial-tanos-347587.localdomain
FIPS 140-3: disabled


         1: Set Virtual Console Keymap
         M: Toggle FIPS 140-3 Mode


         P: Set Password                   (INCOMPLETE)
            Set the password to continue configuration
         F: [DISABLED] Finish Initial Configuration
         S: Shutdown


         Z: Log out


------------------------------------------------------


TanOS Version:        1.9.1


Please select:
```

2. Enter `1` (Set Keymap).
3. Enter `2` to go to a list of available keyboard mappings. Use the spacebar key to page through the list, and then enter the name of the desired mapping.

©2026 Tanium Inc. All Rights Reserved

```
 ----------------------------------------------------
Current keymap: us
Displaying all available keymaps. Space to continue or Q to quit

ANSI-dvorak                     al
al-plisi                        amiga-de
amiga-us                        applkey
at                              at-mac
at-nodeadkeys                   at-sundeadkeys
atari-de                        atari-se
atari-uk-falcon                 atari-us
az                              azerty
ba                              ba-alternatequotes
ba-unicode                      ba-unicodeus
ba-us                           backspace
bashkir                         be
be-iso-alternate                be-latin1
be-nodeadkeys                   be-oss
be-oss_latin9                   be-oss_sundeadkeys
be-sundeadkeys                  be-wang
bg-cp1251                       bg-cp855
bg_bds-cp1251                   bg_bds-utf8
bg_pho-cp1251                   bg_pho-utf8
br                              br-abnt
br-abnt2                        br-dvorak
br-latin1-abnt2                 br-latin1-us
br-nativo                       br-nativo-epo
br-nativo-us                    br-nodeadkeys
br-thinkpad                     by
by-cp1251                       by-latin
bywin-cp1251                    ca
ca-eng                          ca-fr-dvorak
ca-fr-legacy                    ca-multi
ca-multix                       cf
ch                              ch-de_mac
ch-de_nodeadkeys                ch-de_sundeadkeys
```

©2026 Tanium Inc. All Rights Reserved

```
ch-fr                          ch-fr_mac
ch-fr_nodeadkeys               ch-fr_sundeadkeys
ch-legacy                      cm
cm-azerty                      cm-dvorak
cm-french                      cm-mmuock
cm-qwerty                      cn
cn-altgr-pinyin                croat
ctrl                           cz
cz-bksl                        cz-cp1250
cz-dvorak-ucw                  cz-lat2
cz-lat2-prog                   cz-qwerty
cz-qwerty_bksl                 cz-rus
cz-us-qwertz                   de
de-T3                          de-deadacute
de-deadgraveacute              de-deadtilde
de-dsb                         de-dsb_qwertz
de-dvorak                      de-latin1
de-latin1-nodeadkeys           de-mac
de-mac_nodeadkeys              de-mobii
de-neo                         de-nodeadkeys
de-qwerty                      de-ro
de-ro_nodeadkeys               de-sundeadkeys
de-tr                          de_CH-latin1
de_alt_UTF-8                   defkeymap
defkeymap_V1.0                 dk
dk-dvorak                      dk-latin1
dk-mac                         dk-mac_nodeadkeys
dk-nodeadkeys                  dk-winkeys
dvorak                         dvorak-ca-fr
dvorak-es                      dvorak-fr
dvorak-l                       dvorak-r
dvorak-ru                      dvorak-sv-a1
dvorak-sv-a5                   dvorak-uk
dz                             ee
ee-dvorak                      ee-nodeadkeys
ee-us                          emacs
```

©2026 Tanium Inc. All Rights Reserved

```
emacs2                          en-latin9
epo                             epo-legacy
es                              es-ast
es-cat                          es-cp850
es-deadtilde                    es-dvorak
es-mac                          es-nodeadkeys
es-olpc                         es-sundeadkeys
es-winkeys                      et
et-nodeadkeys                   euro
euro1                           euro2
fi                              fi-classic
fi-das                          fi-latin1
fi-latin9                       fi-mac
fi-nodeadkeys                   fi-old
fi-smi                          fi-winkeys
fo                              fo-nodeadkeys
fr                              fr-azerty
fr-bepo                         fr-bepo_latin9
fr-bre                          fr-dvorak
fr-latin0                       fr-latin1
fr-latin9                       fr-latin9_nodeadkeys
fr-latin9_sundeadkeys           fr-mac
fr-nodeadkeys                   fr-oci
fr-old                          fr-oss
fr-oss_latin9                   fr-oss_nodeadkeys
fr-oss_sundeadkeys              fr-pc
fr-sundeadkeys                  fr_CH
fr_CH-latin1                    gb
gb-colemak                      gb-dvorak
gb-dvorakukp                    gb-extd
gb-intl                         gb-mac
gb-mac_intl                     ge
ge-ergonomic                    ge-mess
ge-ru                           gh
gh-akan                         gh-avn
gh-ewe                          gh-fula
```

©2026 Tanium Inc. All Rights Reserved

```
gh-ga                           gh-generic
gh-gillbt                       gh-hausa
gr                              gr-pc
hr                              hr-alternatequotes
hr-unicode                      hr-unicodeus
hr-us                           hu
hu-101_qwerty_comma_dead        hu-101_qwerty_comma_nodead
hu-101_qwerty_dot_dead          hu-101_qwerty_dot_nodead
hu-101_qwertz_comma_dead        hu-101_qwertz_comma_nodead
hu-101_qwertz_dot_dead          hu-101_qwertz_dot_nodead
hu-102_qwerty_comma_dead        hu-102_qwerty_comma_nodead
hu-102_qwerty_dot_dead          hu-102_qwerty_dot_nodead
hu-102_qwertz_comma_dead        hu-102_qwertz_comma_nodead
hu-102_qwertz_dot_dead          hu-102_qwertz_dot_nodead
hu-nodeadkeys                   hu-qwerty
hu-standard                     hu101
ie                              ie-CloGaelach
ie-UnicodeExpert                ie-ogam_is434
il                              il-heb
il-phonetic                     in-eng
iq-ku                           iq-ku_alt
iq-ku_ara                       iq-ku_f
ir-ku                           ir-ku_alt
ir-ku_ara                       ir-ku_f
is                              is-Sundeadkeys
is-dvorak                       is-latin1
is-latin1-us                    is-mac
is-mac_legacy                   is-nodeadkeys
it                              it-geo
it-ibm                          it-intl
it-mac                          it-nodeadkeys
it-scn                          it-us
it-winkeys                      it2
jp                              jp-OADG109A
jp-dvorak                       jp-kana86
jp106                           kazakh
```

©2026 Tanium Inc. All Rights Reserved

```
ke                              ke-kik
keypad                          kr
kr-kr104                        ky_alt_sh-UTF-8
kyrgyz                          la-latin1
latam                           latam-deadtilde
latam-dvorak                    latam-nodeadkeys
latam-sundeadkeys               lk-us
lt                              lt-ibm
lt-lekp                         lt-lekpa
lt-std                          lt-us
lt.baltic                       lt.l4
lv                              lv-adapted
lv-apostrophe                   lv-ergonomic
lv-fkey                         lv-modern
lv-tilde                        ma-french
mac-be                          mac-de-latin1
mac-de-latin1-nodeadkeys        mac-de_CH
mac-dk-latin1                   mac-dvorak
mac-es                          mac-euro
mac-euro2                       mac-fi-latin1
mac-fr                          mac-fr_CH-latin1
mac-it                          mac-pl
mac-pt-latin1                   mac-se
mac-template                    mac-uk
mac-us                          md
md-gag                          me
me-latinalternatequotes         me-latinunicode
me-latinunicodeyz               me-latinyz
mk                              mk-cp1251
mk-utf                          mk0
ml                              ml-fr-oss
ml-us-intl                      ml-us-mac
mm                              mt
mt-us                           ng
ng-hausa                        ng-igbo
ng-yoruba                       nl
```

©2026 Tanium Inc. All Rights Reserved

```
nl-mac                          nl-std
nl-sundeadkeys                  nl2
no                              no-colemak
no-dvorak                       no-latin1
no-mac                          no-mac_nodeadkeys
no-nodeadkeys                   no-smi
no-smi_nodeadkeys               no-winkeys
pc110                           ph
ph-capewell-dvorak              ph-capewell-qwerf2k6
ph-colemak                      ph-dvorak
pl                              pl-csb
pl-dvorak                       pl-dvorak_altquotes
pl-dvorak_quotes                pl-dvp
pl-legacy                       pl-qwertz
pl-szl                          pl1
pl2                             pl3
pl4                             pt
pt-latin1                       pt-latin9
pt-mac                          pt-mac_nodeadkeys
pt-mac_sundeadkeys              pt-nativo
pt-nativo-epo                   pt-nativo-us
pt-nodeadkeys                   pt-olpc
pt-sundeadkeys                  ro
ro-cedilla                      ro-std
ro-std_cedilla                  ro-winkeys
ro_std                          rs-latin
rs-latinalternatequotes         rs-latinunicode
rs-latinunicodeyz               rs-latinyz
ru                              ru-cp1251
ru-cv_latin                     ru-ms
ru-yawerty                      ru1
ru2                             ru3
ru4                             ru_win
ruwin_alt-CP1251                ruwin_alt-KOI8-R
ruwin_alt-UTF-8                 ruwin_alt_sh-UTF-8
ruwin_cplk-CP1251               ruwin_cplk-KOI8-R
```

©2026 Tanium Inc. All Rights Reserved

```
ruwin_cplk-UTF-8                ruwin_ct_sh-CP1251
ruwin_ct_sh-KOI8-R              ruwin_ct_sh-UTF-8
ruwin_ctrl-CP1251               ruwin_ctrl-KOI8-R
ruwin_ctrl-UTF-8                se
se-dvorak                       se-fi-ir209
se-fi-lat6                      se-ir209
se-lat6                         se-latin1
se-mac                          se-nodeadkeys
se-smi                          se-svdvorak
se-us                           se-us_dvorak
sg                              sg-latin1
sg-latin1-lk450                 si
si-alternatequotes              si-us
sk                              sk-bksl
sk-prog-qwerty                  sk-prog-qwertz
sk-qwerty                       sk-qwerty_bksl
sk-qwertz                       slovene
sr-cy                           sun-pl
sun-pl-altgraph                 sundvorak
sunkeymap                       sunt4-es
sunt4-fi-latin1                 sunt4-no-latin1
sunt5-cz-us                     sunt5-de-latin1
sunt5-es                        sunt5-fi-latin1
sunt5-fr-latin1                 sunt5-ru
sunt5-uk                        sunt5-us-cz
sunt6-uk                        sv-latin1
sy-ku                           sy-ku_alt
sy-ku_f                         tj_alt-UTF8
tm                              tm-alt
tr                              tr-alt
tr-crh                          tr-crh_alt
tr-crh_f                        tr-f
tr-intl                         tr-ku
tr-ku_alt                       tr-ku_f
tr-sundeadkeys                  tr_f-latin5
tr_q-latin5                     tralt
```

©2026 Tanium Inc. All Rights Reserved

```
trf                             trf-fgGIod
trq                             ttwin_alt-UTF-8
ttwin_cplk-UTF-8                ttwin_ct_sh-UTF-8
ttwin_ctrl-UTF-8                tw
tw-indigenous                   tw-saisiyat
ua                              ua-cp1251
ua-utf                          ua-utf-ws
ua-ws                           uk
unicode                         us
us-acentos                      us-alt-intl
us-altgr-intl                   us-colemak
us-dvorak                       us-dvorak-alt-intl
us-dvorak-classic               us-dvorak-intl
us-dvorak-l                     us-dvorak-r
us-dvp                          us-euro
us-hbs                          us-intl
us-mac                          us-olpc2
us-workman                      us-workman-intl
uz-latin                        wangbe
wangbe2                         windowkeys

 Current keymap: us
 Enter the desired keymap:
```

Next steps

Tip: To change the keyboard mapping at a later time, enter `A-X-8` (Appliance Configuration > Advanced Configuration > Set Virtual Console Keymap).

(FIPS-compliant organizations) Enable FIPS 140-3 mode before initial setup

About this task

©2026 Tanium Inc. All Rights Reserved

Enabling Federal Information Processing Standards (FIPS) mode causes the Appliance to use a FIPS-validated cryptographic module for all cryptographic operations. It also ensures that services like SSH use only cryptographic algorithms that FIPS 140-3 allows.

If FIPS mode is required for your organization, you can enable it before you continue with initial setup so that the password and keys that you configure during setup are FIPS-compliant.

Best Practice: Enable FIPS mode only if you are required to do so for your organization.

Important: To use FIPS mode, the VM on which the virtual Tanium Appliance is installed must use a CPU type that supports the RDSEED instruction.

Note:

- Enabling FIPS mode in TanOS also puts the Tanium Platform in FIPS mode.
- You can later disable FIPS mode if it is not required and it was inadvertently enabled during setup. For more information, see Enable FIPS 140-3 mode on page 362.

1. Sign in to the TanOS console as the `tanadmin` user.
2. Enter `M` and follow the prompt to enable FIPS 140-3 mode and reboot the Appliance, and then continue initial setup.

Configuration options

- Perform full initial configuration on page 107 if you want to complete all of the initial configuration steps at once from the console.
- Configure IP address only on page 113 if you want to complete the network configuration from the console and then later resume initial configuration elsewhere (for example, in a different location through an SSH connection).

©2026 Tanium Inc. All Rights Reserved

Perform full initial configuration

You can perform initial configuration in the order that you prefer. As you finish configuring settings, their status in the checklist changes from incomplete to complete.

BEFORE YOU BEGIN

Configure the password for the `tanadmin` user account. This is required before you can connect to the network and start initial configuration.

COMPLETE THE INITIAL CONFIGURATION

1. Open the VM host console for the Tanium Appliance and then sign in as the `tanadmin` user with the default password `Tanium1`.

```
------------------------------------------------------


>>> Initial Configuration <<<


Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.


Keymap:     us
IP Address:
Hostname:   initial-tanos-347587.localdomain
FIPS 140-3: disabled


         1: Set Virtual Console Keymap
         M: Toggle FIPS 140-3 Mode


         P: Set Password                   (INCOMPLETE)
            Set the password to continue configuration
         F: [DISABLED] Finish Initial Configuration
         S: Shutdown


         Z: Log out
```

©2026 Tanium Inc. All Rights Reserved

```
-----------------------------------------------------

TanOS Version:        1.9.1

Please select:
```

If the IP address was already configured, sign in with the password that was set in the data center, and then proceed with the rest of the initial configuration steps.

2. Enter `P`, and then follow the prompts to change the password.

```
-----------------------------------------------------

>>> Initial Config -> Set Password <<<

Preparing to change the password for tanadmin

The password policy requires meeting these rules:
 - Minimum of 10 characters long
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
 - At least 1 other character
 - Must not match any of recent 4 passwords
 - Must not be based on a dictionary word
 - Must not contain part of the username

Please enter password (will not be displayed):
Password score: 55 out of 100 (strong)
Please enter password again:

The password change was successful.

Press enter to continue
```

©2026 Tanium Inc. All Rights Reserved

Tip: Follow the password policy guidelines closely. Note the password score that appears and aim for a strong password.

Important: Remember this password and, if possible, store it in a password vault approved by your organization. If you have not created a second privileged user with the tanadmin role, this password cannot be recovered.

3. Press the **Enter** key to return to the **Initial Configuration** menu.

```
------------------------------------------------------


>>> Initial Configuration <<<


Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.


Keymap:     us
IP Address:
Hostname:   initial-tanos-347587.localdomain
FIPS 140-3: disabled


         1: Set Virtual Console Keymap
         M: Toggle FIPS 140-3 Mode


         P: Set Password                    (complete)
         A: Set IP Address                  (INCOMPLETE)
         N: Set FQDN (hostname)             (INCOMPLETE)
         D: Set DNS Nameservers             (INCOMPLETE)
         T: Set NTP (time)                  (INCOMPLETE)
         E: View and Accept EULA            (INCOMPLETE)


         F: [DISABLED] Finish Initial Configuration
         S: Shutdown


         Z: Log out
```

©2026 Tanium Inc. All Rights Reserved

```
-----------------------------------------------------

TanOS Version:        1.9.1

Please select:
```

4. If necessary, enter `A`, and then follow the prompts to set the static IP address, IPv6 settings, and gateway.

```
           >>> Network Configuration <<< >

Note: any existing IP address listed below is NOT persistent/DHCP assigned.

Please provide a static IP address below regardless of the current
configuration. At the end of the initial configuration routine you will be
logged out. If the IP address is changed then you will need to modify your
connection settings to reach the TanOS menu.

Available interfaces:

        #: Interface  State  Link    MAC                IP                  Location
        1: ens160     UP      UP     00:0c:29:35:f4:fa  10.10.10.60/24      virtual

Please select: 1
Current settings:
  Interface: ens160
  IPv4 Address: 10.10.10.60/24
  Default IPv4 Gateway: 10.10.10.2
  IPv6 Address: fe80::20c:29ff:fec3:4afa/64
  IPv6 Gateway:
  Advertised Speeds: 1Gbps 10Gbps 25Gbps

Enter the IPv4 address/prefix (e.g. 10.2.3.4/24): 10.10.10.60/24
Enter the IPv4 gateway address (e.g. 10.2.3.1): 10.10.10.2
Would you like to accept default IPv6 settings? [Yes|No]: yes
```

©2026 Tanium Inc. All Rights Reserved

```
Would you like to accept the current Ethernet advertised speeds? [Yes|No]: yes


New settings:
  Interface: ens160
  IPv4 Address: 10.10.10.60/24
  Default IPv4 Gateway: 10.10.10.2
  Manual IPv6:  No
  IPv6 Address: fe80::20c:29ff:fec3:4afa/64
  IPv6 Gateway:
  Advertised Speeds: 1Gbps 10Gbps 25Gbps


Are these settings correct? [Yes|No]: yes
```

5. After the initial configuration screen appears with the updated IP address configuration, enter `N` and then follow the prompts to configure the fully qualified domain name (FQDN).

```
>>> Initial Config -> Set FQDN <<<


Current hostname (FQDN):


New FQDN: fqdn.example.com



Setting new hostname (FQDN):
fqdn.example.com


Do you want to continue? [Yes|No]: Yes
```



Important: Use an FQDN that is accessible from any computer from which a user will access Tanium Console.

6. After the initial configuration screen appears with the updated FQDN configuration, enter `D` and then follow the prompts to set the DNS name servers.

```
>>> Initial Config -> Set Nameservers <<<


Currently configured nameserver(s):
```

©2026 Tanium Inc. All Rights Reserved

```
Enter the first DNS server address: 10.10.10.10
Enter the second DNS server address:

Setting nameserver 1: 10.10.10.10
Setting nameserver 2:

Do you want to continue? [Yes|No]: Yes
```

7. After the initial configuration screen appears with the updated DNS configuration, enter `T` and then follow the prompts to set the NTP servers.

```
>>> NTP Configuration <<<

Timezone will be automatically set to UTC.

Enter the NTP server information for up to two NTP servers. Each entry consist
of a server name or IP address.
Optionally each server may indicate authentication information using
colons as a separator: >server<:>key-id<:>SHA1|MD5<:key



1.2.3.4
pool.ntp.org
ntp.secret.corp:999:SHA1:0123456789abcdef0123456789abcdef01234567



Please provide the NTP server address: pool.ntp.org
Please provide the second NTP server address (enter blank value for none):

The following settings will be used:

    NTP Server 1: pool.ntp.org
    NTP Server 2:

Are these settings correct? [Yes|No]: Yes
```

©2026 Tanium Inc. All Rights Reserved

> **Tip:** On AWS and GCP appliances, if no NTP server is configured when you finish initial configuration, TanOS automatically sets the default NTP server for the cloud provider. Configure an NTP server manually if you require a specific server.

8. After the initial configuration screen appears with the updated NTP configuration, enter `E` and then use the spacebar to page through the end-user license agreement (EULA). When complete, press the **Q** key, enter your email address, and enter YES to accept it.
   The email address is stored locally only. It is not used externally for any reason.

9. Enter `F` to finish initial configuration. The Appliance reboots, and when you sign in, the initial configuration menu is replaced by the `tanadmin` menu.

   > **Note:** Before you can finish initial configuration, you must have changed the `tanadmin` password, set the host name and DNS server, configured an NTP server, and accepted the EULA. If any requirement is unmet, TanOS reports which steps remain and exits without completing the configuration.

Configure IP address only

In some virtual infrastructure environments, only the VM administrator has access to the VM console to set up new VMs. If necessary, the VM administrator can use the `tanadmin` account to set up the IP address only so the VM host is accessible through SSH.

BEFORE YOU BEGIN

- You must be able to access the VM console.
- Configure the password for the `tanadmin` user account. This is required before you can connect to the network and start initial configuration.

CONFIGURE THE IP ADDRESS SETTINGS

1. Open the VM host console for the Tanium Appliance and then sign in as the `tanadmin` user with the default password `Tanium1`.

   ```
   ------------------------------------------------------
   ```

©2026 Tanium Inc. All Rights Reserved

```
>>> Initial Configuration <<<

Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.

Keymap:     us
IP Address:
Hostname:   initial-tanos-347587.localdomain
FIPS 140-3: disabled

         1: Set Virtual Console Keymap
         M: Toggle FIPS 140-3 Mode

         P: Set Password                   (INCOMPLETE)
            Set the password to continue configuration
         F: [DISABLED] Finish Initial Configuration
         S: Shutdown

         Z: Log out

--------------------------------------------------------

TanOS Version:        1.9.1

Please select:
```

2. Enter `P`, and then follow the prompts to change the password.

```
--------------------------------------------------------

>>> Initial Config -> Set Password <<<

Preparing to change the password for tanadmin

The password policy requires meeting these rules:
 - Minimum of 10 characters long
```

```
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
 - At least 1 other character
 - Must not match any of recent 4 passwords
 - Must not be based on a dictionary word
 - Must not contain part of the username

 Please enter password (will not be displayed):
Password score: 55 out of 100 (strong)
 Please enter password again:

 The password change was successful.

 Press enter to continue
```


Tip: Follow the password policy guidelines closely. Note the password score that appears and aim for a strong password.

3. Press the **Enter** key to return to the **Initial Configuration** menu.

```
--------------------------------------------------


>>> Initial Configuration <<<

 Initial configuration workflow for a new TanOS Appliance.
 All items must be complete before the Appliance can be used.

 Keymap:     us
 IP Address:
 Hostname:   initial-tanos-347587.localdomain
 FIPS 140-3: disabled

          M: Toggle FIPS 140-3 Mode
```

©2026 Tanium Inc. All Rights Reserved

```
         P: Set Password                   (complete)
         A: Set IP Address                 (INCOMPLETE)
         N: Set FQDN (hostname)            (INCOMPLETE)
         D: Set DNS Nameservers            (INCOMPLETE)
         T: Set NTP (time)                 (INCOMPLETE)
         E: View and Accept EULA           (INCOMPLETE)

         F: [DISABLED] Finish Initial Configuration
         S: Shutdown

         Z: Log out

-------------------------------------------------------

TanOS Version:        1.9.1

Please select:
```

4. Enter `A`, and then follow the prompts to specify the IPv4 address with prefix, and the default IPv4 gateway. You can also configure the IPv6 address with prefix, and the IPv6 gateway. The TanOS console confirms that the settings are applied.

```
           >>> Network Configuration <<< >

Note: any existing IP address listed below is NOT persistent/DHCP assigned.

Please provide a static IP address below regardless of the current
configuration. At the end of the initial configuration routine you will be
logged out. If the IP address is changed then you will need to modify your
connection settings to reach the TanOS menu.

Available interfaces:

        #: Interface  State  Link    MAC               IP                 Location
        1: ens160     UP      UP     00:0c:29:35:f4:fa  10.10.10.60/24     virtual
```

©2026 Tanium Inc. All Rights Reserved

```
Please select: 1
Current settings:
  Interface: ens160
  IPv4 Address: 10.10.10.60/24
  Default IPv4 Gateway: 10.10.10.2
  IPv6 Address: fe80::20c:29ff:fec3:4afa/64
  IPv6 Gateway:
  Advertised Speeds: 1Gbps 10Gbps 25Gbps

Enter the IPv4 address/prefix (e.g. 10.2.3.4/24): 10.10.10.60/24
Enter the IPv4 gateway address (e.g. 10.2.3.1): 10.10.10.2
Would you like to accept default IPv6 settings? [Yes|No]: yes
Would you like to accept the current Ethernet advertised speeds? [Yes|No]: yes

New settings:
  Interface: ens160
  IPv4 Address: 10.10.10.60/24
  Default IPv4 Gateway: 10.10.10.2
  Manual IPv6:  No
  IPv6 Address: fe80::20c:29ff:fec3:4afa/64
  IPv6 Gateway:
  Advertised Speeds: 1Gbps 10Gbps 25Gbps

Are these settings correct? [Yes|No]: yes
```

The IP address setting changes from incomplete to complete. You can sign out of the console and connect through SSH later to resume the initial configuration steps. For more information, see Perform full initial configuration on page 107.

Access TanOS remotely

To access your Tanium Appliances remotely, note the following requirements.

- Your local management computer must be connected to a subnet that can reach the Appliance IP address.

©2026 Tanium Inc. All Rights Reserved

- Your management computer must have an SSH client application or terminal emulator that can make a Client connection to the Appliance.
- You must have an SSH client such as PuTTY to sign in to the TanOS console. For PuTTY, use version 0.71 or later.
- You must have an SSH key generator such as ssh-keygen to generate keys for the tancopy user.
- You must have an SFTP client such as WinSCP to copy files to and from the Appliance. For WinSCP, use version 5.15.2 or later.

Tip: Watch the tutorial about how to configure WinSCP for the Tanium Appliance.

Add TanOS system users

About this task

Create additional TanOS system users based on `tanadmin` (privileged) and `tanuser` (restricted) profiles.



Best Practice: Create more than one privileged user with the `tanadmin` role in case you forget the password for the built-in `tanadmin` user.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C-U` (User Administration > TanOS User Management).
3. Enter `A` and follow the prompts to add a system user.

```
          >>> User Administration -> System Users -> Add System User <<<

Adding a system user requires first name, last name, user name and user role.

Attention:
```

©2026 Tanium Inc. All Rights Reserved

```
TanUser Role:  Monitor/Check the status of the appliance, no changes are allowed
TanAdmin Role: Full administrative role to manage the appliance

A temporary password will be generated and the new user is required to change
their password upon first login!

The password policy requires meeting these rules:
- Minimum of 10 characters long
- At least 1 upper case character
- At least 1 lower case character
- At least 1 numeric character
- At least 1 other character
- Must not match any of recent 4 passwords
- Must not be based on a dictionary word
- Must not contain part of the username

Please enter first name: John
Please enter last name: Doe
Please enter desired user name (max 30 chars): john.doe
Which role should be assigned to john.doe?

1: TanUser (Monitoring)
2: TanAdmin (Administrative)

Please select: 2

The temporary password for john.doe is: proudbrownwildfowl

Adding local user john doe ...
Successfully added user john doe (username: john.doe) with role tanadmin.

Press enter to continue
```

Configure SSH keys

TanOS has built-in and customer-created user accounts to access the Appliance operating system and perform tasks.

©2026 Tanium Inc. All Rights Reserved

Before you install a Tanium Appliance role, you must add SSH keys to authenticate access for the `tancopy` built-in user. `tancopy` can make an SFTP connection with SSH key authentication to TanOS and copy files to and from the /incoming and /outgoing directories. For Google Cloud Platform, you must also set up an SSH key for the `tanadmin` user account, even if you primarily plan to use other user accounts with the `tanadmin` role.

Best Practice: Set up SSH key authentication for all TanOS user accounts.

Important: TanOS does not support self-service password reset methods. If you forget your password, you must ask a user with the tanadmin role to reset it for you. You can avoid this risk by setting up SSH key authentication.

Tip: Watch the tutorial about how to configure SSH key authentication for the Tanium Appliance.

BEFORE YOU BEGIN

- You must have an SSH client to sign in to the TanOS console, and an SFTP client to copy files to and from the Appliance.
- You must have an SSH key generator to generate keys for the `tancopy` user.

ADD AND TEST AN SSH KEY FOR THE TANCOPY USER

Add an SSH key for the `tancopy` user, and then test the SFTP connection to confirm that the key works.

Add the SSH key for the tancopy user

1. Use an SSH key generator such as ssh-keygen to generate a public/private key pair. Note:
    - Specify an RSA key with 2048 bits (such as ssh-keygen -t rsa -b 2048).
    - Specify a passphrase that is easy to remember.

©2026 Tanium Inc. All Rights Reserved

- Save the private key to a location that you can access when you set up your SFTP client.

2. Copy the text in the public key file to the clipboard. If you use ssh-keygen, copy the contents of the .pub file that you created.

   Important: In an SSH key exchange, the keys must match exactly, including line endings.

3. Sign in to the TanOS console as a user with the `tanadmin` role.
4. Enter `C-U` (User Administration > TanOS User Management).
5. Enter the line number for the `tancopy` user to go to the user administration menu for this user.

```
          >>> User Administration -> TanOS -> tancopy <<<

Username:         tancopy
Account Enabled:  Yes
Authentication:   SSH Key Only
Password Expires: N/A
SSH Lockout:      No (0)
Multifactor:      Not configured
Protected:        No

Notes:
  * This user account cannot be deleted
  * This user account cannot have a password
  * This user account cannot use multifactor

         A: Manage SSH Authorized Keys
         P: Manage SSH Key Pair
         L: Reset SSH Lockout
         C: [DISABLED] Change Password
         N: [DISABLED] Disable Password Access
         M: [DISABLED] Multifactor Authentication
```

©2026 Tanium Inc. All Rights Reserved

```
          E: Enable Account
          D: Disable Account
          T: [DISABLED] Manage Account Protection
          X: [DISABLED] Delete User

          F: Edit known hosts file

          R: Return to previous menu  RR: Return to top

--------------------------------------------------
```

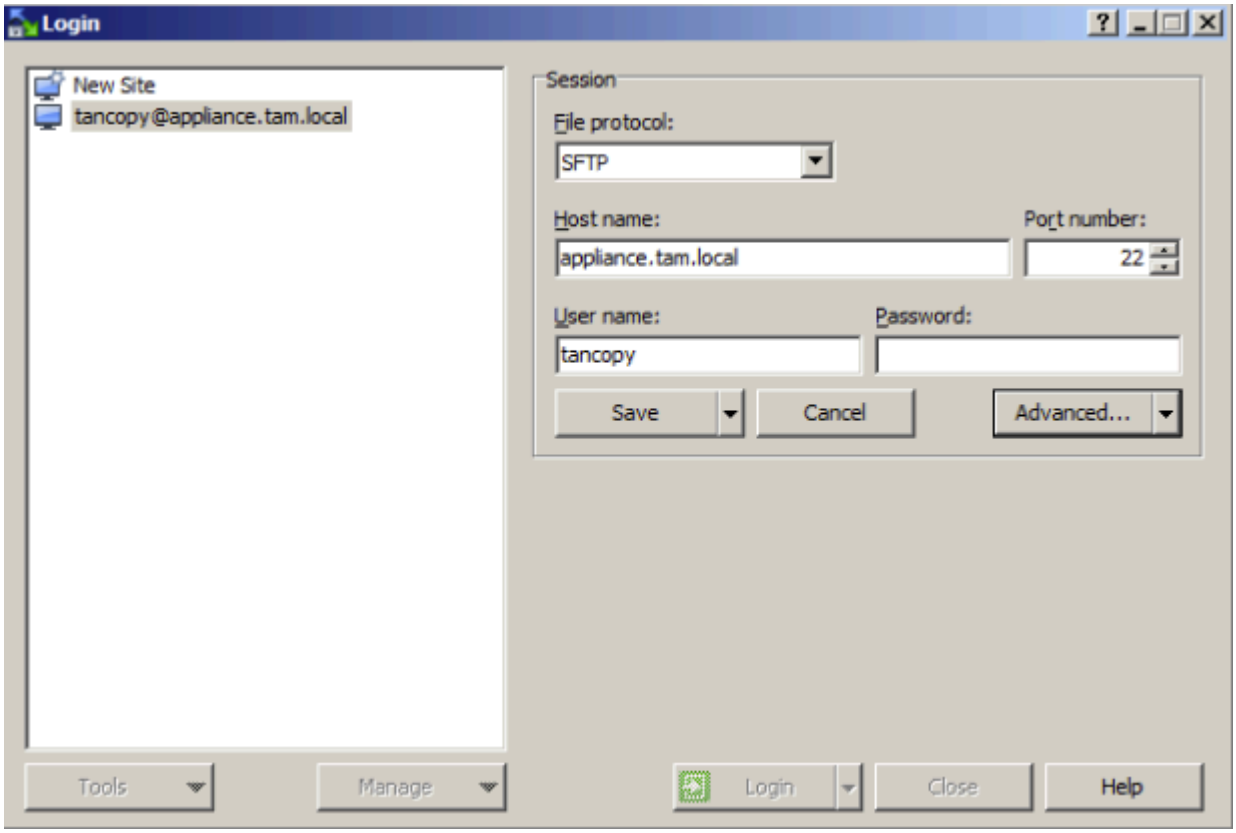
6. Enter `A` (Authorized Keys).
7. Enter `A` and follow the prompts to add the contents of the public key generated in Step 1.

```
            >>> User Administration -> TanOS -> tancopy -> Authorized Keys -> Add
<<<

Account: tancopy
Please paste the public key and press enter:
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA1ClmgkMrbbxB7jND/Y4/
Giupck35xAuGNKfZWqVLM5F0CNXuTScf6v2z
MDxW5TO5tm/U8P9sqh19RDEzTn2RayXzsoZmXyB8abCCpHG4+03Zv05RHiX4i5QomAMBnbZejdA9/
fGTxO1rPo1rdtTq
Z+KCgzbEhHLWUD44+If5RtG+U4kgyzlYsyjgwhfho+BrRY6e7QYBsXVbuBQ9ROGV6PCTB80jXZVAKrAbsTQ1D
VkpuBue
mftv7vOn3b8MKzJ/IY/
LLL1tIgpSGvgvjr2mOJJ+JoZF2XnPVUFmYiDSCkPAzhCyFHILHfOVAfws9n1G6p3fwILqNhvB
oPeaCFaApQ== rsa-key-20200123
 Validating input
 Adding key to authorized keys after validation
 Finished adding authorized keys for tancopy



 Press enter to continue
```


©2026 Tanium Inc. All Rights Reserved

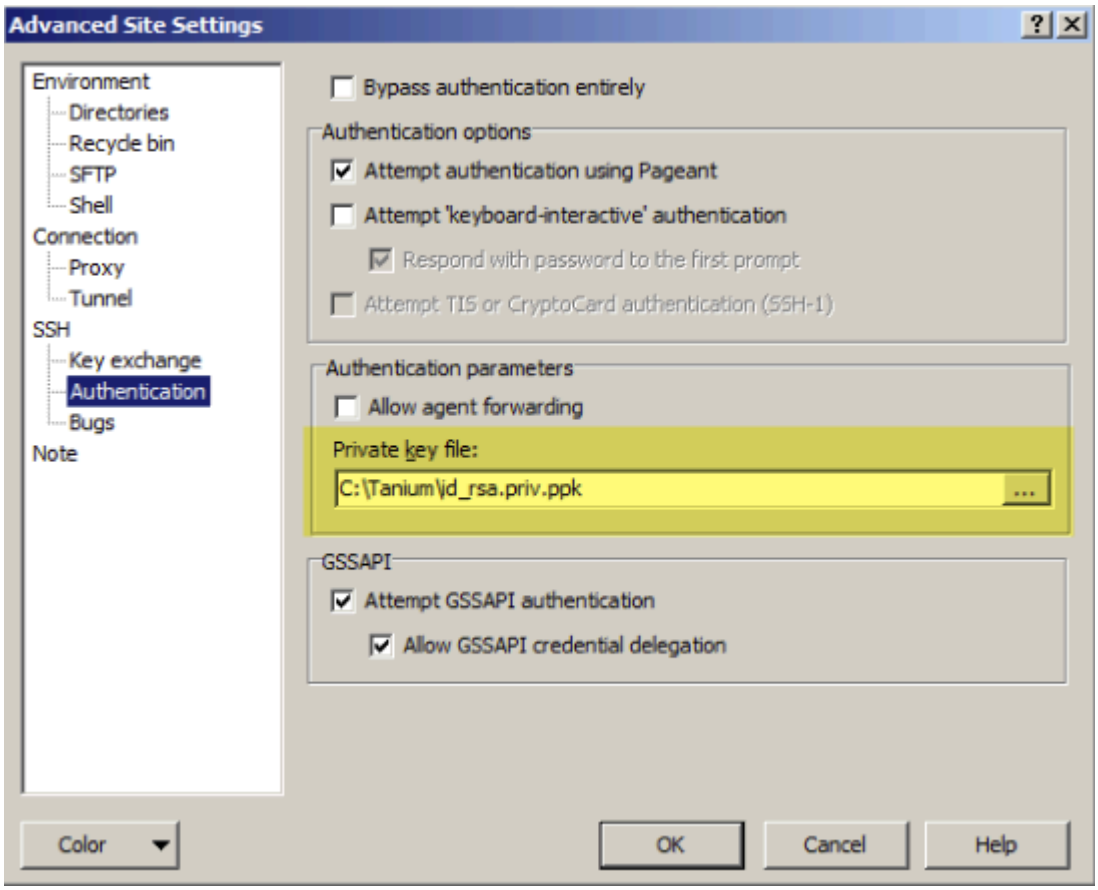
About this task

Use an SFTP client on your management computer, such as WinSCP in Windows or the sftp utility in macOS or Linux, to connect to the Tanium Server Appliance. The following steps demonstrate configuring the connection in WinSCP:

1. Specify `tancopy` for user name.
   Figure 18. WinSCP user name set to tancopy
   

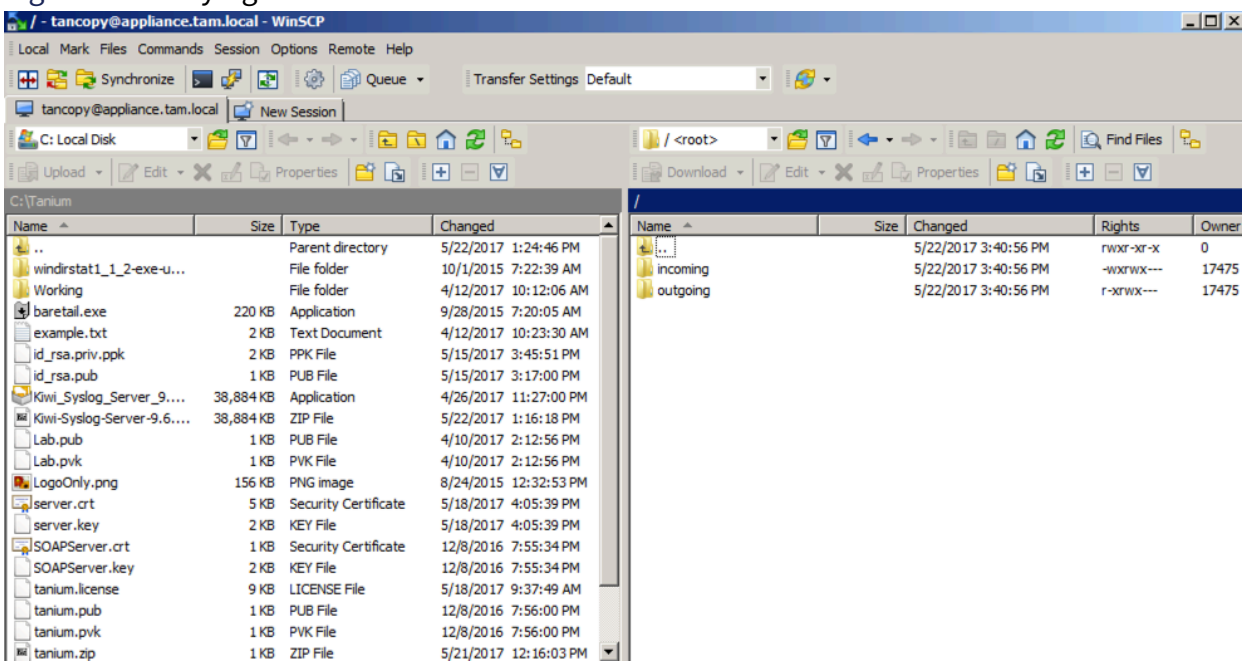
2. Click **Advanced**.
3. Under SSH, browse and select the private key that pairs with the public key uploaded to the Appliance.
   Figure 19. Selecting the private key in WinSCP

©2026 Tanium Inc. All Rights Reserved



4. Save the configuration and click **Login** to initiate the connection.
   Connect to the Appliance and make sure you can access the /incoming and /outgoing directories.

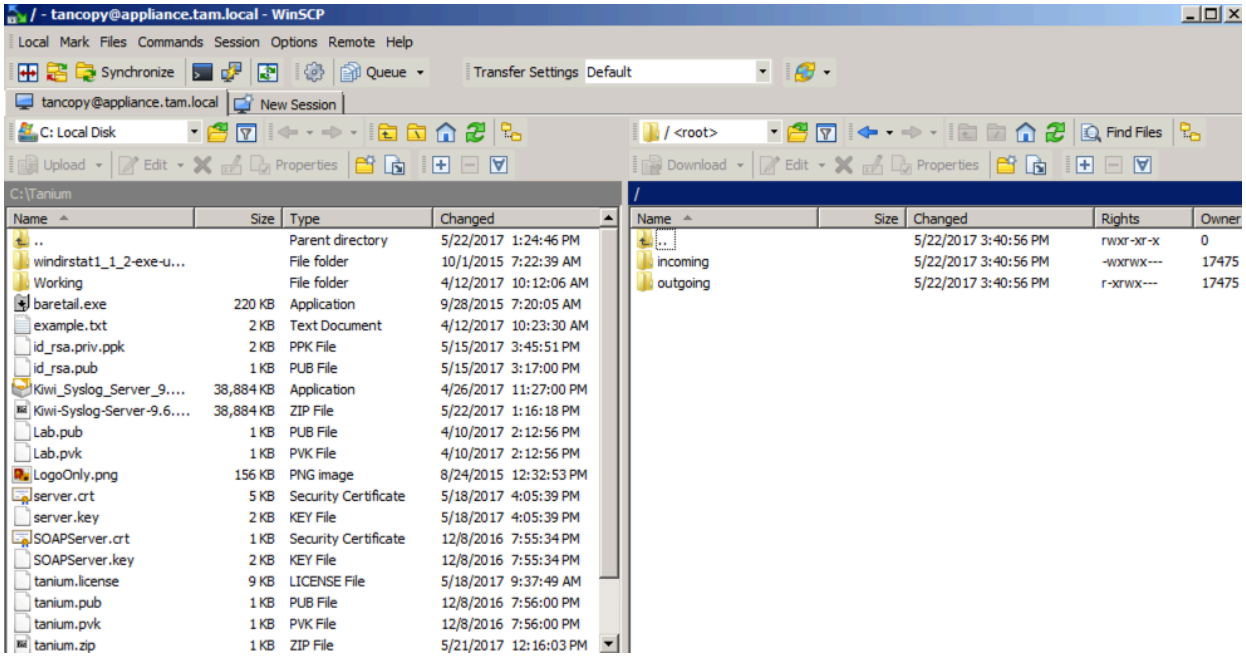
Figure 20. Verifying the SFTP connection in WinSCP



©2026 Tanium Inc. All Rights Reserved

After you connect to the Appliance, upload files to the /incoming directory, and download files from the /outgoing directory.

Figure 21. Testing file transfer in WinSCP



ADD SSH KEYS FOR OTHER TANOS USERS

About this task

It is a best practice to also set up SSH key authentication for TanOS user accounts.

Important: For Google Cloud Platform, you must set up an SSH key for the `tanadmin` user account, even if you primarily plan to use other user accounts with the `tanadmin` role.

Tip: As an alternative to the following procedure, you can use ssh-copy-id to add an SSH public key to any TanOS user with the `tanadmin` profile.

1. Use an SSH key generator such as ssh-keygen to generate a public/private key pair. Note:
   - Specify an RSA key with 2048 bits (such as ssh-keygen -t rsa -b 2048).
   - Specify a passphrase that is easy to remember.
   - Save the private key to a location that you can access when you set up your SFTP

©2026 Tanium Inc. All Rights Reserved

client.

2. Copy all of the text in the public key file to the clipboard. If you use ssh-keygen, copy the contents of the .pub file that you created.

   Important: In an SSH key exchange, the keys must match exactly, including line endings.

3. Sign in to the TanOS console as a user with the `tanadmin` role.
4. Enter `C-U` (User Administration > TanOS User Management).
5. Enter the line number of the user account that you want to manage.

```
>>> User Administration -> TanOS -> tanadmin <<<

 Username:         tanadmin
 Account Enabled:  Yes
 Authentication:   SSH Key or Password
 Password Expires: 2027-01-14 00:00:00 UTC
 SSH Lockout:      No (0)
 Multifactor:      Not configured
 Protected:        No

 Notes:
   * This user account must always have a password
   * This user account cannot be deleted
   * This user account cannot be disabled

          A: Manage SSH Authorized Keys
          P: Manage SSH Key Pair
          L: Reset SSH Lockout
          C: Change/Enable Password (Chosen)
          N: [DISABLED] Disable Password Access
          M: Multifactor Authentication

          E: [DISABLED] Enable Account
          D: [DISABLED] Disable Account
```

©2026 Tanium Inc. All Rights Reserved

```
         T: Manage Account Protection
         X: [DISABLED] Delete User


         F: Edit known hosts file


         R: Return to previous menu  RR: Return to top
```

6. Enter `A` (Authorized Keys).
7. Enter `A` and follow the prompts to paste the public key generated in Step 1.

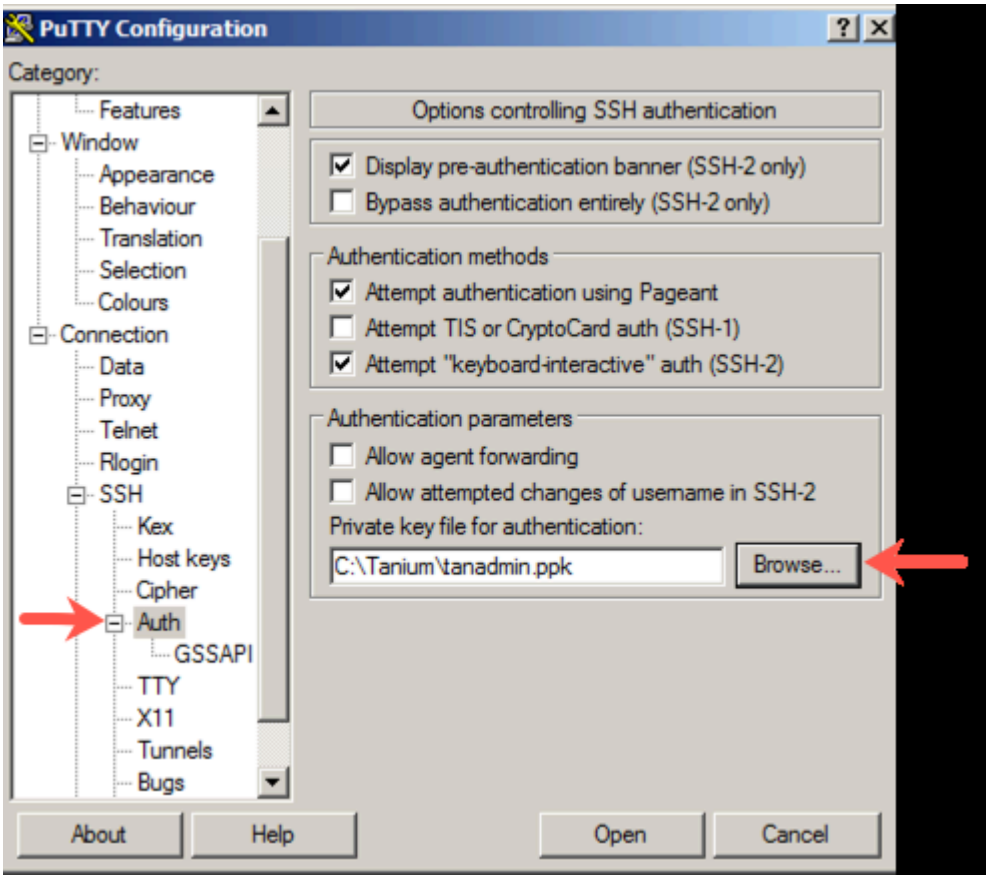
```
            >>> User Administration -> TanOS -> tanadmin -> Authorized Keys -> Add
<<<


 Account: tanadmin
 Please paste the public key and press enter:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCqXUnoyrg4opYQp4DGZoasYy8ud5oJEar9BqRr2RVHMm/
Sxcl4T1sthsN
WS0ECo0j32mCSM3ynYZn2AdJTU6HbKnFM30gtQL7+tpmGrgbkaVEJ9OXoA47JP0o5hbI16UUpuEKJrEBOYovI
srN2gtwKbz
YdOVCxVq5amzqg7/
UrQyUO3rmt54qStiqNIiHI3UjzPWYJwUxz90vU7LWsXYz1CAWBTXnh51kg0lBPFgbRmUZJb0DwLb4Sw
lFZAe5P0RO4RwdmZVgTfsqy+MVuyzaBzGD1z4MlIZ83R6sW+nXtipbzqhFTLykLRLIXobuHjuf0Yy1H7/
ZDJh/qlojce4TC
g/+5e2h1RQ8ZKgECZDJoCdrkAM6y9arHCoZwqEP9MXugQXCO6EMrP39vXajnV3YrDKKLYP1pxWZGOA4ylNqY5
mG1+AofVdG
vAUBztjXfXgC3bgL0Qgp+d3E8JvLRHXfkmRijppvj+BCJUawXJfkMtBEgrxQP9PoDwHrqJj6ey80v8P7DgojQ
w83JumsG3S
+7l0e0Ia02q/
05s2EpOv9jE9aJiLRGKbb4WkjvUSpK1VmDK54qfeSKj6yp3IIt13GBKmkVqKbbZS6gaZ3UTpzq3dj+53YeP
eOe8XMECuxl6aH4nLT4u3CqrCqxTfTa5y1Fi3/e9zI5/AKJlTXWF3ISCQ==
tanadmin@appliance-156.tam.local
 Validating input
 Adding key to authorized keys after validation
 Finished adding authorized keys for tanadmin
```

©2026 Tanium Inc. All Rights Reserved

```
Press enter to continue
```

8. To test, on your management computer, set up an SSH client such as PuTTY to connect to the Tanium Server Appliance:
    a. Specify the Tanium Server IP address, port 22, and SSH connection type.
    b. Under SSH, browse and select the private key that pairs with the public key uploaded to the Appliance.

    Figure 22. Selecting the private key for SSH authentication



    c. Open the SSH session and enter the `tanadmin` user name.
    d. You are prompted for the SSH key passphrase instead of the `tanadmin` password.

```
login as: tanadmin

######################## WARNING ########################

       Unauthorized access is strictly prohibited.

#########################################################

Authenticating with public key "rsa-key-20200119"
```

©2026 Tanium Inc. All Rights Reserved

```
Passphrase for key "rsa-key-20200119":
```

Export the GRUB key

About this task

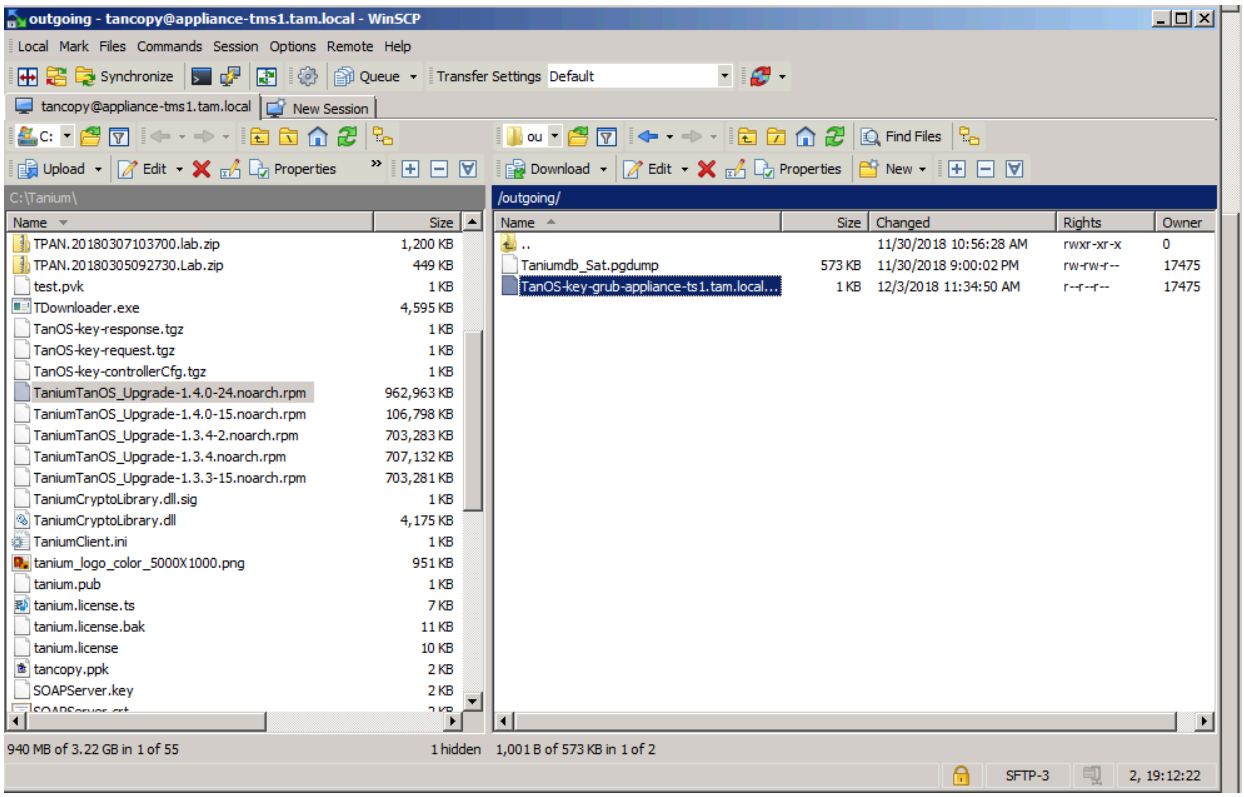
The GRUB key can be used during the boot sequence to diagnose and recover from failure conditions. You can export the key and store it in a safe location. During recovery, you need to provide the key.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-X` (Appliance Configuration > Advanced Configuration).
3. Enter `6` and follow the prompts to export the GRUB key to the /outgoing folder.

```
            >>> Appliance Configuration -> Advanced Menu -> Export Security Key <<<

Once the security key has been placed in the outgoing directory it
will remain until the nightly cleanup job is run. After this time it
will be deleted and must be exported again.
Please be sure to download it and save in a secure location.

Would you like to export the security key? [Yes|No]: yes

The security key has been placed in the sftp outgoing directory.
This location will be cleaned daily at 02:00am appliance time!

Press enter to continue
```

4. Use SFTP to copy the file from the /outgoing directory to your local computer.
   Figure 23. Copying the GRUB key file over SFTP

©2026 Tanium Inc. All Rights Reserved



What to do next

- To save time, complete advanced network configuration before you install Tanium Core Platform Servers. For more information, see Configuring Appliance connections on page 337.
- When these steps are completed, you can continue with the installation of an Appliance Array.

Completing the initial setup (cloud-based Tanium Appliance)

To begin deployment of Tanium Appliances, deploy images to your cloud provider, and then configure basic network, host, and user settings.

Requirements

Requirements for cloud-based Tanium Appliance deployment

Cloud provider	• AWS (x86-64 processors) • AWS GovCloud • Google Cloud Platform (GCP)

©2026 Tanium Inc. All Rights Reserved

	• Microsoft Azure[1] • Microsoft Azure Government[1]

[1] Tanium Appliances are not supported on Microsoft Azure virtual machines that require Accelerated Networking, such as Dv5-, Dsv5-, Ddv5-, Ddsv5-, Dlsv5-, and Dldsv5-series virtual machines.

Set up the environment for the Appliance

Configure your environment to host cloud-based Tanium Appliances.

Deploy Tanium Server and Tanium Module Server Appliances into your private subnets and the Tanium Zone Server Appliances into public subnets.

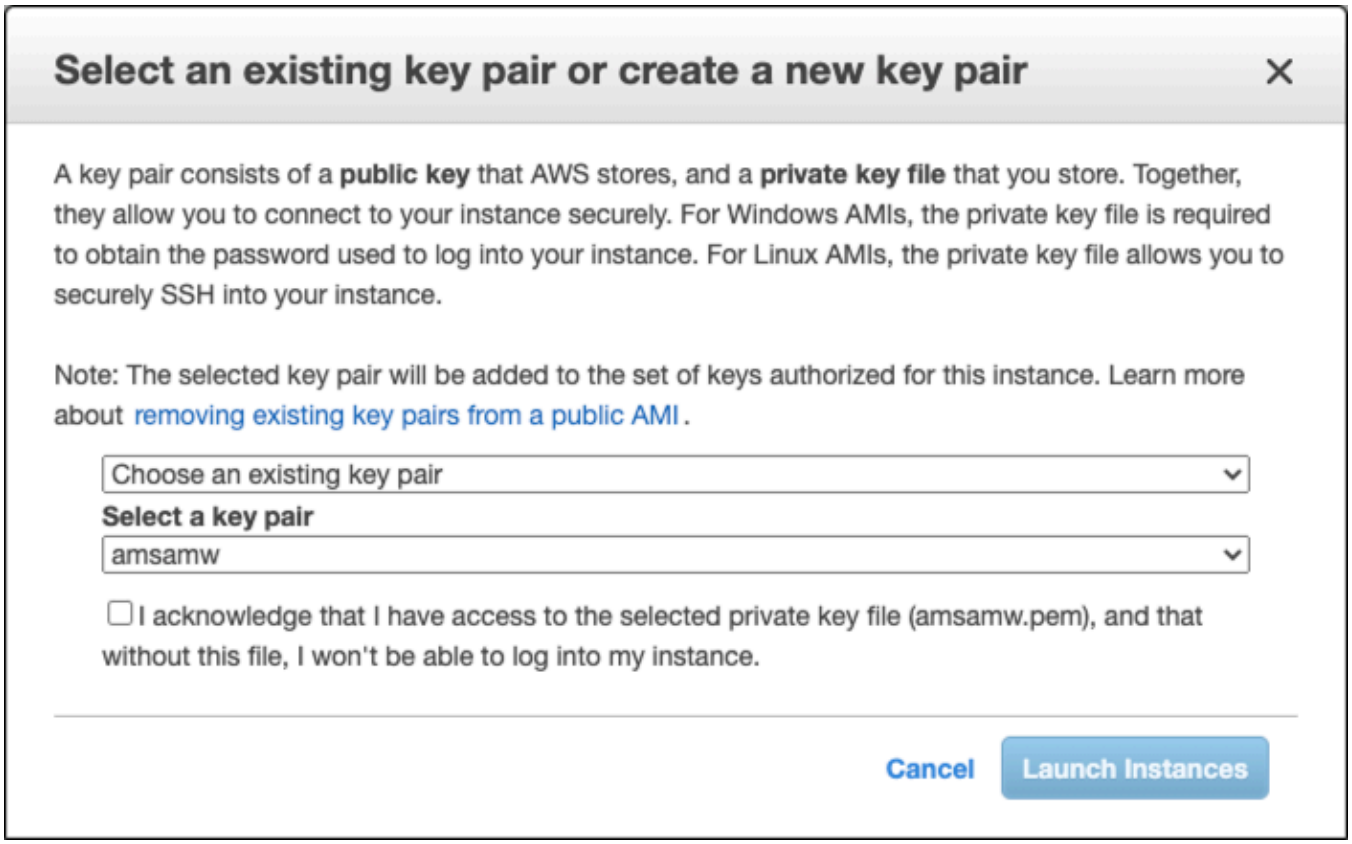
Best Practice: For better resiliency in a cloud-based environment, separate Tanium Server, Tanium Module Server, and Tanium Zone Server Appliances between two zones so that each zone contains each Appliance type.

Deploy the virtual image to the cloud provider

Contact Tanium Support on page 510 to obtain a Tanium Appliance image file for use in a customer cloud. When you configure the image with your cloud provider, you must specify an encryption key pair to initially connect to the image. You can use an existing key pair or generate a new key pair.

Figure 24. AWS key pair selection

©2026 Tanium Inc. All Rights Reserved



CONSIDERATIONS FOR SPECIFIC CLOUD PROVIDERS

Microsoft Azure

For a Microsoft Azure deployment, you must change the initial user name from `azureuser` to `tanadmin` before you deploy the image.

Important:

Tanium Appliances do not support the Accelerated Networking feature in Microsoft Azure. You must disable Accelerated Networking on the network interfaces that are connected to Tanium Appliances.

For this reason, Tanium Appliances are also not supported on Microsoft Azure virtual machines that require Accelerated Networking, such as Dv5-, Dsv5-, Ddv5-, Ddsv5-, Dlsv5-, and Dldsv5-series virtual machines.

Google Cloud Platform

©2026 Tanium Inc. All Rights Reserved

About this task

Use the following steps to prepare the virtual image:

1. Create a cloud storage bucket with appropriate security, and upload the TanOS artifact file (tar.gz) to the bucket.
2. Create an image from the artifact file in cloud storage.
3. Create a VM for each TanOS Appliance using the image that you created.

   > **Note:** The default boot disk size is inadequate for a production Tanium Appliance. At least 500GB of storage is recommended. Increase the size of the boot disk when you create the VM, or add a new disk to the VM. If you use an additional disk, you must increase the storage on the Tanium Appliance after initial setup. For more information, see Increase storage on page 445.

   Additionally, for Google Cloud Platform, you must set up an SSH key for the `tanadmin` user account, even if you primarily plan to use other user accounts with the `tanadmin` role. For more information, see Before you begin on page 139.

   For more information, see the Google Cloud Platform documentation.

(FIPS-compliant organizations) Enable FIPS 140-3 mode before initial setup

About this task

Enabling Federal Information Processing Standards (FIPS) mode causes the Appliance to use a FIPS-validated cryptographic module for all cryptographic operations. It also ensures that services like SSH use only cryptographic algorithms that FIPS 140-3 allows.

If FIPS mode is required for your organization, you can enable it before you continue with initial setup so that the password and keys that you configure during setup are FIPS-compliant.

> **Best Practice:** Enable FIPS mode only if you are required to do so for your organization.

©2026 Tanium Inc. All Rights Reserved

Important: To use FIPS mode, the VM on which the virtual Tanium Appliance is installed must use a CPU type that supports the RDSEED instruction.

Note:

- Enabling FIPS mode in TanOS also puts the Tanium Platform in FIPS mode.
- You can later disable FIPS mode if it is not required and it was inadvertently enabled during setup. For more information, see Enable FIPS 140-3 mode on page 362.

1. Sign in to the TanOS console as the `tanadmin` user.
2. Enter `M` and follow the prompt to enable FIPS 140-3 mode and reboot the Appliance, and then continue initial setup.

Perform full initial configuration

1. Make sure your virtual image is configured to use an encryption key pair, and that the private key is set up on your local computer.
2. Sign in to your cloud provider and use an SSH client to connect to the TanOS console as a user with the `tanadmin` role. If prompted to accept the key fingerprint, enter `yes`.

```
$ ssh tanadmin@10.0.20.212


   >>> Initial Configuration <<<


Initial configuration workflow for a new TanOS Appliance.
All items must be complete before the Appliance can be used.


Keymap:     n/a
IP Address: 10.0.20.12
Hostname:   TanOS-173-AZURE.example.net
FIPS 140-3: disabled


          1: Set Virtual Console Keymap
```

©2026 Tanium Inc. All Rights Reserved

```
         M: Toggle FIPS 140-3 Mode

         N: Set FQDN (hostname)            (complete)
         D: Set DNS Nameservers            (complete)
         T: Set NTP (time)                 (INCOMPLETE)
         E: View and Accept EULA           (INCOMPLETE)

         F: [DISABLED] Finish Initial Configuration
         S: Shutdown

         Z: Log out
```

3. Enter `T` and follow the prompts to set one or more NTP servers.

```
$ ssh tanadmin@10.0.20.212

   >>>  NTP Configuration <<<

 Timezone will be automatically set to UTC.

 Enter the NTP server information for up to two NTP servers. Each entry consist
 of a server name or IP address.
 Optionally each server may indicate authentication information using
 colons as a separator: <server>:<key-id>:<SHA1|MD5>:key

 1.2.3.4
 pool.ntp.org
 ntp.secret.corp:999:SHA1:0123456789abcdef0123456789abcdef01234567

Please provide the NTP server address: pool.ntp.org
Please provide the second NTP server address (enter blank value for none):

 The following settings will be used:

     NTP Server 1: pool.ntp.org
     NTP Server 2:
```

©2026 Tanium Inc. All Rights Reserved

```
Are these settings correct? [Yes|No]:
```

4. Enter `E`, press **Enter**, and then use the spacebar to page through the end-user license agreement (EULA).
5. When complete, enter `Q`, enter your email address, and enter `yes` to accept the EULA. The email address is stored locally only. It is not used externally for any reason.
6. Enter `F` to confirm that you finished initial configuration and to end the session.

```
           >>> Initial Configuration <<<

Initial configuration workflow for a new TanOS Appliance.
All requirements are met to finish Initial Config.

Keymap:     n/a
IP Address: 10.13.0.6
Hostname:   TanOS-173-AZURE.hzavr5qms02ujnqr20gh0gorhb.gx.internal.cloudapp.net
FIPS 140-3: disabled

         1: Set Virtual Console Keymap
         M: Toggle FIPS 140-3 Mode

         N: Set FQDN (hostname)            (complete)
         D: Set DNS Nameservers            (complete)
         T: Set NTP (time)                 (complete)
         E: View and Accept EULA           (complete)

         F: Finish Initial Configuration
         S: Shutdown

         Z: Log out

--------------------------------------------------

TanOS Version:        1.9.1
```

©2026 Tanium Inc. All Rights Reserved

```
Please select:
```

Result

The console configures SSH keys and IPSec settings, and then notifies you that the initial configuration is complete.

Access TanOS remotely

To access your Tanium Appliances remotely, note the following requirements.

- Your local management computer must be connected to a subnet that can reach the Appliance IP address.
- Your management computer must have an SSH client application or terminal emulator that can make a Client connection to the Appliance.
- You must have an SSH client such as PuTTY to sign in to the TanOS console. For PuTTY, use version 0.71 or later.
- You must have an SSH key generator such as ssh-keygen to generate keys for the tancopy user.
- You must have an SFTP client such as WinSCP to copy files to and from the Appliance. For WinSCP, use version 5.15.2 or later.

Tip: Watch the tutorial about how to configure WinSCP for the Tanium Appliance.

Add TanOS system users

About this task

Create additional TanOS system users based on `tanadmin` (privileged) and `tanuser` (restricted) profiles.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Create more than one privileged user with the `tanadmin` role in case you forget the password for the built-in `tanadmin` user.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter `A` and follow the prompts to add a system user.

```
           >>> User Administration -> System Users -> Add System User <<<

Adding a system user requires first name, last name, user name and user role.

Attention:
TanUser Role:  Monitor/Check the status of the appliance, no changes are allowed
TanAdmin Role: Full administrative role to manage the appliance

A temporary password will be generated and the new user is required to change
their password upon first login!

The password policy requires meeting these rules:
- Minimum of 10 characters long
- At least 1 upper case character
- At least 1 lower case character
- At least 1 numeric character
- At least 1 other character
- Must not match any of recent 4 passwords
- Must not be based on a dictionary word
- Must not contain part of the username

Please enter first name: John
Please enter last name: Doe
Please enter desired user name (max 30 chars): john.doe
Which role should be assigned to john.doe?

1: TanUser (Monitoring)
```

©2026 Tanium Inc. All Rights Reserved

```
2: TanAdmin (Administrative)

Please select: 2

The temporary password for john.doe is: proudbrownwildfowl

Adding local user john doe ...
Successfully added user john doe (username: john.doe) with role tanadmin.

Press enter to continue
```

Configure SSH keys

TanOS has built-in and customer-created user accounts to access the Appliance operating system and perform tasks.

Before you install a Tanium Appliance role, you must add SSH keys to authenticate access for the `tancopy` built-in user. `tancopy` can make an SFTP connection with SSH key authentication to TanOS and copy files to and from the /incoming and /outgoing directories. For Google Cloud Platform, you must also set up an SSH key for the `tanadmin` user account, even if you primarily plan to use other user accounts with the `tanadmin` role.

Best Practice: Set up SSH key authentication for all TanOS user accounts.

Important: TanOS does not support self-service password reset methods. If you forget your password, you must ask a user with the tanadmin role to reset it for you. You can avoid this risk by setting up SSH key authentication.

Tip: Watch the tutorial about how to configure SSH key authentication for the Tanium Appliance.

©2026 Tanium Inc. All Rights Reserved

- You must have an SSH client to sign in to the TanOS console, and an SFTP client to copy files to and from the Appliance.
- You must have an SSH key generator to generate keys for the `tancopy` user.

ADD AND TEST AN SSH KEY FOR THE TANCOPY USER

Add an SSH key for the `tancopy` user, and then test the SFTP connection to confirm that the key works.

Add the SSH key for the tancopy user

1. Use an SSH key generator such as ssh-keygen to generate a public/private key pair. Note:
   - Specify an RSA key with 2048 bits (such as ssh-keygen -t rsa -b 2048).
   - Specify a passphrase that is easy to remember.
   - Save the private key to a location that you can access when you set up your SFTP client.
2. Copy the text in the public key file to the clipboard. If you use ssh-keygen, copy the contents of the .pub file that you created.

   Important: In an SSH key exchange, the keys must match exactly, including line endings.
3. Sign in to the TanOS console as a user with the `tanadmin` role.
4. Enter `C-U` (User Administration > TanOS User Management).
5. Enter the line number for the `tancopy` user to go to the user administration menu for this user.

```
           >>> User Administration -> TanOS -> tancopy <<<

Username:         tancopy
Account Enabled:  Yes
Authentication:   SSH Key Only
Password Expires: N/A
SSH Lockout:      No (0)
```

©2026 Tanium Inc. All Rights Reserved

```
Multifactor:      Not configured
Protected:        No

Notes:
  * This user account cannot be deleted
  * This user account cannot have a password
  * This user account cannot use multifactor

         A: Manage SSH Authorized Keys
         P: Manage SSH Key Pair
         L: Reset SSH Lockout
         C: [DISABLED] Change Password
         N: [DISABLED] Disable Password Access
         M: [DISABLED] Multifactor Authentication

         E: Enable Account
         D: Disable Account
         T: [DISABLED] Manage Account Protection
         X: [DISABLED] Delete User

         F: Edit known hosts file

         R: Return to previous menu  RR: Return to top

-------------------------------------------------------
```

6. Enter `A` (Authorized Keys).
7. Enter `A` and follow the prompts to add the contents of the public key generated in Step 1.

```
           >>> User Administration -> TanOS -> tancopy -> Authorized Keys -> Add
<<<

Account: tancopy
Please paste the public key and press enter:
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA1ClmgkMrbbxB7jND/Y4/
Giupck35xAuGNKfZWqVLM5F0CNXuTScf6v2z
```

©2026 Tanium Inc. All Rights Reserved

```
MDxW5TO5tm/U8P9sqh19RDEzTn2RayXzsoZmXyB8abCCpHG4+03Zv05RHiX4i5QomAMBnbZejdA9/
fGTxO1rPo1rdtTq
Z+KCgzbEhHLWUD44+If5RtG+U4kgyzlYsyjgwhfho+BrRY6e7QYBsXVbuBQ9ROGV6PCTB80jXZVAKrAbsTQ1D
VkpuBue
mftv7vOn3b8MKzJ/IY/
LLL1tIgpSGvgvjr2mOJJ+JoZF2XnPVUFmYiDSCkPAzhCyFHILHfOVAfws9n1G6p3fwILqNhvB
oPeaCFaApQ== rsa-key-20200123
 Validating input
 Adding key to authorized keys after validation
 Finished adding authorized keys for tancopy



 Press enter to continue
```

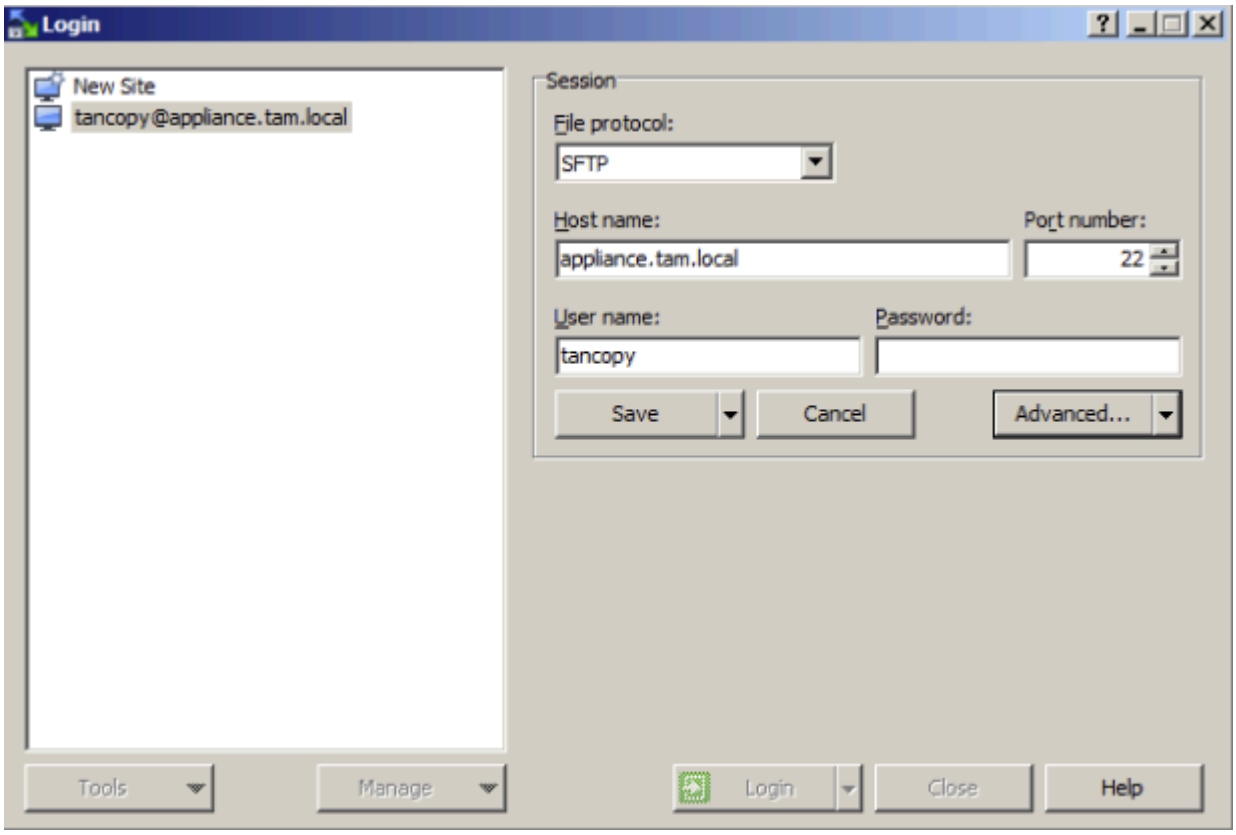
Test the SFTP connection with the SSH key

About this task

Use an SFTP client on your management computer, such as WinSCP in Windows or the sftp utility in macOS or Linux, to connect to the Tanium Server Appliance. The following steps demonstrate configuring the connection in WinSCP:

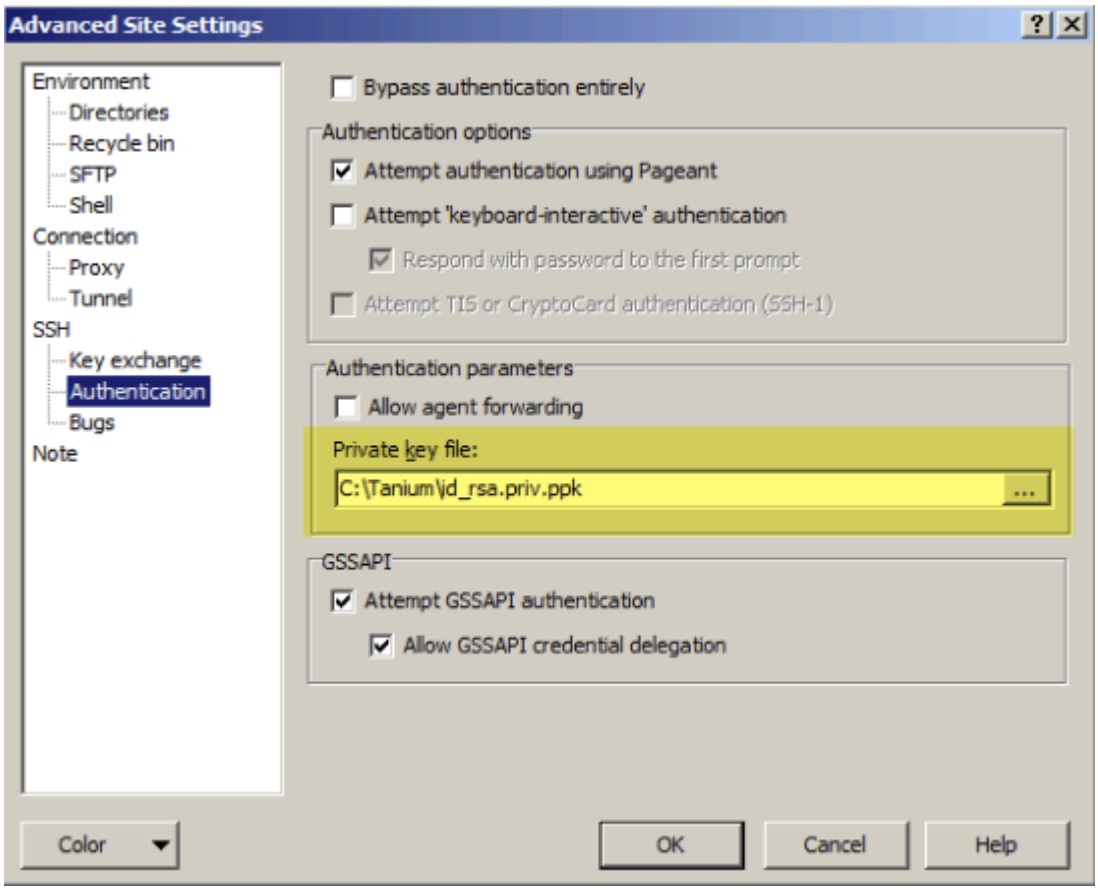
1. Specify `tancopy` for user name.
   Figure 25. WinSCP user name set to tancopy

©2026 Tanium Inc. All Rights Reserved



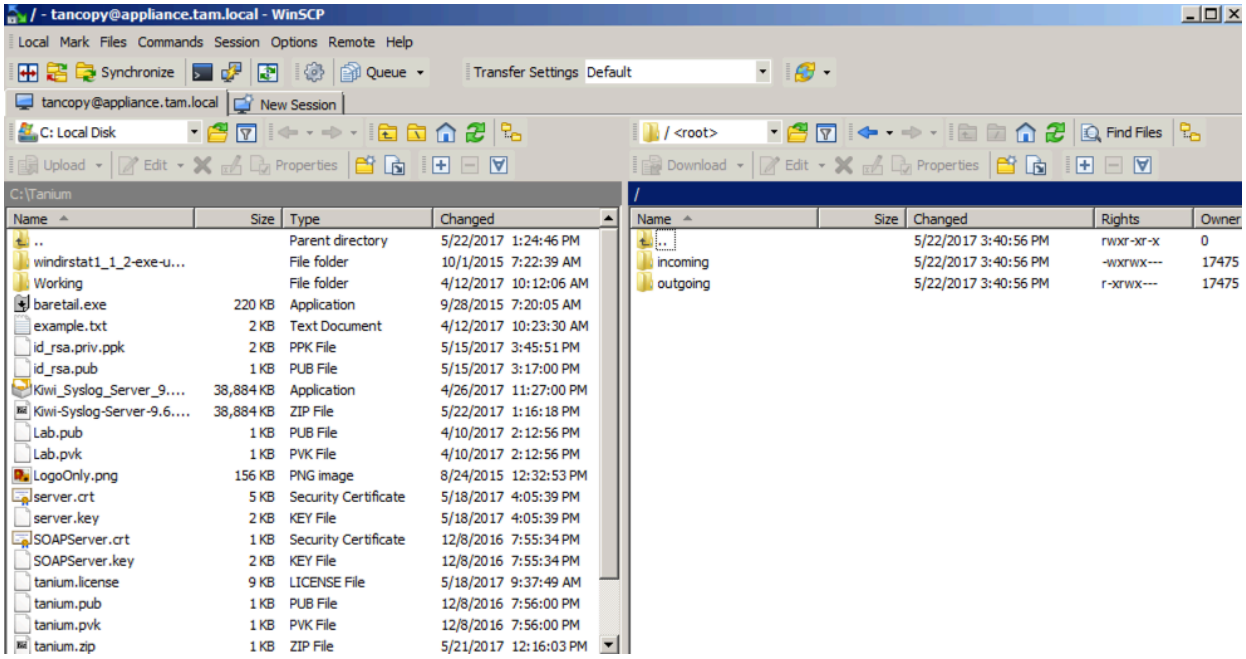
2. Click **Advanced**.
3. Under SSH, browse and select the private key that pairs with the public key uploaded to the Appliance.
   Figure 26. Selecting the private key in WinSCP

©2026 Tanium Inc. All Rights Reserved



4. Save the configuration and click **Login** to initiate the connection.
   Connect to the Appliance and make sure you can access the /incoming and /outgoing directories.

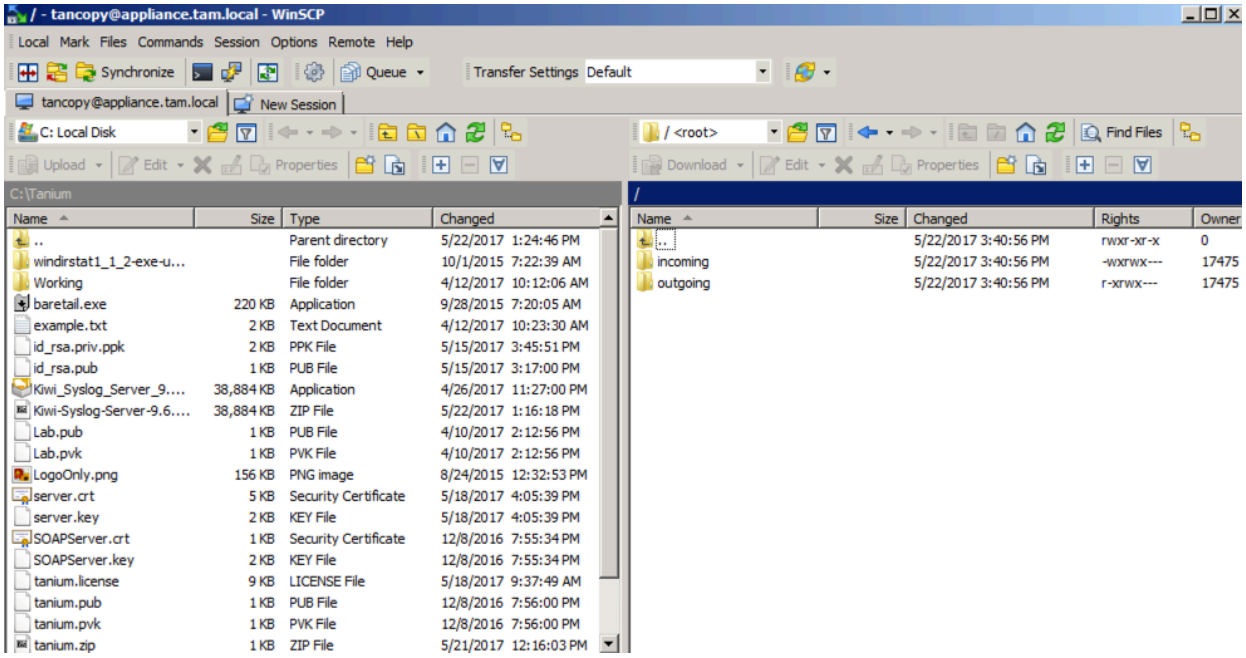
Figure 27. Verifying the SFTP connection in WinSCP



©2026 Tanium Inc. All Rights Reserved

After you connect to the Appliance, upload files to the /incoming directory, and download files from the /outgoing directory.

Figure 28. Testing file transfer in WinSCP



ADD SSH KEYS FOR OTHER TANOS USERS

About this task

It is a best practice to also set up SSH key authentication for TanOS user accounts.

Important: For Google Cloud Platform, you must set up an SSH key for the `tanadmin` user account, even if you primarily plan to use other user accounts with the `tanadmin` role.

Tip: As an alternative to the following procedure, you can use ssh-copy-id to add an SSH public key to any TanOS user with the `tanadmin` profile.

1. Use an SSH key generator such as ssh-keygen to generate a public/private key pair. Note:
   - Specify an RSA key with 2048 bits (such as ssh-keygen -t rsa -b 2048).
   - Specify a passphrase that is easy to remember.
   - Save the private key to a location that you can access when you set up your SFTP

©2026 Tanium Inc. All Rights Reserved

client.

2. Copy all of the text in the public key file to the clipboard. If you use ssh-keygen, copy the contents of the .pub file that you created.

   Important: In an SSH key exchange, the keys must match exactly, including line endings.

3. Sign in to the TanOS console as a user with the `tanadmin` role.
4. Enter `C-U` (User Administration > TanOS User Management).
5. Enter the line number of the user account that you want to manage.

```
>>> User Administration -> TanOS -> tanadmin <<<

 Username:         tanadmin
 Account Enabled:  Yes
 Authentication:   SSH Key or Password
 Password Expires: 2027-01-14 00:00:00 UTC
 SSH Lockout:      No (0)
 Multifactor:      Not configured
 Protected:        No

 Notes:
   * This user account must always have a password
   * This user account cannot be deleted
   * This user account cannot be disabled

          A: Manage SSH Authorized Keys
          P: Manage SSH Key Pair
          L: Reset SSH Lockout
          C: Change/Enable Password (Chosen)
          N: [DISABLED] Disable Password Access
          M: Multifactor Authentication

          E: [DISABLED] Enable Account
          D: [DISABLED] Disable Account
```

©2026 Tanium Inc. All Rights Reserved

```
         T: Manage Account Protection
         X: [DISABLED] Delete User

         F: Edit known hosts file

         R: Return to previous menu  RR: Return to top
```

6. Enter `A` (Authorized Keys).
7. Enter `A` and follow the prompts to paste the public key generated in Step 1.

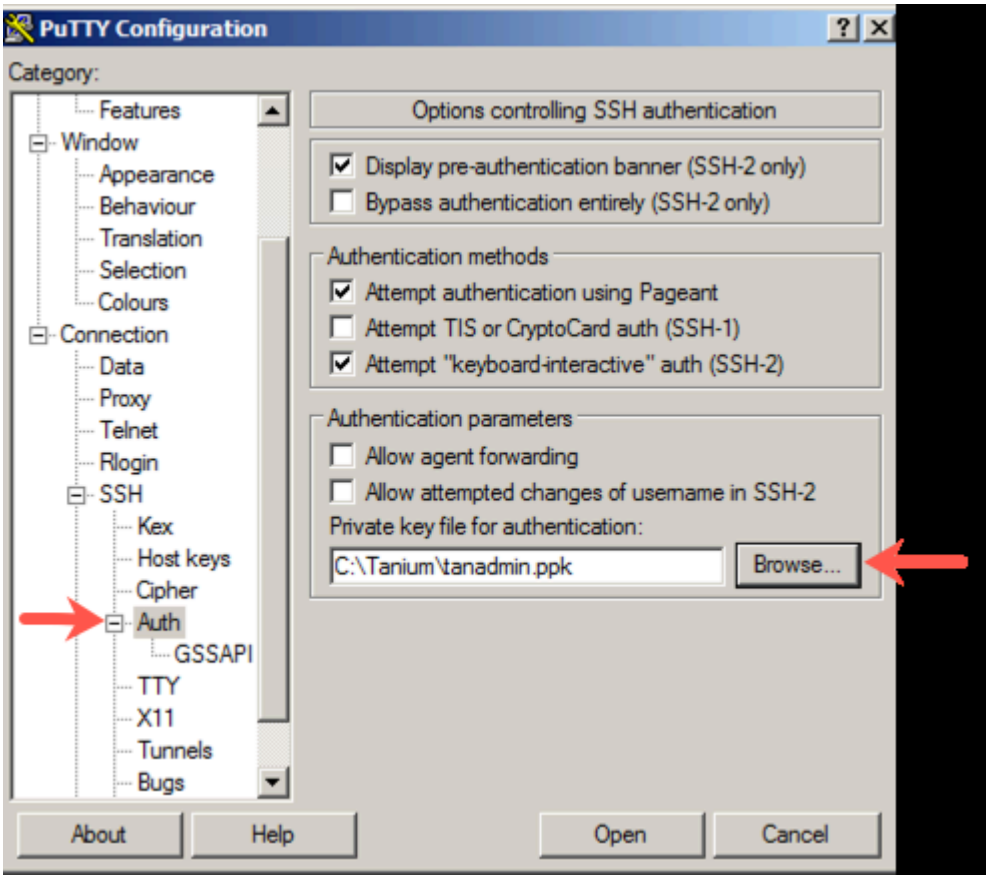
```
           >>> User Administration -> TanOS -> tanadmin -> Authorized Keys -> Add
<<<

 Account: tanadmin
 Please paste the public key and press enter:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCqXUnoyrg4opYQp4DGZoasYy8ud5oJEar9BqRr2RVHMm/
Sxcl4T1sthsN
WS0ECo0j32mCSM3ynYZn2AdJTU6HbKnFM30gtQL7+tpmGrgbkaVEJ9OXoA47JP0o5hbI16UUpuEKJrEBOYovI
srN2gtwKbz
YdOVCxVq5amzqg7/
UrQyUO3rmt54qStiqNIiHI3UjzPWYJwUxz90vU7LWsXYz1CAWBTXnh51kg0lBPFgbRmUZJb0DwLb4Sw
lFZAe5P0RO4RwdmZVgTfsqy+MVuyzaBzGD1z4MlIZ83R6sW+nXtipbzqhFTLykLRLIXobuHjuf0Yy1H7/
ZDJh/qlojce4TC
g/+5e2h1RQ8ZKgECZDJoCdrkAM6y9arHCoZwqEP9MXugQXCO6EMrP39vXajnV3YrDKKLYP1pxWZGOA4ylNqY5
mG1+AofVdG
vAUBztjXfXgC3bgL0Qgp+d3E8JvLRHXfkmRijppvj+BCJUawXJfkMtBEgrxQP9PoDwHrqJj6ey80v8P7DgojQ
w83JumsG3S
+7l0e0Ia02q/
05s2EpOv9jE9aJiLRGKbb4WkjvUSpK1VmDK54qfeSKj6yp3IIt13GBKmkVqKbbZS6gaZ3UTpzq3dj+53YeP
eOe8XMECuxl6aH4nLT4u3CqrCqxTfTa5y1Fi3/e9zI5/AKJlTXWF3ISCQ==
tanadmin@appliance-156.tam.local
 Validating input
 Adding key to authorized keys after validation
 Finished adding authorized keys for tanadmin
```

©2026 Tanium Inc. All Rights Reserved

```
Press enter to continue
```

8. To test, on your management computer, set up an SSH client such as PuTTY to connect to the Tanium Server Appliance:
    a. Specify the Tanium Server IP address, port 22, and SSH connection type.
    b. Under SSH, browse and select the private key that pairs with the public key uploaded to the Appliance.

    Figure 29. Selecting the private key for SSH authentication



    c. Open the SSH session and enter the `tanadmin` user name.
    d. You are prompted for the SSH key passphrase instead of the `tanadmin` password.

```
login as: tanadmin

######################## WARNING ########################

       Unauthorized access is strictly prohibited.

#########################################################

Authenticating with public key "rsa-key-20200119"
```

©2026 Tanium Inc. All Rights Reserved

```
Passphrase for key "rsa-key-20200119":
```

Export the GRUB key

About this task

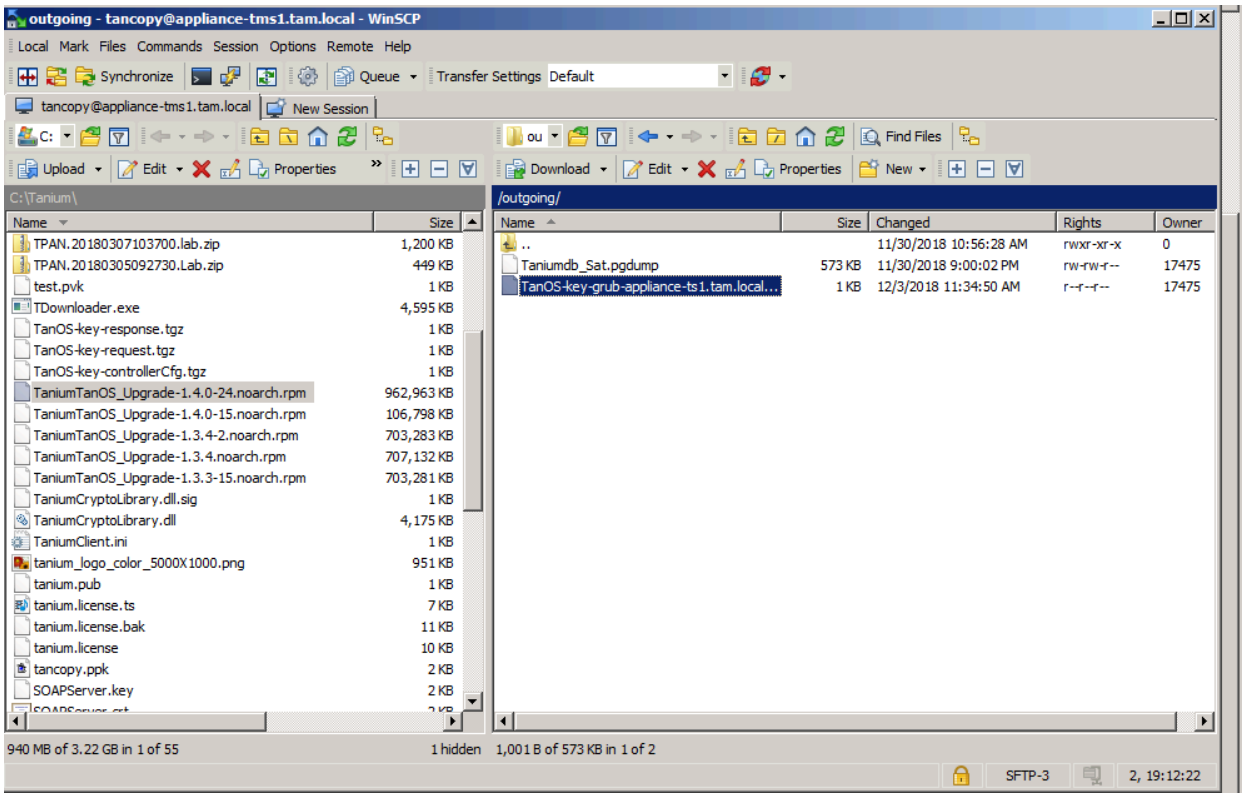
The GRUB key can be used during the boot sequence to diagnose and recover from failure conditions. You can export the key and store it in a safe location. During recovery, you need to provide the key.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-X` (Appliance Configuration > Advanced Configuration).
3. Enter `6` and follow the prompts to export the GRUB key to the /outgoing folder.

```
            >>> Appliance Configuration -> Advanced Menu -> Export Security Key <<<

Once the security key has been placed in the outgoing directory it
will remain until the nightly cleanup job is run. After this time it
will be deleted and must be exported again.
Please be sure to download it and save in a secure location.

Would you like to export the security key? [Yes|No]: yes

The security key has been placed in the sftp outgoing directory.
This location will be cleaned daily at 02:00am appliance time!

Press enter to continue
```

4. Use SFTP to copy the file from the /outgoing directory to your local computer.
   Figure 30. Copying the GRUB key file over SFTP

©2026 Tanium Inc. All Rights Reserved



What to do next

- To save time, complete advanced network configuration before you install Tanium Servers. For more information, see Configuring Appliance connections on page 337.
- When these steps are completed, you can continue with the installation of an Appliance Array.

Configuring proxy server settings for Tanium Appliances

If your network requires outbound connections to pass through a proxy server, configure proxy settings so that Tanium Appliances can reach the internet.

The subsequent topics in this section provide information about proxy server connections, the TDownloader user context, and how to configure proxy settings in Tanium Console and on the Appliance.

Overview of proxy server connections

Some organizations use proxy servers for traffic between internal servers and the Internet. If your

©2026 Tanium Inc. All Rights Reserved

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.

To configure Tanium Client to connect through a Hypertext Transfer Protocol Secure (HTTPS) proxy server to the Tanium Server or Tanium Zone Server, see Connect through an HTTPS proxy server.

The Tanium Server and Module Server use the Tanium Downloader (TDownloader) utility to securely download files. To configure access through proxies, configure TDownloader settings on both Servers.

Note:

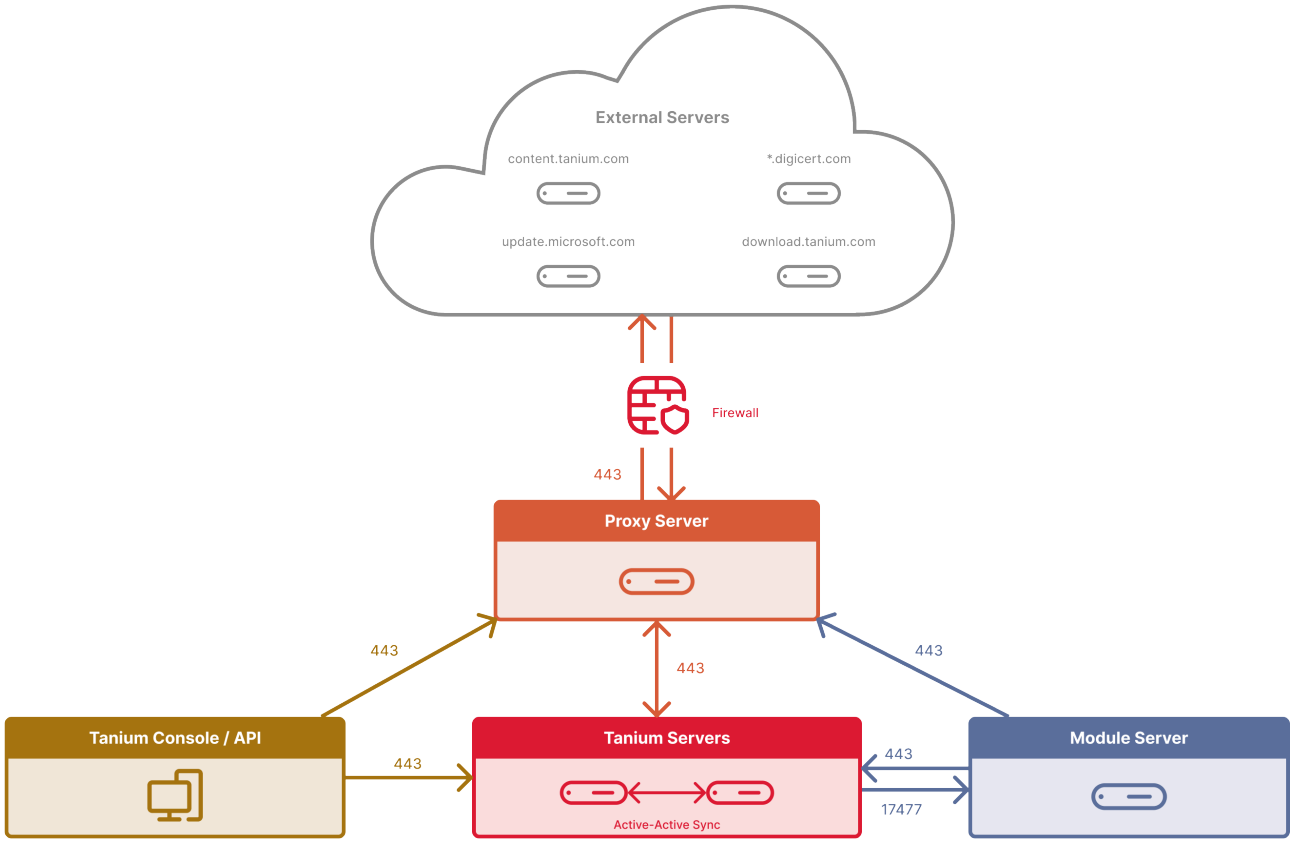
For a list of sites that Tanium Core Platform Servers access, see Internet URLs on page 39.

A remote source might have its own requirements, such as certificate authentication or user authentication. For more information, see Managing remote authentication.

To troubleshoot proxy server issues, see TDownloader logs on page 528.

Figure 31. Tanium deployment with proxy server

©2026 Tanium Inc. All Rights Reserved



The Tanium Core Platform in an Appliance deployment supports an IP address-based proxy server that 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 (FQDNs) of the Tanium Servers and Module Servers to the allow list on the proxy server. If the proxy server requires authentication, configure the account ID and password.

TDownloader user context

For Tanium Appliance deployments, TDownloader runs in the context of the **tanium** service account user.

Tanium Console: Configure proxy settings

In most cases, use Tanium Console to configure proxy settings unless you must configure the settings before you can access the Console. For more information, see the Configuring proxy server settings.

Configure proxy settings

©2026 Tanium Inc. All Rights Reserved

About this task

In most cases, use Tanium Console to configure proxy settings. In some circumstances, you might need to configure proxy settings before you have access to Tanium Console. If necessary, you can configure proxy settings on the Tanium Server or Module Server host.

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

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2` to go to the **Tanium Operations** menu.

```
------------------------------------------------------

            >>> Tanium Operations Menu <<<

        1: Tanium Service Control
        2: Tanium Configuration Settings
        4: Install Custom SOAP Cert
        5: Manage Custom Signing Keys
        7: Download SOAP Certificate
        9: Import CAC Certificate

        A: Configure Module Server(s)
        B: Configure Tanium Cluster
        C: Manage Content
        M: Module Operations

        I: Import public key to Tanium Zone Server

        X: Advanced Operations

        R: Return to previous menu  RR: Return to top
```

©2026 Tanium Inc. All Rights Reserved

```
-----------------------------------------------------
```

3. Enter `2` to go to the **Configuration Settings** menu.

```
-----------------------------------------------------

 >>> Tanium Operations -> Configuration Settings <<<

Note: Some settings may require a service restart to take effect.

          1: Edit Tanium Server Settings
          2: Edit Tanium Server TDL Settings
          3: Add Tanium Server TDL Auth User
          4: Add Tanium Server TDL Auth Cert

          5: Edit Tanium Module Server Settings
          6: Edit Tanium Module Server TDL Settings
          7: Add Tanium Module Server TDL Auth User
          8: Add Tanium Module Server TDL Auth Cert

          9: Edit Tanium Zone Server Settings
          11: Edit isolated subnets list
          12: Edit separated subnets list

          13: Control Root CA Certs

          R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

4. Enter `2` to go to the **Tanium Server TDL Settings** menu or enter `6` to go to the **Module Server TDL Settings** menu.
5. Use the menu to edit proxy server settings.

©2026 Tanium Inc. All Rights Reserved

Platform settings used with proxy servers

Settings	Platform components	Guidelines
BypassCRLCheckHostList	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 this setting in the TDownloader configuration on the Tanium Server and Module Server. If you configure the Tanium Server and Module Server to access Internet sites through a proxy server, you can configure BypassCRLCheckHostList through Tanium Appliance. For more information, see Configuring proxy server settings.
BypassProxyHostList	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 this setting in the TDownloader configuration on the Tanium Server and Module Server. For more information, see Configuring proxy server settings.
ForceIPV6	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 Appliance and Windows deployments. The setting is hidden by default and its default value is 0. Contact Tanium Support for guidance before adding this setting (see Contact Tanium Support on page 510). For more information about proxy server settings, see Configuring proxy server

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
		settings on page 150 .
LogVerbosityLevel	Tanium Server (local) Module Server Zone Server TDownloader	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 Logging levels on page 512 . **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, disable logging to reduce disk writes. Temporarily re-enable logging on individual endpoints for troubleshooting.
ProxyPassword	Tanium Server Module Server TDownloader	For a proxy server that requires authentication, enter the password of the ProxyUserid user that establishes a connection with the proxy server. Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. For more information, see Configuring proxy server settings .
ProxyPort	Tanium Server Module Server TDownloader	Specify the proxy server listening port. Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. For more information, see Configuring proxy server settings .

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
ProxyServer	Tanium Server Module Server TDownloader	Specify the IP address of the proxy server. Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. For more information, see Configuring proxy server settings . **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 to 1.
ProxyType	Tanium Server Module Server TDownloader	Specify the type of proxy server authentication. Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. The possible values are Basic, NTLM, or None. For more information, see Configuring proxy server settings .
ProxyUserid	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. ProxyUserid is a TDownloader setting on the Tanium Server and Module Server. For more information, see Configuring proxy server settings .
TrustedHostList	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]`). TrustedHostList is a TDownloader setting on the Tanium Server and Module Server. For more information, see Configuring proxy server settings .

©2026 Tanium Inc. All Rights Reserved

Installing and managing an Appliance Array

An *Appliance Array* manages the connections and establishes trust between the Tanium Appliances that contain the components of a Tanium deployment. The Appliance Array makes it easy to set up and manage the Appliances.

A typical Appliance Array contains the following Appliances:

- A primary Tanium Server Appliance with an active database
- A secondary Tanium Server Appliance with a passive database
- A Tanium Module Server Appliance
- An optional standby Tanium Module Server Appliance
- One or more Tanium Zone Server Appliances

After you add members to an Appliance Array, you assign and install roles for the Tanium Core Platform components for the Tanium Server, Tanium Module Server, or Tanium Zone Server on the individual Appliances.

When you create an Array on an Appliance, the Appliance becomes an *Array Manager* of the Array.

- An Array Manager can add members, remove members, and refresh the Array.
- When you install a Tanium Server role on an Appliance in the Array, the corresponding Appliance becomes an Array Manager of the Array. Any other Appliances without a Tanium Server role become simply Array members; this could include the Appliance where the Array was created. You might need to Refresh an Appliance Array on page 174 on the affected Appliances to see the change.

©2026 Tanium Inc. All Rights Reserved

Note:

In the following scenarios, a Tanium Server can be a member of an Array without having Array Manager capabilities:

- You add a member to an Array with no role and install Tanium Server directly on the member, rather than through the Array.
- You add an existing Tanium Server to an Array.

To promote a Tanium Server Appliance that is not already an Array Manager, see Promote a Tanium Server to Array Manager on page 172.

Best Practice: Configure both Tanium Servers in a cluster as Array Managers. This is done automatically if you install the Tanium Server role on an Appliance in an Array.

Use the **Appliance Array** menu to create an Array, add Appliances to the Array, assign Tanium roles to the Appliances, and then install the roles *on all Appliances* from a single menu. If you need to add an additional Appliance later on, you can add the Appliance to the Array, and then assign and install a role to use with your existing installation.

Note: SSH communication is required for managing an Appliance Array. If you are deploying a Tanium Zone Server in a network that does not allow SSH communication, you can install the Zone Server separately after you install the Array.

Before you begin

- Power on all Appliances.
- For a physical Tanium Appliance, perform the steps listed in the Tanium Appliance Data Center Guide to install the Tanium Appliances.
- Configure basic network, host, and user settings on all Appliances.
  - For physical Tanium Appliances, see Completing the initial setup (physical Tanium Appliance) on page 60.

©2026 Tanium Inc. All Rights Reserved

    - For virtual Tanium Appliances, see Completing the initial setup (virtual Tanium Appliance) on page 93.
    - For cloud-based Tanium Appliances, see Completing the initial setup (cloud-based Tanium Appliance) on page 130.
- If the `tanadmin` user is set up for SSH key authentication on all Appliances, copy the public key for the `tanadmin` user on the primary Appliance to the `tanadmin` user accounts on the remaining Appliances.
    - For information about how to use TanOS menus to add a public key for a user account, see Add authorized keys on page 229.
    - For information about how to use the CLI to add a public key for a user account, see the add pubkeys command at TanOS management commands on page 600.
- Make sure all Appliances are running TanOS 1.6.0 or later.
- Make sure all Appliances are running the same version of TanOS.
- Make sure your network security administrator has configured security rules to allow communication on the TCP ports that the Tanium Core Platform components use. In addition to the ports that are used by individual Tanium Servers, a Tanium Server in a Tanium cluster sends and receives cluster-related data over an IPsec connection. The network security rules must allow ESP (IP protocol 50) and IKE (500/udp, 4500/udp).

(Optional) Import keys

About this task

The Tanium Server includes a pki.db file that contains the root keys, Tanium Server TLS keys, and message-signing keys for the Tanium Server. If you migrate from a Windows installation, or if you restore the Tanium Server Appliance from a backup, you can reuse the previous pki.db file.

Note: For a Tanium cluster, import the pki.db only to the Appliance that you are using for the primary Tanium Server. The Array setup manages trust between the Tanium Servers automatically. You need the pki.db file only from the primary Tanium Server in an existing deployment or backup.

©2026 Tanium Inc. All Rights Reserved

1. Obtain a copy of the pki.db file from your existing Tanium Server or from a backup file.
2. Use SFTP to copy the pki.db file to the /incoming folder on the Appliance before the install.

Create the Array

1. Sign in to the primary Tanium Server Appliance as a user with the `tanadmin` role.
2. Enter `1`-`M` (Tanium Installation > Appliance Array).
3. Enter `C` and follow the prompts to create an Array.

```
           >>> Installation -> Appliance Array -> Create Array <<<

This activity creates a new array, with the current appliance being the
initial Array Manager. Other appliances can then be added to this
array, provided that either:
  A. The added member has no role (i.e. is not yet a TS, TMS, etc.); or
  B. The Array Manager has a TS (All-in-One or TaniumServer)

Please enter the name of the array: Tanium Appliance Array
Select the address other members would use to contact this appliance
         1: 10.10.10.60

Please select: 1
Successfully created the Appliance Array

Press enter to continue
```

4. Press the **Enter** key to go to the **Appliance Array** menu. The **Appliance Array** menu refreshes with the new Array.
   TanOS assigns the new (pending) role for the Appliance as a Tanium Server.

```
-----------------------------------------------------

       >>> Installation -> Appliance Array <<<

Array Name:              Tanium Appliance Array
```

©2026 Tanium Inc. All Rights Reserved

```
Array UUID:              0f6c41f1-409c-4515-9b8a-f4e5b6798695
Number of Array Members: 1

      Hostname        Current Role           Platform    New Role
   1: ts1             None                   None        Tanium Server

   A: Add Member
   F: Refresh Appliance Array
   I: Install Pending Role Changes
   X: Reset Appliance Array

   R: Return to previous menu

-----------------------------------------------------
```

Add members to the Array

About this task

Note: Before you begin: If the `tanadmin` user is set up for SSH key authentication on all Appliances, copy the public key for the `tanadmin` user on the primary Appliance to the `tanadmin` user accounts on the remaining Appliances. For information about how to use TanOS menus to add a public key for a user account, see Add authorized keys on page 229. For information about how to use the CLI to add a public key for a user account, see the add pubkeys command at TanOS management commands on page 600.

©2026 Tanium Inc. All Rights Reserved

Tip:

If you have instead configured separate public keys for the `tanadmin` user on each Appliance, you can use agent forwarding to authenticate with the added Array members by including the `-A` SSH option when you connect to an Array Manager. This avoids entering the password for new Array members. For example:

```
ssh -A user@Array_manager
```

Agent forwarding requires an SSH agent (such as ssh-agent in OpenSSH) to be running on your local host. For more information, see the documentation for your SSH client.

Perform the following steps to add the other Appliances to the Array.

1. Enter `A` from the **Appliance Array** menu on the primary Tanium Server Appliance.
2. Follow the prompts to add the Appliance to the Array.

```
>>> Installation -> Appliance Array -> Add Member <<<

This activity adds a remote TanOS appliance to the array. Doing so requires
logging into the remote appliance to gather information and provide that
appliance with information about the array. You may be asked to enter the
password for tanadmin on the remote appliance.
Only TanOS 1.6 and later can be added to an Appliance Array.
Initial config must have been run on the remote appliance.

Please enter the remote appliance address: 10.10.10.61
If prompted, please enter the password for tanadmin@10.10.10.61
Password:

The authenticity of host '10.10.10.61 (10.10.10.61)' can't be established.
ECDSA key fingerprint is SHA256:v95SkzzNuh9kP6WTxkXXC9iIAKWfpy+PZss7UoSz1Dk.
ECDSA key fingerprint is MD5:ab:b8:80:86:fb:6b:25:15:00:85:23:09:36:3d:f9:c5.
Are you sure you want to continue connecting (yes/no)?
```

©2026 Tanium Inc. All Rights Reserved

```
Successfully added host 10.10.10.61 to the Appliance Array


Press enter to continue
```

Tip: During the process of adding a member to the Array, the Array Manager asks you to confirm the ECDSA fingerprint of the new member. To verify that the fingerprint is correct, log in to the Appliance you are adding to the Array, view the SSH fingerprints, and confirm that the fingerprint listed for `ECDSA` matches the fingerprint that the prompt displays. For more information, see View SSH fingerprints on page 355. Alternatively, you can use the following CLI command: `ssh -qt user@new-appliance show ssh-host-fingerprints`

3. Press the Enter key to go to the **Appliance Array** menu.
   The **Appliance Array** menu refreshes with the new member.

```
-------------------------------------------------------


       >>> Installation -> Appliance Array <<<


Array Name:               Tanium Appliance Array
Array UUID:               0f6c41f1-409c-4515-9b8a-f4e5b6798695
Number of Array Members: 2

      Hostname        Current Role           Platform    New Role
   1: ts1             None                   None        Tanium Server
   2: ts2             None                   None        No Change


   A: Add Member
   F: Refresh Appliance Array
   I: Install Pending Role Changes
   X: Reset Appliance Array


   R: Return to previous menu


-------------------------------------------------------
```

©2026 Tanium Inc. All Rights Reserved

Repeat these steps to add the remaining Appliances to the Array.

```
-------------------------------------------------------


       >>> Installation -> Appliance Array <<<


Array Name:               Tanium Appliance Array
Array UUID:               0f6c41f1-409c-4515-9b8a-f4e5b6798695
Number of Array Members: 4


      Hostname        Current Role           Platform    New Role
   1: ts1             None                   None        Tanium Server
   2: ts2             None                   None        No Change
   3: tms1            None                   None        No Change
   4: tzs1            None                   None        No Change


   A: Add Member
   F: Refresh Appliance Array
   I: Install Pending Role Changes
   X: Reset Appliance Array


   R: Return to previous menu


-------------------------------------------------------
```


Tip: If you are creating a Tanium cluster or using a standby Module Server, make sure you add members to the Array for the second Tanium Server and standby Module Server. For more information, see Configuring a Tanium cluster on page 168.

Assign roles

About this task

Use the **Appliance Array** menu to assign a Tanium Server, Tanium Module Server, or Tanium Zone Server role to each Appliance.

©2026 Tanium Inc. All Rights Reserved

1. Return to the **Appliance Array** menu on the primary Tanium Server Appliance.
2. Enter the line number for an Appliance without a pending **New Role**.
   The **Manage Member** menu appears.

```
           >>> Appliance Configuration -> Appliance Array -> Manage Member <<<

Serial Number:      VMware-564d7441f288a8d6-a4da1a1bac78aaa5
Name:               ts2
FQDN:               ts2.tam.local
TanOS Version:      1.9.1.1234
Role:               None
Pending Role:       No Change

   T: Assign Role: TaniumServer
   M: Assign Role: TaniumModuleServer
   Z: Assign Role: TaniumZoneServer
   U: Cancel Pending Role Change

   D: Delete Member

   R: Return to previous menu

------------------------------------------------------
```

3. Enter `T`, `M`, or `Z` to assign the corresponding role to the Appliance.
   The **Appliance Array** menu refreshes with the new pending role.

```
------------------------------------------------------

       >>> Installation -> Appliance Array <<<

Array Name:              Tanium Appliance Array
Array UUID:              0f6c41f1-409c-4515-9b8a-f4e5b6798695
Number of Array Members: 4

      Hostname        Current Role       Platform       New Role
```

```
   1: ts1            None              None          Tanium Server
   2: ts2            None              None          Tanium Server
   3: tms1           None              None          No Change
   4: tzs1           None              None          No Change

   A: Add Member
   F: Refresh Appliance Array
   I: Install Pending Role Changes
   X: Reset Appliance Array

   R: Return to previous menu  RR: Return to top

-------------------------------------------------------
```

Repeat these steps to assign roles to the remaining Appliances in the Array.

```
-------------------------------------------------------

       >>> Installation -> Appliance Array <<<

Array Name:              Tanium Appliance Array
Array UUID:              0f6c41f1-409c-4515-9b8a-f4e5b6798695
Number of Array Members: 4

      Hostname        Current Role     Platform      New Role
   1: ts1             None             None          Tanium Server
   2: ts2             None             None          Tanium Server
   3: tms1            None             None          Tanium Module Server
   4: tzs1            None             None          Tanium Zone Server

   A: Add Member
   F: Refresh Appliance Array
   I: Install Pending Role Changes
   X: Reset Appliance Array

   R: Return to previous menu
```

©2026 Tanium Inc. All Rights Reserved

```
------------------------------------------------
```

Important: If you close the **Appliance Array** menu before you install Tanium, you must reassign roles.

CONFIGURING A TANIUM CLUSTER

If you add two Tanium Servers to an Appliance Array, TanOS automatically configures a Tanium cluster.

Best Practice: Use a redundant cluster of Tanium Servers to ensure continuous availability in the event of an outage or scheduled maintenance.

Important: Monitor the replication status between Tanium Servers to make sure that the cluster is healthy and providing redundancy. A `Database Replication` error in the health check indicates an issue with replication in the Tanium Server cluster. To manually check replication status, see Managing the Tanium Core Platform on TanOS on page 266 and Monitoring and maintaining the Tanium Appliance on page 417. As a best practice, configure a monitoring method that quickly alerts you to issues. For more information, see Monitoring and maintaining the Tanium Appliance on page 417.

Note: A Tanium cluster does not scale Tanium capacity or improve performance.

For information about managing replication and failover in an existing Tanium cluster, see Manage a Tanium cluster on page 328. For information about using a Tanium cluster as part of a backup and redundancy plan, see Use a Tanium Server cluster for redundancy on page 383.

In a Tanium cluster deployment:

- The Tanium Server application setup is active-active and the database component is active-passive.
- Tanium Clients use a Tanium Server list to automatically find a backup Server in the event the first Tanium Server that is assigned to them is unavailable due to an outage or scheduled

©2026 Tanium Inc. All Rights Reserved

maintenance.

- The Tanium Servers read and write to the active database on the first Appliance. Data is asynchronously replicated from the first Appliance database to the second Appliance database.
- The local authentication user configuration is actively synchronized between the two Appliances.
- IPsec ensures end-to-end security between the two Appliances.
- Each Tanium Server has a Tanium Console with its own URL.
- Tanium solutions are installed on a shared Module Server, and you only need to import solutions on one Tanium Console.
- Each Tanium Server passes messages (such as answers to questions) to the other Tanium Servers.
- Package files that are uploaded to one Server are synchronized to the other Tanium Servers.

Tanium cluster requirements and limitations

A Tanium cluster deployment has the following requirements:

- Each Tanium Server must run the same software version, including build number. For example, if you are installing Tanium Core Platform 7.9.3.2345 on one Tanium Server, you must install 7.9.3.2345 on all Servers; you cannot install 7.9.3.1234 on a different Tanium Server.
- Each Tanium Server in the Tanium cluster must meet or exceed the requirements for the total number of endpoints targeted by your deployment. Each must be able to independently handle load from the full deployment in the event of failure.
- The Tanium cluster members must be able to connect to each other via a reliable Ethernet connection. Connections require a minimum throughput of 1 Gbps and a maximum round-trip latency of 30 ms.
- Each Tanium cluster member must be able to access the Internet to download files from designated domains. Access can be either direct or made through a proxy server.

©2026 Tanium Inc. All Rights Reserved

- Each Tanium cluster member must be able to connect to the shared Module Server.

CONFIGURING A STANDBY MODULE SERVER

If you add two Module Servers to an Appliance Array, you can schedule a Module Server sync to use the second Module Server as a standby. For information about managing synchronization of a secondary Module Server, see Manage the standby Module Server on page 329. For information about using a standby Module Server as part of a backup and redundancy plan, see Use a standby Module Server for redundancy on page 386.



Important: A second Module Server does not function as a standby Module Server until you schedule the Module Server sync.

Install Tanium roles

About this task

Perform the following steps to install the Tanium Core Platform components on the Appliances in the Appliance Array. When you use the following process to install Tanium through an Appliance Array, the installation process automatically copies the required RPM file from the primary Tanium Server to each Appliance in the Array.

BEFORE YOU BEGIN

The installation package for Tanium Core Platform is a ZIP file (<tanium.version>_linux_server_package_8.zip) that includes files for the Tanium Server, Tanium Module Server, and Tanium Zone Server. Use one of the following methods to access the installation package:

- Obtain the token URL from Tanium Support to gain access to the installation packages for Tanium Core Platform. You can download the installation package from the token URL directly to the Appliance during role installation.
- Download the installation package from the **Artifacts** section of your Tanium Account, and then use SFTP to copy the ZIP file to the /incoming folder of the primary Tanium Server Appliance. For more information, see View Tanium artifacts and Reference: Transfer files to and from the Appliance on page 621.

©2026 Tanium Inc. All Rights Reserved

> **Note:** This method is necessary if you have a proxy server that your Tanium Server must use to reach the internet, or if you are in an air-gapped environment. After you install Tanium, you can configure proxy settings from Tanium Console, which are used for future upgrades.

INSTALL ROLES

1. From the **Appliance Array** menu, enter `I`.
2. Follow the prompts to install pending roles.
   - When prompted, enter the line number of the Tanium Core Platform version that you want to install.
   - If you install roles to a new Array, specify a password for the initial Tanium Console admin user (**tanium**) when prompted.
   - If the Array already contains an Appliance with the Tanium Server role, specify a Tanium Console user and password with administrative credentials when prompted.
   - If you have the token URL, enter `T` and then enter the URL.
   - If you copied the pki.db file to the /incoming folder on the Appliance, the installer discovers the file and prompts you to install it. Enter `YES` to continue.

Result

TanOS installs the components of the Tanium Core Platform on the selected Appliances.

> **Tip:** After you install the Tanium roles to the Appliances, you can add more Appliances to the Array. To do so, add the Appliance to the Array, assign a role to the Appliance, install the pending role, and then perform any additional required configuration for the Tanium role.

What to do next

- Schedule sync jobs on page 329 for the standby Module Server.
- If you are deploying a Tanium Zone Server in a network that does not allow SSH communication, install the Zone Server separately on page 176.
- If you are deploying Zone Servers and you plan to use Direct Connect, install the Direct

©2026 Tanium Inc. All Rights Reserved

Connect Zone Proxy on page 183 on each Zone Server.

- Verify the installation on page 196, including uploading the Tanium license on page 198.

Additional management tasks for an Appliance Array

PROMOTE A TANIUM SERVER TO ARRAY MANAGER

About this task

An Array Manager is a Tanium Server that can sign in to and issue commands to other Array members. The following Tanium Servers are automatically assigned the Array Manager designation:

- The Tanium Server on which you set up the Array. For more information, see Create the Array on page 161.
- Up to two Tanium Servers in an Array that are upgraded from 1.6.*x* to 1.7*x*
- An Appliance on which you install Tanium Server using the existing Array Manager

In the following scenarios, a Tanium Server can be a member of an Array without having Array Manager capabilities:

- You add a member to an Array with no role and install Tanium Server directly on the member, rather than through the Array.
- You add an existing Tanium Server to an Array.

Best Practice: Configure both Tanium Servers in a cluster as Array Managers. This is done automatically if you install the Tanium Server role on an Appliance in an Array.

Use the following steps to promote a Tanium Server to Array Manager.

1. On an Array Manager, sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `1` to open the **Tanium Installation** menu.
3. Enter `M` to open the **Manage Appliance Array** menu.

©2026 Tanium Inc. All Rights Reserved

4. Enter the line number of the Appliance to promote to Array Manager.
5. Enter `P` to promote the Appliance to Array Manager.

REMOVE AN APPLIANCE FROM AN APPLIANCE ARRAY

About this task

From an Array Manager of an Array, you can remove other Appliances from the Array, including other Array Managers.

Note: An Appliance cannot remove itself from an Array. To remove an Appliance, you must sign in to another Array Manager of the Array to perform the steps. To remove the last member of an Array, reset the Array.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `1-M` (Tanium Installation > Appliance Array).
3. Enter the line number of the Appliance that you want to remove from the Array.

```
           >>> Appliance Configuration -> Appliance Array -> Manage Member <<<

Report from remote appliance 'appliance-162-2' at '10.10.10.65'

Serial Number:      be04e9e1-c5e7-46e5-975e-93320a8c8792
Name:               appliance-162-2
TanOS Version:      1.9.1.1234
Role:               Tanium Server
TaniumServer:       7.9.3.1234

         D: Delete Member

         R: Return to previous menu

-----------------------------------------------------
```

4. Enter `D` and follow the prompts to remove the Appliance from the Array.

```
           >>> Appliance Configuration -> Appliance Array -> Delete Member <<<

Report from remote appliance 'appliance-162-2' at '10.10.10.65'

Serial Number:      be04e9e1-c5e7-46e5-975e-93320a8c8792
Name:               appliance-162-2
TanOS Version:      1.9.1.1234
Role:               Tanium Server
TaniumServer:       7.9.3.1234

This operation will remove a member from the array.

1. The member will be asked to leave
2. The controlling appliance will forget about the member
3. All remaining members will be informed of the removal

As a result all appliances associated with the array will be updated and
will no longer recognize the appliance as part of the array.

Are you sure you want to remove appliance-160-2 from the array? [Yes|No]:
```

REFRESH AN APPLIANCE ARRAY

About this task

From an Array Manager of an Array, you can refresh the Array to retrieve current membership from the other Appliances in the Array. This information is refreshed on all Appliances in the Array.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `1`-`M` (Tanium Installation > Appliance Array).
3. Enter `F` and follow the prompts to refresh the Array.

```
           >>> Appliance Configuration -> Appliance Array -> Refresh Array <<<
```

©2026 Tanium Inc. All Rights Reserved

```
This action will communicate with each member of the array, retrieve current
information, and re-distrubute that information to all array members.

Do you want to continue? [Yes|No]: yes

Getting update from ts2 (10.10.10.61)
Getting update from tms1 (10.10.10.62)
Getting update from tzs1 (10.10.10.63)
Sending update to ts2 (10.10.10.61)
Sending update to tms1 (10.10.10.62)
Sending update to tzs1 (10.10.10.63)

Press enter to continue
```

RESET AN APPLIANCE ARRAY

About this task

Reset an Appliance Array to remove the Appliance from the Array. If the Appliance is the only member of the Array, reset the Array to delete the Array.

Tip: To delete an Array, sign in to an Array Manager of the Array, remove all other members of the Array, and then reset the Array.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `1`-`M` (Tanium Installation > Appliance Array).
3. Enter `X` and follow the prompts to reset the Array.

```
          >>> Appliance Configuration -> Appliance Array -> Reset Array <<<

This appliance is the sole member of an existing array. Since it is the sole
member, resetting the array will not affect other appliances.
```

©2026 Tanium Inc. All Rights Reserved

```
Do you want to drop this appliance from the array? [Yes|No]: yes

Press enter to continue
```

MEASURE THE DATA TRANSFER RATE BETWEEN AN ARRAY MANAGER AND AN ARRAY MEMBER

About this task

You can measure the data transfer rate between an Array Manager and another Appliance in the Array to help diagnose network issues between Appliances.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `1-M` (Tanium Installation > Appliance Array).
3. Enter the line number for the Appliance with which to measure the data transfer rate.
4. Enter `N` to begin the measurement.

Configuring optional components

As necessary in your environment, you can install and configure individual Zone Servers not managed by the Array, Direct Connect Zone Proxies, a Tanium All-in-One deployment for demos, or Cloud Access Points.

The subsequent topics in this section detail the steps to install and configure these components.

Installing individual Zone Servers

About this task

> **Important:** An Appliance Array is required to manage Tanium Servers and Tanium Module Servers in a Tanium Appliance deployment. For more information about how to install an Appliance Array, see Installing and managing an Appliance Array on page 158.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Use the Appliance Array to manage Tanium Zone Servers as well. Install and configure a Zone Server separately from the Appliance Array only if the network in which the Zone Server is installed does not allow SSH communication.

If your deployment includes a Tanium Zone Server that is installed in a network that does not allow SSH communication, you can install and upgrade the Zone Server separately from the Appliance Array.

The Tanium Zone Server role installation creates the Tanium Zone Server and configuration database. You must also install the Tanium Zone Server Hub add-on on the Tanium Server and configure the Zone Server Hub to listen for connections from the Zone Server.

This section provides procedures for the following workflow:

1. Deploying one or more Zone Server Appliances in the network
2. Installing the Zone Server Hub add-on on the Tanium Server Appliance and configure a Zone Server list that defines the Zone Servers with which it can communicate
3. Establishing trust with the Tanium Server, Zone Server Hub, and Zone Server

   Important: After you install an individual Zone Server separately from the Appliance Array, you must also upgrade it separately at the same time you upgrade the Appliance Array. The procedure is the same, but it must be done separately on each Zone Server that is not an Array member. For more information, see Upgrade TanOS on Tanium Appliances on page 469.

BEFORE YOU BEGIN

- Make sure basic network, host, and user settings are configured.
  - For physical Tanium Appliance, see Completing the initial setup (physical Tanium Appliance) on page 60.
  - For virtual Tanium Appliance, see Completing the initial setup (virtual Tanium Appliance) on page 93.
  - For cloud-based Tanium Appliance, see Completing the initial setup (cloud-based Tanium Appliance) on page 130.

©2026 Tanium Inc. All Rights Reserved

- Make sure your network security administrator has configured security rules to allow communication on the TCP ports that the Tanium Core Platform components use. For a complete list of network requirements, see Network connectivity and firewall on page 32.
- Download the Tanium Core Platform installation package from the **Artifacts** section of your Tanium Account. This ZIP file includes the RPM files for the Tanium Server, Tanium Module Server, and Tanium Zone Server.

  Best Practice: To avoid copying Tanium Server and Module Server files onto a host in a separate network, download the package from the **Artifacts** section of your Tanium Account, extract only the Zone Server RPM from ZIP file, and use SFTP to copy only that file to the /incoming folder of the Zone Server Appliance.

INSTALL THE ZONE SERVER ROLE

1. Sign in to the Zone Server Appliance as a user with the `tanadmin` role.
2. Enter `1-4` (Tanium Installation > Install Tanium Zone Server).
3. Enter the line number of the Tanium Core Platform version that you want to install.
4. Enter `YES` to continue with the installation.

IMPORT THE TANIUM SERVER PUBLIC KEY FILE TO THE ZONE SERVER

1. Download the public key file (tanium-init.dat) through Tanium Console. For more information, see Download infrastructure configuration files (keys).
2. Use SFTP to copy the tanium-init.dat file to the /incoming directory on the Zone Server Appliance.
3. Sign in to the Zone Server Appliance as a user with the `tanadmin` role.
4. Enter `2` (Tanium Operations).
5. Enter `I` and follow the prompts to copy the Tanium Server public key file (tanium-init.dat) into the Zone Server installation directory.

```
>>> Tanium Operations -> TaniumZoneServer - Import Public Key <<<
```

©2026 Tanium Inc. All Rights Reserved

```
This action is to install the incoming Tanium public key onto the Tanium Zone
Server.

Incoming tanium-init.dat: Yes  (MD5: c36c02a7aedec9521fc89569d2a83192)

1) SFTP to this appliance using tancopy
2) Upload the public key file (tanium-init.dat) into the incoming directory
3) Continue below with yes, the file will be copied

The Tanium Zone Server will restart as part of this operation.

Would you like to install this file? [Yes|No]: yes

Finished installing new public key

Press enter to continue
```

INSTALL THE ZONE SERVER HUB

About this task

You must also install the Zone Server Hub add-on on the Tanium Server in the Array.

1. Sign in to the Tanium Server Appliance as a user with the `tanadmin` role.
2. Enter `1` (Tanium Installation).
3. Enter `A` and follow the prompts to install the Tanium Zone Server Hub add-on.

SET UP ALLOWEDHUBS ON THE ZONE SERVER APPLIANCE

1. Sign in to the Zone Server Appliance as a user with the `tanadmin` role.
2. Enter `2-2` (Tanium Operations > Configuration Settings).
3. Enter `9` to edit the Tanium Zone Server settings.

©2026 Tanium Inc. All Rights Reserved

```
           >>> Tanium Operations -> Configuration Settings -> Edit <<<

   Editing: Tanium Zone Server Config Settings

 # Line Content

 1: FIPSMode 0
 2: LogVerbosityLevel 1
 3: Version 7.9.3.1234

A: Add a line
R: Return to previous menu  RR: Return to top
```

4. Enter `A` to add a new setting.
5. For the key, enter `AllowedHubs`.
6. For the value, enter the IP address of the Tanium Server.

```
           >>> Tanium Operations -> Configuration Settings -> Edit <<<

   Editing: Tanium Zone Server Config Settings

 # Line Content

 1: FIPSMode 0
 2: LogVerbosityLevel 1
 3: Version 7.9.3.1234

A: Add a line
R: Return to previous menu  RR: Return to top

Please select: a

Please enter the new setting key: AllowedHubs
Value: 10.10.10.50
```

©2026 Tanium Inc. All Rights Reserved

CONFIGURE TRUST MAPPINGS

When you install a Zone Server separately from the Appliance Array, you must enable trust between the Tanium Server, Tanium Zone Server Hub, and Tanium Zone Servers so that they can communicate with each other.

Approve trust for the Zone Server Hub

1. Sign in to the TanOS console of the Zone Server Hub Appliance as a user with the `tanadmin` role.
2. Enter `@` to go to the **About the Appliance** page. Note the value of the TZS Hub Registration Fingerprint field.

```
            Tanium Zone Server Pub Key MD5:   Not Available
Tanium Zone Server Init Key MD5:  Not Available
TZS Hub Registration Fingerprint: 43:e6:3b:8c:d7:98   <----------
Tanium License MD5:               Not Available
```

3. Sign in to Tanium Console as a user with the `Admin` role and the password you set when you installed the Tanium Server.
4. From Tanium Console, go to **Administration** > **Configuration** > **Zone Servers** and open the **Zone Server Hubs** tab.
5. Verify that the fingerprint of the Zone Server Hub matches the fingerprint shown in the **TZS Hub Registration Fingerprint** field in the **About the Appliance** page in the TanOS console.
6. If the fingerprints are identical, return to Tanium Console, click **Accept/Deny** next to the Zone Server Hub, and click **Accept**.

   Note: If the fingerprint or IP address of a Zone Server Hub is 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.

7. Enter your credentials and click **OK**.

Map the Zone Server to the Zone Server Hub

©2026 Tanium Inc. All Rights Reserved

About this task

After you approve trust for Zone Server Hub, perform the following steps for each Zone Server.

1. Sign in to the TanOS console of the Zone Server Appliance as a user with the `tanadmin` role.
2. Enter `@` to go to the **About the Appliance** page. Note the value of the **TZS Registration Fingerprint** field.

```
            Tanium Zone Server Pub Key MD5:  Tanium Zone Server installed but no pub
found
TZS Registration Fingerprint:    fa:3f:30:13:c5:be   <----------
Tanium License MD5:              Not Installed
```

3. Sign in to Tanium Console as a user with the `Admin` role and the password you set when you installed the Tanium Server.
4. From Tanium Console, go to **Administration** > **Configuration** > **Zone Servers** and open the **Zone Server Hubs** tab.
5. Beside the Zone Server Hub, click **Add Zone Server**, enter the IP address of the Zone Server, and click **OK**.
   Tanium Console might take a few minutes to show the mapping. When it does, the mapping **Status** appears as **Pending** next to the Zone Server on the **Zone Servers** tab.
6. Verify that the fingerprint of the Zone Server matches the fingerprint shown in the **TZS Registration Fingerprint** field in the **About the Appliance** page in the TanOS console.
7. If the fingerprints are identical, return to Tanium Console, go to **Administration** > **Configuration** > **Zone Servers** and open the **Zone Servers** tab. Click **Accept/Deny** next to the Zone Server, and click **Accept**.
   In the Zone Server tile, the mapping *Status* changes to **Approved**.

   > **Note:** If the fingerprint or IP address of a Zone Server is wrong, decommission the Zone Server before denying trust for it. Denied trust is irreversible for any particular instance of a Zone Server. To subsequently approve trust, you must uninstall and reinstall the Zone Server so that it generates a new fingerprint.

WHAT TO DO NEXT

©2026 Tanium Inc. All Rights Reserved

- If you plan to use Direct Connect, install the Direct Connect Zone Proxy on page 183 on each Zone Server.
- Verify the installation on page 196, including uploading the Tanium license on page 198.

Installing and managing a Direct Connect Zone Proxy

The subsequent topics in this section provide information about Direct Connect Zone Proxies, including how to import and configure Direct Connect, obtain and install the proxy on each Zone Server Appliance, check installed versions, and upgrade or remove the proxy.

ABOUT DIRECT CONNECT ZONE PROXIES

For installations with Direct Connect, install a zone proxy to enable connections to endpoints through the Zone Server Appliance. This configuration is required to use Direct Connect with endpoints that connect to the Module Server through a Zone Server.

IMPORT AND CONFIGURE DIRECT CONNECT

In Tanium Console, go to **Administration** > **Configuration** > **Solutions** and import Direct Connect. For more information about how to import Direct Connect, verify the installation, and then set up Direct Connect, see Installing Direct Connect. When you reach the steps to configure zone proxies, use the steps in the following sections to install the Direct Connect Zone Proxy to the Zone Server Appliance.

OBTAIN THE DIRECT CONNECT ZONE PROXY INSTALLER FILE

Obtain the Direct Connect Zone Proxy installer file for the Zone Server Appliance from Tanium Support on page 510. The upgrade package is provided as a token URL.

INSTALL THE DIRECT CONNECT ZONE PROXY ON EACH ZONE SERVER APPLIANCE

About this task

For the initial installation, you must repeat the following procedure each Zone Server Appliance in your Array. You can either provide the token URL for the installer during the installation process or manually upload the RPM file to /incoming.

©2026 Tanium Inc. All Rights Reserved

Tip: You can upgrade all Zone Proxy Appliances at the same time from the Tanium Server Appliance. For more information, see Upgrade the Direct Connect Zone Proxy on all Zone Server Appliances on page 186.

1. Sign in to the TanOS console of the Zone Server Appliance as a user with the `tanadmin` role.
2. Enter `1-D` (Tanium Installation > Tanium Direct Connect Zone Proxy).
3. If you have not uploaded a file to /incoming, enter `T` to enter the URL of a token download, and follow the prompts to download the installer.
4. Enter a number from the list to install the Direct Connect Zone Proxy.

```
 Please select: 1
 Tanium Direct Connect Zone Proxy rpm signature verified

 Installing Tanium Direct Connect Zone Proxy from tanium-direct-connect-zone-pro
xy-1.0.0-33.x86_64.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:tanium-direct-connect-zone-proxy-################################# [100%]
Proxy configuration written to /opt/Tanium/TaniumDirectConnectZoneProxy/settings
/settings.json

The following steps are required to complete your Zone Proxy Server
configuration:
1. IMPORTANT: Copy the provision secret and certificate from this console.
2. In the Direct Connect settings, on the *Add Zone Proxy* configuration
page, paste the provision secret and certificate in the *Provisioning
Payload* field.
3. Complete the remaining steps on the *Add Zone Proxy* configuration page.
For more details on these steps, see the Direct Connect User Guide.

-----BEGIN PROVISION SECRET-----
g9Q7yWoLs9aZKFtPFvfEFE+18zqbfX0ARosgk)MMDLwyTAIOSzAO419FDiGIWHN
```

©2026 Tanium Inc. All Rights Reserved

```
ChQoK27yYOorvUAfLZUQtU06MAObziluTQ7tRAqLLvKq0sZMg7grmMA/nDHtmRK
vc49dNA9nL8ygt44WnJXjKUjrjrEy63W1w3FNKwDHDtozGNHfOLtltmwiLvvFDg
CRbjdb86uwT1wT1BLGxMipXEF1NmPSsYjgenuhJtpz0jowZVMvfYkr2GLJIdl2i
UzBLU2295iwg7bYnC21v3A==
-----END PROVISION SECRET-----
-----BEGIN CERTIFICATE-----
MIIC9DCCAdwCCQDbV02DC5Fy5DANBgkqhkiG9w0BAQsFADA8MQswCQYDVQQGEwJV
UzELMAkGA1UECAwCQ0ExEzARBgNVBAcMCkVtZXJ5dmlsbGUxCzAJBgNVBAsMAklU
MB4XDTIwMDExMjE2NTUwM1oXDTIxMDExMTE2NTUwM1owPDELMAkGA1UEBhMCVVMx
CzAJBgNVBAgMAkNBMRMwEQYDVQQHDApFbWVyeXZpbGxlMQswCQYDVQQLDAJJVDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPWvZ1E/5cJ+dzHBW9gZ5rdD
A2sto5NQrHyFScM6tVTHowjEEhWDJQUjTGSreOcn7/QvBATqddcDYfJzpTjz+8hw
6cb+I17BhkcCzHhH7Jdz/7Ilx/5YFY7ooV1jTQnoW1oOJF/BhAg4R41YWRvp2pcB
jUXVdz9bD1NinffrcyiZhQdw3BoVlE9PHZgXlwkvHiLNVu0RJnEtMDEUlHHNcnmP
RqRgmm9a1yns3JyWmUv00hPn0eLucCYMIzutuAV6kEJmZG8F8lbYBRBlGGq7T2LJ
aVDtHxF6pguocXxm4Sz93S2t1+zvjtTqB5GiINhgKjdWFAtGAobCq7WaQH8lY88C
AwEAATANBgkqhkiG9w0BAQsFAAOCAQEAQtHLvLe0nsAiWtU79D+1PuDai+SqK61Y
pIOvqC0/jJ93tU1Q+v9SUhGkDfIiynDhoZvDAN4+8PG532++zhrUN1QyCjJ27/ux
CuTfq3QFo+viJHjR2TGvb5aH41tPKwS/Vxv/vO1GPsYcjZ73vErEI5ffRswZM1Tb
ypgvG5bVRfCg/Q/O3/q5PoJ/BYmx6W7NH0pFFEs95SyhEaecKwjSALTztnCDRP+L
8aXh9jKcdOfZtHocFgZtYTJgqlTryPGV8UJBVctKVz/C4TP0qrnznZDcjCKjxOkI
777GHvH1vaU1pZ+6KZpTjHklJXWqIcyd1xeO5gYMfTLX5ZGRcYCTIA==
-----END CERTIFICATE-----
```

5. Copy the provision secret and certificate that appears at the end of the installation. Follow the steps that appear to return to the Direct Connect settings in Tanium Console to complete the configuration. For information about how to configure a zone proxy in Direct Connect, see Configure Zone Proxies.
6. Press **Q** and **Enter** to exit the installation.

CHECK INSTALLED VERSIONS OF THE DIRECT CONNECT ZONE PROXY

About this task

You can check the version of the Direct Connect Zone Proxy that is installed on each Zone Proxy Appliance from the Tanium Server Appliance.

©2026 Tanium Inc. All Rights Reserved

1. Sign in to the TanOS console of the Tanium Server Appliance as a user with the `tanadmin` role.
2. Enter `1-D` (Tanium Installation > Tanium Direct Connect Zone Proxy).
3. Enter `L` to display the versions of the Direct Connect Zone Proxy that are installed on Zone Servers in the Array.

```
Please select: L


 Displaying versions of installed DEC Proxy on Zone Servers.


zs1: 1.3.0-0
zs2: 1.3.0-0
zs3: 1.3.0-0
```

UPGRADE THE DIRECT CONNECT ZONE PROXY ON ALL ZONE SERVER APPLIANCES

About this task

You can upgrade the Direct Connect Zone Proxy on all Zone Proxy Appliances at the same time from the Tanium Server Appliance. You can either provide the token URL for the installer during the installation process or manually upload the RPM file to /incoming.

1. Sign in to the TanOS console of the Tanium Server Appliance as a user with the `tanadmin` role.
2. Enter `1-D` (Tanium Installation > Tanium Direct Connect Zone Proxy).
3. If you have not uploaded a file to /incoming, enter `T` to enter the URL of a tokens download, and follow the prompts to download the installer.
4. Enter a number from the list to upgrade the Direct Connect Zone Proxy.

```
 Please select: 1
Filename: tanium-direct-connect-zone-proxy-1.2.3-0.x86_64.rpm
Package Name: tanium-direct-connect-zone-proxy-1.2.3-0
SHA256: bff47e35c34749140cf091f65aafd37ff9e9a04b2759608ff9f756e94e0f9a54


zs1: 1.1.0-14
zs2: 1.1.0-14
```

©2026 Tanium Inc. All Rights Reserved

```
zs3: 1.1.0-14


 Do you want to upgrade to Tanium Direct Connect Zone Proxy? [Yes|No]: Yes
Copying file tanium-direct-connect-zone-proxy-1.2.3-0.x86_64.rpm to zs1 (10.0.72.125)
Finished copying file
Upgrading zs1 DEC Proxy to 1.2.3-0
Copying file tanium-direct-connect-zone-proxy-1.2.3-0.x86_64.rpm to zs2 (10.0.72.126)
Finished copying file
Upgrading zs2 DEC Proxy to 1.2.3-0
Copying file tanium-direct-connect-zone-proxy-1.2.3-0.x86_64.rpm to zs3 (10.0.72.127)
Finished copying file
Upgrading zs3 DEC Proxy to 1.2.3-0
Removed symlink /etc/systemd/system/multi-user.target.wants/tanium-direct-connect-
zone-proxy.service.
 Press enter to continue
```

5. Press **Enter** to exit the upgrade.

REMOVE THE DIRECT CONNECT ZONE PROXY

1. Sign in to the TanOS console of the Zone Server Appliance as a user with the `tanadmin` role.
2. Enter `1-D` (Tanium Installation > Tanium Direct Connect Zone Proxy).
3. Enter `X` and follow the prompts to remove the Direct Connect Zone Proxy.

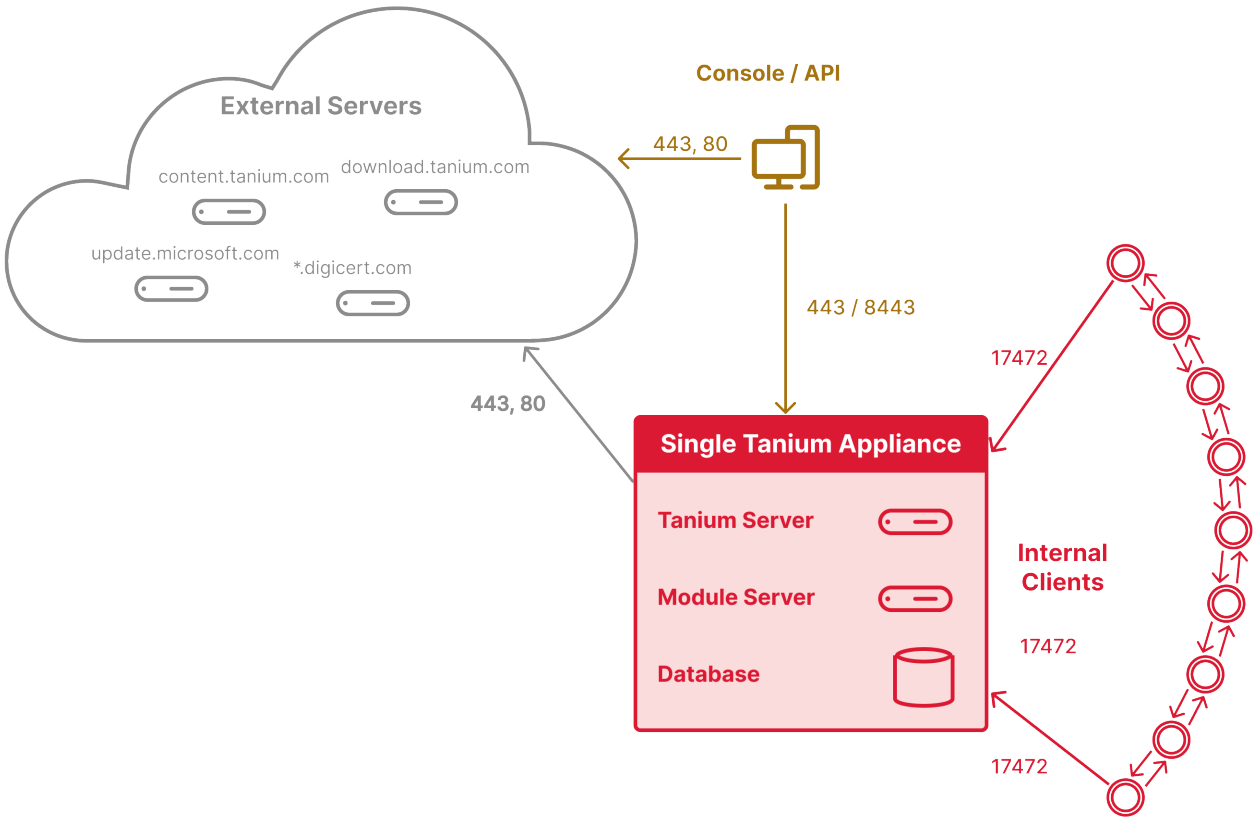
Installing a Tanium All-in-One for demos

In an All-in-One deployment, the Tanium™ Server, the Tanium™ Module Server, and a database server reside on the same Tanium Appliance. All-in-One deployments are supported only for proof-of-concept (POC) demonstrations.

> **Note:** Use Tanium Appliances configured with the All-in-One role only for evaluation purposes. Tanium does not support All-in-One deployments in production environments. Do not allow a Tanium Appliance that is configured with the All-in-One role to accept inbound connections from the internet.

©2026 Tanium Inc. All Rights Reserved

Figure 32. All-in-One deployment



The All-in-One role installation creates the necessary Tanium Core Platform Servers, SSL certificates, SSH keys, and configuration databases.

BEFORE YOU BEGIN

Make sure:

- Basic network, host, and user settings are configured.
    - For physical Tanium Appliances, see Completing the initial setup (physical Tanium Appliance) on page 60.
    - For virtual Tanium Appliances, see Completing the initial setup (virtual Tanium Appliance) on page 93.
    - For cloud-based Tanium Appliances, see Completing the initial setup (cloud-based Tanium Appliance) on page 130.
- Network firewall rules allow Tanium processes to communicate as expected. For more

©2026 Tanium Inc. All Rights Reserved

information, see Network connectivity and firewall on page 32.

INSTALL THE TANIUM ALL-IN-ONE ROLE

Before you begin

The installation package for Tanium Core Platform is a ZIP file (<tanium.version>_linux_server_package_8.zip) that includes files for the Tanium Server, Tanium Module Server, and Tanium Zone Server. Use one of the following methods to access the installation package:

- Obtain the token URL from Tanium Support to gain access to the installation packages for Tanium Core Platform. You can download the installation package from the token URL directly to the Appliance during role installation.
- Download the installation package from the **Artifacts** section of your Tanium Account, and then use SFTP to copy the ZIP file to the /incoming folder of the primary Tanium Server Appliance. For more information, see View Tanium artifacts and Reference: Transfer files to and from the Appliance on page 621.

  Note: This method is necessary if you have a proxy server that your Tanium Server must use to reach the internet, or if you are in an air-gapped environment. After you install Tanium, you can configure proxy settings from Tanium Console, which are used for future upgrades.

Note:

You can optionally use a Zone Server with an All-in-One Appliance if it is appropriate for your proof-of-concept environment. For this configuration, follow the steps Installing and managing an Appliance Array on page 158 instead of the following procedure, and install the **Tanium Server (All-In-One)** and **Tanium Zone Server Service** roles on the Appliances in the Array.

You cannot add additional Tanium Servers or Module Servers to an Array that contains an All-in-One Appliance.

©2026 Tanium Inc. All Rights Reserved

Install the All-in-One role

1. Sign in to the Appliance as a user with the `tanadmin` role.
2. Enter `1-1` (Tanium Installation > Install Tanium All-in-One).
3. When prompted, specify a password for the initial Tanium Console user (**tanium**).

```
            >>> Tanium Installation -> Install All in One <<<

Tanium Server installation detected.

A password for the initial Tanium application user (tanium) is required.



The password policy requires meeting these rules:
 - Minimum 10 characters long
 - Maximum 20 characters long
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
 - At least 1 other character
 - Must not be based on a dictionary word
 - Must not contain part of the username

Please enter password (will not be displayed):
Password score: 50 out of 100 (strong)
Please enter password again:
```

4. Choose an option to install the Tanium platform:
   - If you uploaded the file to the /incoming folder on the Appliance, the installer discovers the file and prompts you to do the installation.
   - If you have the token URL, enter `T`, enter the URL, and then follow the prompts.
5. Enter `YES` to continue with the installation.

Result

The installation takes approximately one minute to complete.

©2026 Tanium Inc. All Rights Reserved

WHAT TO DO NEXT

Verify the installation on page 196, which includes uploading the Tanium license on page 198.

Installing and managing a Tanium Cloud Access Point

A Tanium Cloud Access Point is an optional component that facilitates communication with Tanium Cloud™ from networks that have restricted access to Tanium Cloud, when it is not possible to use a customer-supplied proxy server. A Tanium Appliance that is configured with the Tanium Cloud Access Point role resides within the restricted network, and Tanium Clients can use it as a proxy to reach the Tanium Cloud. A Tanium Cloud Access Point is not required for unrestricted networks.

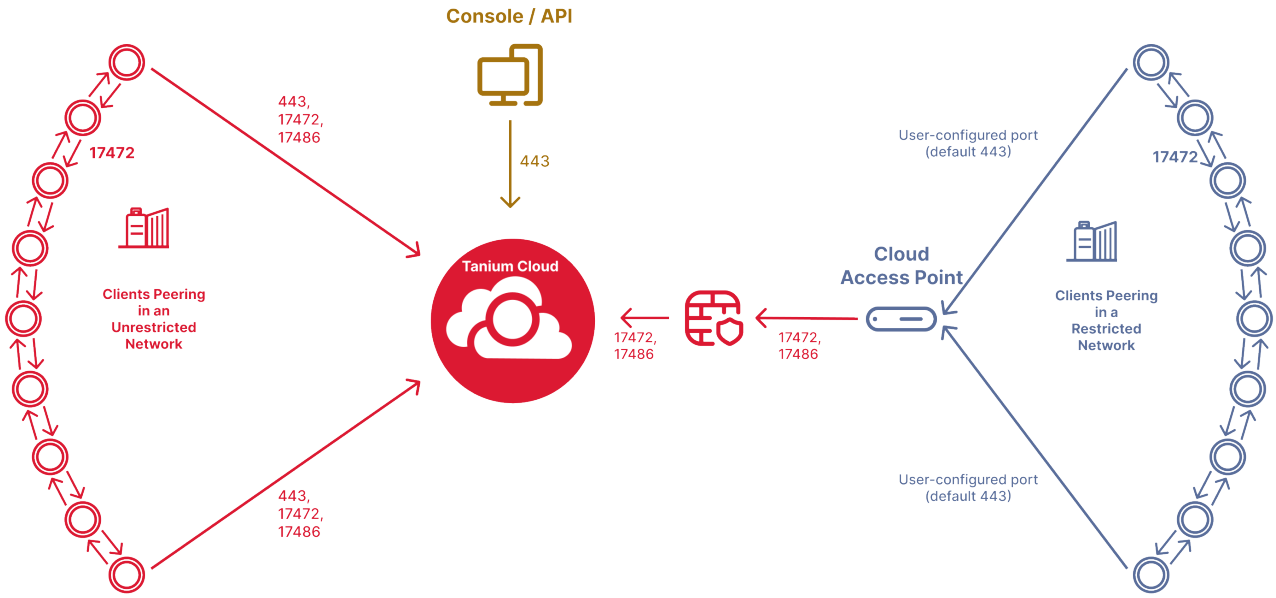
Best Practice: To avoid additional necessary infrastructure in your network, connect endpoints directly to Tanium Cloud when possible, or route through an existing proxy solution. Use a Tanium Cloud Access Point only when network restrictions outside your control prevent direct communication from endpoints to Tanium Cloud Client edge URLs and existing proxy infrastructure is not already in place. For more information about using your own proxy server, see Connect through an HTTPS forward proxy server.

Note:

- Though the Tanium Cloud Access point is supplied by Tanium, management of the Tanium Cloud Access Point is a customer responsibility, as part of the customer responsibility to provide Tanium Client access to Tanium Cloud. For more information about customer responsibilities in Tanium Cloud, see Responsibilities.
- A Tanium Cloud Access Point can route only Tanium-specific traffic.
- Do not connect more than 10,000 endpoints to a Cloud Access Point.

Figure 33. Tanium Client connectivity through a Cloud Access Point

©2026 Tanium Inc. All Rights Reserved



For more information about Tanium Cloud, see the Tanium Cloud User Guide.

BEFORE YOU BEGIN

Make sure:

- Basic network, host, and user settings are configured.
  - For physical Tanium Appliances, see Completing the initial setup (physical Tanium Appliance) on page 60.
  - For virtual Tanium Appliances, see Completing the initial setup (virtual Tanium Appliance) on page 93.
- Network firewall rules allow Tanium processes to communicate as follows:

Network communication ports for Tanium Cloud Access Point

Source	Destination	Port	Protocol	Purpose
Tanium Clients	Tanium Cloud Access Point	User-configured in Cloud Access Point	TCP	Client communication with the Tanium Cloud Access Point
Tanium Cloud	Tanium Cloud	17472, 17486	TCP	Tanium Cloud Access Point

©2026 Tanium Inc. All Rights Reserved

Source	Destination	Port	Protocol	Purpose
Access Point				communication to Tanium Cloud

Additional requirements depend on your environment and how you provide administrative access to the Appliance that you use for the Cloud Access Point. For more information, see Network connectivity and firewall on page 32.

INSTALL THE TANIUM CLOUD ACCESS POINT ROLE

1. Sign in to the Appliance as a user with the `tanadmin` role.
2. Enter `1-5` (Tanium Installation > Install Tanium Cloud Access Point).
3. When prompted, specify each host name from the Tanium Cloud Client edge URLs and the port that you want Tanium Clients to use to communicate with the Cloud Access Point.

```
            >>> Tanium Installation -> Install Tanium Cloud Access Point <<<

The Cloud Access Point role will be installed on this appliance.

The following settings will be used to configure the Tanium Cloud Access Point
service. Please have the provided hostnames for Tanium Client connections
and the desired listen port ready for input.

Would you like to continue? [Yes|No]: Yes

Installing Cloud Access Point Role...

Tanium Cloud Server 1: sample-zsb1

Tanium Cloud Server 2: sample-zsb2

Tanium Client Listen Port: 443
```

©2026 Tanium Inc. All Rights Reserved

> **Note:** You must include the port in the **ProxyServers** setting of Tanium Client on each endpoint.

What to do next

- Configure any existing Tanium Clients on the restricted network to connect to the Tanium Cloud Access Point. Use the Tanium Client command line interface (CLI) to configure the **ProxyServers** setting on each endpoint to the FQDN or IP address and port of the Tanium Cloud Access Point.
- When you deploy any new Tanium Clients, configure the **ProxyServers** setting to the FQDN or IP address and port of the Tanium Cloud Access Point during deployment.

For more information, see Configure proxy connections without a PAC file.

MANAGE THE CLOUD ACCESS POINT SERVICE

About this task

You can start, stop, restart, enable, and view status details for the Cloud Access Point (squid) service.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-P-S` (Tanium Operations > Manage Cloud Access Point > Service Control).
3. Use the menu to select an action to start, stop, restart, enable, or view status details for the service.
4. Follow the prompts to perform the action.

RECONFIGURE A TANIUM CLOUD ACCESS POINT

About this task

You can change the Tanium Cloud Server names and Tanium Client listening port for an existing Tanium Cloud Access Point.

1. Sign in to the Appliance as a user with the `tanadmin` role.
2. Enter `2-P-C` (Tanium Operations > Manage Cloud Access Point > Configure Cloud Access

©2026 Tanium Inc. All Rights Reserved

Point).

3. When prompted, specify each host name from the Tanium Cloud Client edge URLs and the port that you want Tanium Clients to use to communicate with the Cloud Access Point.

```
            >>> Tanium Installation -> Install Tanium Cloud Access Point <<<

The Cloud Access Point role will be installed on this appliance.

The following settings will be used to configure the Tanium Cloud Access Point
service. Please have the provided hostnames for Tanium Client connections
and the desired listen port ready for input.

Would you like to continue? [Yes|No]: Yes

Installing Cloud Access Point Role...

Tanium Cloud Server 1: sample-zsb1

Tanium Cloud Server 2: sample-zsb2

Tanium Client Listen Port: 443
```

> **Note:** You must include the port in the **ProxyServers** setting of Tanium Client on each endpoint.

REVIEW THE CLOUD ACCESS POINT LOG

About this task

The Cloud Access Point log records access information for Tanium Clients that connect to Tanium Cloud through the Cloud Access Point.

©2026 Tanium Inc. All Rights Reserved

Tip: When you view a log, you can use commands similar to ex editor commands to search for patterns (keywords).

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-1-6` (Tanium Support > Logs > Cloud Access Point).
3. Select an item to view the log, follow its growth, delete it, or export it to the /outgoing directory.

Completing and verifying the Tanium Core Platform installation on Tanium Appliances

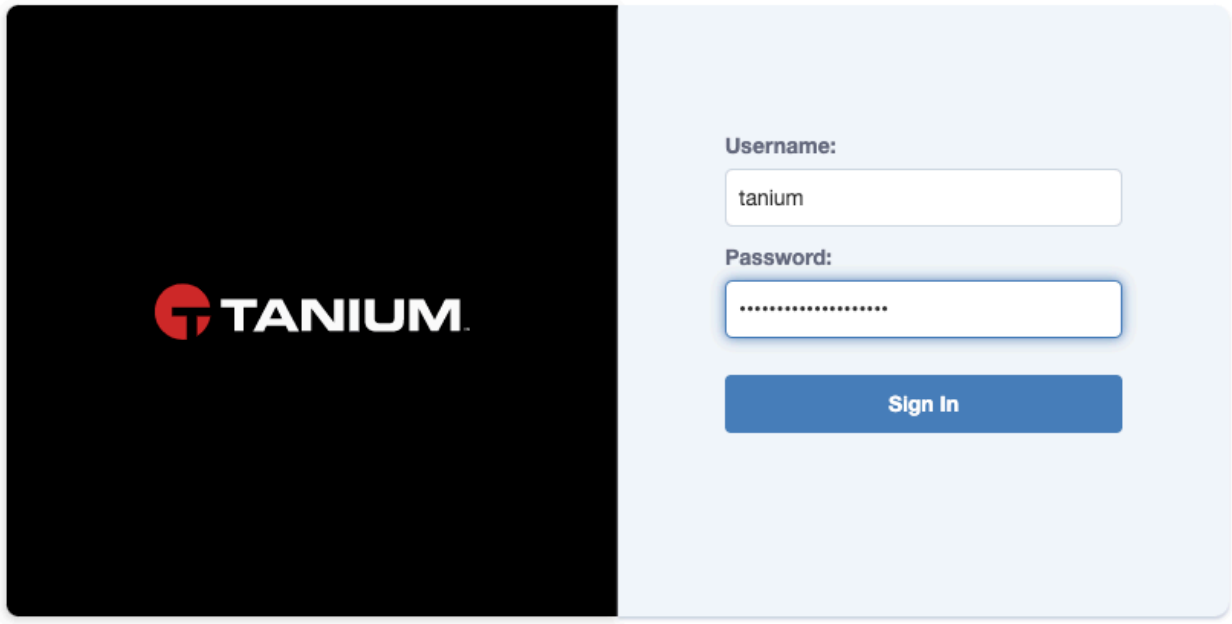
After you install the Tanium Server (standalone or redundant cluster), Tanium Module Server, and optional Tanium Zone Server, verify that the Servers are installed correctly and can communicate with all the necessary components of the Tanium Core Platform.

Sign in to Tanium Console

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.

   Figure 34. Tanium Console sign-in page

©2026 Tanium Inc. All Rights Reserved



2. Enter the user name `Tanium` and the password that you set when you installed the Tanium Server.
   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.

   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
   - Managing Tanium solutions
   - Tanium Home page

3. From the **Solutions** page, import Interact. For more information, see Managing Tanium solutions.
   The Interact workbench includes the user interface for questions and results.

©2026 Tanium Inc. All Rights Reserved

Upload the Tanium license

Use Tanium Console to upload the license file. For more information, see Managing the Tanium license.

Deploy the Tanium Client to your lab computers

Deploy one or more Tanium Clients to endpoints in your environment so that you can test basic client-server registration. If you set up multiple Tanium Server Appliances, specify the FQDNs of both Tanium Servers so the Tanium Clients use the **ServerNameList** setting to select a Tanium Server.

For comprehensive information on Client deployment options, see the Tanium Client Management User Guide.

Verify Tanium components in the deployment

VERIFY THE BASIC DEPLOYMENT

1. From the Tanium **Home** page, ask the following question to verify that endpoints with the Tanium Client respond:
   `Get Computer Name and Tanium Server Name from all machines`
2. Click **Search** and review the results grid to verify that all endpoints with the Tanium Client report successfully.
3. You can also go to the **Client Status** page to review recent Client registration details. Go to **Administration** > **Configuration** > **Client Status** to go to the page.

VERIFY THE ZONE SERVER DEPLOYMENT

1. Use the Tanium Client Management service to deploy the Tanium Client to an endpoint in your environment. In the configuration for Tanium Server, specify the Zone Server FQDN (appliance-zs.tam.local in this example).
2. In Interact, ask `Get Computer Name and Tanium Server Name from all machines` and verify that the Tanium Client on the Zone Server reports through the Tanium Zone Server.

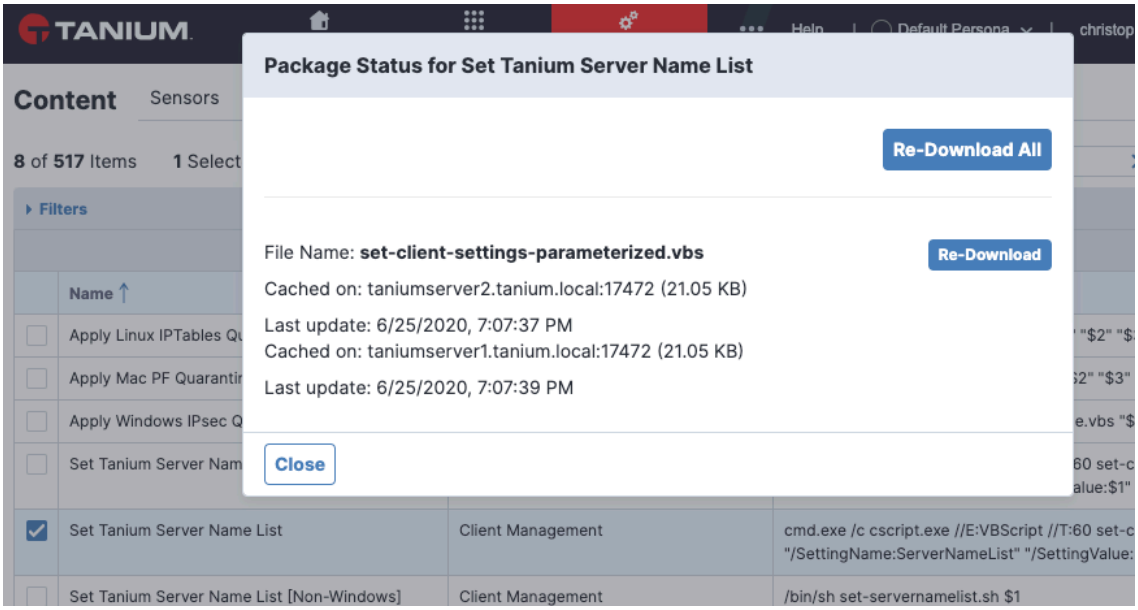
©2026 Tanium Inc. All Rights Reserved

VERIFY A TANIUM CLUSTER DEPLOYMENT

About this task

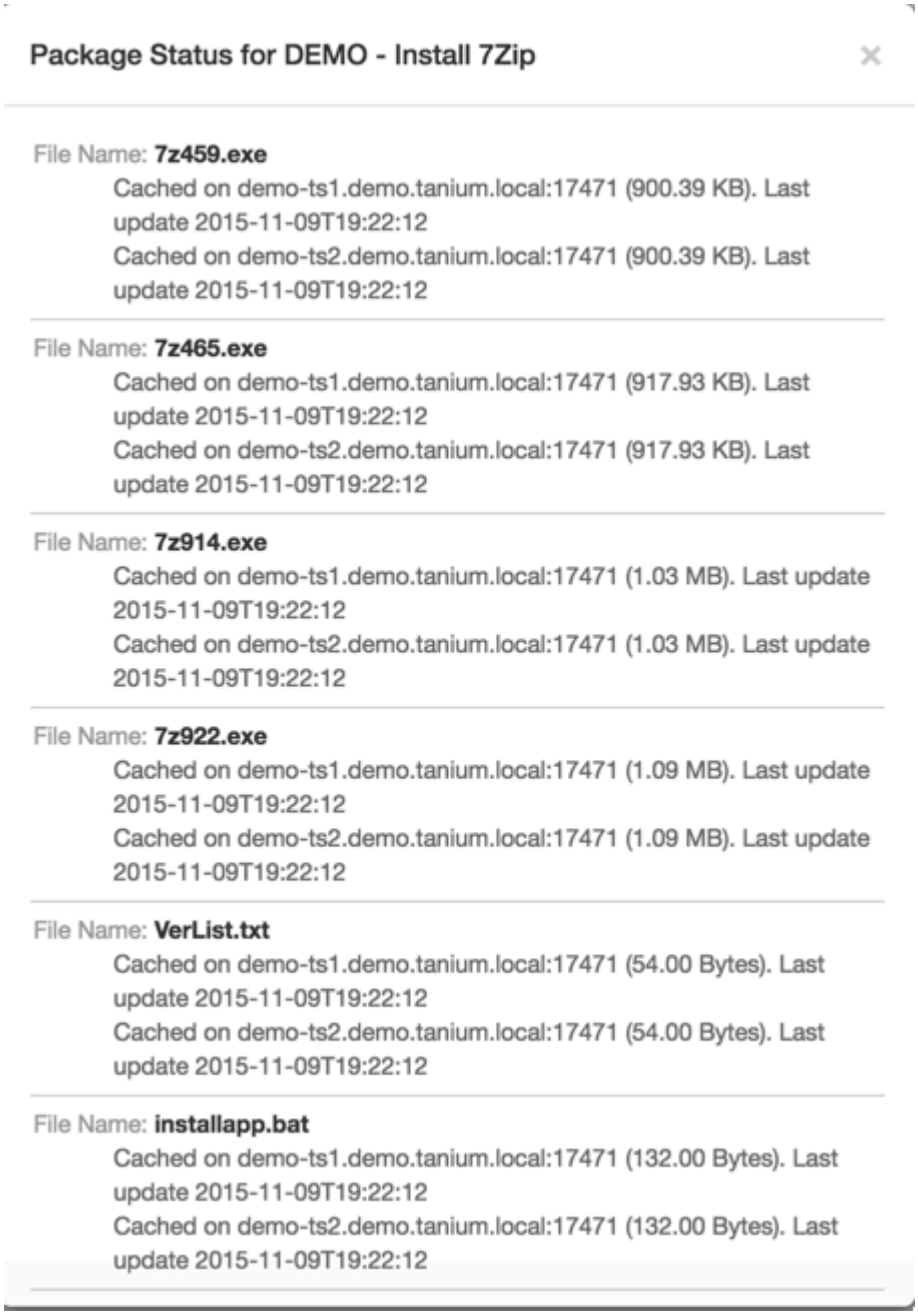
Perform the following additional verifications if you installed a Tanium Cluster through an Appliance Array on page 158.

1. In Interact, ask `Get Tanium Server Name List from all machines`. Verify that both Tanium Servers are active.
2. Verify that both Servers can download packages with URL-specified files when such a package is created or imported. The **Set Tanium Server Name** package is an example of a package with URL-specified files:
   a. Go to **Administration** > **Content** > **Packages**.
   b. Select the row for **Set Tanium Server Name List**.
   c. Click **Status** and check that the files have been downloaded and are now cached on both Servers.
   Figure 35. Verifying package cache status on both Tanium Servers



3. Create a new package and specify a locally uploaded file. After you have saved the package, wait a moment for cluster sync to occur, and then check that the files are downloaded and cached by both Servers.
   Figure 36. Verifying local package cache status

©2026 Tanium Inc. All Rights Reserved



©2026 Tanium Inc. All Rights Reserved

Working with Appliances in an air-gapped environment

If either of the following components does not have internet access, you must use an air gap installation to set up a TanOS Appliance:

- The Tanium Server
- Tanium Console

After you complete the air gap installation, you can use the **Airgap Operations** menu to configure the Tanium deployment to access Tanium content in the air-gapped environment.

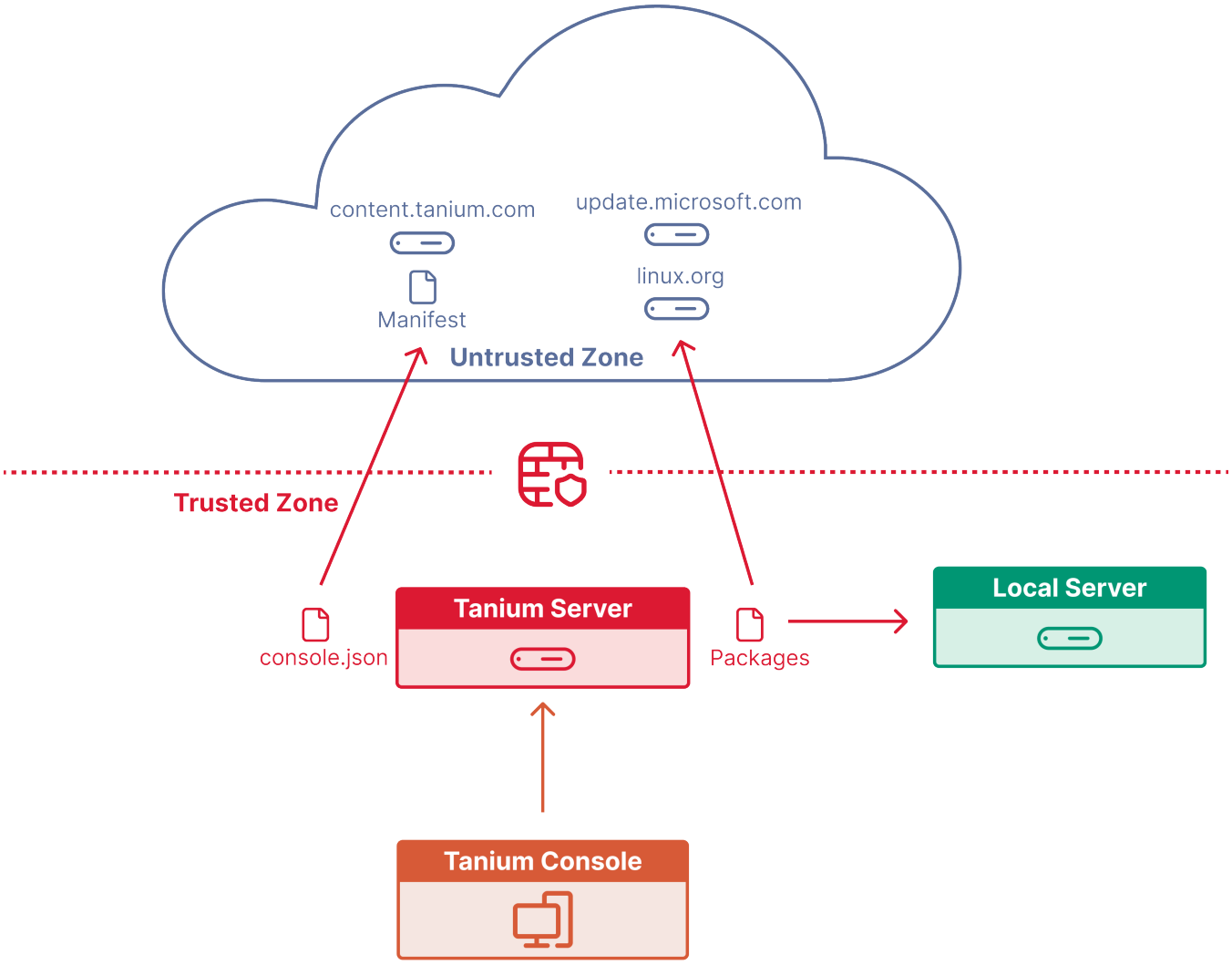
Note: Upgrades to TanOS in an air-gapped environment use the same procedures as other environments, with the exception that you must always copy upgrade files to the /incoming directory on the Appliance. For more information, see Upgrade TanOS on Tanium Appliances on page 469.

Overview

In an internet-connected Tanium deployment, the Tanium Server connects to content.tanium.com to read a manifest file that enumerates the solutions that can be imported into the deployment. This is the listing you see when you navigate to the **Solutions** page in Tanium Console (see Managing Tanium solutions). When a user performs the operation to import the solution, the solution imports from the remote location. In addition, a Tanium package might reference external files that exist on public sites or a local server.

Figure 37. Importing solutions in an internet-connected Tanium deployment

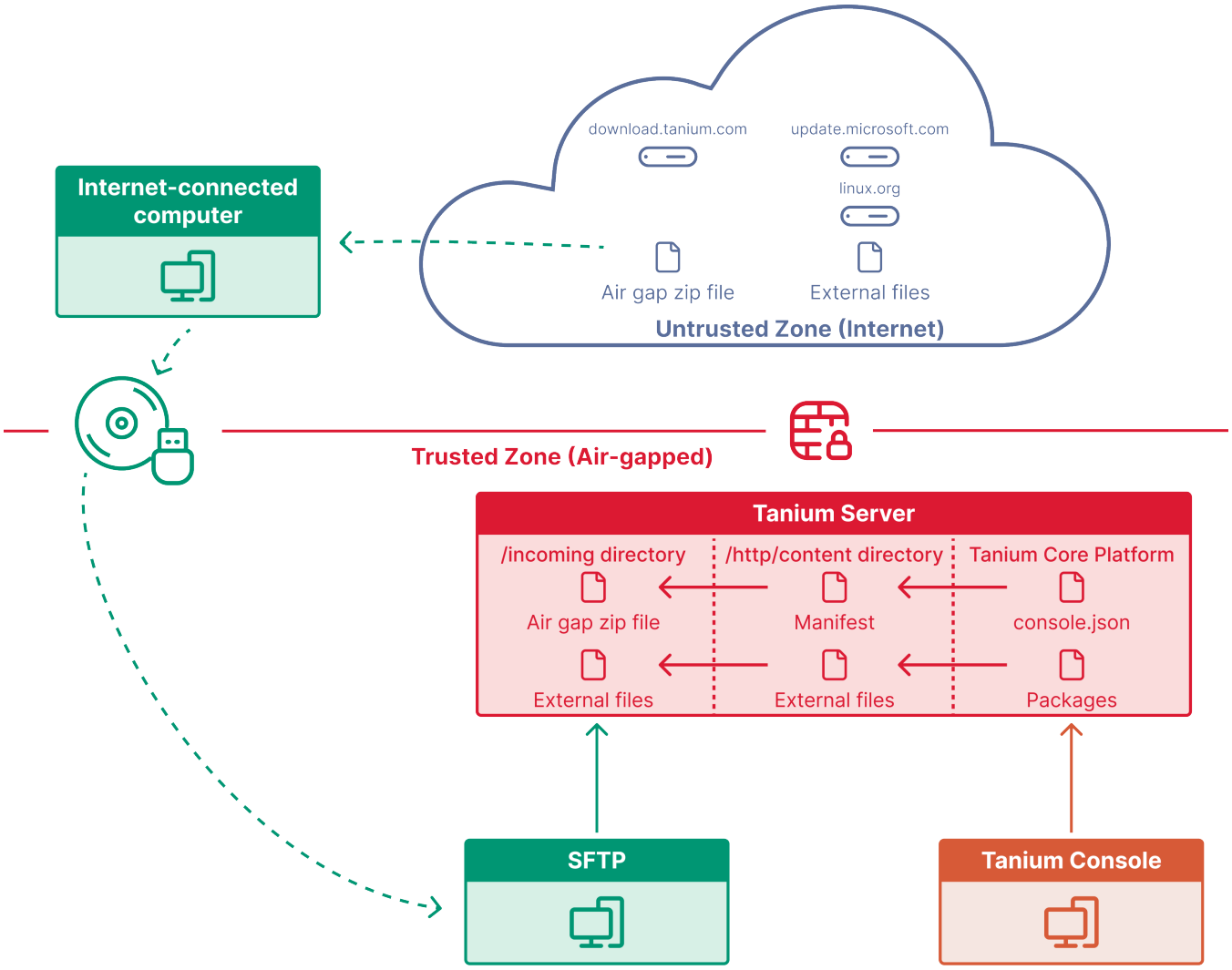
©2026 Tanium Inc. All Rights Reserved



In an air-gapped environment, the Tanium Server does not have access to the internet and cannot directly access content that is ordinarily downloaded from content.tanium.com and other internet locations. To support customer deployments in air-gapped environments, Tanium provides air gap support versions of solution modules and content packs. You must download this content from an internet-connected computer, move it to a local computer within the air-gapped environment, and upload it to the Tanium Server using SFTP. The air gap installation process installs the manifest locally on the Tanium Server. Content import is then done locally on the Tanium Server host computer, and the air gap versions of content replace references to content.tanium.com and other remote URLs with references to the local host.

Figure 38. Importing solutions in an air-gapped Tanium deployment

©2026 Tanium Inc. All Rights Reserved



Perform initial setup of an air-gapped environment

Initial setup of an air-gapped Tanium deployment includes the initial setup of the included Appliances, installation of a full update (which includes the air-gapped version of solution modules and content packs), and a few additional configuration tasks that are specific to air-gapped installations.

Before you begin

Make sure you have access to these files that you must bring into the air-gapped environment:

- Tanium license file
- TanOS physical or virtual Appliance image

©2026 Tanium Inc. All Rights Reserved

- Air gap full zip (content zip) file
    - Tanium_Airgap_X.X_X.X.X.X_YYYY-MM-DD.zip
    - Contact Tanium Support on page 510 to obtain this file.
- Content signing key utility
    - KeyUtility-X.X.X.X.zip
    - Contact Tanium Support on page 510 to obtain this file.
- Software to:
    - Connect to the Tanium Appliances through SSH.
    - Transfer files to and from the Appliance through SFTP.
    - Generate SSH keys.
- Additional module content
    - Mandatory: Default Computer Groups XML file
    - Optional, depending on modules and scenarios:
        - If necessary, air-gapped versions of modules that are more recent than those in the full ZIP package
        - THR Signals
        - Comply standards
        - Comply engines
        - OS patches
        - Tanium Client installers

Prepare a TanOS installation for an air-gapped environment

Initial configuration of an air-gapped environment is similar to that of a typical internet-connected

©2026 Tanium Inc. All Rights Reserved

environment, but you must supply a Tanium license during installation and configure the TrustedHostList setting on each Tanium Server and Module Server.

COMPLETE INITIAL SETUP

Follow the initial configuration steps relevant to your TanOS environment:

- Completing the initial setup (physical Tanium Appliance) on page 60
- Completing the initial setup (virtual Tanium Appliance) on page 93
- Completing the initial setup (cloud-based Tanium Appliance) on page 130

SUPPLY A TANIUM LICENSE

About this task

Obtain a valid license and the Tanium Core Platform installation package from Tanium Support on page 510, and upload them to the Appliance:

1. On your management computer, set up an SFTP client such as WinSCP to connect to the Appliance.
2. Use the SFTP client to copy your license file (tanium.license) and installation package (<tanium.version>_linux_server_package_8.zip) to the /incoming directory on the Appliance. TanOS uses the installation package to install the Tanium roles when you configure the Appliance Array, and it copies the license to the appropriate location during installation of the Tanium Server role.

   Important: Do not skip these steps and upload the license later directly through Tanium Console. Upload the license file manually so that when you install the Tanium Core Platform Server roles, the license gets applied automatically.

INSTALL AN APPLIANCE ARRAY AND TANIUM ROLES

Follow the steps in Installing and managing an Appliance Array on page 158.

After you install the Array and Tanium roles, you have a standard installation of Tanium. For example,

©2026 Tanium Inc. All Rights Reserved

if you sign in to Tanium Console, it tries to import Tanium Interact and some default content from content.tanium.com and then fails. To update from local files, you must convert the installation into an air-gap installation.

UPDATE THE TRUSTEDHOSTLIST SETTINGS ON EACH TANIUM SERVER

About this task

Add FQDNs and IP addresses for all Tanium Servers and Tanium Module Servers to both the TrustedHostList and the TDL TrustedHostList on each Tanium Server:

1. Sign in to the TanOS console on the Tanium Server as a user with the `tanadmin` role.
2. Enter `2`-`2`-`1` (Tanium Operations > Configuration Settings > Edit Tanium Server Settings).
3. Enter the line number of the `TrustedHostList` setting and then enter `E` (Edit line).
4. Modify the setting so that it contains the following comma-separated entries, and then press Enter:
    - The FQDN of each Tanium Server
    - The FQDN of each Module Server
    - The IP address of each Tanium Server
    - The IP address of each Module Server
    - `localhost`
    - `127.0.0.1`

    For example, a configured setting might look like the following:

    ```
    ts1.mycompany.com,ts2.mycompany.com,tms1.mycompany.com,tms2.mycompany.co
    ```

5. Enter `R`-`R`-`2` (Return to previous menu > Return to previous menu > Edit Tanium Server TDL Settings).
6. Enter the line number of the `TrustedHostList` setting, enter `E` (Edit line), and modify the setting to match the Tanium Server TrustedHostList setting you configured in step 4.

UPDATE THE TRUSTEDHOSTLIST SETTINGS ON EACH MODULE SERVER

About this task

Add FQDNs and IP addresses for all Tanium Servers and Tanium Module Servers to both the

©2026 Tanium Inc. All Rights Reserved

TrustedHostList and the TDL TrustedHostList on each Module Server:

1. Sign in to the TanOS console on the Module Server as a user with the `tanadmin` role.
2. Enter `2-2-5` (Tanium Operations > Configuration Settings > Edit Tanium Module Server Settings).
3. Add the TrustedHostList setting:
    a. Enter `A` (Add a line).
    b. For the key, enter `TrustedHostList`.
    c. For the value, enter the same setting that you configured in step 4 of Update the TrustedHostList settings on each Tanium Server on page 206.
4. Enter `R-6` (Return to previous menu > Edit Tanium Module Server TDL Settings).
5. Add the TrustedHostList setting:
    a. Enter `A` (Add a line).
    b. For the key, enter `TrustedHostList`.
    c. For the value, enter the same setting that you configured in step 4 of Update the TrustedHostList settings on each Tanium Server on page 206.

Install a full update

A full update is a ZIP package that includes the air-gapped version of solution modules, production content packs, and lab content packs.

A full update sets the Tanium Server manifest location to its own host name, instead of content.tanium.com. The update also generates the manifest.xml file. The location of all the entries in the file are set to the name of the Tanium Server, instead of content.tanium.com. Tanium publishes a full update a few times per year when Tanium Server releases occur.

In a clustered environment, the update sets the Tanium Server manifest location and content location for both Servers to the Tanium Server you are updating. Install the update only on the primary Tanium Server; the secondary Tanium Server subsequently downloads the content from the primary Tanium Server.

BEFORE YOU BEGIN

- If you are installing the full update for the first time, complete the steps in Prepare a TanOS installation for an air-gapped environment on page 204.

©2026 Tanium Inc. All Rights Reserved

- Read the release notes for the content packs and modules included in the air gap ZIP file. Make sure that you understand the changes introduced in every release in the path from the current release to the target release.
- Run a health check on page 488 on each Appliance in the environment to make sure each Appliance is in a healthy state before you perform the update.

DOWNLOAD THE ZIP FILE

1. From a computer with internet access, download the air gap ZIP file.
2. Copy the ZIP file to a location that is available to the Appliances.

INSTALL THE UPDATE

1. Use SFTP to copy the air gap ZIP file to the /incoming directory on the Tanium Server Appliance. The file name provided by Tanium must be preserved.
2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `2-C-1` (Tanium Operations > Manage Content > Install Airgap Content).
4. Enter the line number of the file that you want to install.
5. Follow the prompts to install the air gap ZIP file.

```
------------------------------------------------------


    >>> Tanium Operations -> Airgap Installer <<<

This feature is used to install a Tanium Airgap content package.

Airgap files should be placed in the incoming directory using sftp tancopy.
File names as provided by Tanium must be preserved. This installer supports
the following Airgap content file types.

* Air Gap Individual Zip     Airgapped-*-Installer.zip
* Air Gap Bundle Zip         Tanium_Airgap_*.zip
* Air Gap Bundle RPM         TaniumAirgap-*.rpm
```

©2026 Tanium Inc. All Rights Reserved

```
Air Gap Bundle files are very large and will take several minutes to install.

 Continue with installation of Tanium_Airgap_2026H2_Ux_yyyy-mm-dd.zip ? [Yes|No]: yes
 Running airgap installer
 Validating file signature
################################## [100%]
Updating / installing...
################################## [100%]

 Enter Console URI (minus protocol prefix): ts1.tam.local

 Console URI is: https://ts1.tam.local/content/manifest.xml
 Creating content signing key
 Pruning Airgap content
Nothing to prune
NO airgap content directory found
 Installing content

 Re-Apply Tanium Server ACLs
 Removing Airgap RPM

 Airgap installation complete

 Tanium Server Manifest URL changed to custom (https://ts1.tam.local/content/
manifest.xml)

 Press enter to continue
```

For the console URI, enter the public FQDN of the Server.

6. Press **Enter** to return to the **Manage Content** menu.

Result

When you install the air gap ZIP file, TanOS automatically makes the following changes:

- Sets the manifest URL and the labs manifest URL on the Tanium Servers to the URL for the Tanium Server on which you are installing the update. For more information, see Change the

air gap manifest URLs on page 223.

- Sets the `is_airgap` global setting on the Tanium Servers to `1`.
- Sets the `content_base_url` global setting on the Tanium Servers to `https://fqdn/content`, where `fqdn` is the fully qualified domain name of the Tanium Server on which you are installing the update.

Sign in to Tanium Console and let the Server complete the initial import

At this point, the Tanium installation is converted into an air gap installation.

Sign in to Tanium Console for the first time through the FQDN of the primary Tanium Server. After this step, the system automatically imports Default Content.

Note: If the initial import process fails:

- Make sure the URL you are using to access Tanium Console contains the exact same host name listed in the manifest URL configuration on the Appliance. For example, do not use the IP address to connect to the console if the manifest lists the FQDN of the Appliance.
- Make sure you did not forget to set the location of the LABS manifest. For more information, see Install a full update on page 207.

Import recommended content

1. As a test, import Interact to make sure it works.

   Important: If the import fails, check all the TrustedHostList settings, modify as needed, and then try this step again.

2. Download, sign, and import the Default Computer Groups XML file.
   An air-gapped version of the Default Computer Groups content is not available, because the content does not include sensors or packages.

©2026 Tanium Inc. All Rights Reserved

To sign the file before you import it, follow the instructions in Authenticating content files.

> **Note:** After successfully importing Default Computer Groups, it does not appear on the**Content** > **Solutions** page even though it was installed successfully.

3. Import Tanium Client Management.

> **Important:** To deploy Tanium Clients with Client Management in an air-gapped environment, you must upload Tanium Client files. For more information, see Manage versions of the Tanium Client available for deployments and upgrades.

Import content packs and modules

About this task

After you install full or individual updates, you can import the related content packs and modules into Tanium.

After you install a full update, if you want to install the modules and content that came with the update, then you can proceed to install them. If you want to use more recent versions of the modules than what shipped with the full ZIP package, see Install an individual update on page 214. To install additional updates for individual modules, see Update external files for individual modules on page 218.

1. Sign in to Tanium Console on the primary Tanium Server as a user with the Administrator reserved role, which is required to import content.
2. From the Main menu, go to the **Administration** > **Configuration** > **Solutions** page.
3. Click **Import** > **Import Files**.
4. Perform one of the following steps to select the file:
   - Drag and drop files from your file explorer.
   - Click **Browse for File**, select the file, and click **Open**.
5. Review the content to import. In most cases, when you import Tanium-produced content, select the options to merge the categories configuration and to overwrite all of the other configurations, including the designated content set.
6. Click **Begin Import**. If prompted, enter your credentials and click **OK**.

©2026 Tanium Inc. All Rights Reserved

7. Review the messages to make sure the import completes successfully, and then click **Close**.

Tip: If you encounter errors importing content, check the trusted host list configuration on all Tanium Server and Tanium Module Server Appliances to ensure the air gap Server IP address is trusted. For more information, see Configuring Appliance security on page 354 and Edit TDownloader settings on page 316.

Update an existing air gap installation

To perform updates in an air-gapped environment, you obtain and install different types of update packages, and then import the included modules and content.

Types of air gap updates

Full updates

Tanium Server releases occur a few times per year. For each Tanium Server release, Tanium publishes a ZIP package that includes the air-gapped version of solution modules, production content packs, and lab content packs. A full update is also used for initial setup of an air-gapped environment.

Individual updates

Tanium product releases occur weekly. Usually, a few solution modules or content packs are updated. If a solution module or content pack update is published, Tanium posts a ZIP file that contains the content XML and external files for the update.

Additional external files updates

External files for Tanium Comply, Tanium Deploy, Tanium Patch, and Tanium Threat Response might require updates more frequently than full or individual update releases. These files can be obtained and installed separately.

When to perform an update

CUSTOMER LAB

©2026 Tanium Inc. All Rights Reserved

Install updates at the direction of Tanium Support. Updates in the lab are completed in preparation for a rollout to production.

The following list is a typical work flow for update management:

- Install the available full update initially when you first set up the air-gapped installation of TanOS.
- Install full updates shortly after they are made available.
- Install individual updates for the solution modules and content that you support shortly after they are made available.
- Install additional external file updates regularly.

Tip: Make a habit of tracking weekly release announcements. Read the release notes to identify items included in the release that might improve the user experience and organizational objectives.

CUSTOMER PRODUCTION

Install updates only after you complete testing in the lab environment.

Before you begin

Make sure you have access to these files that you must bring into the air-gapped environment:

- The appropriate update package. Contact Tanium Support on page 510 to obtain this file.
- Content signing key utility
    - KeyUtility-X.X.X.X.zip
    - Contact Tanium Support on page 510 to obtain this file.
- Software to:
    - Connect to the Tanium Appliances through SSH.

©2026 Tanium Inc. All Rights Reserved

        - Transfer files to and from the Appliance through SFTP.
- Additional module content
        - Mandatory: Default Computer Groups XML file
        - Optional, depending on modules and scenarios:
            - If necessary, air-gapped versions of modules that are more recent than those in the full ZIP package
            - THR Signals
            - Comply standards
            - Comply engines
            - OS patches
            - Tanium Client installers

Install a full update to update an existing air-gapped installation

You can install each full update as it is released to update Tanium Core Platform Servers, modules, and content. For more information, see Install a full update on page 207.

After installing the full update, import updated content packs and modules. For more information, see Import content packs and modules on page 211.

Install an individual update

You can install each individual update as it is released to apply the latest module and content pack updates.

BEFORE YOU BEGIN

Read the release notes for the content pack or module included in the air gap installer file. Make sure that you understand the changes introduced in every release in the path from the current release to the target release.

©2026 Tanium Inc. All Rights Reserved

Note: The Tanium Server requires that content files imported into Tanium Console are signed, and the signatures verified by public keys stored on the Tanium Server. The public keys for content developed by Tanium and delivered through content.tanium.com are included with the installation.

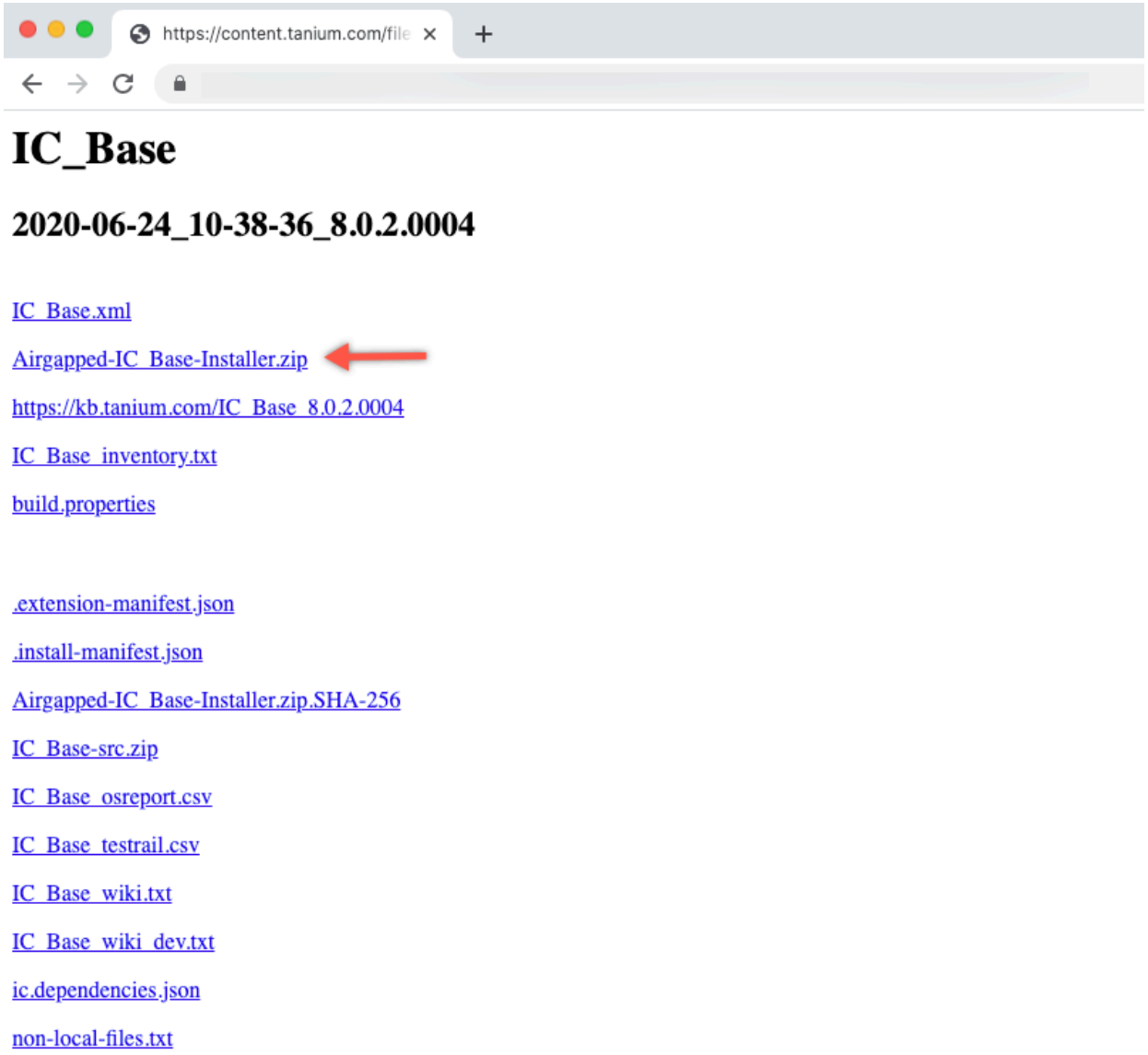
DOWNLOAD THE UPDATE FILE

About this task

Note: The installer supports both RPM and ZIP air gap files. The following instructions demonstrate an install with a ZIP file.

1. From a computer with internet access, download the air gap ZIP file.
   Figure 39. Downloading the air gap update file

©2026 Tanium Inc. All Rights Reserved



2. Copy the file to a location that is available to the Appliances.

INSTALL THE UPDATE

1. Use SFTP to copy the air gap ZIP file to the /incoming directory on the Tanium Server Appliance.
2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `2-C-1` (Tanium Operations > Manage Content > Install Airgap Content).
4. Enter the line number of the file that you want to install.
5. Follow the prompts to install the air gap ZIP file, but do not press **Enter** after the install

©2026 Tanium Inc. All Rights Reserved

completes.

```
 ------------------------------------------------------


     >>> Tanium Operations -> Airgap Installer <<<

This feature is used to install a Tanium Airgap content package.

Airgap files should be placed in the incoming directory using sftp tancopy.
File names as provided by Tanium must be preserved. This installer supports
the following Airgap content file types.

* Air Gap Individual Zip     Airgapped-*-Installer.zip
* Air Gap Bundle Zip         Tanium_Airgap_*.zip
* Air Gap Bundle RPM         TaniumAirgap-*.rpm

Air Gap Bundle files are very large and will take several minutes to install.

   #  File name
   1: Airgapped-IC_Base-Installer.zip

Please select file by line number (enter to exit): 1

 Continue with installation of Airgapped-IC_Base-Installer.zip ? [Yes|No]: yes
 Running airgap installer
 Validating file signature

 Airgap installer script completed.

 The XML file for install of the Airgap content can be downloaded
 from the following URL
     https://ts1.tam.local:8443/content/IC_Base/2020-06-24_10-38-36_1.2.3.4567/
IC_Base.xml

 Re-Apply Tanium Server ACLs
 Removing Airgap installer files
```

©2026 Tanium Inc. All Rights Reserved

```
Airgap installation complete


Press enter to continue
```

6. Copy the URL that appears for the XML file.
7. Press Enter to go to the **Manage Content** menu.
8. Download the XML file to your local computer. For example, you can open the URL in a web browser and save the file to your computer. Depending on the configuration, you might need to change the FQDN of the Server to the IP address.
9. Use keyutility.exe to generate a cryptographic key pair and use it to sign the XML file. For more information, see Enable import of user-created content in an Appliance deployment on page 325.

```
C:\Tanium\KeyUtility.exe signcontent TaniumLab.pvk IC_Base.xml
Signature Created.


C:\Tanium>
```

WHAT TO DO NEXT

After installing the individual update, import updated content packs and modules. For more information, see Import content packs and modules on page 211.

Update external files for individual modules

External files for Tanium Comply, Tanium Deploy, Tanium Patch, and Tanium Threat Response might require updates more frequently than full or individual update releases. These files can be obtained and installed separately.

UPDATE THE TANIUM COMPLY ENGINE PACKAGES

In an internet-connected environment, Tanium Comply automatically connects to content.tanium.com to download updates for key components used in endpoint scans. In an air-gapped environment, you must update these components manually through Tanium Console. For complete instructions, see Configure Comply for an air-gapped environment.

©2026 Tanium Inc. All Rights Reserved

CONFIGURE AN ALTERNATE LOCATION FOR THE PREDEFINED PACKAGE GALLERY IN TANIUM DEPLOY

The Predefined Package Gallery in Tanium Deploy provides a collection of common software packages that are hosted at content.tanium.com. These packages are preconfigured and ready to deploy to endpoints. By default, the Tanium Server in an air-gapped environment cannot directly access Deploy Gallery package definitions. You can configure an alternative Gallery location so that a Tanium Server in an air-gapped environment can still download the Gallery. For complete instructions, see Configure an alternate location for the Predefined Package Gallery.

UPDATE TANIUM PATCH FILES

About this task

When the Tanium Server is in an air-gapped environment, the Server cannot download patches from the internet. You must configure Patch to install patches from an alternate file location in the Patch settings for Windows endpoints.

To update Tanium Patch files, follow the steps in Downloading patches in an air-gapped environment, but perform the following steps after you download the remote package files:

1. Rename the ZIP file to content-results.zip and copy to a location that is available to the Tanium Server Appliance.
2. Use SFTP to copy the ZIP file to the /incoming directory on the Tanium Server Appliance.
3. Sign in to the TanOS console as a user with the `tanadmin` role.
4. Enter `2-C-4` (Tanium Operations > Manage Content > Manage Web Server Content).
5. Enter `1` to go to the **Tanium Web Server Content Installer** menu and follow the prompts to install the content-results.zip file.
6. Verify the configuration as instructed in the Patch documentation.

INSTALL OR UPDATE TANIUM THREAT RESPONSE SIGNALS

In an internet-connected environment, Tanium Threat Response automatically connects to content.tanium.com to download updates for Tanium Signals. In an air-gapped environment, you must update the Tanium Signals files manually.

©2026 Tanium Inc. All Rights Reserved

Download the Tanium Signals file

1. From a computer with internet access, go to the content download URL and download the DetectSignalsV4.zip file.
2. Use a ZIP program to add another ZIP layer. The extra layer is required to import the ZIP file to the Tanium Server Appliance. For example:
    a. Go to **Administration** > **Configuration** > **Solutions**, search for **Distribute Tanium Standard Utilities**, and download 7za.exe.
    b. Create an archive named content-DetectSignalsV4.zip that includes the file DetectSignalsV4.zip.

```
cmd> 7za a content-DetectSignalsV4.zip DetectSignalsV4.zip
7-Zip (a) 18.05 (x86) : Copyright (c) 1999-2018 Igor Pavlov : 2018-04-30

Scanning the drive:
1 file, 13644 bytes (14 KiB)
Creating archive: content-DetectSignalsV4.zip

Add new data to archive: 1 file, 13644 bytes (14 KiB)

Files read from disk: 1
Archive size: 13735 bytes (14 KiB)

Everything is Ok
```

> **Note:** The file must be named content-DetectSignalsV4.zip. TanOS expects the prefix content-.

    c. Copy the file to a location that is available to the Tanium Server Appliance.

Install or update the Tanium Signals file

1. Install the content on the Tanium Server Appliance:
    a. Use SFTP to copy the Tanium Signals ZIP file to the /incoming directory on the Tanium Server Appliance.
    b. Sign in to the TanOS console as a user with the `tanadmin` role.
    c. Enter `2`-`C`-`4` (Tanium Operations > Manage Content > Manage Web Server Content).

©2026 Tanium Inc. All Rights Reserved

d. Enter `1` to go to the **Tanium Web Server Content Installer** menu and follow the prompts to install the Tanium Signals ZIP file.

2. Specify the location on the Appliance for the Tanium Signal's manifest URL setting.
   a. In a web browser, sign in to Tanium Console, and go to **Modules** > **Threat Response**.
   b. From the Threat Response menu, go to **Intel** > **Sources**.
   c. Edit the **Tanium Signals** source. If the source does not exist, click **New Source** and complete the configuration.
   d. For the manifest URL, specify the URL for the zip file that you installed in the previous steps. The URL has the following form: https://<TS FQDN>/content/files/DetectSignalsV4.zip. The file name of the zip file is case sensitive.
   e. Save the configuration.
   f. From the **Sources** page in Threat Response, make sure the **Intel Count** populates with items in the **Tanium Signals** row.

> **Note:** It might take up to the time configured for the **Subscription Interval** in the Tanium Signals source (60 minutes by default) for the intel to update from the Tanium Signals file.

> **Tip:**
>
> If the Tanium Signals file does not install or update as expected, try the following:
>
> - If the Server deployment uses self-signed certificates, select the **Ignore SSL** option.
> - If you encounter errors importing content, check the trusted host list configuration on both the Tanium Server and Tanium Module Server to ensure the air gap Server IP address is trusted.
> - On the Module Server, check the Threat Response log (TanOS menu path `3-2-<Threat Response menu number>-2`). Export the log and search for the string signals.downloadSignalsZip to see the logs related to the download operation.

View the air gap usage report

©2026 Tanium Inc. All Rights Reserved

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2`-`C` (Tanium Operations > Manage Content).
3. Enter `2` to go to the **Airgap Content Usage** report.

```
-----------------------------------------------------


  >>> Tanium Operations -> Airgap Content Usage <<<


   UsedKB Solution                   Solution_ID            Sol_Vers Action
   ====== ========                   ===========            ======== ======
  149068K Connect                    99-200-0008         1.2.3.4567 Delete


Delete will prune 150M bytes from 1 solutions
Delete will preserve 0 bytes from 0 solutions


 Press enter to continue
```

View the air gap installation log

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3`-`1`-`1`-`9` (Tanium Support Menu > Tanium Log Files > TanOS Appliance > Airgap Log).
3. Enter `V` to view the current log file, or enter the line number of a previous log file if the relevant log entries have been rotated out of the current log file.

Prune unused air gap content

About this task

You can prune solutions that have been upgraded to a later version and content that was included in an update but that has not been imported.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2`-`C`-`3` (Tanium Operations > Manage Content > Prune Airgap Content).
3. Follow the prompts to prune the air gap content.

©2026 Tanium Inc. All Rights Reserved

Manage web server content

TanOS has menus to support installation and management of air-gapped web server content.

Before you begin

Use SFTP to copy the air gap content files to the /incoming directory on the Appliance. The file names must be in the content-*.zip format. The web content installs to the <Tanium Server>/http/content/ files directory.

Install content

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-C-4-1` (Tanium Operations > Manage Content > Manage Web Server Content > Tanium Web Server Content Installer).
3. Follow the prompts to install the content.

Delete content by list

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-C-4` (Tanium Operations > Manage Content > Manage Web Server Content).
3. Enter `3` and follow the prompts to delete the content.

Change the air gap manifest URLs

About this task

The *manifest* and *lab manifest* refer to the URL Tanium Console uses to locate solution modules and content packs available for download and use. The default locations point to content.tanium.com. In an air-gapped deployment, the manifest URLs are different. Use the TanOS menu to change them to the air gap content location. If a lab license is in use, you must change both the manifest and lab manifest locations.

©2026 Tanium Inc. All Rights Reserved

Note: When you install a full update, TanOS automatically changes the manifest URL and the labs manifest URL to the URL for the air gap Server IP address, and it is only necessary to follow these steps if the manifest is not located on the Tanium Server. For more information, see Install a full update on page 207.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-C-B` (Tanium Operations > Manage Content > Manifest URL Change).
3. Use the menu to change the manifest URL.

©2026 Tanium Inc. All Rights Reserved

Managing TanOS users

Use TanOS to manage TanOS system user accounts, which allow users to access the TanOS console on the Tanium Appliance. These user accounts include the predefined TanOS users `tanadmin` and `tancopy`. The **TanOS User Management** menu (`C-U`) contains options to manage these users. TanOS users are separate from Tanium users who can access the Tanium™ Console. TanOS users are also local to each Appliance; users are not shared across Appliances.

Tip:

- You can optionally use your enterprise LDAP server to manage TanOS authentication. For more information about using LDAP for TanOS users, see Configure LDAP authentication for TanOS system users on page 252.
- For more information about the predefined TanOS user accounts, see Completing the initial setup (physical Tanium Appliance) on page 60, Completing the initial setup (virtual Tanium Appliance) on page 93, or Completing the initial setup (cloud-based Tanium Appliance) on page 130.
- Users with the `tanadmin` role can also manage Tanium Console users for demo or testing purposes, using the local authentication service in TanOS. For more information, see Configure the local authentication service for Tanium Console users on page 294.

The subsequent topics in this section provide details about managing TanOS users.

Change the password for the current TanOS user

About this task

©2026 Tanium Inc. All Rights Reserved

Note:

- Use these steps to reset the password for the TanOS user who is currently signed in. On TanOS 1.7.3 or later, the password reset prompt appears if the user password expires. To reset the password for another TanOS user, see Enable or disable a system user account on page 238.
- You can change your password from within TanOS only if you are signed in as a locally administered TanOS user. The option to change your password is not available if you are signed in as an LDAP user.

Tip: When your password expires within 14 days, TanOS displays a **Password Expiration Warning** each time you sign in to the console, showing the number of days remaining.

1. Sign in to the TanOS console.
2. Enter `P` and follow the prompts to change the password.

```
          >>> User Administration -> TanOS -> tanadmin -> Change Password <<<


Preparing to change the password for tanadmin

The password policy requires meeting these rules:
 - Minimum of 10 characters long
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
 - At least 1 other character
 - Must not match any of recent 4 passwords
 - Must not be based on a dictionary word
 - Must not contain part of the username
```

©2026 Tanium Inc. All Rights Reserved

```
 Please enter password (will not be displayed):
Password score: 55 out of 100 (strong)
 Please enter password again:


 The password change was successful.


 Press enter to continue
```

Result

After the password changes, you are signed out.

Manage SSH keys for TanOS users

The installation process generates a public/private ECDSA SSH key pair for the `tanadmin` user. Use the **User Administration** menus to perform the following functions:

- Regenerate the key pair.
- Generate keys for the other TanOS special users.
- Add authorized keys to support inbound user connections.
- View the public key so you can copy and paste it into other Appliance configurations.

Tip:

You can use the ssh-copy-id command in OpenSSH to add an SSH public key from your local host to any TanOS user with the `tanadmin` role on the Tanium Appliance. For example:

```
ssh-copy-id -i public_key_file user@appliance
```

Before you begin

- You must have an SSH client to sign in to the TanOS console and an SFTP client such as WinSCP to copy files to and from the Appliance.

©2026 Tanium Inc. All Rights Reserved

- You must have an SSH key generator such as ssh-keygen to generate keys for the user.

Generate keys

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter the line number of the user account that you want to manage.

```
   >>> User Administration -> TanOS -> MyUser <<<

Username:         MyUser
Account Enabled:  Yes
Authentication:   SSH Key or Password
Password Expires: 2027-01-14 00:00:00 UTC
SSH Lockout:      No (0)
Multifactor:      Not configured
Protected:        No

Notes:
  * This user account cannot be deleted

         A: Manage SSH Authorized Keys
         P: Manage SSH Key Pair
         L: Reset SSH Lockout
         C: Change/Enable Password (Randomized)
         N: Disable Password Access
         M: Multifactor Authentication

         E: Enable Account
         D: Disable Account
         T: Manage Account Protection
         X: Delete User

         F: Edit known hosts file

         R: Return to previous menu  RR: Return to top
```

©2026 Tanium Inc. All Rights Reserved

```
-----------------------------------------------------
```

4. Enter `P` to manage the SSH key pair.

```
           >>> User Administration -> TanOS -> tanadmin -> Key Pair <<<

Account: tanadmin
No SSH keys found for user tanadmin. Please create key pair first

         G: Generate ssh key pair

         R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

5. Enter `G` to generate a public/private key pair.

```
           >>> User Administration -> Manage -> User -> SSH <<<

       Account: tanadmin
       Action:  Generate SSH Keys
       No .ssh directory for user tanadmin found - creating and securing it
       keygen process finished successful
       Finished generating keys for tanuser

       Press enter to continue
```

Add authorized keys

1. Use an SSH key generator such as ssh-keygen to generate a public/private key pair. Note:
    - Specify an ECDSA key (such as ssh-keygen -t ecdsa) or an RSA key with at least 2048 bits.
    - Specify a passphrase that is easy to remember.
    - Save the private key to a location that you can access when you set up your SFTP client.

©2026 Tanium Inc. All Rights Reserved

2. Copy all of the text in the public key file to the clipboard. If you use ssh-keygen, copy the contents of the .pub file that you created.

   Important: In an SSH key exchange, the keys must match exactly.

3. Sign in to the TanOS console as a user with the `tanadmin` role.
4. Enter `C-U` (User Administration > TanOS User Management).
5. Enter the line number for the `tancopy` user to go to the user administration menu for this user.

```
          >>> User Administration -> TanOS -> tancopy <<<

Username:         tancopy
Account Enabled:  Yes
Authentication:   SSH Key Only
Password Expires: N/A
SSH Lockout:      No (0)
Multifactor:      Not configured
Protected:        No

Notes:
  * This user account cannot be deleted
  * This user account cannot have a password
  * This user account cannot use multifactor

        A: Manage SSH Authorized Keys
        P: Manage SSH Key Pair
        L: Reset SSH Lockout
        C: [DISABLED] Change Password
        N: [DISABLED] Disable Password Access
        M: [DISABLED] Multifactor Authentication

        E: Enable Account
        D: Disable Account
        T: [DISABLED] Manage Account Protection
```

©2026 Tanium Inc. All Rights Reserved

```
          X: [DISABLED] Delete User

          F: Edit known hosts file

          R: Return to previous menu  RR: Return to top

-------------------------------------------------------
```

6. Enter `A` (Authorized Keys).
7. Enter `A` and follow the prompts to add the contents of the public key generated in Step 1.

```
            >>> User Administration -> TanOS -> tancopy -> Authorized Keys -> Add
<<<

Account: tancopy
Please paste the public key and press enter:
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA1ClmgkMrbbxB7jND/Y4/
Giupck35xAuGNKfZWqVLM5F0CNXuTScf6v2z
MDxW5TO5tm/U8P9sqh19RDEzTn2RayXzsoZmXyB8abCCpHG4+03Zv05RHiX4i5QomAMBnbZejdA9/
fGTxO1rPo1rdtTq
Z+KCgzbEhHLWUD44+If5RtG+U4kgyzlYsyjgwhfho+BrRY6e7QYBsXVbuBQ9ROGV6PCTB80jXZVAKrAbsTQ1D
VkpuBue
mftv7vOn3b8MKzJ/IY/
LLL1tIgpSGvgvjr2mOJJ+JoZF2XnPVUFmYiDSCkPAzhCyFHILHfOVAfws9n1G6p3fwILqNhvB
oPeaCFaApQ== rsa-key-20200123
 Validating input
 Adding key to authorized keys after validation
 Finished adding authorized keys for tancopy



 Press enter to continue
```

View public keys

1. Sign in to the TanOS console as a user with the `tanadmin` role.

©2026 Tanium Inc. All Rights Reserved

2. Enter `C-U` (User Administration > TanOS User Management).
3. Enter the line number for the `tancopy` user to go to the user administration menu for this user.

```
          >>> User Administration -> TanOS -> tancopy <<<

Username:         tancopy
Account Enabled:  Yes
Authentication:   SSH Key Only
Password Expires: N/A
SSH Lockout:      No (0)
Multifactor:      Not configured
Protected:        No

Notes:
  * This user account cannot be deleted
  * This user account cannot have a password
  * This user account cannot use multifactor

         A: Manage SSH Authorized Keys
         P: Manage SSH Key Pair
         L: Reset SSH Lockout
         C: [DISABLED] Change Password
         N: [DISABLED] Disable Password Access
         M: [DISABLED] Multifactor Authentication

         E: Enable Account
         D: Disable Account
         T: [DISABLED] Manage Account Protection
         X: [DISABLED] Delete User

         F: Edit known hosts file

         R: Return to previous menu  RR: Return to top
```

©2026 Tanium Inc. All Rights Reserved

```
-------------------------------------------------------
```

4. Enter `P` to go to the **Key Pair** menu to view the public key.

```
           >>> User Administration -> TanOS -> tancopy -> Key Pair <<<

 Account: tancopy
 SSH Public Key for user tancopy:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDZCvC+
nF93Nqmv2lrlUJoDTrwCnpJkcm5Er5ywNFNem5MJZZd0esToJTpY43gb8XppB5JP7SdHVJk2M3Nm0DP+xapjA
L35Cs/
bdX48kwDc0R1m4Qc7/4aqQQkBcF/
95Z3OrpD1EVW0bwF3KlsX9vEojQ3sO4PjNBQJxTepLI+iU1IQzu44OvUx4A7Jpk
ZSZBL+t1KdyNl75vZ8vCfcG4KqdHqwVds1XIplaW77LcN8+G4kYUthlpWVrSLvWtKdZztGG+Kasj0y/
VSqhlP7AHorU
mDzuV4z4AOB7+UI8lcx8B5FPEverfNhPAXkemOrqnkd0oolLKeoEdiaakqANJHboI5gFJPJe1v1ZLDr47wXYq
nGBccm
1Tp/MQyMvtf98HKesBk4qXOgvBICLs44/pLVqXou/
3c+sI+uCj1aNDlTjmpvG1TBLAuuCUiu3SkUi3zcZxlvqRD/YgVq/
w9yGryG7pamAmBkYVXYqIx0JHfjxhO6er+pAZOpXPV8B4p3ie7lhzOJO+g7JRHwOEo+yLOyCU9yWwfvs6dsP7
RqKS4EL
asTLFnaKFT4D+sxZnEIxJPpy/gO8tQdfm69fz6RXh8GkWt/2CyyQ4DWVXt5AXLt6YbMFk0nNVbnOVih1/
g6yHsTcxQKP
zVDO/6fQ/tb33kbj5M5KhC1YI3pXxjMYZN1aQ

          G: Generate ssh key pair

          R: Return to previous menu  RR: Return to top

-------------------------------------------------------
```

Configure TanOS system users

You can create TanOS users that have `tanadmin` or `tanuser` permissions. The system users with the `tanadmin` role have access to all menus. System users with the `tanuser` role have access to status menus.

©2026 Tanium Inc. All Rights Reserved

You can also protect a user with the `tanadmin` role, which gives the account the same properties as the `tanadmin` special user and allows you optionally to unprotect and disable the `tanadmin` special user.

Best Practice: Create more than one privileged user with the `tanadmin` role in case you forget the password for the built-in `tanadmin` user or your main protected user.

Tip: You can optionally use your enterprise LDAP server to manage TanOS authentication. For more information, see Configure LDAP authentication for TanOS system users on page 252.

Note: TanOS includes a `tanldap` user account, which appears in the TanOS User Management menu, and a `tancomm` user account, which does not appear in the TanOS User Management menu. These user accounts are used internally to facilitate communication among Tanium Appliances. Do not sign in to either of these user accounts.

Add a system user

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter `A` and follow the prompts to add a system user.

```
           >>> User Administration -> System Users -> Add System User <<<

Adding a system user requires first name, last name, user name and user role.

Attention:
TanUser Role:  Monitor/Check the status of the appliance, no changes are allowed
TanAdmin Role: Full administrative role to manage the appliance

A temporary password will be generated and the new user is required to change
```

©2026 Tanium Inc. All Rights Reserved

```
their password upon first login!

The password policy requires meeting these rules:
- Minimum of 10 characters long
- At least 1 upper case character
- At least 1 lower case character
- At least 1 numeric character
- At least 1 other character
- Must not match any of recent 4 passwords
- Must not be based on a dictionary word
- Must not contain part of the username

Please enter first name: John
Please enter last name: Doe
Please enter desired user name (max 30 chars): john.doe
Which role should be assigned to john.doe?

1: TanUser (Monitoring)
2: TanAdmin (Administrative)

Please select: 2

The temporary password for john.doe is: proudbrownwildfowl

Adding local user john doe ...
Successfully added user john doe (username: john.doe) with role tanadmin.

Press enter to continue
```

Disable password access

About this task

When you disable password access for a user, the user can only sign in through SSH using the configured SSH private key. You can disable password access for any user except the `tanadmin` special user.

©2026 Tanium Inc. All Rights Reserved

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter the line number of the user that you want to manage.
4. Enter `N` and follow the prompts to disable password access for the user.

```
-----------------------------------------------------

 >>> User Administration -> TanOS -> john.doe <<<

Username:         john.doe
Account Enabled:  Yes
Authentication:   SSH Key or Password
Password Expires: 2027-01-14 00:00:00 UTC
SSH Lockout:      No (0)
Multifactor:      Not configured
Protected:        No

         A: Manage SSH Authorized Keys
         P: Manage SSH Key Pair
         L: Reset SSH Lockout
         C: Change/Enable Password (Randomized)
         N: Disable Password Access
         M: Multifactor Authentication

         E: Enable Account
         D: Disable Account
         T: [DISABLED] Manage Account Protection
         X: Delete User

         F: Edit known hosts file

         R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

©2026 Tanium Inc. All Rights Reserved

```
TanOS Version:        1.9.1

Please select: N

Disabling the password for an account means that
1. The user can only log in via SSH (not a serial console or equivalent)
2. The user can only log in using the configured SSH private key
3. The user will not need to change their password periodically

This operation can be reversed by setting a password again.

Do you want to disable password access for john.doe? [Yes|No]: yes
Successfully removed the password.

Press enter to continue
```

Reset a user password or enable password access

About this task

Password access is enabled by default. If you disable password access for a user and want to re-enable password access or if you need to reset a user password, perform the following steps.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter the line number of the user that you want to manage.
4. Enter `C` to enable password access or reset the password for the selected user.
    - If you enable the password for the current user, enter a password.
    - If you enable password access for another user, TanOS generates a random password.

```
           >>> User Administration -> System Users -> Reset Password  <<<

A temporary password will be generate and the user is required to change
```

©2026 Tanium Inc. All Rights Reserved

```
their password upon login!

The password policy requires meeting these rules:
 - Minimum of 10 characters long
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
 - At least 1 other character
 - Must not match any of recent 4 passwords
 - Must not be based on a dictionary word
 - Must not contain part of the username

The temporary password for tanuser is: temporarypassword
Successfully reset password for user tanuser.

Resetting ssh lockout for user tanuser ...
Successfully reset any lockout for user tanuser.

Press enter to continue
```

Enable or disable a system user account

About this task

You can temporarily disable a system user account without deleting it.

Important: You cannot disable a protected user. You can disable the `tanadmin` special user only if another protected user exists and you unprotect the `tanadmin` special user. See Protect or unprotect a user account with the tanadmin role on page 239.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter the line number of the user that you want to manage.
4. Enter `D` to disable the user account, or enter `E` to enable an account that was previously disabled.

©2026 Tanium Inc. All Rights Reserved

Protect or unprotect a user account with the tanadmin role

About this task

You can protect a user with the `tanadmin` role, which gives the account the same properties as the `tanadmin` special user and applies the following conditions:

- The user account cannot be disabled or deleted.
- The user can protect or unprotect other user accounts.
- The user can sign in to the appliance console if the account is locked for SSH sign-in.
- On a physical Tanium Appliance or virtual Tanium Appliance, you cannot disable password access for the account.
- On cloud-based Tanium Appliance, you cannot delete all SSH keys for the account.

By default, the built-in `tanadmin` special user is protected. If you have at least one other protected user, you can optionally unprotect and disable the `tanadmin` special user.

> **Important:** You must have at least one protected user at all times. You cannot unprotect the last protected user.

1. Sign in to the TanOS console as the `tanadmin` special user or another user that has the `tanadmin` role and is already protected.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter the line number of the user that you want to manage.
4. Enter `T` to toggle protection of the user.

Delete a system user

About this task

©2026 Tanium Inc. All Rights Reserved

Important: You cannot delete the `tanadmin` or `tancopy` special users or a protected user. See Protect or unprotect a user account with the tanadmin role on page 239.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter the line number of the user that you want to manage.
4. Enter `X` and confirm to delete the user.

Edit known hosts

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter the line number of the user that you want to manage.

```
   >>> User Administration -> TanOS -> MyUser <<<


Username:         MyUser
Account Enabled:  Yes
Authentication:   SSH Key or Password
Password Expires: 2027-01-14 00:00:00 UTC
SSH Lockout:      No (0)
Multifactor:      Not configured
Protected:        No

Notes:
  * This user account cannot be deleted


         A: Manage SSH Authorized Keys
         P: Manage SSH Key Pair
         L: Reset SSH Lockout
         C: Change/Enable Password (Randomized)
         N: Disable Password Access
         M: Multifactor Authentication
```

©2026 Tanium Inc. All Rights Reserved

```
          E: Enable Account
          D: Disable Account
          T: Manage Account Protection
          X: Delete User

          F: Edit known hosts file

          R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

4. Enter `F` to edit the known hosts file. You can delete existing fingerprints from the file, or you can scan a remote host to automatically add fingerprints.
    - To delete a fingerprint, enter a line number and confirm the deletion.
    - To scan a remote host and automatically add all discovered fingerprints, enter `S` and follow the prompts.

```
 -----------------------------------------------------
  >>> User Administration -> TanOS -> tanadmin <<<

  Username: tanadmin
  File:     /home/tanadmin/.ssh/known_hosts

  Action:   Select line number to delete
  #: Host Key                    Host
  1: AAAAE2VjZHN...qsTE1rkC2o=   192.168.15.253
  2: AAAAC3NzaC1...kHgZ1TUXjDW   192.168.15.253

  S: Scan remote host keys

  R: Return to previous menu  RR: Return to top

 -----------------------------------------------------
Please select: s

  Enter the remote host to scan: 192.168.15.115
```

©2026 Tanium Inc. All Rights Reserved

```
Found additional host keys for 192.168.15.115

192.168.15.115 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzd...
192.168.15.115 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIL2FCJQS3...
192.168.15.115 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDLtuGBN...

Do you want to add these entries to known_hosts? [Yes|No]: y

Done adding 3 entries
Press enter to continue
```

View history of sign in attempts

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`I` (User Administration > Recent Login Information).
3. Use options `A`, `B`, and `C` to view the history of sign in attempts.

Configure global authentication requirements and global multifactor authentication

You can configure the Appliance to use multifactor authentication (MFA) to validate TanOS user accounts on each sign-in through an SSH connection. You can optionally require users to authenticate with a password, an SSH key, a time-based one-time password (TOTP), or any combination of these.

The following sign-in behaviors apply to each combination of password and key authentication:

- Both password and key configured as optional: If a user has an SSH key configured and supplies it during sign-in, no password is required. If the key is not supplied or not configured, the user must enter a password.
- Both password and key configured as required: Each user must have an SSH key configured and must supply both the password and key to sign in.
- **Password configured as required and key configured as optional:** Each user must supply a

©2026 Tanium Inc. All Rights Reserved

password to sign in, regardless of whether an SSH key is configured or supplied.

- **Password configured as optional and key configured as required:** Each user must have an SSH key configured and must supply the key to sign in. No password is required or requested during sign-in.

You can configure multifactor authentication as a global setting or for individual users, and you can exempt selected accounts from global multifactor authentication settings. To configure MFA settings for individual users, see Configure individual multifactor authentication on page 245.

Multifactor authentication settings determine whether users must also supply a TOTP during sign-in, along with a password and key as required. If you disable multifactor authentication globally, a user is required to supply a TOTP during sign-in only if that user has multifactor authentication configured individually. If you enable multifactor authentication globally, each users must configure multifactor authentication and supply a TOTP to sign-in.



Note:

- Tanium Appliances use Google Authenticator for multifactor authentication.
- You cannot enable global multifactor authentication if an LDAP connection is configured to manage TanOS system users. For more information, see Configure LDAP authentication for TanOS system users on page 252.

Require key authentication globally

About this task

Perform the following steps to require all users who sign-in through SSH to use an authorized key configured in their profiles.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C-M-K` (User Administration > Multifactor Global Settings > Require key authentication).
3. Enter `E` and follow the prompts to enable global key authentication.

©2026 Tanium Inc. All Rights Reserved

Make key authentication optional globally

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`M`-`K` (User Administration > Multifactor Global Settings > Require key authentication).
3. Enter `D` and follow the prompts to disable global key authentication.

Require password authentication globally

About this task

Perform the following steps to require all users who sign-in through SSH to input a password, even when a user provides an SSH key.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`M`-`P` (User Administration > Multifactor Global Settings > Require password authentication).
3. Enter `E` and follow the prompts to enable global key authentication.

Make password authentication optional globally

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`M`-`P` (User Administration > Multifactor Global Settings > Require password authentication).
3. Enter `D` and follow the prompts to disable global key authentication.

Enable global multifactor authentication

About this task

Best Practice: If you want to exempt specific accounts from requiring multifactor authentication, you should exempt the accounts before you enable global multifactor authentication to minimize disruption. To exempt a user from multifactor authentication, see Exempt a user from global multifactor requirements on page 245.

©2026 Tanium Inc. All Rights Reserved

Important: To make sure an admin user can still sign in through SSH after you enable multifactor authentication, you must either exempt at least one admin user or configure multifactor authentication individually for at least one admin user before you enable multifactor authentication globally. For more information, see Exempt a user from global multifactor requirements on page 245 or Configure Google Authenticator for a user on page 247.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`M`-`M` (User Administration > Multifactor Global Settings > Require Multifactor Authentication).
3. Enter `E` and follow the prompts to enable global multifactor authentication.

Disable global multifactor authentication

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`M`-`M` (User Administration > Multifactor Global Settings > Require Multifactor Authentication).
3. Enter `D` and follow the prompts to disable global multifactor authentication.

Configure individual multifactor authentication

In addition to global multifactor authentication, you can configure multifactor authentication for individual users or exempt individual users from global multifactor authentication requirements.

Tip: To manage global multifactor authentication settings, see Configure global authentication requirements and global multifactor authentication on page 242.

Exempt a user from global multifactor requirements

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter the line number of the user that you want to edit.

©2026 Tanium Inc. All Rights Reserved

```
   >>> User Administration -> TanOS -> MyUser <<<

Username:         MyUser
Account Enabled:  Yes
Authentication:   SSH Key or Password
Password Expires: 2027-01-14 00:00:00 UTC
SSH Lockout:      No (0)
Multifactor:      Not configured
Protected:        No

Notes:
  * This user account cannot be deleted

         A: Manage SSH Authorized Keys
         P: Manage SSH Key Pair
         L: Reset SSH Lockout
         C: Change/Enable Password (Randomized)
         N: Disable Password Access
         M: Multifactor Authentication

         E: Enable Account
         D: Disable Account
         T: Manage Account Protection
         X: Delete User

         F: Edit known hosts file

         R: Return to previous menu  RR: Return to top

-------------------------------------------------------
```

4. Enter `M` to manage the multifactor authentication settings for the user.

```
-------------------------------------------------------

       >>> User -> tanadmin -> Multifactor <<<
```

```
Current Configuration: Not configured

         E: Exempt User from Multifactor Requirement
         G: Configure Google Authenticator for User

         V: View Configuration

         X: Reset User Multifactor Settings

         R: Return to previous menu  RR: Return to top

--------------------------------------------------------
```

5. Enter `E` and follow the prompts to exempt the user from all multifactor authentication requirements.

```
  >>> User -> tanadmin -> Multifactor Exemption <<<

This will disable the requirement for multifactor for this user, even if
multifactor is globally enforced.

Would you like to continue? [Yes|No]: yes

Resetting MFA user configuration and disabling MFA requirement for user
Adding user tanuser to group tanmfano

Press enter to continue
```


Tip: To remove the exemption for the user, perform the steps in Reset user multifactor settings on page 251.

Configure Google Authenticator for a user

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).

©2026 Tanium Inc. All Rights Reserved

3. Enter the line number of the user that you want to edit.

```
   >>> User Administration -> TanOS -> MyUser <<<

Username:         MyUser
Account Enabled:  Yes
Authentication:   SSH Key or Password
Password Expires: 2027-01-14 00:00:00 UTC
SSH Lockout:      No (0)
Multifactor:      Not configured
Protected:        No

Notes:
  * This user account cannot be deleted

         A: Manage SSH Authorized Keys
         P: Manage SSH Key Pair
         L: Reset SSH Lockout
         C: Change/Enable Password (Randomized)
         N: Disable Password Access
         M: Multifactor Authentication

         E: Enable Account
         D: Disable Account
         T: Manage Account Protection
         X: Delete User

         F: Edit known hosts file

         R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

4. Enter `M` to manage the multifactor authentication settings for the user.

```
-----------------------------------------------------

       >>> User -> tanadmin -> Multifactor <<<
```

©2026 Tanium Inc. All Rights Reserved

```
Current Configuration: Not configured

         E: Exempt User from Multifactor Requirement
         G: Configure Google Authenticator for User

         V: View Configuration

         X: Reset User Multifactor Settings

         R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

5. Enter `G` and follow the prompts to configure Google Authenticator for the user.

View user multifactor settings

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter the line number of the user that you want to edit.

```
   >>> User Administration -> TanOS -> MyUser <<<

Username:         MyUser
Account Enabled:  Yes
Authentication:   SSH Key or Password
Password Expires: 2027-01-14 00:00:00 UTC
SSH Lockout:      No (0)
Multifactor:      Not configured
Protected:        No

Notes:
  * This user account cannot be deleted

         A: Manage SSH Authorized Keys
```

```
         P: Manage SSH Key Pair
         L: Reset SSH Lockout
         C: Change/Enable Password (Randomized)
         N: Disable Password Access
         M: Multifactor Authentication

         E: Enable Account
         D: Disable Account
         T: Manage Account Protection
         X: Delete User

         F: Edit known hosts file

         R: Return to previous menu  RR: Return to top

-------------------------------------------------------
```

4. Enter `M` to manage the multifactor authentication settings for the user.

```
-------------------------------------------------------

       >>> User -> tanadmin -> Multifactor <<<

Current Configuration: Not configured

         E: Exempt User from Multifactor Requirement
         G: Configure Google Authenticator for User

         V: View Configuration

         X: Reset User Multifactor Settings

         R: Return to previous menu  RR: Return to top

-------------------------------------------------------
```

5. Enter `V` to show the multifactor authentication settings for the user.

©2026 Tanium Inc. All Rights Reserved

Reset user multifactor settings

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`U` (User Administration > TanOS User Management).
3. Enter the line number of the user that you want to edit.

```
   >>> User Administration -> TanOS -> MyUser <<<


Username:         MyUser
Account Enabled:  Yes
Authentication:   SSH Key or Password
Password Expires: 2027-01-14 00:00:00 UTC
SSH Lockout:      No (0)
Multifactor:      Not configured
Protected:        No

Notes:
  * This user account cannot be deleted

         A: Manage SSH Authorized Keys
         P: Manage SSH Key Pair
         L: Reset SSH Lockout
         C: Change/Enable Password (Randomized)
         N: Disable Password Access
         M: Multifactor Authentication

         E: Enable Account
         D: Disable Account
         T: Manage Account Protection
         X: Delete User

         F: Edit known hosts file

         R: Return to previous menu  RR: Return to top

-------------------------------------------------------
```

©2026 Tanium Inc. All Rights Reserved

4. Enter `M` to manage the multifactor authentication settings for the user.

```
-----------------------------------------------------


       >>> User -> tanadmin -> Multifactor <<<

Current Configuration: Not configured


         E: Exempt User from Multifactor Requirement
         G: Configure Google Authenticator for User


         V: View Configuration


         X: Reset User Multifactor Settings


         R: Return to previous menu  RR: Return to top


-----------------------------------------------------
```

5. Enter `X` and follow the prompts to reset the multifactor authentication settings for the user.

Configure LDAP authentication for TanOS system users

You can optionally configure an LDAP connection to use Active Directory or another directory service to manage TanOS system users.

©2026 Tanium Inc. All Rights Reserved

Note:

- You cannot delete the `tanadmin` and `tancopy` special users. These user accounts are always administered locally within TanOS. Even if an LDAP query returns either of these user names, the locally administered user and associated password takes precedence.
- This LDAP configuration applies only for authentication in the TanOS console. For information about using LDAP for Tanium users, see Integrating with LDAP servers.
- TanOS requires TLS encryption using StartTLS for communication with the LDAP server, and the standard port is 389. 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.
- If you configure an LDAP connection to manage TanOS system users, you cannot enable global multifactor authentication. For more information, see Configure global authentication requirements and global multifactor authentication on page 242.

Manage the authentication certificate for the LDAP server

TanOS requires TLS encryption using StartTLS for communication with the LDAP server. You must import the LDAP server root certificate authority (CA) certificate. The certificate must be in PEM format. On the Appliance, you have the option to paste the contents of the LDAP server root CA certificate or import the file.

©2026 Tanium Inc. All Rights Reserved

Note:

- If you import a new certificate after you have already configured LDAP server connection settings, you must re-enter the bind credentials for the connection. For more information, see Configure specific LDAP connection settings on page 257.
- Secure certificates for Server and Client systems are required. The certificates have a minimum bit size of 2048 for RSA and 256 for ECDSA. To check key sizes, use OpenSSL from a CLI. If your Tanium license includes Tanium Certificate Manager, see View short keys for the steps to check the key sizes in your environment.

OPTION 1: PASTE THE LDAP SERVER ROOT CA CERTIFICATE CONTENTS

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`A`-`M` (User Administration > AD/LDAP TanOS Authentication > Manage AD/LDAP Certificate).
3. Enter `P` and follow the prompts to paste the contents of the LDAP server root CA certificate file.

```
------------------------------------------------------


>>> User Management -> AD/LDAP TanOS Authentication -> Paste Certificate <<<


Please paste the certificate text (Empty line to end):
-----BEGIN CERTIFICATE-----
MIIEYzCCAsugAwIBAgIQHIaS1rg5zQdeFajAwRMjdjANBgkqhkiG9w0BAQsFADCB
jTEeMBwGA1UEChMVbWtjZXJ0IGRldmVsb3BtZW50IENBMTEwLwYDVQQLDChtYXR0
LmphcnZpc0BNTEMwMlpXNUZDTUQ2VCAoTWF0dCBKYXJ2aXMpMTgwNgYDVQQDDC9t
a2NlcnQgbWF0dC5qYXJ2aXNATUxDMDJaVzVGQ01ENlQgKE1hdHQgSmFydmlzKTAe
Fw0yMjA4MjUxNjQyMjlaFw0yNDExMjUxNzQyMjlaMFwxJzAlBgNVBAoTHm1rY2Vy
dCBkZXZlbG9wbWVudCBjZXJ0aWZpY2F0ZTExMC8GA1UECwwobWF0dC5qYXJ2aXNA
TUxDMDJaVzVGQ01ENlQgKE1hdHQgSmFydmlzKTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAM3mTuqiIk5b8GI7M0JUsYA/4eucvCpC6eOAhLA6MkL5rsFf
ZYg7hi7wLnxZWB7uU8/44XExA2Ez4rDb3HDUVcv8rZXbKtwk0pQdol/KY77X9Cfw
wR6UeucVizR3UbmDKfwG24ktlFxlsR4Uy/oLgwyiT/PiUSuB4qMY0NaljAG4wTZu
```

©2026 Tanium Inc. All Rights Reserved

```
KYPX5mh29zxMi9oOkInqJH6QqgX72mYglpExtMHC0LRaacJPP1WjI8E1uSiBknYE
NBpRTP2y4yWe7e7PnrWzEz/7nMOE/UrCWcdy8/Iapd3asHSinGrdcV/jRkU7Sr9s
VvctWpQbMClol4Gah860Ilk0dckluLV+UFrA+EsCAwEAAaNvMG0wDgYDVR0PAQH/
BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMB8GA1UdIwQYMBaAFL/3vApgNNHk
pDLfc+FAGkg+VbacMCUGA1UdEQQeMByCC2xvY2FsZG9tYWlugg0qLmxvY2FsZG9t
YWluMA0GCSqGSIb3DQEBCwUAA4IBgQBgxYa7sEeQZKaYxsemoig+l34BA+fxieO4
k4OpmPcyfEAqbCtDVCTwJ5bFeF4LjwYhHddwq9qSvuD6NWJhR4lO2JahGFZPIakS
VarVMBxm8ktn4XKxoFuSf5YSwFD4QjusWlVBXFokjdHVInLLoSkiBBKMonlDbiZw
zXxVR0GaOMgRLJfoVz9hmOZpWPhkOxfSwTdyLJgeqtSf237laZhXyFRFmBM/F0Zd
upitvpc9zpcjdRVFC5rO0YVWmBKtSr9vemOIZJtBYrTC1EuOvAbJPiMg2EXNZt9H
My2vKMLrQ4La7vsM3Er9w02qKNtWXrLIvx65P81anVUhRKmLBsMtQgoIOFi5uk8t
OkOdTcFUlJbVP5vGa9ZQSnopZw1jYF6IpKkKHpA0WMWFez5peQ8ZdRt7IgY/q1CE
cDUcl9LAwQkeZ9g5B0uZ6VX7tP5oafLqChptskp3xDR/IfduX7dOuSCQNYbPAtlb
lKgJjqSTaM4vmsWOPhlkoLmqLh4IyAk=
-----END CERTIFICATE-----

Validating input

Certificate successfully installed

 Press enter to continue

-------------------------------------------------------
```

OPTION 2: IMPORT THE LDAP SERVER ROOT CA CERTIFICATE FILE

1. Use SFTP to copy the certificate file to the /incoming directory of the Tanium Server Appliance.
2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `C`-`A`-`M` (User Administration > AD/LDAP TanOS Authentication > Manage AD/LDAP Certificate).
4. Enter `I` and follow the prompts to import the LDAP server root CA certificate file.

MANAGE THE IMPORTED LDAP SERVER ROOT CA CERTIFICATE

©2026 Tanium Inc. All Rights Reserved

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`A` (User Administration > AD/LDAP TanOS Authentication).
3. Enter `M` to go to the **Manage AD/LDAP Certificate** menu and view the certificate information. Use the menu options to manage the certificate.

Configure the LDAP server connection settings

Best Practice: Import the LDAP server root CA certificate before you configure the LDAP server connection settings. Though you can complete the configuration without the certificate, TanOS cannot connect to the LDAP server during the process to validate the users or groups that you enter for `tanadmin` and `tanuser` role mappings.

COMPLETE THE WALK-THROUGH CONFIGURATION

About this task

The walk-through configuration provides a series of prompts that help you complete the necessary settings for an LDAP server connection. The prompts provide contextual information for each setting. For a reference of the settings that you configure during the walk-through configuration, see Configure specific LDAP connection settings on page 257.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`A` (User Administration > AD/LDAP TanOS Authentication).
3. Enter `W` to go to the **Walkthrough Configuration** screen. Follow the prompts to configure the connection to the LDAP server.
   After you complete the configuration, the full **AD/LDAP TanOS Authentication** menu becomes available.

```
------------------------------------------------------


>>> User Management -> AD/LDAP TanOS Authentication <<<


            Certificate: Installed
          Configuration: Valid (Online)
```

©2026 Tanium Inc. All Rights Reserved

```
          M: Manage AD/LDAP Certificate
          C: Configure AD/LDAP TanOS Authentication
          W: Walkthrough Configuration

          S: Detailed Status
          V: Verify AD/LDAP User or Group
          T: Troubleshooting

          E: Export configuration to SFTP outgoing
          I: Import configuration from SFTP incoming

          X: Reset ALL AD/LDAP TanOS Auth Settings

          R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

CONFIGURE SPECIFIC LDAP CONNECTION SETTINGS

About this task

Use the **Configure AD/LDAP TanOS Authentication** menu to change specific LDAP connection settings.



Best Practice: For the initial configuration, use the walk-through configuration. Use this menu to configure specific settings that you need to change after the initial configuration is complete. For more information, see Complete the walk-through configuration on page 256.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C-A-C` (User Administration > AD/LDAP TanOS Authentication > Configure AD/LDAP TanOS Authentication).
3. Use the menu options to modify the following settings as necessary:

©2026 Tanium Inc. All Rights Reserved

LDAP connection settings for TanOS authentication

Setting	Menu Key	Description
Enable	`E`	Specifies whether LDAP authentication is enabled for authenticating TanOS system users. For more information, see Enable or disable LDAP authentication on page 265 .
Domain	`D`	The domain by which the system and logs refer to the LDAP configuration. This setting does not affect the connection to the LDAP server.
Host	`H`	The host name of the LDAP server **Note:** • TanOS requires TLS encryption for communication with the LDAP server. The host name configured for this setting must match the common name or subject alternative name in the TLS certificate presented by the LDAP server. An IP address is not usually not valid. • If you change the host name in an existing configuration, you must re-enter the bind credentials for the connection. (Enter `C` from the **Configure** menu.)
Port	`P`	The port on which to connect to the LDAP server **Tip:** This is typically port 389. **Note:** If you change the port number in an existing configuration, you must re-enter the bind credentials for the connection. (Enter `C` from the **Configure** menu.)
Bind Credentials	`C`	The user name used to sign in to and query the LDAP server in a format accepted by the server, and the password for the user name

©2026 Tanium Inc. All Rights Reserved

Setting	Menu Key	Description
		Tip: The following user name formats are commonly used, depending on the configuration of your Active Directory or LDAP server: • User principal name (UPN): An email-style user name, such as `user@domain.name` • Distinguised name (DN): A string of LDAP attributes that identify the user, such as `CN=User Name, OU=Department, DC=domain, DC=com`
Base Search DN	`B`	The base DN from which TanOS queries the directory
Schema	`S`	The schema used by the LDAP server. TanOS supports Active Directory, RFC2307, RFC2307bis, Red Hat Identity Manager (IdM), and FreeIPA.
Referrals	`Q`	Specifies whether TanOS allows the LDAP server to refer the query to other connected LDAP servers when you have multiple LDAP servers in your organization  **Important:** • Referrals can significantly increase the time required to process a query. • TanOS does not always allow a user returned from a referral to sign on, depending on the configuration of the directory.
SSH Public Key Attribute	`K`	The LDAP attribute that contains the SSH public key for each user  **Important:** The user that is specified for the **Bind Credentials** setting must have read access to this attribute.

©2026 Tanium Inc. All Rights Reserved

Setting	Menu Key	Description
		Tip: This attribute is commonly `sshPublicKey` .
Users Filter	`U`	The LDAP search filter to use to limit the users that the LDAP server returns for the query. Leave this setting blank to return all users under the base search DN.  **Note:** Most LDAP servers do not support using wildcard characters or nested groups with the `MemberOf` attribute in a filter.
Groups Filter	`G`	The LDAP search filter to use to limit the groups that the LDAP server returns for the query. Leave this setting blank to return all groups under the base search DN.

TanOS Roles Mapping	`M`	The LDAP users or groups that map to the `tanadmin` and `tanuser` roles.
		Enter `A` to go to the **tanadmin Mappings** menu and manage the users or groups that map to the `tanadmin` role. Users in these groups have access to all TanOS menus.
		`----------`
		`>>> User Management -> AD/LDAP TanOS Auth -> tanadmin Mappings <<<`
		`1: Administrators (Group)`
		`2: TanOS Admins (Group)`
		`A: Add Mapping`
		`I: Manually Input Mapping`
		`X: Remove ALL tanadmin Mappings`
		`R: Return to previous menu RR: Return to top`
		`----------`
		Enter `U` to go to the **tanuser Mappings** menu and manage the users or groups that map to the `tanuser` role. Users in these groups have access to TanOS status menus.
		`----------`

©2026 Tanium Inc. All Rights Reserved

Setting	Menu Key	Description

		<pre>>>> User Management -> AD/LDAP TanOS Auth -> tanuser Mappings <<<
		
		1: TanOS Users (Group)
		
		A: Add Mapping
		I: Manually Input Mapping
		X: Remove ALL tanuser Mappings
		
		R: Return to previous menu RR: Return to top
		
		----------</pre> 	
		Within either mappings menu, enter `A` to add a mapping. If TanOS can successfully connect to the LDAP server, it displays a searchable list of users or groups; type to filter the list or use the arrow keys to select an entry. If TanOS cannot connect to the LDAP server or no users or groups are found, you are prompted to manually enter the mapping. Enter `I` to bypass the searchable list and manually input a mapping at any time.
		
		Note:
		
		• Avoid assigning users in the directory to both a group that is mapped to the `tanadmin` role and a group that is mapped to the `tanuser` role. If a user is assigned both roles, the user can perform most administrative tasks in TanOS, but permissions might be unpredictable. You can review users with conflicting mappings in the **Detailed Status** report. For more information, see View the LDAP connection status and query results on page 262.
		
		• You cannot delete the `tanadmin` and `tancopy` special users. These user accounts are always administered locally within TanOS. Even if an LDAP query returns either of these user names, the locally administered user and associated password takes precedence.

©2026 Tanium Inc. All Rights Reserved

4. Enter `V` to validate the updated configuration.

   Note: This option validates that the required settings are configured, but it does not verify the connection to the LDAP server. If TanOS successfully connects to the server, `Configuration: Valid (Online)` appears in the **AD/LDAP TanOS Authentication** menu after you apply the configuration. The **Detailed Status** report displays additional information and any errors that occur during the query. For more information, see View the LDAP connection status and query results on page 262.

5. Enter `A` to apply the updated configuration.

View the LDAP connection status and query results

About this task

The **Detailed Status** report displays the following information:

- Users and groups returned from the LDAP query
- Users that map to the `tanadmin` and `tanuser` roles
- Any connection errors or errors that the query returns

Note: This report is available only after you have configured a connection to an LDAP server.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C-A` (User Administration > AD/LDAP TanOS Authentication).
3. Enter `S` to display the **Detailed Status** report.

```
Viewing AD/LDAP TanOS Authentication Status, press 'q' to exit



System Security Services Daemon (sssd)
--------------------------------------
Online status: Online
```

©2026 Tanium Inc. All Rights Reserved

```
Active servers:
LDAP: dc01.localdomain

Discovered LDAP servers:
- dc01.localdomain

Object Counts
-------------
Visible users: 4
Visible groups: 2

Users with tanadmin: 1
Users with tanuser: 1
Users with conflicting mappings: 0

Visible Users
-------------
Administrator
Guest
tanos.domain.admin
tanos.domain.user

Visible Groups
--------------
TanOS Admins
TanOS Users

Users With Privileges Based on Mappings
---------------------------------------
User                      Role
====                      ====
tanos.domain.user               tanuser
tanos.domain.admin               tanadmin
(END)
```

Verify that the LDAP query returns a specific user

About this task

> **Note:** This menu is available only after you have configured a connection to an LDAP server.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`A`-`V` (User Administration > AD/LDAP TanOS Authentication > Verify User/Group).
3. Enter `U` to verify a user.
4. Follow the prompts to enter a user name to verify.

Verify that the LDAP query returns a specific group

About this task

> **Note:** This menu is available only after you have configured a connection to an LDAP server.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`A`-`V` (User Administration > AD/LDAP TanOS Authentication > Verify User/Group).
3. Enter `G` to verify a group.
4. Follow the prompts to enter a group name to verify.

Export the LDAP configuration for use on another TanOS Appliance

About this task

> **Note:** This menu is available only after you have configured a connection to an LDAP server.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`A` (User Administration > AD/LDAP TanOS Authentication).
3. Enter `E` to export the LDAP configuration.

©2026 Tanium Inc. All Rights Reserved

The exported configuration is stored as ldapauth.conf in the /outgoing directory.

Import an LDAP configuration that was exported from another TanOS Appliance

1. Use SFTP to copy the ldapauth.conf file to the /incoming directory of the TanOS Appliance where you want to import the configuration.
2. Sign in to the TanOS console on the TanOS Appliance where you want to import the configuration as a user with the `tanadmin` role.
3. Enter `C`-`A` (User Administration > AD/LDAP TanOS Authentication).
4. Enter `I` to import the LDAP configuration.

Enable or disable LDAP authentication

About this task

After you complete the configuration for an LDAP connection and TanOS successfully connects to the Active Directory or LDAP server, LDAP authentication is automatically enabled for the Appliance. You can disable or re-enable LDAP authentication with the configuration still in place.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`A`-`C`-`E` (User Administration > AD/LDAP TanOS Authentication > Configure AD/LDAP TanOS Authentication > Enable/Disable).
3. Enter `D` to disable LDAP authentication, or enter `E` to enable LDAP authentication.

   Note: If you disable LDAP authentication, TanOS might close sessions for any users who are signed on with user names authenticated with LDAP.

©2026 Tanium Inc. All Rights Reserved

Managing the Tanium Core Platform on TanOS

The subsequent topics in this section provide information about management of Tanium services, configuration settings, managing certificate and public key files, and managing Tanium Console users.

Secure Tanium Console, API, and Module Server access on Tanium Appliances

The subsequent topics in this section provide information about certificates and keys, CA-issued Tanium Server SOAP certificates, installing a custom certificate, and optionally enabling HTTP Strict Transport Security for Tanium Console access.

Overview of certificates and keys

About this task

Tanium user and module operations require connections to the Tanium Servers, Module Server, and Tanium module services. The Tanium Core Platform uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) certificates and keys to secure connections to the Tanium Server and Module Server (illustrated in Figure 2 on page 270). For example, when you use Tanium™ Patch to deploy patches to endpoints, the Tanium Core Platform establishes connections in the following order:

1. User system (browser or CLI) to the Tanium Server (Tanium Console or API)
2. Tanium Server to Tanium Module Server
3. Module Server to Patch service
4. Patch service to Tanium Server
   The Tanium Server and Module Server installers generate self-signed certificates. You can replace the self-signed certificates on Tanium Servers with certificates issued by a commercial certificate authority (CA) or your enterprise CA.

©2026 Tanium Inc. All Rights Reserved

Best Practice: To facilitate troubleshooting, use the self-signed certificates during initial installation and replace them with CA-issued certificates later. This practice enables you to separate potential installation issues from TLS connection issues. Using a CA-issued certificate is highly recommended for Tanium Console and API access on the Tanium Server.

Note: Tanium Console and API access require user authentication through sign-in credentials, but not for securing the TLS connection.
To troubleshoot Console and API access issues, see Authentication log on page 519.

For more information about the Tanium™ Protocol that secures communication among the Tanium Servers, Zone Server, Zone Server Hub, and Tanium Clients, see Securing Tanium Server, Zone Server, and Tanium Client access on page 288. To manage the keys that the Tanium Protocol uses, see Managing Tanium keys.

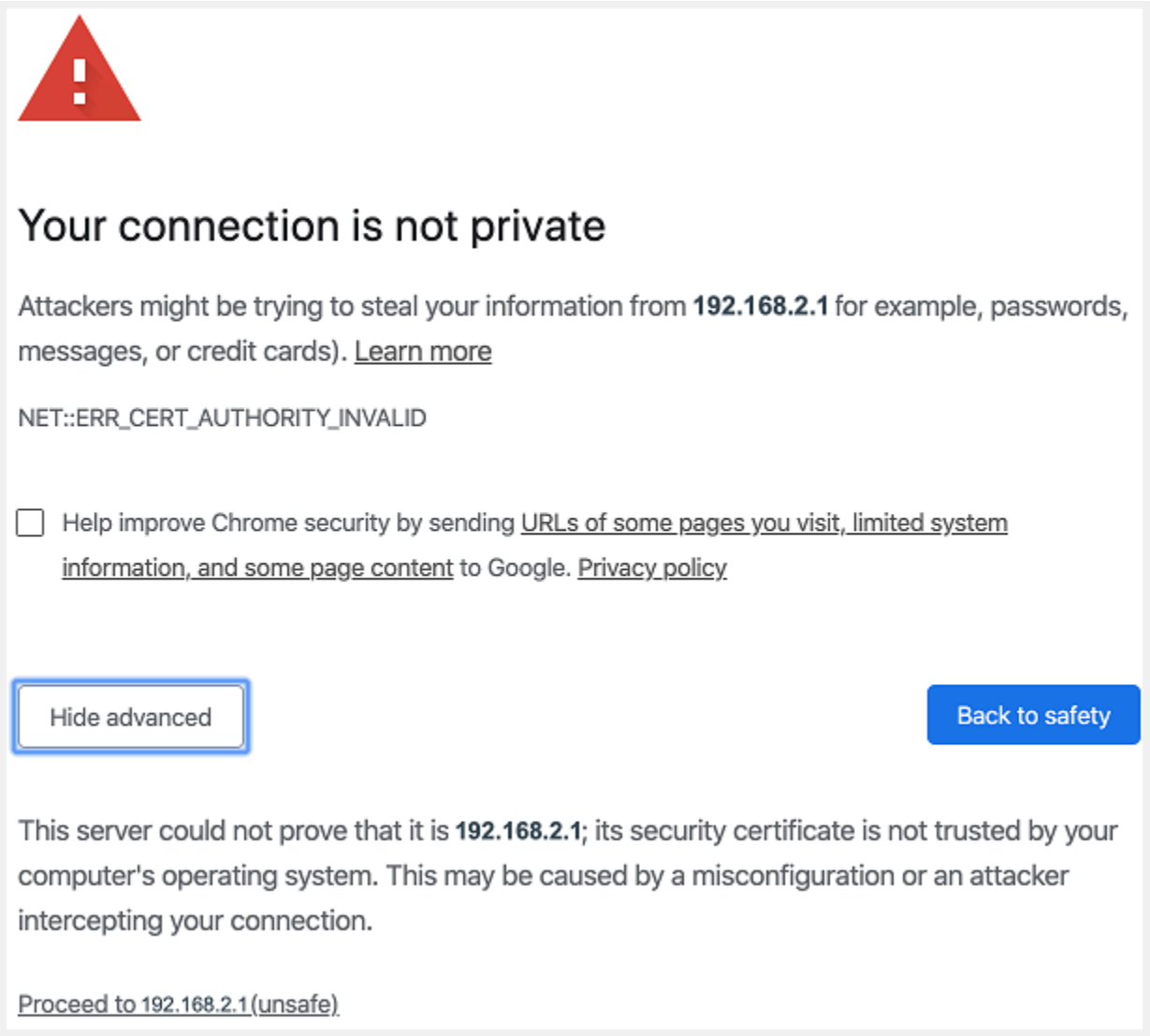
TANIUM CONSOLE AND API

Users access Tanium Console or the Tanium API on the Tanium Server to perform Tanium operations such as issuing questions or deploying actions. The Console and API communicate over Hypertext Transfer Protocol Secure (HTTPS), which uses SSL/TLS certificates and keys to secure client-server connections. When a user accesses Tanium Console or the Tanium API, the user system is the client and the Tanium Server is the server. To secure the connection, the Tanium Server presents its SOAPServer.crt certificate to prove its identity to the Client and uses its SOAPServer.key private key to complete the TLS handshake. For Console or API access, Clients do not have to prove their identity to secure the connection. Figure 2 on page 270 illustrates these processes.

When you install the Tanium Server on a Tanium Appliance, it generates a self-signed SOAPServer.crt certificate. If you use a self-signed certificate, users see a certificate validation error when they access Tanium Console or the Tanium API. The error occurs because the CA certificates on the user system cannot validate the self-signed certificate. The following figure shows an example of such an error when users try to connect from a browser to Tanium Console.

Figure 40. Certificate validation error

©2026 Tanium Inc. All Rights Reserved



Even though browsers provide the option to access Tanium Console despite the error, avoiding that option is a security best practice. Therefore, Tanium highly recommends that you replace the self-signed SOAPServer.crt certificate with a CA-issued certificate. If the Tanium Server is currently using a self-signed certificate, you can replace it at any time.

SIGNED AND ENCRYPTED SAML AUTHENTICATION ON THE TANIUM SERVER

About this task

Some identity providers require a digital signature on Security Assertion Markup Language (SAML) requests from a service provider such as the Tanium Server. If you are using such an identity provider for Tanium Console authentication, you must provide a request-signing certificate (SAMLEncryption.crt) and private key (SAMLEncryption.key) to enable the identity provider to authenticate requests. The Server uses the key to sign the requests and the identity provider uses the

©2026 Tanium Inc. All Rights Reserved

certificate to validate the signature.

To determine the requirements of the SAML certificate and best practices for generating the certificate and key, see your identity provider documentation.

For more information about using a SAML identity provider with Tanium Console, see Integrating with a SAML IdP.

MODULE SERVER COMMUNICATION

When users use Tanium Console or the Tanium API to work with Tanium modules, the Tanium Server communicates with the Tanium Module Server, the Module Server accesses the Tanium module services that it hosts (such as Patch), and the module services communicate back with the Tanium Server (see Figure 2 on page 270).

The Tanium Server and Module Server communicate over HTTPS, and both Servers must prove their identities through certificates. The Tanium Server presents SOAPServer.crt to prove its identity, while the Module Server presents ssl.crt. The Servers use the associated private keys (SOAPServer.key and ssl.key) to complete the TLS handshake that secures the connection. To verify the Tanium Server identity, the Module Server checks that its trusted.crt file contains the SOAPServer.crt that the Tanium Server presented. In an active-active deployment, trusted.crt must contain the SOAPServer.crt of both Tanium Servers. Tanium Servers also verify the Module Server identity by checking that their trusted-module-servers.crt file contains the ssl.crt that the Module Server presented. The Module Server registration process generates trusted.crt on the Module Server and trusted-module-servers.crt on the Tanium Server. The Module Server installation process generates ssl.crt.

The Module Server opens a single HTTPS listener to route requests from the Tanium Server to Tanium module services, which listen only on localhost. TLS termination occurs on the Module Server, which forwards the requests locally over non-TLS connections from the HTTPS listener to the appropriate module service.

Module services connect to the Tanium Server over TLS and verify that the certificate that the Tanium Server presented during the TLS handshake is included in the trusted.crt file on the Module Server. Because module services use the same API as Tanium Console users, Client certificate validation is not enforced.

If you replace the SOAPServer.crt certificate on the Tanium Server, you must re-register the Module Server with the Tanium Server to regenerate the trusted.crt and trusted-module-servers.crt files.

©2026 Tanium Inc. All Rights Reserved

The following table summarizes the certificates and keys that the Tanium Core Platform uses for connections to the Module Server:

Certificates and keys for Module Server connections

Location	File Name	Purpose
Module Server	ssl.crt ssl.key	HTTPS certificate and private key that the Module Server presents to secure incoming connections from the Tanium Server or outgoing connections to Tanium services.
	trusted.crt	Contains the SOAPServer.crt of the Tanium Servers with which the Module Server has registered. The Module Server uses trusted.crt to validate Tanium Server certificates.
Tanium Server	SOAPServer.crt SOAPServer.key	HTTPS certificate and private key that the Tanium Server presents to secure outgoing connections to the Module Server or incoming connections from the systems of Tanium Console users or Tanium API users.
	trusted-module-servers.crt	Contains the ssl.crt of the Module Server that has registered with the Tanium Server. The Tanium Server uses trusted-module-servers.crt to validate the Module Server certificate.

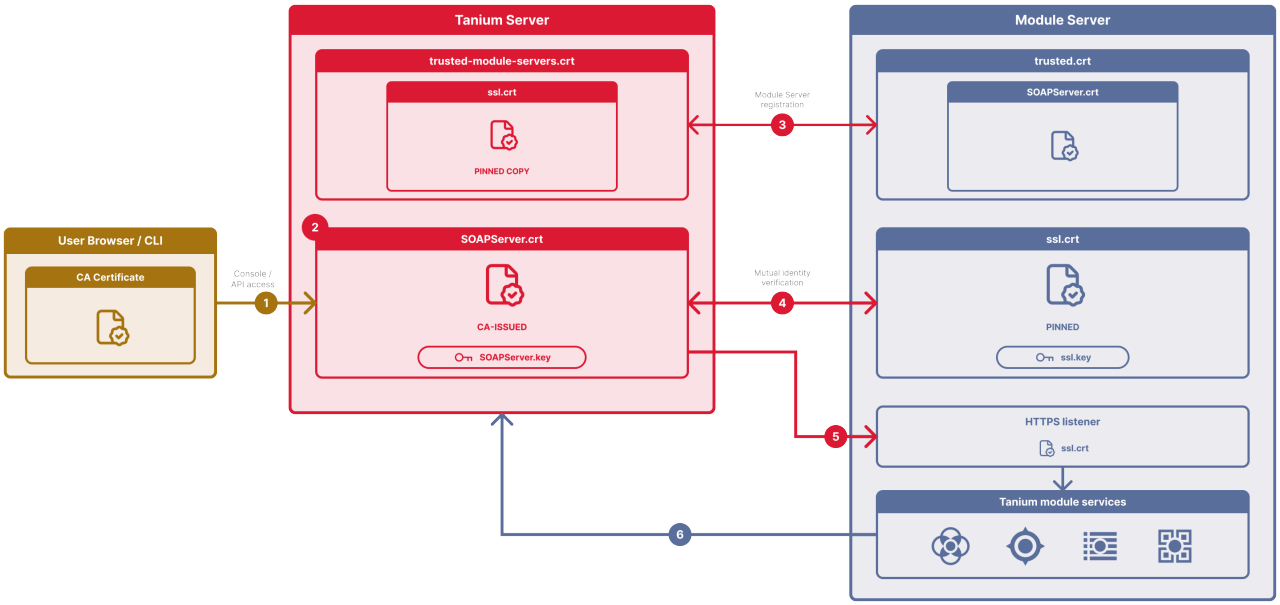
Note: The Tanium Server verifies the Module Server using certificate pinning: the Tanium Server checks that the ssl.crt presented by the Module Server matches the copy stored in trusted-module-servers.crt. As a result, an expired ssl.crt does not prevent communication between the Tanium Server and the Module Server and does not reduce the security of that connection.

SSL/TLS CONNECTION PROCESSES AND SETUP TASKS

The following figure illustrates the components, processes, and setup tasks involved in securing connections to the Tanium Server (Tanium Console or API) and Module Server.

Figure 41. SSL/TLS connections

©2026 Tanium Inc. All Rights Reserved



The following processes correspond to the numbers in Figure 2 on page 270.

1	Tanium Console/API access When a user system connects to Tanium Console or the Tanium API, the Tanium Server presents its SOAPServer.crt certificate to prove its identity to the user system. In Figure 2 on page 270, the Server uses a CA-issued version of SOAPServer.crt (2) instead of a self-signed version. Therefore, the user system uses a CA certificate to validate SOAPServer.crt.
2	Replace self-signed certificate with CA-issued certificate Generate a certificate signing request (CSR) and associated private key SOAPServer.key for the Tanium Server. You submit the CSR to your CA, which uses a CA certificate and associated private key to digitally sign the requested certificate (SOAPServer.crt). The CA signing certificate must also be present on the systems from which users access Tanium Console or the Tanium API (1). The Tanium Server can then use the requested CA-issued certificate instead of a self-signed certificate.
3	Module Server registration When installing the Module Server role in an Appliance Array, TanOS automatically establishes trust. For subsequent communication between the Servers, including during version upgrades, trust is already established, and the Servers automatically check trusted-module-servers.crt and trusted.crt during their mutual identity verification (4).

©2026 Tanium Inc. All Rights Reserved

	Note: For information about installing the Module Server role in an Appliance Array, see Installing and managing an Appliance Array on page 158 .
4 4	Mutual identity verification To establish a secure TLS connection, the Tanium Server and Module Server prove their identities to each other. During the TLS handshake, the Tanium Server presents its SOAPServer.crt certificate to the Module Server, which verifies that its trusted.crt file contains SOAPServer.crt . Also during the handshake, the Module Server presents its ssl.crt certificate to the Tanium Server, which verifies that its trusted-module-servers.crt file contains ssl.crt .
5 5	Module Server to Tanium module services The Module Server opens a single HTTPS listener to route requests from the Tanium Server to Tanium module services, which listen only on localhost. The Module Server forwards the requests locally over non-TLS connections from the HTTPS listener to the appropriate module service.
6 6	Module services to the Tanium Server Module services connect to the Tanium Server over TLS and verify that the certificate that the Tanium Server presented during the TLS handshake is included in the trusted.crt file on the Module Server. Because module services use the same API as Tanium Console users, Client certificate validation is not enforced for this connection (in contrast with the connection described in 4).

CA-issued Tanium Server SOAP certificates

If your organization prefers to use CA-issued certificates to secure connections to systems, you can replace the self-signed certificates that the Tanium Server (SOAPServer.crt) generated during installation. In an active-active deployment, you can use the same CA-issued SOAPServer.crt (and associated private key) for both Tanium Servers as long as the Subject Alternative Name in the certificate specifies both Server names. Alternatively, you can use a distinct CA-issued certificate for each Tanium Server.

Obtaining a CA-issued certificate involves submitting a CSR to the CA and generating an associated private key. Use Tanium Console to create a CSR and replace the SOAPServer.crt certificate for the Tanium Server. For more information, see Managing SSL/TLS certificates.

The CA uses a CA certificate and its associated private key to digitally sign the certificate that you requested. If a CA-issued certificate replaces SOAPServer.crt on the Tanium Server, then the CA signing certificate must also be present on the systems from which users access Tanium Console or the Tanium API. For Console users, the CA signing certificate must be in the trusted certificates store

©2026 Tanium Inc. All Rights Reserved

of their browsers. For API users, the CA signing certificate must be in the location specified in API calls, as shown in the `--cacert <file path>` option in the following example:

```
$ curl -s --cacert <file path> -X POST --data-binary @<sign in>.json https://localhost/api/
v2/session/login
```

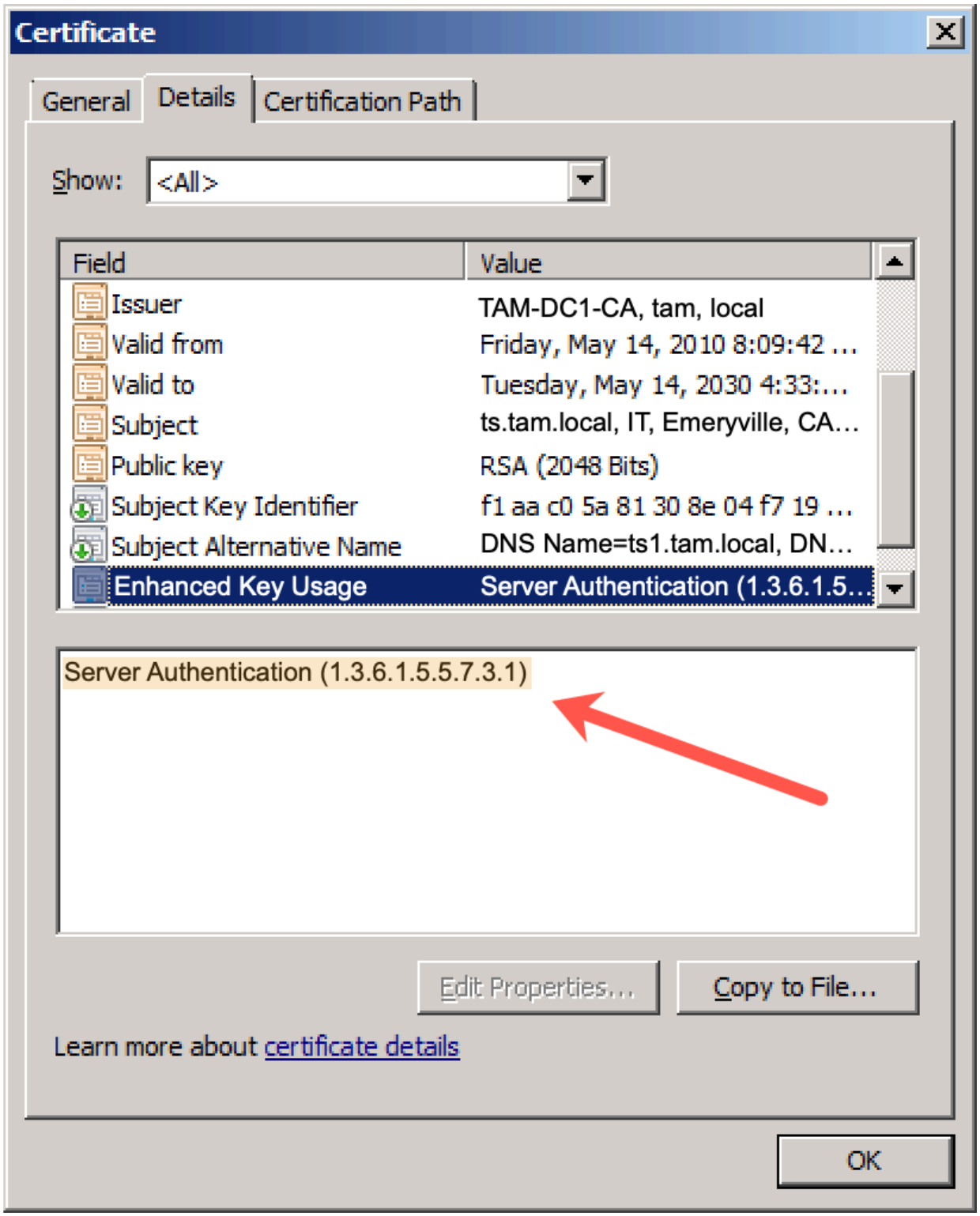
CERTIFICATE REQUIREMENTS

About this task

Work with your CA to obtain a certificate with the following specifications for the Tanium Server SOAP certificate:

- X.509 certificate with TLS Web Server Authentication extended key usage

©2026 Tanium Inc. All Rights Reserved



- Separate certificate and private key files.

Important: You must remove the passphrase from the key file.

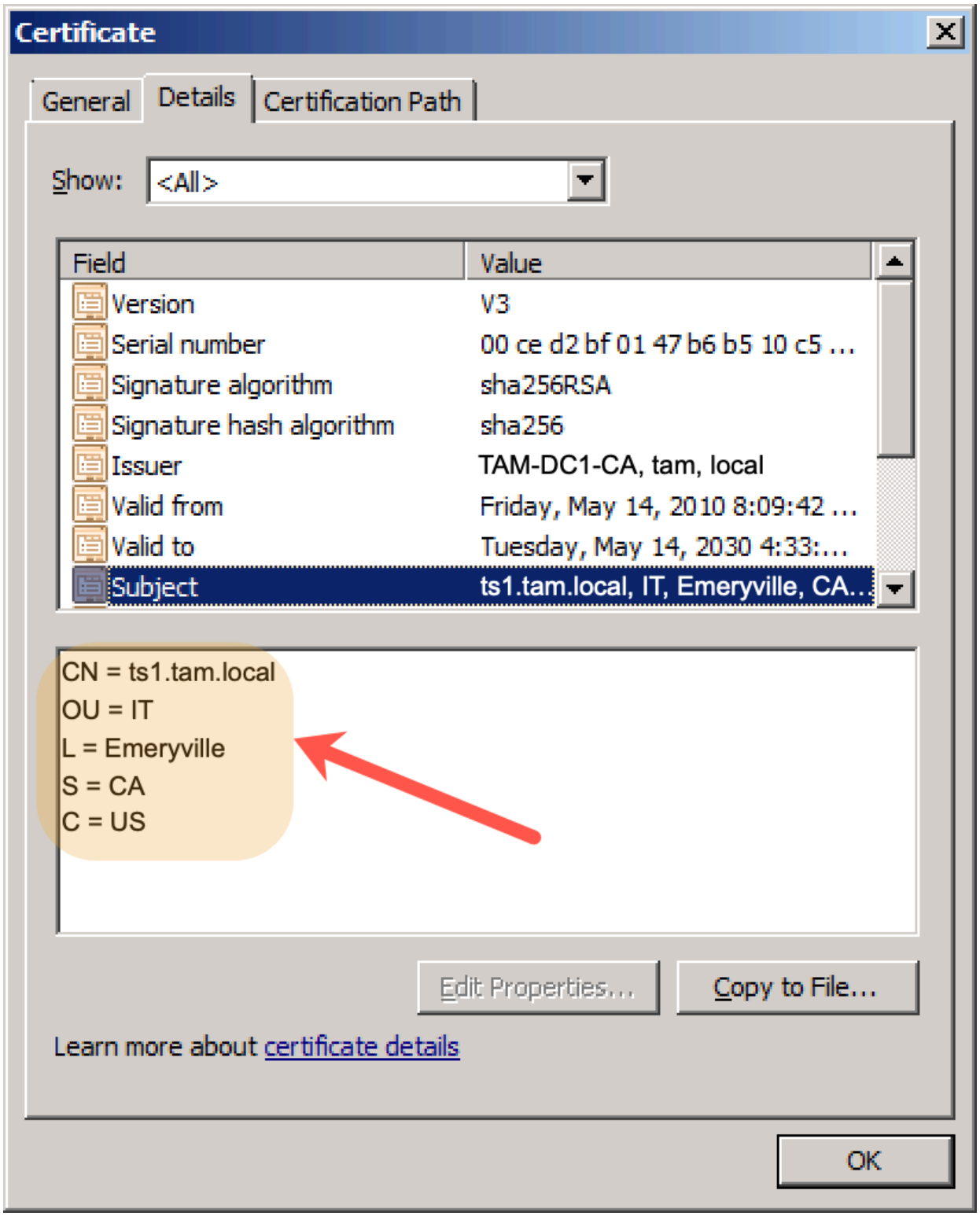
©2026 Tanium Inc. All Rights Reserved

- PEM format (Base64 encoded)
- Certificate signed with a SHA-256 hashing algorithm
- ECC key, or an RSA key with a length of at least 2048 bits

  Tip: Secure certificates for server and client systems are required. To check key sizes, use OpenSSL from a CLI. If your Tanium license includes Tanium Certificate Manager, see View short keys for the steps to check the key sizes in your environment.

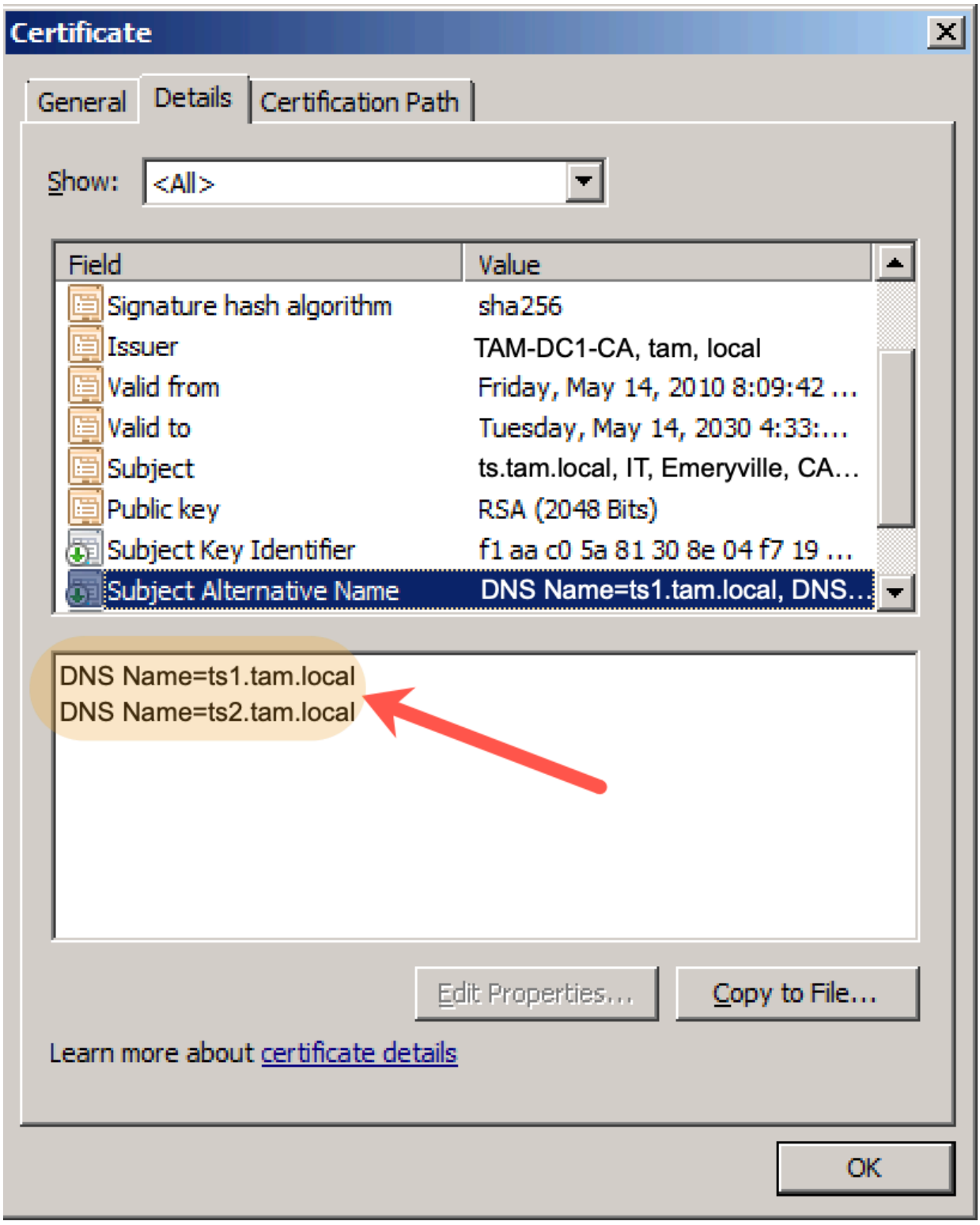
- Common Name (CN) that specifies the fully qualified domain name (FQDN) or IP address of the Tanium Server.

©2026 Tanium Inc. All Rights Reserved



- Subject Alternative Name that also specifies the FQDN or IP address of the Server, as well as that of the secondary Tanium Server in an active-active deployment where both Servers use the same certificate. Web browsers typically require the Subject Alternative Name to be present, regardless of whether the certificate applies to multiple Servers.

©2026 Tanium Inc. All Rights Reserved



- If the certificate is part of a chain that includes an intermediate certificate, the certificate file must include the entire chain. If you receive the certificates as individual files, build a single file for the chain:

    1. Use a text editor to create a new text file.

©2026 Tanium Inc. All Rights Reserved

2. Paste the entire body of each certificate into the text file in the following order:

    a. Server certificate (SSL.crt or SOAPServer.crt)

    b. Intermediate certificate

    c. CA certificate

    > **Note:** Be sure to include the beginning tag (`-----BEGIN CERTIFICATE----`) and ending tag (`-----END CERTIFICATE----`) of each certificate.

3. Save the text file with the file name of the original server certificate (SSL.crt or SOAPServer.crt).

Install a custom certificate

About this task

You can replace the self-signed certificates generated by the Tanium Server and Tanium Module Server installers with an SSL certificate issued by a commercial or enterprise certificate authority (CA). You can also add a SAML certificate to a Tanium Server to enable digital signing of authentication requests from the Tanium Server and encryption of responses from a SAML identity provider.

> **Best Practice:** Though the option to install a replacement Tanium Server SOAP certificate is available in TanOS, in Tanium Core Platform 7.6.2 or later, use Tanium Console to replace the certificate on the Tanium Server. For more information, see Managing SSL/TLS certificates.

> **Note:** In a Tanium cluster, repeat the following procedures to upload and install the certificate and key files to each Tanium Server.

©2026 Tanium Inc. All Rights Reserved

Note: For detailed information about the SSL certificates used in a Tanium deployment, see CA-issued Tanium Server SOAP certificates on page 272.

INSTALL THE SOAP OR SAML CERTIFICATE FILE ON A TANIUM SERVER OR THE SSL CERTIFICATE FILE ON A MODULE SERVER

About this task

Install the new, CA-issued certificate and associated private key on the Tanium Server or Module Server. When installing a certificate on the Tanium Server in an active-active deployment, perform these steps on each Tanium Server. When replacing the Module Server certificate, perform these steps on both the active Module Server and standby Module Server if implemented. Because the steps include stopping and restarting the Servers, perform this task during a maintenance window.

1. Use SFTP to copy the new CA-issued SOAP certificate and key files to the /incoming directory on the Appliance.
2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `2` (Tanium Operations).
4. Select a menu option depending on which certificate you are installing:
   - **Tanium Server replacement SOAP certificate:** Enter `4` to initiate the **Install Custom SOAP Cert** process.

```
------------------------------------------------------

>>> Tanium Operations -> Install Custom SOAP Cert <<<

This menu will allow you to install a custom SOAP Certificate on the Tanium
Server.
The detailed process and requirements can be reviewed at:

https://help.tanium.com/bundle/ug_appliance_onprem/page/appliance/
ssl_certificates.html#custom_CA

Attention: the Tanium Server service will be restarted during this operation!
```

©2026 Tanium Inc. All Rights Reserved

```
Please ensure that you have completed the following steps before continuing:

1) Follow the instructions on help.tanium.com to generate a key/cert pair
2) Upload the SOAPServer.key and SOAPServer.crt files into the incoming

Would you like to continue? [Yes|No]:
```

- **Tanium Server SAML certificate:** Enter `S` to initiate the **Install SAMLEncryption Cert** process.

```
------------------------------------------------------

>>> Tanium Operations -> Install SAMLEncryption Cert <<<

This menu will allow you to install a SAMLEncryption Certificate on the Tanium
server. The detailed process and requirements can be reviewed at:

https://help.tanium.com/bundle/ug_appliance_onprem/page/appliance/
ssl_certificates.html#custom_CA

Attention: the Tanium Server service will be restarted during this operation!

Please ensure that you have completed the following steps before continuing:

1) Follow the instructions on help.tanium.com to generate a key/cert pair
2) Upload the SAMLEncryption.key and SAMLEncryption.crt files into the
incoming

Would you like to continue? [y/n]:
```

- **Module Server:** Enter `M` to initiate the **Module Server SSL Certificate** process.

5. Follow the prompts to install the certificate and key files that you uploaded:
    a. Enter `Yes` at the prompt to proceed with the installation.
    b. Select the certificate that you are importing, verify that the displayed certificate details are correct, and enter `Yes` at the prompt.

```
```

©2026 Tanium Inc. All Rights Reserved

```
                                >>> Tanium Operations -> Install Custom SOAP
Cert -> Select Certificate <<<

Pick a certificate (.pem or *.crt) to import. Press ENTER to re-scan the
incoming directory.

   1: SOAPServer.crt                                              2.1K
      subject= /C=DE/ST=BE/L=Berlin/OU=IT

   R: Return, no selection

Please select: 1

Examining SOAPServer.crt
MD5: fd9bbe48d6ea10037d3d240f96c0c211

Not After: Sep 2 09:43:41 2023 GMT
Subject: C=DE, ST=BE, L=Berlin, OU=IT

SOAPServer.crt: C=DE, ST=BE, L=Berlin, OU=IT

Use this file? [Yes|No]:
```

c. Select the private key that you are importing.
The Appliance verifies that the key is valid and matches the certificate.

```
>>> Tanium Operations -> Install Custom SOAP Cert -> Select Key <<<

Pick a key (.key or *.key.pem) to import. Press ENTER to re-scan the incoming
directory.

   1: SOAPServer.key                                              1.8K
      Valid RSA Key, matching certificate

   R: Return, no selection

Please select: 1
```

©2026 Tanium Inc. All Rights Reserved

```
Creating backup of existing files.

Would you like to backup existing SOAP files to tancopy outgoing? [Yes|No]:
```

d. Enter `Yes` at the prompt to create a backup of the files in the /outgoing directory of the tancopy user.
The Tanium Appliance stops the Tanium Server or Module Server service, installs the new certificate and key, and restarts the service.

```
Creating backup of existing files.

Would you like to backup existing SOAP files to tancopy outgoing? [Yes|No]:
yes
Existing SOAP files have been placed in the sftp outgoing directory.
This location will be cleaned daily at 02:00am Appliance time
Stopping the Tanium Server service - this might take a while...
Installing new certificate...
Starting the Tanium Server service...
Successfully installed new SOAP certificate and restarted the Tanium Server
```

e. To re-register the Module Server, enter `Yes` at the prompt and enter the user name and password of a Tanium Console admin user.

```
This Appliance is part of an Appliance Array containing a remote Tanium Module
Server.
The TMS needs to re-register with this Appliance to begin using the newly
loaded certificate.

Do you want to register the TMS now? [Yes|No]: yes
Enter the Tanium Console admin user name: tanium
Enter Tanium Console admin user password:
```

6. **(Module Server only)** You must manually re-register the Module Server after replacing the Module Server SSL certificate. Follow the steps in Manually register the remote Module Server with each Tanium Server on page 282.

MANUALLY REGISTER THE REMOTE MODULE SERVER WITH EACH TANIUM SERVER

After you replace the certificate and private key on the Module Server, you must manually register the

©2026 Tanium Inc. All Rights Reserved

primary Module Server with the Tanium Server. This process includes configuring the Module Server on the Tanium Server and then enabling the Module Server. In an active-active deployment, you must register the Module Server with each Tanium Server. Because the steps include stopping and restarting services, perform this task during a maintenance window.

Important:

- Re-register only the primary Module Server.
- Do not use these steps when replacing the certificate on a Tanium Server. Allow the Module Server to automatically re-register while following the prompts.

Configure the Module Server on the Tanium Server

1. Sign in to a Tanium Server Appliance as a user with the `tanadmin` role.
2. Enter `2`-`A` (Tanium Operations > Configure Module Server(s)).
3. Enter `1` and follow the prompts to configure the Module Server address, which specifies the address the Tanium Server uses to connect to the Module Server. Be sure to copy the certificate fingerprint. You need the certificate fingerprint to configure the Module Server.

```
            >>> Tanium Operations ->  Configure Module Server(s) ->  Configure Module
Server Address <<<

 Before continuing, please have the following at hand:
 - Hostname of the remote Module Server
 - Domain name of the remote Module Server
 - IP of the remote Module Server

 After completing this step and until step 2 (registration) has been completed on the
remote
 Module Server, this Tanium Server will have limited functionality!
 The following fingerprint is required for step 2:
```

©2026 Tanium Inc. All Rights Reserved

```
800BBFB2942BD9A033F39CBC61049BCE68DEBDF789B38E05569AC0C0794D0BD985C1CF9A0CB73420FCC53
F01756E51F28
 7D29B6D62DFFD5781909E8BCA6E7202

 Would you like to continue? [Yes|No]: yes

 Continue with change.
 Please enter the IP of the remote Module Server: 10.10.10.103
 Please enter the hostname (NOT FQDN) of the remote Module Server: appliance-tms1
 Please enter the domain name of the remote Module Server: tam.local

 Disabling local Module Server instance (if exist)
 Setting new Tanium Module Server address 10.10.10.103
 Changing hosts file

 Would you like to restart the Tanium Server service?
 Attention - this might take a long time! [Yes|No]: yes

 Restarting the Tanium Server service

 Attention:
 Step 1 of the Remote Module Server configuration process completed successful.
 Step 2 needs to be completed on the Remote Module Server. Follow the instructions
 in "Tanium Operations (2) -> Register Remote Module Server (A)"
 This Tanium Server will not be functional until step 2 has been completed as well.

 The following fingerprint is required for step 2 - please copy it:

800BBFB2942BD9A033F39CBC61049BCE68DEBDF789B38E05569AC0C0794D0BD985C1CF9A0CB73420FCC53
F01756E51F28
 7D29B6D62DFFD5781909E8BCA6E7202

 Press enter to continue
```

Enable the remote Module Server

©2026 Tanium Inc. All Rights Reserved

1. Sign in to the Tanium Module Server Appliance as a user with the `tanadmin` role.
2. Enter `2-A` (Tanium Operations > Register Module Server).
3. Enter `2` and follow the prompts to enable the remote Module Server and to configure its connection with the Tanium Server. Specify the Tanium Console admin user (**tanium**, not a TanOS user).

```
            >>> Tanium Operations -> Configure Module Server(s) -> Enable Module
Server <<<

 Before continuing, please have the following at hand:
 - Hostname of the Tanium Server
 - Domain name of the Tanium Server
 - IP of the Tanium Server
 - Credentials of a Tanium User with administrative privileges
 - Fingerprint of the Tanium Server certificate (obtained in Step 1)

 Would you like to continue? [Yes|No]: yes

 Going ahead with Module Server registration
 Please enter the IP of the Tanium Server: 10.10.10.101
 Please enter the hostname (NOT FQDN) of the Tanium Server: appliance-ts1
 Please enter the domain name of the Tanium Server: tam.local
 Please enter the Tanium Console administrative user name: tanium
 Please enter the password (will not be displayed):
 Please enter the fingerprint of the Tanium Servers certificate:
800BBFB2942BD9A033F39CBC61049BCE

68DEBDF789B38E05569AC0C0794D0BD985C1CF9A0CB73420FCC53F01756E51F287D29B6D62DFFD5781909
E8BCA6E7202

 Verified entered fingerprint successfully
 Registering Module Server with 10.10.10.101 (60 second timeout)...
 Added hosts entry
 Registration completed successful
```

```
Restarting Module Server to ensure settings have taken

Restart complete

Press enter to continue
```

For a cluster, register the Tanium Servers individually.

```
           >>> Tanium Operations -> Configure Remote Module Server -> Enable Module
Server <<<

Before continuing, please have the following at hand:
- Hostname of the Tanium Server
- Domain name of the Tanium Server
- IP of the Tanium Server
- Credentials of a Tanium User with administrative privileges
- Fingerprint of the Tanium Server certificate (obtained in Step 1)

Would you like to continue? [Yes|No]: yes

Going ahead with Module Server registration
Please enter the IP of the Tanium Server: 10.10.10.102
Please enter the hostname (NOT FQDN) of the Tanium Server: appliance-ts2
Please enter the domain name of the Tanium Server: tam.local
Please enter the Tanium Console administrative user name: tanium
Please enter the password (will not be displayed):
Please enter the fingerprint of the Tanium Servers certificate:
800BBFB2942BD9A033F39CBC6

1049BCE68DEBDF789B38E05569AC0C0794D0BD985C1CF9A0CB73420FCC53F01756E51F287D29B6D62DFFD
5781
 909E8BCA6E7202

Verified entered fingerprint successfully
Registering Module Server with 10.10.10.102 (60 second timeout)...
Added hosts entry
```

```
Registration completed successful

Restarting Module Server to ensure settings have taken

Restart complete

Press enter to continue
```

Restart Tanium Server and Module Server services

Restart all Tanium services on both the Tanium Server and Module Server Appliances. For more information, see Restart services or networking on page 495.

(Optional) Enable HTTP Strict Transport Security for Tanium Console access

About this task

If you have installed a valid CA-issued certificate, you can optionally enable HTTP Strict Transport Security (HSTS) on the Tanium Server. To do so, you add the `Strict-Transport-Security` HTTP header, which notifies browsers to always use HTTPS to connect to Tanium Console after a user accesses the Console using HTTPS the first time. In an active-active deployment, you must perform this procedure on both Tanium Servers.

Important: Do not enable HSTS if you have not installed a CA-issued certificate. Doing so disables access to Tanium Console.

1. From the Tanium Console Main menu, go to **Administration** > **Configuration** > **Settings** > **Advanced Settings** and click **Add Setting**.
2. Configure the following properties and then click **Save.**
   - **Setting Type**: Local
   - **Platform Setting Name**: `DefaultHeaders`
   - **Value Type**: Text
   - **Value**: `Strict-Transport-Security: max-age=31536000;`

©2026 Tanium Inc. All Rights Reserved

`includeSubDomains`

> **Tip:** You can use any value that your organization policies recommend for `max-age`, which is the value that instructs the browser on how long, in seconds, to use HSTS for the Tanium Server address. The recommended minimum value is `31536000` (one year).

Secure Tanium Server, Zone Server, and Tanium Client access on Tanium Appliances

The subsequent topics in this section provide information about TLS in the Tanium Core Platform, HSM integration, configuring the TLS requirement for Tanium Client connections, configuring TLS on Tanium Clients, verifying TLS connections, and updating the TLS configuration after a key pair change.

Overview of TLS in the Tanium Core Platform

Communication protocols

All supported versions of the Tanium Core Platform use the following protocols for communication among platform components:

- Tanium™ Protocol: This application protocol is proprietary to Tanium and uses TLS 1.3 to encrypt communication.

  > **Important:** You cannot use network devices such as firewalls to decrypt and inspect Tanium Protocol traffic.

- Hypertext Transfer Protocol Secure (HTTPS): The Tanium Core Platform uses TLS 1.3 to encrypt HTTPS communication among platform components. The components negotiate the TLS version for HTTPS connections with external servers but enforce TLS 1.2 as the minimum version.

The following table lists the connections among Tanium Core Platform components and the protocol that each connection uses. The numbers correspond to the connections in Figure 1 on page 290.

©2026 Tanium Inc. All Rights Reserved

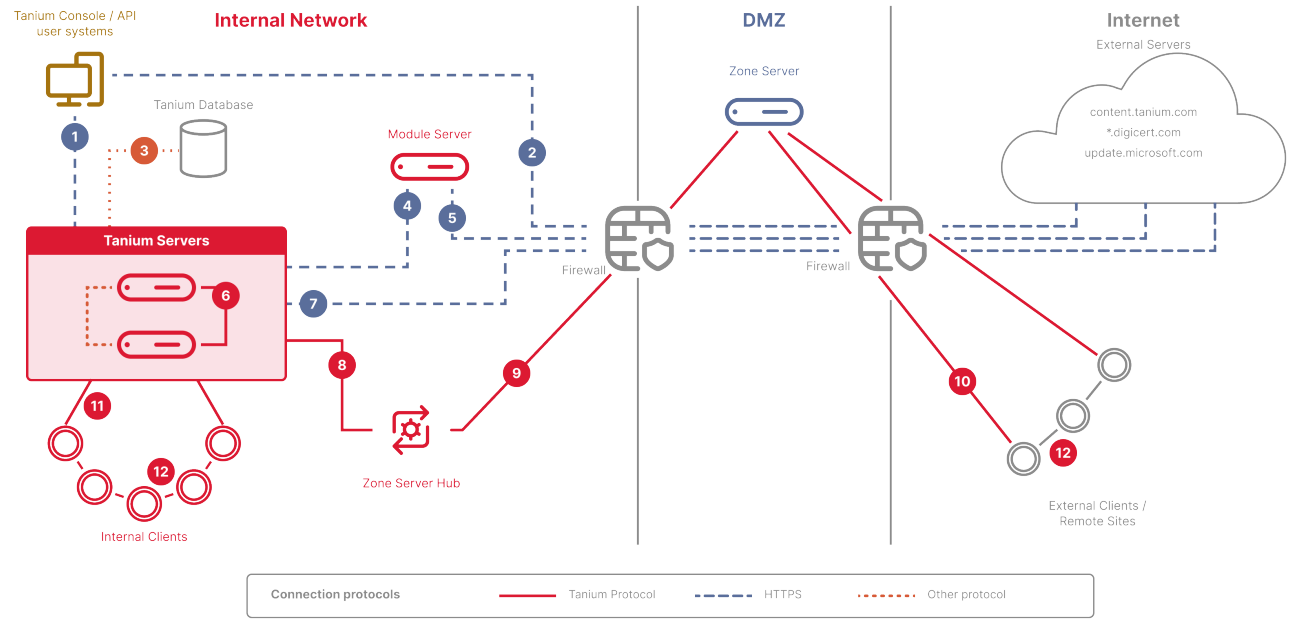
TLS communication in the Tanium Core Platform

	Connection	Protocol
1	Tanium Console or API user systems to Tanium Servers	HTTPS
2	Tanium Console or API user systems to external servers, such as content.tanium.com	HTTPS
3	(Windows only) Tanium Servers to Tanium database in deployments where the database is not on the Tanium Server host	By default, communication is over TCP/IP without encryption, but configuring encryption is a best practice. Consult your database administrator.
4	Tanium Servers to Tanium Module Server	HTTPS
5	Module Server to external servers	HTTPS
6	Tanium Server to Tanium Server in an active-active deployment	Tanium Protocol Tanium Appliances use IPsec to secure Tanium database traffic and Lightweight Directory Access Protocol (LDAP) synchronization traffic.
7	Tanium Servers to external servers	HTTPS
8	Tanium Servers to Zone Server Hub Figure 1 on page 290 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 deployments, you install the hubs on the same hosts as the Tanium Servers.	Tanium Protocol
9	Zone Server Hub to Zone Server	Tanium Protocol
10	Tanium Clients (external) to Zone Server	Tanium Protocol
11	Tanium Clients (internal) to Tanium Servers	Tanium Protocol

©2026 Tanium Inc. All Rights Reserved

Connection		Protocol
12	Tanium Client to Tanium Client (external and internal)	Tanium Protocol

Figure 42. TLS communication in the Tanium Core Platform



Note: To manage the certificates and keys that the Tanium Core Platform uses for HTTPS traffic, see Securing Tanium Console, API, and Module Server access on page 266.

To manage the certificates and credentials for securing connections between Tanium Core Platform Servers and remote sources of content (such as packages), see Managing remote authentication.

For additional details and procedures related to the digital keys for Tanium Protocol traffic, see Managing Tanium keys.

The Tanium Core Platform supports TLS for additional connections that various Tanium modules and shared services require. For more information, see the User Guides for your Tanium products.

To troubleshoot TLS communication issues, see PKI TLS logs on page 523.

TLS COMMUNICATION PROCESS

©2026 Tanium Inc. All Rights Reserved

TLS communication starts when a TLS client initiates a TLS handshake to establish a secure connection with a server. The following are examples in the context of the Tanium Core Platform:

- The Zone Server acts as a client when registering with the Tanium Server.
- The Tanium Client acts as a client when registering with the Zone Server or Tanium Server.
- A Tanium Server acts as a client when performing active-active synchronization with another Tanium Server.

During the TLS handshake, the client and server generate a shared, unique session key, which they use to secure communication for the duration of their session. You can configure TLS as optional for Tanium Clients. If the handshake fails and TLS is optional, the client and server attempt a non-TLS (unencrypted) connection instead. If the handshake fails and TLS is configured as required, the client and server cannot connect.

SUPPORTED CIPHER SUITES

About this task

The Tanium Core Platform supports the following cipher suites for creating keys and encrypting information in TLS communication:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_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

©2026 Tanium Inc. All Rights Reserved

After a fresh installation or upgrade, TLS is required for the Tanium Server (including between Tanium Servers in an active-active deployment), Zone Server, and Zone Server Hub, and you cannot disable it. The Tanium Server installer generates the TLS public and private keys that are used to set up TLS for connections with the Tanium Server.

After a fresh installation or upgrade, TLS is required by default for endpoints. You can optionally configure this requirement.

This applies when you install the Tanium Server role on a Tanium Appliance (see Assign roles on page 165).

Contact Tanium Support on page 510 and consult your network security team before modifying the TLS configuration. Whether TLS is available and required depends on the Tanium Core Platform version, components, and infrastructure:

HSM integration

If your organization uses a hardware security module (HSM) to store and manage keys, you can configure the Tanium Server to integrate with the HSM. For more information, see Securing keys with an HSM.

(Optional) Configure the TLS requirement for Tanium Client connections

About this task

The Tanium Core Platform also requires TLS for incoming connections from endpoints by default. You can configure the TLS requirement for Tanium Client.

From the Tanium Console Main menu, go to **Administration** > **Configuration** > **Settings** > **Advanced Settings**, and configure the **require_client_tls_315_flag** setting for connections from Tanium Clients to the Tanium Server:

- `1` (default): The Tanium Server allows connections from endpoints with Tanium Client 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. Contact Tanium Support before setting the value to `0`.

©2026 Tanium Inc. All Rights Reserved

Note: These settings also apply to connections from Tanium Clients to the Zone Server if you deploy one.

Configure TLS on Tanium Clients

After a fresh installation or upgrade, TLS is enabled and required by default. Tanium strongly recommends that you use these default settings.

1. From the Main menu, go to **Administration** > **Configuration** > **Client Status**.
2. In the **Filter by Registration** section, select **Registered using TLS** and **Registered unencrypted** if they are not already enabled.
   The **Using TLS** column indicates which Tanium Clients have TLS enabled or disabled.
3. From the Main menu, go to **Administration** > **Configuration** > **Settings** > **Advanced Settings** and configure the **TLSMode** setting for the Tanium Clients.
   - `0` (TLS not used): TLS is disabled.
   - `1` (TLS required): If a TLS handshake fails, the Tanium Client cannot communicate with other Clients or the Servers. This is the default value.

   On the Tanium Client endpoint, the setting name is **Server_TLSMode**, with the **Server_** prefix indicating that the Tanium Client received the settings from platform settings on the Tanium Server during registration, and future registration updates might change the settings.

   In some cases, you might want a Tanium Client to use a setting that differs from the Tanium Server platform setting. To override the Tanium Server platform settings, add the **TLSMode** setting (without the **Server_** prefix) to the Tanium Client settings on the Client endpoints.

Result

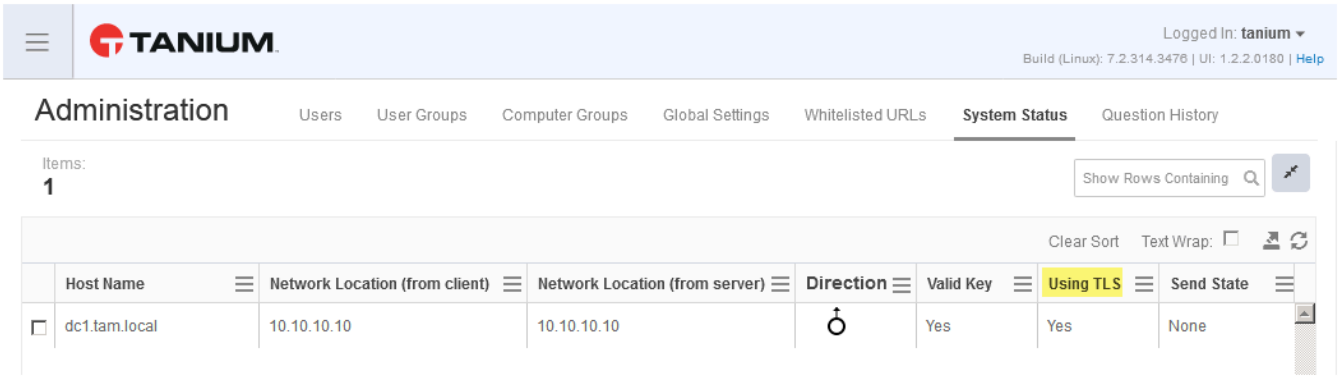
Note: It takes two to six hours (the randomized client-reset interval) for Clients to register and receive the updated settings.

Verify the TLS connections

About this task

©2026 Tanium Inc. All Rights Reserved

Verify whether Tanium Clients used TLS to connect with the Tanium Server or Zone Server when the Clients last registered: from the Main menu, go to **Administration** > **Configuration** > **Client Status** and check the **Using TLS** column.



Update the TLS configuration when you make changes to key pair

About this task

When you add or revoke Tanium root keys, the Tanium Server automatically propagates the changes to all subordinate keys on the platform Servers and Tanium Clients (see Managing Tanium keys).

Configure the local authentication service for Tanium Console users

You can use the local authentication service to set up Tanium Console user accounts for demo or testing purposes.

Best Practice: For production use, configure Tanium Console to use a SAML identity provider or an external LDAP server to authenticate Tanium users. For more information, see Integrating with a SAML IdP or Integrating with LDAP servers.

©2026 Tanium Inc. All Rights Reserved

Note:

- If you use the local authentication service together with LDAP integration, you must use the following user filter in the LDAP configuration:

  ```
  (&(objectClass=person)(uidNumber>=20000))
  ```

- The **Local Authentication Service** menu is available only after you install the Tanium Server on the Appliance.
- In an active-active deployment, the local authentication service synchronizes local Tanium Console user accounts across both Tanium Servers in the cluster.

Add a local user

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`L` (User Administration > Local Tanium User Management).
3. Enter `1` and follow the prompts to add a local user.

```
           >>> Appliance User Administration -> Local Authentication -> Add Local
User <<<

 Adding a local user requires first name, last name and a user name.

 Attention:
 Please assign the new user appropriate roles and rights in the Tanium application!

 Please enter first name: John
 Please enter last name: Doe
 Please enter desired user name (max 20 chars): john.doe



 The password policy requires meeting these rules:
  - Minimum 10 characters long
```

©2026 Tanium Inc. All Rights Reserved

```
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
 - At least 1 other character
 - Must not be based on a dictionary word
 - Must not contain part of the username

Please enter password (will not be displayed):
Password score: 50 out of 100 (strong)
Please enter password again:

Successfully added user John Doe (username: john.doe) to the local authentication
service.
Press enter to continue
```

4. Sign in to Tanium Console as an administrator, create a user with the same user name, and assign roles to it. For more information, see Managing users.

Set a user password

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C-L-2` (User Administration > Local Tanium User Management > Manage Local Users).
3. Enter the user line number to go to the **User** menu.

```
 ------------------------------------------------------


>>> User Administration -> Tanium Users -> tanldap <<<


  UserID:         tanldap
  Name:           tanldap tanldap
  Lock Time:      n/a
  Expiry Time:    n/a


          1: Delete User
          2: Set Password
```

```
         R: Return to previous menu  RR: Return to top


-------------------------------------------------------
```

4. Enter `2` and follow the prompts to set the user password.

```
 -------------------------------------------------------

>>> User Administration -> Tanium Users -> tanldap <<<

 UserID:         tanldap
 Name:           tanldap tanldap
 Lock Time:      n/a
 Expiry Time:    n/a

         1: Delete User
         2: Set Password

         R: Return to previous menu  RR: Return to top

 -------------------------------------------------------

 TanOS Version:        1.9.1

 Please select: 2

 Setting new password for tanldap



 The password policy requires meeting these rules:
  - Minimum 10 characters long
  - At least 1 upper case character
  - At least 1 lower case character
  - At least 1 numeric character
  - At least 1 other character
  - Must not be based on a dictionary word
  - Must not contain part of the username
```

©2026 Tanium Inc. All Rights Reserved

```
Please enter password (will not be displayed):
```

Delete a user

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`L`-`2` (User Administration > Local Tanium User Management > Manage Local Users).
3. Enter the user line number to go to the **User** menu.

```
 ------------------------------------------------------


>>> User Administration -> Tanium Users -> tanldap <<<


  UserID:          tanldap
  Name:            tanldap tanldap
  Lock Time:       n/a
  Expiry Time:     n/a


          1: Delete User
          2: Set Password


          R: Return to previous menu  RR: Return to top


 ------------------------------------------------------
```

4. Enter `1` and follow the prompts to delete the user.

Disable the local authentication service

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`L` (User Administration > Local Tanium User Management).
3. Enter `A` and follow the prompts to enable or disable the local authentication service.

```
           >>> User Administration -> Enable/Disable Local Authentication <<<
```

©2026 Tanium Inc. All Rights Reserved

```
Current status of the Local Authentication Service:
Enabled
Active

Warning: make sure that you have configured the Tanium application to use an
external authentication service prior to disabling the local authentication service!

Would you like to disable the Local Authentication Service? [Yes|No]: yes

Disabling Local Authentication Service

Local Authentication Service has been disabled.
Press enter to continue
```

Note: Although Tanium Console contains a **soap_enable_local_auth** platform setting to disable local authentication, that setting is not supported for Tanium Appliance installations.

Modify the local authentication service security policy

About this task

The local authentication service security policy has the following default settings.

TanOS local authentication service security policy default settings

Setting	Factory Default	Description
Password Minimum Age (days)	1	The minimum number of days between password changes. A value of `0` indicates the password can be changed at any time. Valid range is `0` - `20`.
Password Maximum Age (days)	90	The age at which a current password expires. A value of `0` indicates the password does not expire. Valid range is `0` - `360`. The maximum age must be equal to or greater than the minimum age.
Password	10	The minimum number of characters allowed in a password. Valid range is `0` - `30`.

©2026 Tanium Inc. All Rights Reserved

Setting	Factory Default	Description
Minimum Length		
Password History	5	The number of most recent passwords that a user cannot reuse. A setting of `0` allows reuse of any previous passwords. Valid range is `0` - `10`.
Password Lockout	True	`True` locks out a user after the number of failed password attempts configured for **Password Maximum Failure** and requires an administrator to unlock the account. `False` disables the password lockout.
Password Maximum Failure	5	The number of failed password attempts before a user is locked out when **Password Lockout** is set to `True`. A setting of `0` allows unlimited failed attempts. Valid range is `0` - `10`.

To modify the default settings:

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `C`-`L`-`B` (User Administration > Local Tanium User Management > Security Policy Local Authentication Service).
3. Follow the prompts to modify the settings.

Configure smart card authentication for Tanium Console users on Tanium Appliances

The Tanium™ Console supports *smart card authentication*. A smart card is physical credential that has a microchip and data, such as secure certificates and keys. Smart cards are also known as common access cards (CAC) and personal identity verification (PIV) cards. Endpoint systems are set up with smart card readers, and end users use their smart card to authenticate and gain access.

Requirements

When smart card authentication is enabled, the Tanium Server and Tanium Module Server must reside on separate hosts. All authentication to Tanium Console requires smart cards unless the

©2026 Tanium Inc. All Rights Reserved

authentication request is from one of the following sources:

- The system hosting the Tanium Server through the local loopback address (127.0.0.1 for IPv4 or [::1] for IPv6).
- The Module Server connection to the Tanium Server.

Consequently, any additional integrations that you want to automate must reside on one of the two hosts. The following are some examples:

- SSRS plugin
- Microsoft Excel plugin (unless using the version that supports smart card authentication)
- Tanium™ Connect for Lightweight Directory Access Protocol (LDAP) synchronization
- PyTan
- Third-party security operations center (SOC) websites that query Tanium for data



Important: An air gap deployment with smart card authentication has additional caveats:

- Links to content that is hosted on the Tanium Server must use the local loopback address. This is because the TDownloader service that downloads content to the Tanium Server cannot present a certificate.
- Links to Tanium module or shared service imports use both the local loopback address (for the workbench) and the Tanium Module Server fully qualified domain name (FQDN) for the portion of the solution installed on the Module Server.

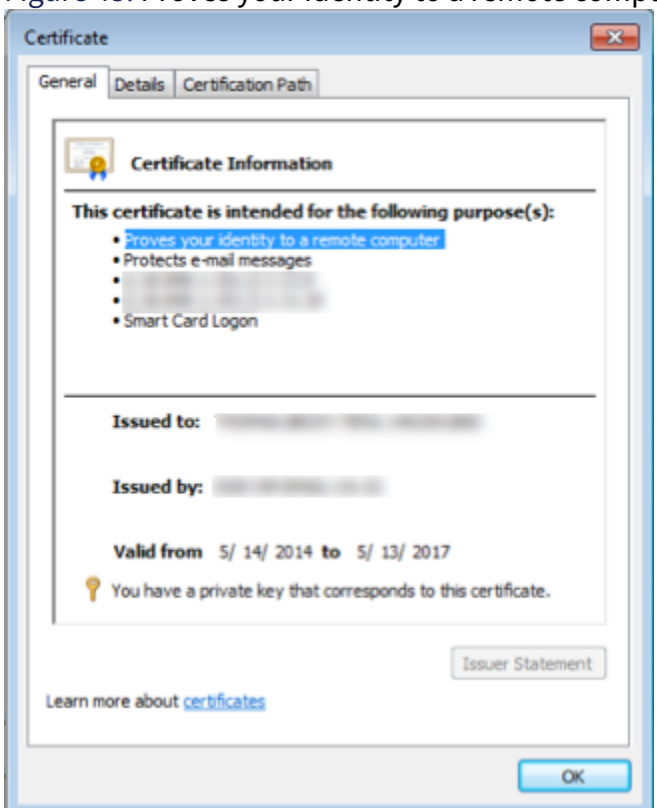
Create a certificate

About this task

Smart card authentication for Tanium Console access depends on the public key infrastructure (PKI) of your organization. You can get started if you have a Client certificate that is signed by the root certificate authority (CA) certificate for the domain where the Tanium Server is deployed. Make sure the certificate has the **Proves your identity to a remote computer** attribute.

©2026 Tanium Inc. All Rights Reserved

Figure 43. Proves your identity to a remote computer

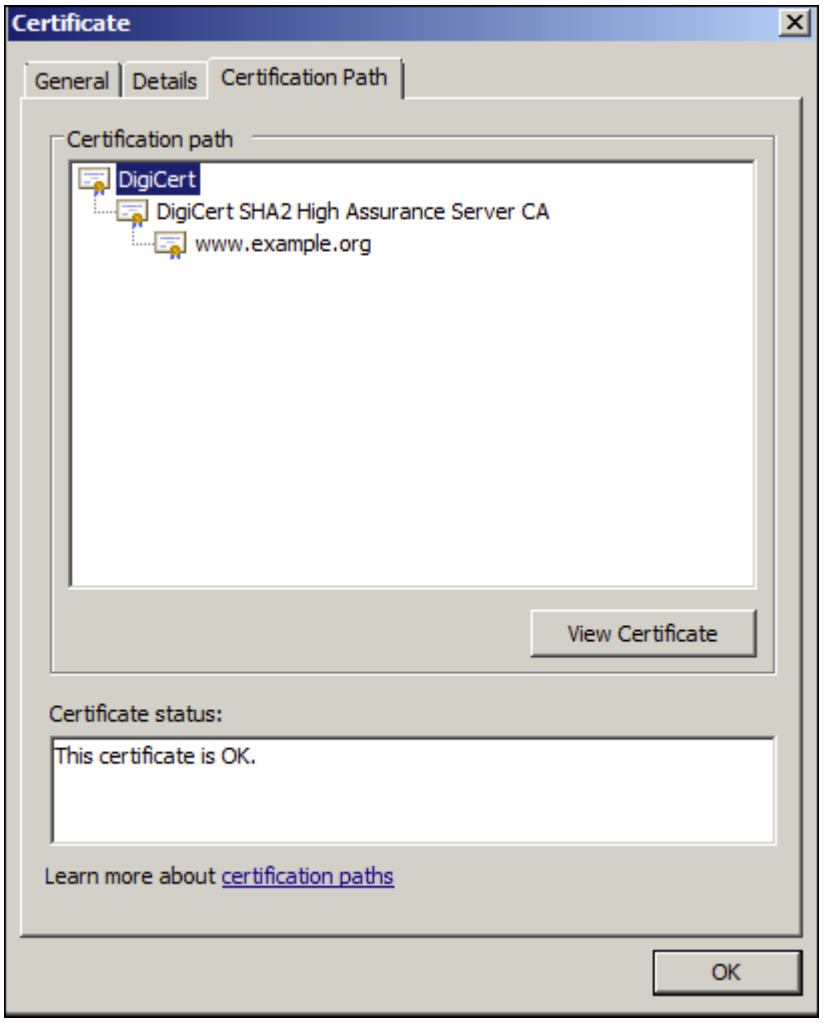


Create a new certificate file from certificates that you extract from the Client certificate. Usually, you need to extract only the root certificate. If this does not work, you might also need to add intermediate certificates to the certificate chain.

EXTRACT THE CERTIFICATES

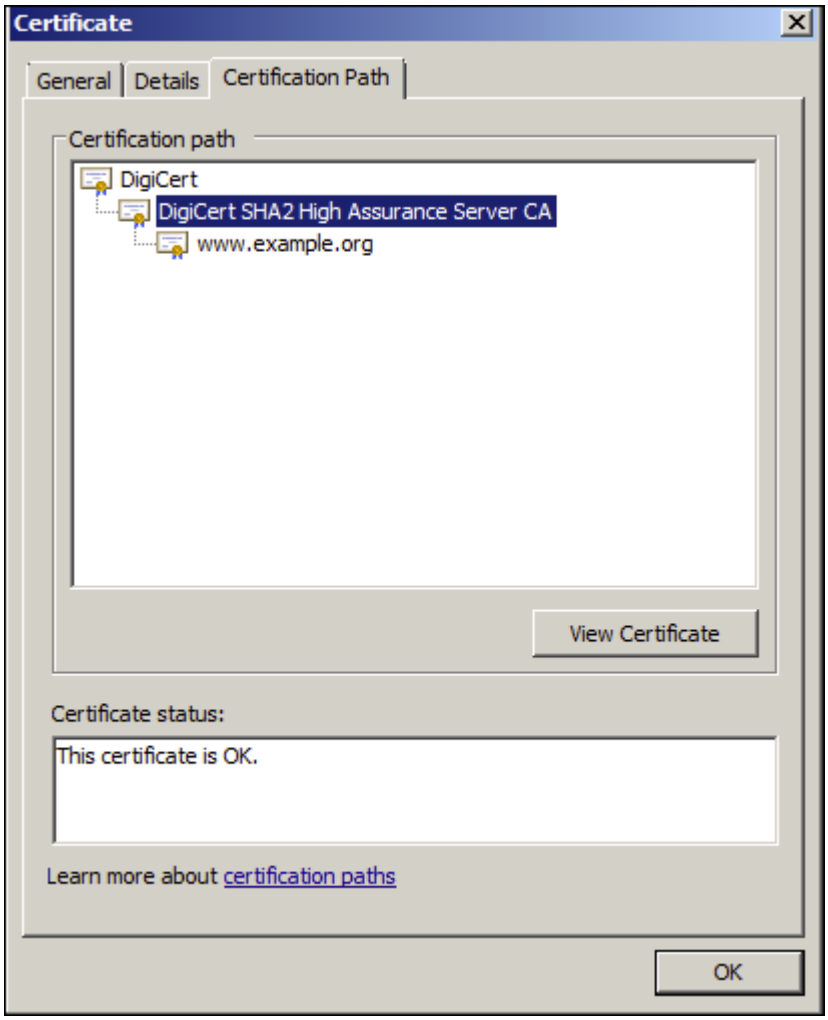
1. Get a copy of a Client certificate file that is signed by the root CA certificate for the domain. For more information, see Figure 1 on page 302.
2. On a Windows endpoint, double-click the certificate file to open it in the Windows Certificate Snap-In.
3. On the **Certification Path** tab, select the root certificate. In this example, DigiCert is the root certificate.

©2026 Tanium Inc. All Rights Reserved



4. Go to the **Details** tab and click **Copy to File** to display the Certificate Export Wizard.
5. Select **Base-64 encoded X.509 (.CER)**.
6. Select a folder and specify a file name such as example1.cer.
7. Review the settings and click **Finish** to save the certificate.
8. If your deployment has intermediate CA certificates, repeat these steps to extract them. Go to the **Certification Path** tab and select the next certificate in the chain. In the following example, DigiCert SHA2 High Assurance Server CA is the next certificate. Export this certificate with a name such as example2.cer.

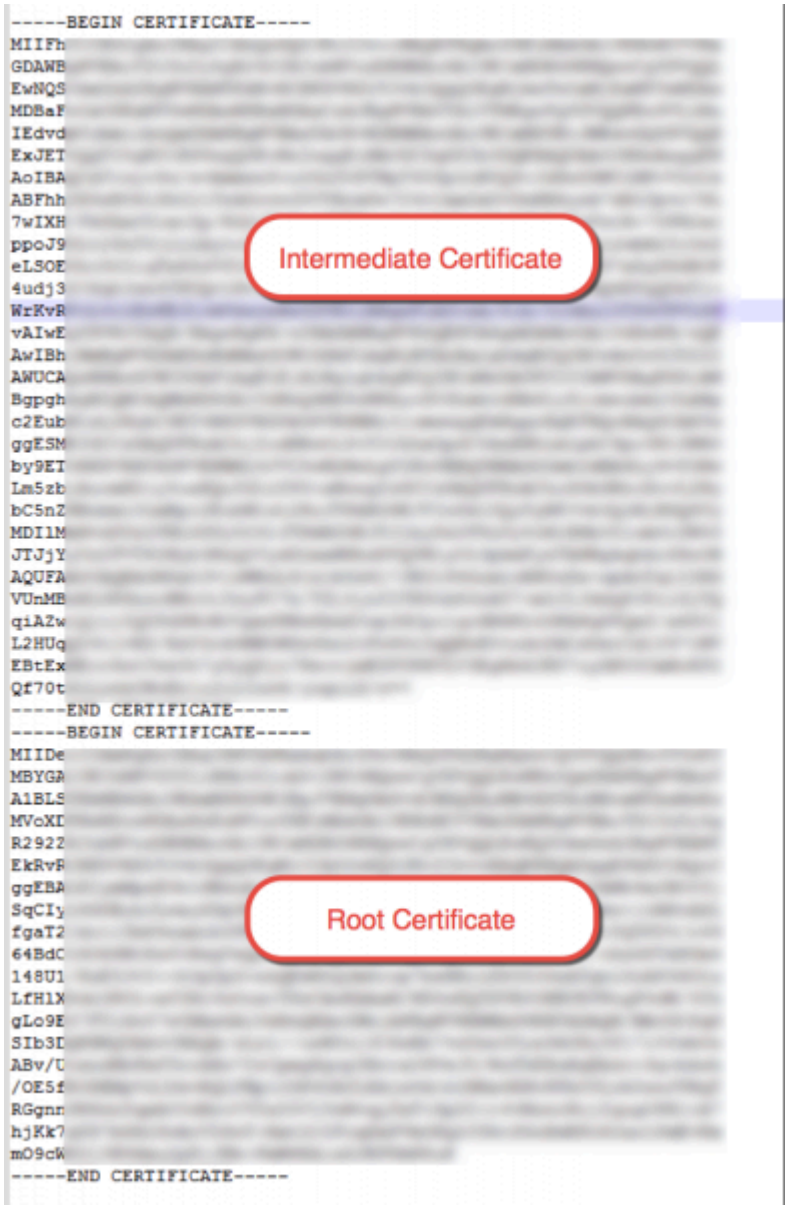
©2026 Tanium Inc. All Rights Reserved



CREATE A NEW CERTIFICATE FILE

1. Create a file named cac.pem.
2. Copy and paste in the contents of each certificate in the chain into the file.

©2026 Tanium Inc. All Rights Reserved



Important:

- Each section of the certificate file must start with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`.
- There must be only one carriage return between each certificate in the chain.
- There must be no extra white spaces or carriage returns at the beginning or end of the file.
- The preceding example shows the root certificate last, which is a convention that Tanium Support uses.

©2026 Tanium Inc. All Rights Reserved

3. Save the file.

Configure CAC

About this task

Important: Add your CAC account user name (EDIPI) as a Tanium Administrator before enabling CAC.

STEP 1: INSTALL THE CERTIFICATE

About this task

Upload and install the certificate:

1. Use SFTP to copy the certificate file (PEM format) to the /incoming directory on the Tanium Server appliance.
2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `2` to go to the **Tanium Operations** menu.

```
------------------------------------------------------

            >>> Tanium Operations Menu <<<

        1: Tanium Service Control
        2: Tanium Configuration Settings
        4: Install Custom SOAP Cert
        5: Manage Custom Signing Keys
        7: Download SOAP Certificate
        9: Import CAC Certificate

        A: Configure Module Server(s)
        B: Configure Tanium Cluster
        C: Manage Content
        M: Module Operations
```

©2026 Tanium Inc. All Rights Reserved

```
        I: Import public key to Tanium Zone Server

        X: Advanced Operations

        R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

4. Enter `9` and follow the prompts to import and install the CAC certificate file.

STEP 2: ADD THE REQUIRED TANIUM SERVER CONFIGURATION SETTINGS

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2` to go to the **Tanium Operations** menu.

```
-----------------------------------------------------

            >>> Tanium Operations Menu <<<

        1: Tanium Service Control
        2: Tanium Configuration Settings
        4: Install Custom SOAP Cert
        5: Manage Custom Signing Keys
        7: Download SOAP Certificate
        9: Import CAC Certificate

        A: Configure Module Server(s)
        B: Configure Tanium Cluster
        C: Manage Content
        M: Module Operations

        I: Import public key to Tanium Zone Server

        X: Advanced Operations

        R: Return to previous menu  RR: Return to top
```

©2026 Tanium Inc. All Rights Reserved

```
-----------------------------------------------------
```

3. Enter `2` to go to the **Configuration Settings** menu.

```
-----------------------------------------------------

 >>> Tanium Operations -> Configuration Settings <<<

Note: Some settings may require a service restart to take effect.

          1: Edit Tanium Server Settings
          2: Edit Tanium Server TDL Settings
          3: Add Tanium Server TDL Auth User
          4: Add Tanium Server TDL Auth Cert

          5: Edit Tanium Module Server Settings
          6: Edit Tanium Module Server TDL Settings
          7: Add Tanium Module Server TDL Auth User
          8: Add Tanium Module Server TDL Auth Cert

          9: Edit Tanium Zone Server Settings
          11: Edit isolated subnets list
          12: Edit separated subnets list

          13: Control Root CA Certs

          R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

4. Enter `1` to go to the **Tanium Server Config Settings** menu.

```
>>> Tanium Operations -> Configuration Settings -> Edit <<<
Editing: Tanium Server Config Settings

1: AddressMask 16777215
2: AllowedHubs 127.0.0.1
```

©2026 Tanium Inc. All Rights Reserved

```
3: AuthPluginTimeoutSeconds 60
4: AuthenticationPlugin InternalPython:tanium_pam4/pam_workflow.py
5: ClientCertificateAuth /opt/Tanium/TaniumServer/cac.pem
6: ClientCertificateAuthField X509v3 Subject Alternative Name
7: ClientCertificateAuthRegex .*:\s(\d+)@.*
8: ConsoleSettingsJSON /opt/Tanium/TaniumServer/http/config/console.json
9: EnforceAllowedHubs 1
10 ForceSOAPSSLClientCert 1
11: LogPath /opt/Tanium/TaniumServer/Logs
12: LogVerbosityLevel 1
13: ModuleServer 10.10.10.103,appliance-tms1.tam.local:17477
14: ModuleServerPort 17477
15: ReportingTLSCertPath /opt/Tanium/TaniumServer/reporting.crt
16: ReportingTLSKeyPath /opt/Tanium/TaniumServer/reporting.pvk
17: SQLConnectionString postgres:10.70.164.248@user=postgres dbname=tanium sslmo
de=require sslcert=/opt/Tanium/.postgresql/postgresql.crt sslkey=/opt/Tanium/.
postgresql/postgresql.key sslcompression=1
18: ServerPort 17472
19: ServerSOAPPort 8443
20: TrustedCertPath /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
21: TrustedHostList host1.example.com,192.168.0.1
22: Version 7.9.3.1234

A: Add a line
R: Return to previous menu  RR: Return to top
```

5. Use the menu to add Tanium Server settings as described in the Table 9. Enable CAC settings on page 310 table.
6. Restart the Tanium Server service. For more information, see Start, stop, and restart Tanium services. You can now Sign in to Tanium Console with your CAC.
   The following table summarizes the settings you must add to enable CAC.

©2026 Tanium Inc. All Rights Reserved

Enable CAC settings

Setting Name	Guidelines
ForceSOAPSSLClientCert	Optional. If the registry value does not exist (but other CAC/PIV registry values do exist), or is set to a value of `1`, CAC/PIV authentication becomes mandatory.
ClientCertificateAuthField	Optional. If it is not defined, certificate authentication matches on the Subject field. Specify a value for this key if you want to match on a different attribute. Many organizations use `X509v3 Subject Alternative Name`. Example: `X509v3 Subject Alternative Name` Note : X509v3 is typically hidden when displayed in Windows. Note that X509v3 is case sensitive.
ClientCertificateAuthRegex	Optional. If it is not defined, the default regular expression (regex) is used to match the user identifier. The default is `.*CN=(.*)$`. **Best Practice:** The following expression is the best practice to match any Subject Alternative Name entry: `.*:\s(\d+)@.*`
ClientCertificateAuth	Defines the location of the certificate file to use for authentication, such as: /opt/Tanium/TaniumServer/cac.pem Note : The path name is case sensitive.
CACTrustedAddresses	Defines which endpoints to exempt from CAC authentication requirements. These systems will not require a CAC/PIV certificate to authenticate and will work for all Tanium assets. Specify the Tanium Server and Tanium Module Server. Specify additional addresses to exempt any other trusted systems and components. In an active-active deployment, you must configure this setting on both Tanium Servers to prevent errors with TDownloader.
cac_ldap_server_url	Optional. If it is defined, requires that Tanium validate every CAC/PIV authentication attempt with LDAP to determine the state of the account that is signing in. Because this does not use the Windows authentication subsystem, the service account running Tanium must have the privileges to look up accounts through a direct LDAP query.

©2026 Tanium Inc. All Rights Reserved

Setting Name	Guidelines
	Use the following syntax, where `LDAP` must be uppercase: `LDAP://<LDAP FQDN>` If multiple domains are in use, specify a global catalog in the syntax `GC://<domain>`. **Best Practice:** Also configure LDAP integration in Tanium Console, and assign roles, computer groups, and personas to user groups and users that are imported from the LDAP server. For more information, see Integrating with LDAP servers.
CertLDAPQueryField	Optional. If it is defined, it specifies an LDAP user naming attribute. If it is not defined, the default attribute is used. Valid values are: • `userPrincipalName` — The sign in name for the user. • `sAMAccountName` — A sign in name that supports previous version of Windows.
CertLDAPCertField	Optional. Add this setting in conjunction with the **cac_ldap_server_url** setting. This setting specifies a secondary attribute to query within the X509 certificate. Usually, this value is expected to match **ClientCertificateAuthField** with a value of `X509v3 Subject Alternative Name`. If it is not defined, certificate authentication matches on the Subject attribute. **Note:** X509v3 is typically hidden when displayed in Windows. The string `X509v3` is case sensitive.

CertLDAPCertFieldRegex	Optional. Add this attribute in conjunction with the **cac_ldap_server_url** setting. This setting specifies a regular expression that accounts for the User Principal Name (UPN) Suffix when a secondary LDAP lookup occurs. This is necessary because LDAP synchronization matches UPN without the UPN Suffix.
	If it is not defined, whatever is returned in the user naming attribute is used.
	The following example is most commonly used. It returns the full UPN:
	`.*\:\s*([^@]+@.*)$`
	The following example returns just the numeric value from the UPN:
	`([^@]+)@.*$`

Next steps

©2026 Tanium Inc. All Rights Reserved

Note: To disable CAC authentication, remove the CAC settings and then restart the Tanium Server service.

Troubleshoot smart card authentication

About this task

- Check the configuration for typos, such as extra spaces or letter case errors.
- Test whether the system works with just the required registry keys. Then enable and test optional settings, such as the LDAP integration settings.
- In an active-active deployment, configure the **CACTrustedAddresses** value with entries for each Tanium Server and the Module Server to avoid errors by the Tanium Downloader (TDownloader) service during package synchronization.
- Set the logging level to 41 or higher on the Tanium Server and Module Server to record the following events. For more information, see Configure Server logging levels. If you Create a custom log on page 512 that records only these events, use `.*Client Certificate auth.*` as the filter regex. After generating logs at level 41, search for the following log entries:
  - If **ClientCertificateMatchField** is set and does not match:
    - No regex match:

      ```
      Client Certificate auth logon denied, match failed
      ```

    - Field used for regex not found in the CA certificate:

      ```
      Client Certificate auth logon denied, match property
      not present
      ```

  - If **ClientCertificateMatchField** passes or is empty, the user is extracted using the **ClientCertificateAuthField** and **ClientCertificateAuthRegex**:
    - If **ClientCertificateAuthRegex** is not matched:

      ```
      Client Certificate auth logon denied, regex not
      ```

©2026 Tanium Inc. All Rights Reserved

```
matched
```

- If **ClientCertificateAuthField** is not found:

  ```
  Client Certificate auth logon denied, field not found
  ```

- If the regex matches and the field is found but the name is not valid:

  ```
  Client Certificate auth logon denied, unknown user
  ```

- Any other error or information message also starts with:

  ```
  Client Certificate auth
  ```

Start, stop, and restart Tanium services on Tanium Appliances

About this task

Manage Tanium™ Core Platform Servers and the database server with these common service control commands:

- Start
- Stop
- Restart
- Disable
- Enable

Use the TanOS menus to stop, start, or restart a service, regardless if the service is enabled or disabled.

To issue a command:

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-1` (Tanium Operations > Tanium Service Control).
3. Enter the line number of the service that you want to manage to view the service commands.

©2026 Tanium Inc. All Rights Reserved

```
          >>> Tanium Operations -> Tanium Service Control -> Service <<<

   Service          State       Status
   taniumserver      enabled     running

        1: Start service
        2: Stop service
        3: Restart service
        4: Disable service
        5: Enable service
        6: Status Details

        R: Return to previous menu

--------------------------------------------------------
```

4. Enter the number associated with the service control command to issue it.

Manage Tanium Core Platform settings on Tanium Appliances

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-2` (Tanium Operations > Configuration Settings).
3. Enter the line number for the Tanium Core Platform Server on which to modify settings.
4. Use the menu to view and edit settings. Enter the line number for a setting to edit that setting, or enter `A` to add a new setting.

Next steps

Tip: For a reference of Tanium Core Platform Server settings, see Reference: Deployment-related Tanium Core Platform settings in an Appliance deployment on page 632.

©2026 Tanium Inc. All Rights Reserved

Note: Some changes to settings, such as changing the **ServerPort** setting, require you to restart the service for the modified Server for the change to take effect. For more information, see Start, stop, and restart Tanium services on Tanium Appliances on page 313.

Manage the TDownloader configuration on Tanium Appliances

Tanium Downloader (TDL) is a utility that the Tanium Core Platform uses to download files from other servers, including updates from content.tanium.com.

Add an authentication user for TDownloader

About this task

Some servers require user authentication. If necessary, add user credentials for the Tanium Server TDownloader instance and the Module Server TDownloader instance.

Tip: You can use Tanium Console to manage authentication certificates for remote sources. For more information, see Managing remote authentication.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-2` (Tanium Operations > Configuration Settings).
3. Enter `3` (Tanium Server TDL Auth User) or `7` (Tanium Module Server TDL Auth User) and follow the prompts to configure user credentials for the server URL or Windows file share from which you want to download files.

```
------------------------------------------------------


>>> Tanium Operations -> Configuration Settings <<<


Note: Some settings may require a service restart to take effect.


        1: Edit Tanium Server Settings
        2: Edit Tanium Server TDL Settings
        3: Add Tanium Server TDL Auth User
```

©2026 Tanium Inc. All Rights Reserved

```
        4: Add Tanium Server TDL Auth Cert


        5: Edit Tanium Module Server Settings
        6: Edit Tanium Module Server TDL Settings
        7: Add Tanium Module Server TDL Auth User
        8: Add Tanium Module Server TDL Auth Cert

        9: Edit Tanium Zone Server Settings
        11: Edit isolated subnets list
        12: Edit separated subnets list

        13: Control RedHat CA Cert

        R: Return to previous menu  RR: Return to top

-------------------------------------------------------


 TanOS Version:1.9.1

 Please select: 7
 URL: https://www.test.com/share
 Username: taniumsvc
Password:
Password (confirm):
```

Note: The URL field can contain the path for a Windows file share, such as \\tam.local\dc1\share. For file access using Tanium, read-only permissions are sufficient. If you want to share files from a Windows share location, you must provide read-write permissions at a minimum. For more information about file and share permissions, see the Microsoft Windows documentation.

Note: For security reasons, Tanium does not support hidden shares, such as c$.

4. Review the resulting configuration.

Edit TDownloader settings

©2026 Tanium Inc. All Rights Reserved

About this task

Use this menu to add and edit settings for the Tanium Server TDownloader instance or the Module Server TDownloader instance. For example, edit the **LogVerbosityLevel** setting to adjust the log verbosity, or if your deployment uses proxies and contains only IPV6 addresses, add the ForceIPV6 setting to force the TDownloader to resolve proxy addresses as IPV6.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-2` (Tanium Operations > Configuration Settings).
3. Enter `2` to show the TDL settings.

```
------------------------------------------------------


>>> Tanium Operations -> Configuration Settings -> Edit <<<


   Editing: Tanium Server Downloader Settings


 # Line Content


 1 LogVerbosityLevel 41
 2 TrustedCertPath /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
 3 TrustedHostList ts1.tam.local,localhost,127.0.0.1,ts2.tam.local


A: Add a line
R: Return to previous menu


Please select a line number or menu item:
```

   - To add a new setting, enter `A` and follow the prompts to enter a key-value pair.
   - To edit a setting, enter the line number of the setting, enter `E`, and type in the new value of the setting.
   - To delete a setting, enter the line number of the setting, and enter `D`.

   You can configure the following settings for TDownloader. For the full list of deployment-related settings, see Deployment-related settings reference on page 633.

©2026 Tanium Inc. All Rights Reserved

Platform settings used with TDownloader

Settings	Platform components	Guidelines
BypassCRLCheckHostList	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 this setting 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 Appliance. For more information, see Configuring proxy server settings.
BypassProxyHostList	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 this setting 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 proxy server settings.
ForceIPV6	Tanium Server	In deployments where traffic between Tanium Core Platform Servers and

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
	Module Server TDownloader	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 Appliance and Windows deployments. The setting is hidden by default and its default value is `0`. Contact Tanium Support for guidance before adding this setting (see Contact Tanium Support on page 510). For more information about proxy server settings, see Configuring proxy server settings on page 150.
LogVerbosityLevel	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 Logging levels on page 512. **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.
ProxyPassword	Tanium Server Module Server TDownloader	For a proxy server that requires authentication, enter the password of the ProxyUserid user that establishes a connection with the proxy server. Configure this setting according to the infrastructure and server type: Tanium Appliance: Configure this setting in the TDownloader

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
		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 proxy server settings .
ProxyPort	Tanium Server Module Server TDownloader	Specify the proxy server listening port. Configure this setting 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 proxy server settings .
ProxyServer	Tanium Server Module Server TDownloader	Specify the IP address of the proxy server. Configure this setting 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 proxy server settings . **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 to `1` .
ProxyType	Tanium Server Module Server TDownloader	Specify the type of proxy server authentication. Configure this setting according to the infrastructure and server type: Tanium Appliance: Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. The possible values are `Basic` , `NTLM` , or `None` . Windows: Configure this setting in the Tanium Server and Module Server configurations. The possible values are `Basic` or `NTLM` .

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
		For more information, see Configuring proxy server settings .
ProxyUserid	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 proxy server settings .
TrustedCertPath	Tanium Server TDownloader	Path to the certificate file used for secure connections to the Tanium Console port.
TrustedHostList	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 proxy server settings .

Tip: You can use Tanium Console to manage proxy settings. For more information, see Configure proxy server settings.

Add an authentication certificate for TDownloader

©2026 Tanium Inc. All Rights Reserved

About this task

Tip: You can use Tanium Console to manage authentication certificates for remote sources.

For more information, see Managing remote authentication.

Servers from which you want to download files might require certificate authentication. Use this menu to add a Client certificate and key to the Tanium Server TDownloader instance or the Module Server TDownloader instance.

1. Use SFTP to copy the Client certificate file and key file to the /incoming folder.
2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `2-2` (Tanium Operations > Configuration Settings).
4. Enter `4` (Add Tanium Server TDL Auth Cert) or `8` (Add Tanium Module Server TDL Auth Cert) and follow the prompts to upload the certificate and key file and configure TDownloader to use them for the server URL from which you want to download files.

```
------------------------------------------------------


 >>> Tanium Operations -> Configuration Settings <<<


Note: Some settings may require a service restart to take effect.


         1: Edit Tanium Server Settings
         2: Edit Tanium Server TDL Settings
         3: Add Tanium Server TDL Auth User
         4: Add Tanium Server TDL Auth Cert


         5: Edit Tanium Module Server Settings
         6: Edit Tanium Module Server TDL Settings
         7: Add Tanium Module Server TDL Auth User
         8: Add Tanium Module Server TDL Auth Cert


         9: Edit Tanium Zone Server Settings
         11: Edit isolated subnets list
```

©2026 Tanium Inc. All Rights Reserved

```
          12: Edit separated subnets list

          13: Control Root CA Certs

          R: Return to previous menu  RR: Return to top

------------------------------------------------------

 TanOS Version:        1.9.1

 Please select: 4

Upload the certificate and key files into tancopy's incoming/ directory and
then provide the names of those files here to be loaded into the configuration
database.

 URL: https://cdn.redhat.com
 Certificate filename: client-certificate.pem
 Key filename: client-key.pem
```

5. Review the resulting configuration.

Manage additional authentication certificates

About this task

You can add additional authentication certificates to be used by TDownloader and other connections from Tanium solutions. For example, some proxy server configurations require an intermediate certificate.

Note: Not all proxy servers require an intermediate certificate to be installed. Add the intermediate certificate only if TDownloader and Tanium modules cannot connect to external servers without it.

©2026 Tanium Inc. All Rights Reserved

Tip:

- You can use Tanium Console to manage authentication certificates for remote sources. For more information, see Managing remote authentication.
- You can include multiple certificates in the same file, such as the root certificate for your organization and the intermediate certificate for a proxy server.

1. Use SFTP to copy a certificate file and key file to the /incoming folder.
2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `2-2` (Tanium Operations > Configuration Settings).
4. Enter `13` (Control Root CA Certs) and use the menu to install the certificate.

```
          >>> Control Root CA Certs <<<

        1: proxy_intermediate.pem (Not installed)

        A: Add Root CA Cert

        R: Return to previous menu

------------------------------------------------------
```

Edit the Zone Server isolated subnets or separated subnets list on Tanium Appliances

About this task

Though isolated subnets and separated subnet configurations on Tanium Servers are synchronized to Zone Servers, you can override these settings with settings on individual Zone Servers. Use the TanOS menus to configure the isolated subnets list or the separated subnets list for Zone Servers.

Isolated subnets contain endpoints for which you want to disable Tanium Client peering. Separated

©2026 Tanium Inc. All Rights Reserved

subnets specify exceptions to the peering boundaries that the address mask configured for the Tanium Server defines. For more information, see Overview of Tanium Client peering settings.

Tip: For information about configuring isolated or separated subnets on Tanium Servers, see Configure isolated subnets and Configure separated subnets.

1. Sign in to the TanOS console of the Zone Server Appliance as a user with the `tanadmin` role.
2. Enter `2-2` (Tanium Operations > Configuration Settings).
3. Enter `11` to edit the IsolatedSubnets.txt file or `12` to edit the SeparatedSubnets.txt file.

```
            >>> Tanium TanOS -> Tools -> Edit Files -> IsolatedSubnets.txt <<<

          #: Line Content

          1: 192.168.1.0/24

          A: Add a line

          R: Return to previous menu

------------------------------------------------------
```

4. Use the menu to specify the subnet in CIDR format.

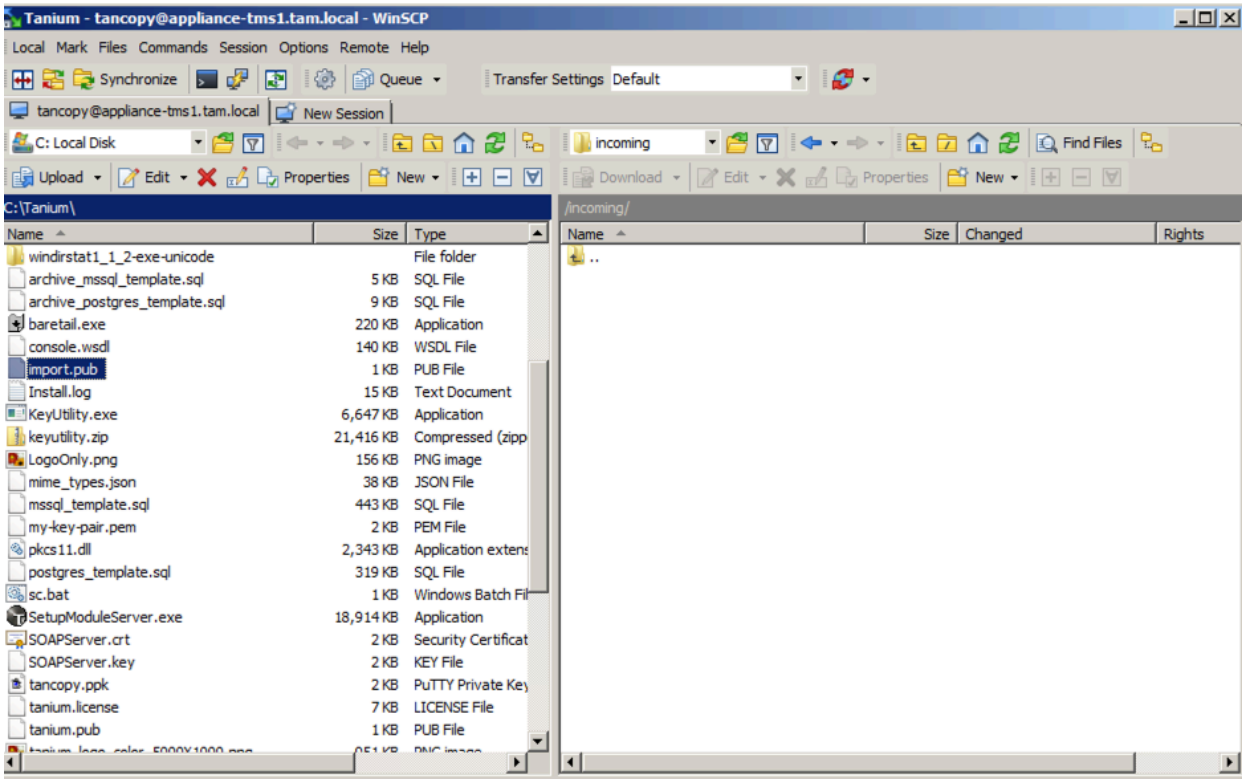
Enable import of user-created content in an Appliance deployment

About this task

The Tanium Server requires content files that are imported into Tanium Console to be signed, and the signatures are verified by public keys stored on the Tanium Server. The public keys for content developed by Tanium and delivered through content.tanium.com are included with the installation. To import user-created content, you must use a utility provided by Tanium to sign the content, and you must upload the public key from that pair to the Tanium Server. In an active-active cluster,

©2026 Tanium Inc. All Rights Reserved

perform the following steps for each active Tanium Server in the deployment.

1. Contact Tanium Support for instructions on how to download the content signing key utility (keyutility.exe). For more information, see Support for Tanium Appliances on page 510.
2. Use keyutility.exe to generate a cryptographic key pair and use it to sign the user-created content you want to import into the Tanium Server. For more information, see Authenticating content files.
3. Rename the public key file from that key pair import.pub and use SFTP to upload it to the /incoming folder of the Tanium Server Appliance.
   Figure 44. Uploading the content signing key over SFTP
   

4. Sign in to the TanOS console as a user with the `tanadmin` role.
5. Enter `2-5` (Tanium Operations > Install Content Signing Keys).
6. Enter `A` to go to the **Add Content Signing Key** menu and follow the prompts to import the public key file.

```
            >>> Tanium Operations -> Install Content Signing Certificate -> Add
Content Signing Key <<<
```

©2026 Tanium Inc. All Rights Reserved

```
 Please use the tancopy account to transfer the public key via sftp into the incoming
directory
 The filename of the public key must be import.pub

 Would you like to continue? [Yes|No]: yes

 Continue with adding content signing key.

 Found candidate file with md5 dc170530b4a5f957dd3e97b1edbd076a

 Please enter the key's owner first name: John
 Please enter the key's owner last name: Doe
 Installed new content signing key for the Tanium Server:
 SELF_John_Doe_1521239953.pub with md5 dc170530b4a5f957dd3e97b1edbd076a
 Installed new content signing key for the Tanium Module Server:
 SELF_John_Doe_1521239953.pub with md5 dc170530b4a5f957dd3e97b1edbd076a

Press enter to exit.
```


Tip: You can also use the Install Content Signing Keys menu to list and delete existing key files.

Result

You can now upload signed user-created content to the Tanium Server on the Appliance. In a Tanium Cluster, Tanium Servers write content to the shared Tanium database. Therefore, after you import content on a Tanium Server in an Tanium cluster, the content is available on the other Tanium Server.

- For information about how to use keyutility.exe to sign content, see Authenticating content files.
- For information about how to upload signed content to the Tanium Server, see Manage services and content.

Tip: Watch the tutorial about how to manage content signing keys for the Tanium Appliance.

©2026 Tanium Inc. All Rights Reserved

Manage a Tanium cluster

A Tanium cluster uses two Tanium Servers to provide continuous availability during scheduled maintenance or an outage. For more information, see Configuring a Tanium cluster on page 168.

Manually configure a Tanium cluster

Important: Use an Appliance Array for easy setup and management of the Appliances in your deployment. When you install two Tanium Server roles in an Array, TanOS automatically configures a Tanium cluster. For more information about how to install an Appliance Array, including the necessary Tanium Appliance server roles, see Installing and managing an Appliance Array on page 158.

If you are unable to use the Appliance Array, see Tanium Appliance Deployment Guide (version 1.7.2): Configure a Tanium cluster for instructions to manually configure a Tanium cluster.

Perform database failover

1. On the secondary, or passive, Appliance, sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-B-F` (Tanium Operations > Cluster Configuration > Database Server Failover).
3. Follow the prompts to perform the failover to the secondary Appliance database and promote the secondary Appliance database to primary.
4. To demote the original primary Tanium Server database to the passive role, on the original primary Appliance, reinitialize replication. For more information, see Reinitialize replication on page 329.

Check replication status

1. On either Tanium Server in the cluster, sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-B` (Tanium Operations > Cluster Configuration).
3. Enter `S` to display the replication status between the cluster members.

©2026 Tanium Inc. All Rights Reserved

Tip: To see the database replication history, see View database replication status and history on page 455.

Reinitialize replication

About this task

You can reinitialize replication on the passive, or secondary, database, which removes all existing database contents and replaces them with the contents from the currently active database. After you perform a failover, you can initialize replication from the newly active secondary Appliance to the original primary Appliance by performing this procedure on the original primary Appliance.

1. On the Tanium Server Appliance with the passive database, sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-B-E` (Tanium Operations > Cluster Configuration > Reinitialize Replication).
3. Follow the prompts to reinitialize replication between the cluster members, and, if applicable, demote the original primary Tanium Server.

Manage the standby Module Server

If you add two Module Servers to your Appliance Array, you can schedule a Module Server sync to use the second Module Server as a standby.

Schedule sync jobs

About this task

The Module Server sync job schedule determines the times and frequency at which files are copied from the active Module Server to the Standby Module Server.



Important: The Module Server sync stops services on the Tanium Module Server to capture the module data. During this time, users can still access Tanium and ask questions, but the module workbenches are unavailable until the backup completes.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Schedule a Module Server sync to run at least weekly during a time that has minimal impact. Avoid running the sync too frequently in order to minimize interruptions in the use of Tanium modules.

Note: The Module Server sync that you schedule manages synchronization of Module Server files. Replication of the database is separate and occurs automatically. To view the status of database replication, see View detailed status for Module Server sync on page 330.

1. Sign in to the source Module Server Appliance as a user with the `tanadmin` role.
2. Enter `2-D-5` (Tanium Operations > Module Server Sync > Schedule TMS Sync).
3. Use the menu to configure the schedule:
    a. Enter `1` or `2` to toggle the enabled/disabled status for the schedule.
    b. Enter `4` or `5` to set the schedule by days of the month or days in a week.
        - A comma (,) indicates separate days. For example, `1,15`.
        - A hyphen (-) indicates contiguous days. For example, `mon-fri`.
        - Specify days of the week with three-letter abbreviations: sun, mon, tue, wed, thu, fri, sat.
    c. Enter `6` to set the time of day.
    d. Enter `7` to make your changes active.

View detailed status for Module Server sync

About this task

The top of the Module Server Sync menu shows configuration status and the last return code for the sync job. You can use menu `1` to view detailed status.

1. Sign in to the source Module Server Appliance as a user with the `tanadmin` role.
2. Enter `2-D` (Tanium Operations > Module Server Sync).
3. Enter `1` to view the status.

©2026 Tanium Inc. All Rights Reserved

```
Secured connectivity to remote IP 10.0.72.129 is working


  >>> Database Replication Health <<<


 Cluster Role:          Primary Server
 Cluster member:        10.0.72.129
 Sender Process:        RUNNING (pass)
 WAL Process:           walsender
 WAL Process Segment:   0/5000148
 WAL Process Status:    streaming
 Replication Active:    Yes (pass)
 Replication Lag
 In Recovery Mode:      NO (pass)
 Remote DB Address:     10.0.72.129
 Remote DB Net Latency: 1ms
 State:                 streaming
 Sync State:            async
 Backend Start:         2022-08-2622:38:21.93646+00
 Sent Log Location:     0/5000148
 Write Log Location:    0/5000148
 Replay Log Location:   0/5000148
 Flush Log Location:    0/5000148
 SSL Mode:              ON (pass)
 SSL CRL File:          ON (pass)
 Max Replication slots in postgresql configuration: 1 (pass)
 Replication slot is active (pass)
 Slot Name:             node_a_slot
 Slot Type:             physical
 Slot Active:           t
 Slot Active PID:       5257
 Slot Restart LSN:      0/5000148
Active sync state (source)


Current time: Fri Aug 26 23:07:50 UTC 2022
Last sync log:
#### Starting Module Server sync ####
```

©2026 Tanium Inc. All Rights Reserved

```
Start time: Fri Aug 26 22:47:08 UTC 2022
SYNC_ROLE 1 found

===============

2022-08-26 22:47:08 Starting 1/3: TaniumModuleServer (top)
2022-08-26 22:49:16 Finished 1/3: TaniumModuleServer (top)

===============

2022-08-26 22:51:24 Starting 2/3: Grouping directories by running services
2022-08-26 22:51:24 Finished 2/3: Grouping directories by running services

===============

2022-08-26 22:51:24 Starting 3/3: Final cleanup
2022-08-26 22:57:47 Finished 3/3: Final cleanup
End time: Fri Aug 26 22:57:47 UTC 2022
%%%% Ended Module Server sync %%%%%

Last return code: OK 2022-08-26T22:47:08
```

Promote the standby Module Server

The Module Server service on the standby Appliance is not enabled while the active Appliance is running. To make the standby Appliance active, such as in the event of a failure on the active Module Server, promote the standby Module Server. You can perform this promotion to test a planned Module Server failover or to recover a failed Module Server with a standby Module Server. For more information, see Test a planned Module Server failover or recover a failed Module Server with a standby Module Server on page 386.

Change the Tanium content manifest URL

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2`-`C`-`B` (Tanium Operations > Manage Content > Manifest URL Change).

©2026 Tanium Inc. All Rights Reserved

3. Use the menu to change the manifest URL.

Configure solution module file share mounts

Tanium™ Connect and Tanium™ Detect can write consumable files to disk. You can configure the Module Server to copy these files to a Common Internet File System (CIFS) or Network File System (NFS) share on a file server, or to an *internal share* on the Appliance itself. An internal share is a directory that the `tancopy` user can access using SFTP.

If you configure an internal share, the `tancopy` user can make an SFTP connection to the Appliance with SSH key authentication and copy files to or from the /modules/connect or /modules/detect directory (depending on which shares are configured). For information about adding SSH keys for the `tancopy` user, see one of the following sections:

- Physical Tanium Appliance: Configure SSH keys on page 60
- Virtual Tanium Appliance: Configure SSH keys on page 93
- Cloud-based Tanium Appliance: Configure SSH keys on page 130

Best Practice: When two Module Servers are deployed in an active standby configuration, file share mounts are not replicated. Configure each Module Server in the same way to maintain functionality in the event of a failover.

Add a file share mount

1. Sign in to the TanOS console on the Tanium Module Server as a user with the `tanadmin` role.
2. Enter `A-6` (Appliance Configuration > Share Configuration).
3. Enter the line number of the mount you want to create and complete the configuration to add a file share mount.

```
           >>> Appliance Configuration -> Share Configuration -> Create Mount
Connect <<<
```

©2026 Tanium Inc. All Rights Reserved

```
Before configuring shares, ensure you have the following information at hand,
depending on the type of share you are configuring.

CIFS:
- hostname/IP of the server (do not use a cname if the server is Windows OS)
- share name
- credentials (username, domain, password)

NFS:
- hostname or IP of the server
- export name

Internal:
- tancopy (SFTP) access to the appliance

Would you like to continue? [Yes|No]: yes

Please enter share type (cifs/nfs/internal): cifs
Please enter the servername for mount: 192.168.154.219
Please enter the share name / export: connect
Please enter the user name: bernd
Please enter the domain name: tam.local
Please enter the password (will not be displayed):
Checking if CIFS mounting would be successful (might take a while)
Mount successfully established, creating permanent connection
Added CIFS share permanently.
Press enter to exit
```

List a file share mount

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-6-A` (Appliance Configuration > Share Configuration > List Mounts).

Test a file share mount

1. Sign in to the TanOS console on the Tanium Module Server as a user with the `tanadmin`

©2026 Tanium Inc. All Rights Reserved

role.

2. Enter `A-6` (Appliance Configuration > Share Configuration).
3. Enter `B` to test file share mounts.

```
            >>> Appliance Configuration -> Share Configuration -> Test Mounts <<<

Share for connect service mounted, we expect write access to succeed:
Write test successful
Read test successful

Share for detect service mounted - we expect write access to succeed:
Write test successful
Read test successful



Press enter to exit
```

Manage advanced Tanium Core Platform features on Tanium Appliances

Use the Advanced Operations menu to make additional changes that might be required in atypical environments.



Important: Contact Tanium Support on page 510 before you change advanced options.

Enable UseTBBAllocatorStats

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-X` (Tanium Operations > Advanced Operations).
3. Enter `2` and follow the prompts to enable UseTBBAllocatorStats.

©2026 Tanium Inc. All Rights Reserved

```
           >>> Tanium Configuration -> Advanced Menu -> Toggle UseTBBAllocatorStats
<<<

 Toggling this setting will trigger a service restart - which might take a long time!

 Current setting: disabled

 Would like to enable UseTBBAllocatorStats? [Yes|No]: yes
 Stopping tanium service (this might take a very long time)...
 Enabling UseTBBAllocatorStats...
 Restarting daemon...
 Restarting tanium server service...
 Finished toggling setting and successfully restarted tanium service.

 Press enter to continue
```

Upload an HTML banner

About this task

You can add a page to provide information or warnings to users before they sign in to Tanium Console. For complete details, see Customizing the Console and Interact. You can use the TanOS Advanced Operations menu to upload the banner.html file.

1. Use SFTP to upload the HTML banner file to the /incoming folder.
2. Enter `2-X` (Tanium Operations > Advanced Operations).
3. Enter `4` and follow the prompts to copy the HTML banner file to the appropriate location.

©2026 Tanium Inc. All Rights Reserved

Configuring Appliance connections

You are prompted to configure basic host and network settings when you complete the initial configuration. Use the **Appliance Configuration** menu to modify the configuration as necessary.

> **Note:** Changes to the network configuration cause network services to restart. If you connect over a remote SSH connection and change the configuration for the interface with which you are connected, your SSH connection terminates.

Modify the host name and DNS configuration

Host, domain, DNS server, and /etc/hosts settings are configured during the initial setup. If necessary, you can use the **Hostname/DNS Configuration** menu to make changes.

> **Note:** Contact Tanium Support if you plan to change the Tanium Server host name. Tanium Support needs the new host name to update the Tanium license for you. For more information, see Support for Tanium Appliances on page 510.

Modify the host name

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-1` (Appliance Configuration > Hostname/DNS Configuration).
3. Enter `1` and follow the prompts to change the host name, which must be a fully qualified domain name (FQDN).

```
           >>> Appliance Configuration -> Hostname/DNS Configuration -> Hostname
<<<
```

©2026 Tanium Inc. All Rights Reserved

```
Current hostname (FQDN):
ts1.test.tanium.local

Please contact Tanium Support prior to changing the hostname of an
active TanOS appliance!

New FQDN: ts1.test.tanium.local
```

Important: Use an FQDN that is accessible from any computer from which a user accesses Tanium Console.

Modify the DNS server

About this task

Tip: You can change the DNS servers on all Appliances in the Array at the same time from the Array Manager.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-1` (Appliance Configuration > Hostname/DNS Configuration).
3. Enter `2` and follow the prompts to update the DNS servers.
4. (Array Manager only) Enter `y` to make the updates on all Array Members, or `n` to make the updates only on the current Appliance.
5. Enter `y` to complete the changes.

```
           >>> Appliance Configuration -> Hostname/DNS Configuration -> Domain Name
<<<

Currently configured name server(s):
192.168.76.2
```

©2026 Tanium Inc. All Rights Reserved

```
Would you like to change the DNS Server address? [Yes|No]: yes
Please provide the first DNS server address: 10.10.10.10
Please provide second DNS server address:
This appliance can manage other members in the array.
Do you want to update all array members? [Y/n]: y

Setting nameserver 1: 10.10.10.10
Setting nameserver 2:
Update all members: Yes

Do you want to continue? [y/n]: y
Running command on 192.168.15.121: set nameservers 10.10.10.10
Running command on 192.168.15.122: set nameservers 10.10.10.10
Running command on 192.168.15.123: set nameservers 10.10.10.10
Running command on 192.168.15.124: set nameservers 10.10.10.10
Running command on 192.168.15.125: set nameservers 10.10.10.10
Done updating DNS entries
Press enter to continue
```

Modify the hosts file

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-1` (Appliance Configuration > Hostname/DNS Configuration).
3. Enter `3` and use the **manual_hosts** menu to update the /etc/hosts file.

```
  >>> Tanium TanOS -> Tools -> Edit Files -> manual_hosts <<<

#### Contents of /etc/hosts #####
# Generated 2022-03-07 19:06:46
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

# This appliance
10.20.70.11 ts1.test.tanium.local ts1
```

©2026 Tanium Inc. All Rights Reserved

```
# Appliance array members
10.20.70.12 ts2.test.tanium.local ts2
10.20.70.13 tms1.test.tanium.local tms1
10.20.70.14 tms2.test.tanium.local tms2
10.20.70.15 tzs.test.tanium.local tzs

# Manual entries
# No manual entries
################################

             file is empty

          A: Add a line

          R: Return to previous menu  RR: Return to top
```

Enable or disable a network interface, change the IP address, or modify the MTU size

About this task

Note: If you are changing the IP addresses of multiple Appliances, start with the primary Tanium Server.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-2-1` (Appliance Configuration > Networking > Network Interfaces).
3. Enter the line number of the interface that you want to configure to go to the selected **Network Interface** menu.

```
           >>> Appliance Configuration -> Networking -> Network Interface <<<

Current settings:
```

```
  Interface: ens160eno12399
  IPv4 Address: 10.10.10.60/24
  Default IPv4 Gateway: 10.10.10.2
  IPv6 Address: fe80::20c:29ff:feed:26f/64
  IPv6 Gateway:
  User Desired Setting (State): UP
  Interface Status (Link): UP
  Carrier Detected: YES
  Connected Speed: 10000Mb/s Full:
  Advertised Speeds: 1Gbps 10Gbps

         I: Manage IP address
         M: Manage MTU Size
         U: Set Interface Up
         D: Set Interface Down
         S: Set Advertised Speeds

         R: Return to previous menu  RR: Return to top

-------------------------------------------------------
```

4. Use the menu to change the IP address, change the MTU size, or enable or disable the network interface.
5. If you changed the IP address of the Appliance, you must also update the IP address in the Appliance Array:

   Note: You must perform this set of steps separately, even if you are changing the IP address of the Array Manager itself.

   a. Sign in to the Array Manager a user with the `tanadmin` role.
   b. Enter `1-M` (Tanium Installation Menu > Manage Appliance Array).
   c. Enter the line number for the Appliance on which you changed the IP address.
   d. Enter `I` to update the IP address of the Array member.

```
          >>> Installation -> Appliance Array -> Manage Member <<<
```

```
Address:            10.10.10.71
Serial Number:      f74f4d5b36bfe8c7ebfd8f7a13ae9618
Name:               tanos-tms2
FQDN:               tanos-tms2.local
TanOS Version:      1.9.1
Role:               Tanium Module Server (Standby)
TaniumModuleServer: 7.9.3.1234
Pending Role:       No Change
Array Manager:      No

  A: Assign Role: All-in-One
  T: Assign Role: TaniumServer
  M: Assign Role: TaniumModuleServer
  Z: Assign Role: TaniumZoneServer
  U: Cancel Pending Role Change

  D: Delete Member
  I: Update IP Address
  N: Measure Data Transfer Rate

  R: Return to previous menu  RR: Return to top

------------------------------------------------------------------------
--

TanOS Version:1.9.1

Please select: I

This operation will update the array's records of the remote appliance's IP
address. It does not change the network settings on the remote appliance.
First
change the network settings on the remote appliance and then use this
operation to inform the array members of the change.

Please enter the remote appliance IP address: 10.10.10.119
```

©2026 Tanium Inc. All Rights Reserved

Note: If you have changed the IP address of multiple Array members, you might see errors when you update the IP address of each member on the Array Manager. Updating the IP address of the final Array Member resolves these temporary errors.

Note:

- You must also update the DNS records in your domain configuration for any Appliances that have new IP addresses. For the specific steps, review the documentation from your domain provider.
- Test the functionality of the Tanium solutions in your environment after you change server IP addresses. Some solutions have settings that might need be changed. For more information, see the user guide for each solution. For example, if you change the IP address of the Module Server, and the **Fully Qualified Domain Name** configured for the Module Server in the **Endpoint Connection** settings for Direct Connect is set to only the old IP address Module Server, you must update that setting in Direct Connect before you can connect to an endpoint using Direct Connect functionality. (For more information about that specific setting, see Configure Endpoint Connection settings.)

Modify advertised Ethernet speeds (physical Tanium Appliance only)

About this task

In some environments, you might need to modify the Ethernet speeds that the network interface controller (NIC) advertises for auto-negotiating connections.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-2-1` (Appliance Configuration > Networking > Network Interfaces).
3. Enter the line number of the interface that you want to configure to go to the selected **Network Interface** menu.

©2026 Tanium Inc. All Rights Reserved

```
           >>> Appliance Configuration -> Networking -> Network Interface <<<

 Current settings:
   Interface: ens160eno12399
   IPv4 Address: 10.10.10.60/24
   Default IPv4 Gateway: 10.10.10.2
   IPv6 Address: fe80::20c:29ff:feed:26f/64
   IPv6 Gateway:
   User Desired Setting (State): UP
   Interface Status (Link): UP
   Carrier Detected: YES
   Connected Speed: 10000Mb/s Full:
   Advertised Speeds: 1Gbps 10Gbps

          I: Manage IP address
          M: Manage MTU Size
          U: Set Interface Up
          D: Set Interface Down
          S: Set Advertised Speeds

          R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

4. Enter `S` to configure the advertised Ethernet speeds.

```
           >>> Appliance Configuration -> Networking -> Interface Speed (eno12399)
<<<

The following speeds can be used for autonegotiation. Select the number
corresponding to the desired speed to toggle if it will be advertised.

WARNING: Changing this setting could interrupt the network
connection or leave the network interface unable to successfully negotiate
carrier. Toggling one of these will take effect immediately!
```

©2026 Tanium Inc. All Rights Reserved

```
    [X] - Speed will be advertised for autonegotiation
    [ ] - Speed will not be advertised for autonegotiation

 1: [X] 1Gbps
 2: [X] 10Gbps
 3: [X] 25Gbps

 E: Enable all supported speeds

 R: Return to previous menu  RR: Return to top

-------------------------------------------------------
```

Reset a network interface

About this task

Use the Reset Interface option to remove the IP address and other configuration from a network interface, restoring it to a default unconfigured state. After the reset, the interface comes back up with no IP address assigned.

> **Important:**
>
> If you are connected to the Appliance over the interface that you reset, your session is disconnected.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-2-1` (Appliance Configuration > Networking > Network Interfaces).
3. Enter the line number of the interface that you want to reset.
4. Enter `X` and confirm the prompt to reset the interface.

Set up an IPsec tunnel

About this task

©2026 Tanium Inc. All Rights Reserved

Use IPsec to ensure end-to-end security between two Tanium Server Appliances. An IPsec tunnel is automatically configured when you install an Appliance Array on page 158.

1. Start two SSH terminal sessions so you can copy and paste between them:
   - First Tanium Server Appliance
   - Second Tanium Server Appliance
2. Sign in to each of the Tanium Server Appliances as a user with the `tanadmin` role and enter `A-2-2` (Appliance Configuration > Networking Configuration > IPSEC).
3. On the second Appliance, copy the IPsec host key to the clipboard:
   a. From the **IPSEC** menu, enter `1` to view the local IPsec host key.

```
            >>> Appliance Configuration -> IP -> IPSEC -> Display Host Key
<<<

 Local Host Key Information:

0sAwEAAbnlzZ6venWVMdFLWEHGNEd6bMnNMVBkH+Ye3f7y360CbeBa6SSTOzI0NqHNOCnTWBDEMVWp
fE3Dk/2feh1rjH
pNpMdhknhO5+8B47Q9HsH7DEGN4VoybNtH42xVKnApD51CGkH4Ns2o7JfHLUo+Dkv1Tw03b2vGNs/
m//bLcUHwFKQLd1
xKNOkR4BhbQ0d7AVctY5tIKzhA8BS+aIkI7XuKCfy9YEMPOgyWVvPY2UTRXwvTcvK0+JHyxuu0UL6y
vIVKeV1H8ohSbr
DD213ut8lDQJ6KbJQ5Zl/
x3A0LrgTg8l0jNCGIB6d0oPiKpL7vePApViTTAgGh2l2b3KiwZldH6fof/h+dADWWuwcgge
k4NzyI1DRtBbdA5bWuAEYdzC3038/N++FQnKJ5QRXe+b9O9aHf8VTUjZbFWc/
5Q0wYeQ1GoTny1OiWArEDJUoW8IYUQI
qPvmItG76zKwfIL1z07dMIAs71W3L/
X0QthogKCAYYawktpgukqJ3HHGkAWQFHgHKoJxVhJeF4Lw46G2OQaO1Eg5LHzY
GS6BnEUG896yXvlxZJWZgG7Y9yj3mIea9ltV7/
ifPIbXoMRkWMYbnK81biqw1j2yPJfj6MrHet5LrI+kUpA8FUCgY1tI
dQPdXMU6F0K+wWapSzCtbs8D343LYOMmiKgP2rZpFPOEc9

 Press enter to continue
```

   b. Copy the key to the clipboard.

©2026 Tanium Inc. All Rights Reserved

4. On the first Appliance, from the **IPSEC** menu, enter `3` and follow the prompts to configure this side of the IPsec tunnel. When prompted, paste the IPsec host key for the second Appliance.

```
           >>> Appliance Configuration -> IP -> IPSEC -> Configure IPSEC <<<

 To configure IPSEC connectivity between TanOS systems the following information is
required

 - Local IP address
 - Remote IP address
 - Remote host key

 Any exiting configuration will be overwritten!

 Would you like to continue with IPSEC configuration? [Yes|No]: yes
 Please provide the local ip address: 192.168.76.101
 Please provide the remote ip address: 192.168.76.102
 Please provide the remote hostkey:
0sAwEAAbnlzZ6venWVMdFLWEHGNEd6bMnNMVBkH+Ye3f7y360CbeBa6SSTO
zI0NqHNOCnTWBDEMVWpfE3Dk/
2feh1rjHpNpMdhknhO5+8B47Q9HsH7DEGN4VoybNtH42xVKnApD51CGkH4Ns2o7JfHLUo+
Dkv1Tw03b2vGNs/
m//bLcUHwFKQLd1xKNOkR4BhbQ0d7AVctY5tIKzhA8BS+aIkI7XuKCfy9YEMPOgyWVvPY2UTRXwvTcvK
0+JHyxuu0UL6yvIVKeV1H8ohSbrDD213ut8lDQJ6KbJQ5Zl/
x3A0LrgTg8l0jNCGIB6d0oPiKpL7vePApViTTAgGh2l2b3K
iwZldH6fof/h+dADWWuwcggek4NzyI1DRtBbdA5bWuAEYdzC3038/N++FQnKJ5QRXe+b9O9aHf8VTUjZbFWc/
5Q0wYeQ1Go
Tny1OiWArEDJUoW8IYUQIqPvmItG76zKwfIL1z07dMIAs71W3L/
X0QthogKCAYYawktpgukqJ3HHGkAWQFHgHKoJxVhJeF4
Lw46G2OQaO1Eg5LHzYGS6BnEUG896yXvlxZJWZgG7Y9yj3mIea9ltV7/
ifPIbXoMRkWMYbnK81biqw1j2yPJfj6MrHet5Lr
I+kUpA8FUCgY1tIdQPdXMU6F0K+wWapSzCtbs8D343LYOMmiKgP2rZpFPOEc9
```

5. On the first Appliance, copy the IPsec host key to the clipboard:
    a. From the **IPSEC** menu, enter `1` to view the local IPsec host key.

©2026 Tanium Inc. All Rights Reserved

b. Copy the key to the clipboard.

6. Go to the second Appliance and complete the IPsec configuration:
   a. From the **IPSEC** menu, enter `3` and follow the prompts to configure the IPsec tunnel on the second Appliance. When prompted, paste the IPsec host key for the first Appliance.
   b. Enter `6` to test the connection from the second Appliance.

```
           >>> Appliance Configuration -> IP -> IPSEC -> Test IPSEC <<<

Testing secured connectivity to the remote ip.

Secure connectivity to remote IP 192.168.76.101 is working


Press enter to continue
```

7. Go back to the first Appliance and enter `6` to test the connection.

View the IPSEC configuration for an Appliance

1. Sign in to the Appliance as a user with the `tanadmin` role.
2. Enter `A-2-2` (Appliance Configuration > Networking Configuration > IPSEC).
3. Enter `2` to display the IPSEC configuration.

```
           >>> Appliance Configuration -> IP -> IPSEC -> Display IPSEC Configuration
<<<

Current configuration:

conn tanos
  left=172.16.115.122
pcjs1MBKlrG7mgzWU7rVHvH0o/ZGoUOCn1mvtANoYEODzwbSHT1WM+ZtndzwcyAj/V1sEVs
  leftrsasigkey=AAAAB3NzaC1yc2EAAAADAQABAAABgQCWIw43lJhtp9VG1phnrjy4exh
2L1k1pG2yTFggzVEjl/dI9w7pfKJworsp3oYW8XvMiVtN4k7MnMzjLu7BNCZB93iwdokWxi
```

```
qEcK9BteS2CjXWIgkriRA0fwLt2vDtY0OtKVsyKyZkqIE0VDNuHNj2XOgSorzvup9un71eG
Jah9A6FcOWfH/xd6XyAr4ytwDdCi8a2zRTrX28vQr0S9sKHstZxxRGOUQydYwOQDfobRufi
7XGixUsIWDHj5PI2PtzW3XOObn6m4YP6pRLW0X8FzAnT9Ad23cPtEkrtGNlmL91vpkTMKB3
xFcyAAhmbJzmOT+/B3fharzA3inVFRY/ou5lKcfTw1leglf1u5KQgwrOLyHMqeL3MJWYsxH
B/Wcu0tDXONQjWkjFWwWEw4yg2QgfKHwU3rjH31Md8PqRvU+cadMLNAM+ZOUyWj+aH5R9vt
9PLtM3tKSxe3M4DuwP73dDzMv3by/8inSBtLmIyDyTOjHZgEJu91I4t9Qq0h4U

  right=172.16.115.123
  rightrsasigkey=AAAAB3NzaC1yc2EAAAADAQABAAABgQDj8h1WKKKGw7KVHTFIPA8ATq
eGwXVzmjlcLBgJb8MnIpnp3GMCoxHw0t+UeITkTi4hvbUae/wmOR92zTn9n8GR7R+T/u7j3
NRFY/BNIRiOCwOhxkfHfP0ALYAkFKrAo9jA3F7DFR8ey9gXCX1ftzjU+EKFx/asy9YhIqWI
hzpRs86ImfaRKSDZZTZrR+Fp3Bo2ja2hdWcTdmBI77JprcTFiYPg3gDXd7yJ1w6LQyEnWcs
dqHPJCDQ9KrB0WyDZ/3cEdpV9nC5I+4Ysi4jAuxqjY8kElrbzKJZ5045T3UHb2Rafc7Myn8
Ecb3OseBPY/IFmXuXYztZQy12q7M7VeAHoLhtkgXPwKxXYNoPpg7qtWXMOksxFiQutdYKHC
euzzcUHdP+k8/oS7jg7EcQG6xxxCOh3jhO73Fx0frgBHSEisUxSSHOTFKIhulwFiMRZDp/O
yaI2xA7WY0FtBtLTAGu1vUKMrV/zHIEg4tTGU5m4FS+9nG9BlbEki1ePJ8Ilpls

  authby=rsasig
  # load and initiate automatically
  auto=start
  encapsulation=auto
  salifetime=230m
  ikev2=insist
  ike=aes_gcm256-sha2;dh21


 Press enter to continue
```

Modify the routing configuration

About this task

You can add a static route, if necessary.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-2-3` (Appliance Configuration > Networking > Routing).

©2026 Tanium Inc. All Rights Reserved

3. Use the menu to manage the routing table.

Configure NIC teaming (physical Tanium Appliance only)

The Tanium Appliance supports active/passive network interface controller (NIC) teaming. Active/passive NIC teaming allows multiple interfaces to be placed in a group to support NIC failover. When you configure the NIC team, you must select interfaces of the same type.

Create NIC team

About this task

To create a NIC team, there must be two NICs available for teaming. If you have a physical Tanium Appliance, make sure to enable the tanremote user on page 62 and configure the iDRAC interface on page 420.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-2-T` (Appliance Configuration > Networking > NIC Teaming).
3. Enter `A` and follow the prompts to create the NIC team configuration.

Result

Note: When you create a NIC team, the system automatically assigns a MAC address from one of the NICs to the team. The NIC Teaming menu displays the details for each NIC team, including the assigned MAC address.

Manage NIC team

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-2-T` (Appliance Configuration > Networking > NIC Teaming).
3. Enter the line number of the NIC team that you want to manage.
4. Use the **NIC Team** menu to change the IP address, delete the NIC team, or view the status.

```
>>> Appliance Configuration -> Networking -> NIC Team <<<
```

©2026 Tanium Inc. All Rights Reserved

```
Current settings:
  Interface: team1
  IPv4 Address: 10.10.10.61/24
  Default IPv4 Gateway: 10.10.10.2
  IPv6 Address:
  IPv6 Gateway:

        C: Change Team IP Address
        D: Delete
        S: Show Status

        R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

Modify the NTP configuration

About this task

Tip: You can change the NTP configuration on all Appliances in the Array at the same time from the Array Manager.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-3` (Appliance Configuration > NTP Configuration).
3. Enter the line number of the existing NTP server to modify or remove, or enter `A` to add a new NTP server.
4. Follow the prompts to add, modify, or remove the NTP server. To add or modify an NTP server, enter the NTP server address and whether the server requires authentication. If the NTP server requires authentication, enter the NTP key ID, NTP key type, and NTP key at the prompts.
5. (Array Manager only) Enter `y` to make the updates on all Array Members, or `n` to make the updates only on the current Appliance.

©2026 Tanium Inc. All Rights Reserved

6. Enter `y` to complete the changes.

```
            >>> Appliance Configuration -> NTP Configuration <<<

Currently configured ntp servers:
   0.pool.ntp.org

Current NTP Status: Normal

Current NTP Peers:
   ntpserver-1.walkeritg.org

  1: 0.pool.ntp.org

  A: Add NTP server

  R: Return to previous menu  RR: Return to top

--------------------------------------------------------------------------------

Please select: A
Please enter the NTP server address: 1.pool.ntp.org
Does this server require authentication? [y/N]: n
This appliance can manage other members in the array.
Do you want to update all array members? [Y/n]: y
Save changes and restart NTP? [y/n]: y
Running command on 192.168.15.121: set ntp 0.pool.ntp.org 1.pool.ntp.org
Running command on 192.168.15.122: set ntp 0.pool.ntp.org 1.pool.ntp.org
Running command on 192.168.15.123: set ntp 0.pool.ntp.org 1.pool.ntp.org
Running command on 192.168.15.124: set ntp 0.pool.ntp.org 1.pool.ntp.org
Running command on 192.168.15.125: set ntp 0.pool.ntp.org 1.pool.ntp.org
Done updating NTP settings
Press enter to continue
```

©2026 Tanium Inc. All Rights Reserved

Change from a static IP address to DHCP (virtual Tanium Appliance only)

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A` (Appliance Configuration).
3. Enter `7` and follow the prompts to use DHCP.

©2026 Tanium Inc. All Rights Reserved

Configuring Appliance security

The subsequent topics in this section provide information about controlling inbound SSH and HTTPS access, including SSH banner text and fingerprints, and about configuring LDAPS or StartTLS authentication and security policy rules. They also cover hardening the Appliance with FIPS 140-3 mode, SELinux, and AIDE reporting, setting the menu timeout, and managing the RAID controller security key and the GRUB key.

Manage inbound SSH access rules

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A`-`A`-`2` (Appliance Configuration > Security > Manage SSH).
3. From this menu, you can add or delete rules that restrict SSH access to hosts from specified subnets only.
    - Enter `A` and follow the prompts to add a new rule.
    - Enter the line number of an existing rule and follow the prompts to delete the rule.

Configure SSH banner text

About this task

You can add custom SSH banner text to TanOS.

1. Use SFTP to copy a file named banner_ssh.txt to the /incoming folder.
2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `A`-`A` (Appliance Configuration > Security).
4. Enter `3` to add the banner file.

```
           >>> Appliance Configuration -> Security -> Manage SSH -> Configure SSH
Banner <<<
```

©2026 Tanium Inc. All Rights Reserved

```
Uploaded banner_ssh.txt file found in tancopy incoming.
TanOS will replace the existing banner with the new file.
Log out of ssh and re-connect to view the banner.

Banner file copy successful

Press enter to continue
```

View SSH fingerprints

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A`-`A` (Appliance Configuration > Security).
3. Enter `4` to view the SSH fingerprints.

```
            >>> Appliance Configuration -> Security -> Manage SSH -> Display SSH
Fingerprints <<<

2048 SHA256:Mb6VUEjcXGBd+d+gVF3isQ2zPztAY1KkYH17xTB+vOQ= /etc/ssh/
ssh_host_rsa_key.pub (RSA)
256 SHA256:L0IXFHyMonAdPYs/ohgDVwdO23wDi0zCo4bRW4Gafog= /etc/ssh/
ssh_host_ecdsa_key.pub (ECDSA)
256 SHA256:KT7IGcJHsm3ZO+iOXrxCUk0Wuvdl2/NoybHvHT5al3Q= /etc/ssh/
ssh_host_ed25519_key.pub (ED25519)

Press enter to continue
```

Manage inbound HTTPS access rules

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A`-`A`-`6` (Appliance Configuration > Security > Manage HTTPS).
3. From this menu, you can add or delete rules that restrict HTTPS access to hosts from specified subnets only.
    - Enter `A` and follow the prompts to add a new rule.

©2026 Tanium Inc. All Rights Reserved

- Enter the line number of an existing rule and follow the prompts to delete the rule.

Configure LDAPS or StartTLS

If you have requirements to use the LDAPS or StartTLS protocol for the LDAP sync connection to the back-end LDAP server, you must import the LDAP server root certificate authority (CA) certificate and then enable the LDAPS/StartTLS configuration. You can import multiple root CA certificates if necessary. The certificates must be in PEM format. On the Appliance, you have the option to paste the contents of the LDAP server root CA certificate or import the file. You do not have to do both.



Note:

- The LDAP server root CA certificate must be able to validate the LDAP server certificate. The subject field of the LDAP server certificate must match the host field in the LDAP configuration.
- Secure certificates for Server and Client systems are required. The certificates have a minimum bit size of 2048 for RSA and 256 for ECDSA. To check key sizes, use OpenSSL from a CLI. If your Tanium license includes Tanium Certificate Manager, see View short keys for the steps to check the key sizes in your environment.



Important: In a clustered environment, upload the LDAP server CA certificate to both Tanium Servers.

Paste the LDAP server root CA contents

About this task



Note: To add multiple CA certificate files, put all certificates in one file and paste them in them in together.

1. Sign in to the TanOS console as a user with the `tanadmin` role.

©2026 Tanium Inc. All Rights Reserved

2. Enter `A-A-A` (Appliance Configuration > Security > LDAP CA Certificate Management).
3. Enter `1` and follow the prompts to paste the contents of the LDAP server root CA certificate file.

```
            >>> Appliance Configuration -> LDAP Sync CA Cert Mgmt -> Create
Certificate <<<

 Please paste the certificate text (Empty line to end):
-----BEGIN CERTIFICATE-----
MIIC+TCCAeGgAwIBAgIgT6zZwxXi3vGl+DFiachhuiDEc/Rak9ECxUEhRcHZx8ww
DQYJKoZIhvcNAQELBQAwFDESMBAGA1UEAwwJbG9jYWxob3N0MB4XDTA5MTIwNDA4
MTY1NVoXDTI5MTIwNDA0NDA1NVowFDESMBAGA1UEAwwJbG9jYWxob3N0MIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2xC69YszWNu1p4pdyC1rWGtiqEWg
X+s1Hykq23bDzA56CqbsM3FO+HkDSty6HLCDZttDOJ4EG+DvVjOGSdyTPDF/O2B1
Ztc1hxr/YSGu/4zm/SEgrHpw4iU4+fEcyK8LXlS19o36mZ1J/jy7LU4JFe6MLcIQ
c6Stq1FbUJl7M7qO6NwIAaWnjX0gw3jpCtYHPqwGw9K0Sg0a5Rrsbam64srrm2Yl
q9P7lMtJqTpwmglg8CxJ6QEPEyzprF6VNaNnT6KUlNhc634KChGXw5otwsU4lfvW
2Yti1C8ofG96fGwFr189KqjWTCXI/K7eCDi/9AYnmFgvJbuUdUF9fVS/oQIDAQAB
ozcwNTAdBgNVHQ4EFgQU9P/VO7ipszDcUQaWdE3RmH0w/gwwFAYDVR0RBA0wC4IJ
bG9jYWxob3N0MA0GCSqGSIb3DQEBCwUAA4IBAQAb0TK8LhdsdWbaPIQFI2K2QgKt
OvBuf4j1Mbm0rT1hyOyvpP0Bl429gr7AwDlnSZgBQzjIVjtUpgLlTlarZmAnaaLz
/EBY4cq9PGPXeLEiFGNh6/LQfGt5Gx7y/hpv+xutPS2uo2IBhidlePNuLoAX3tY4
B4vW1LFcD2mkPXvZHeZ4vrmpls1nxLo+wP7pgvLxL6GqYi6hZVAuHrKmsvsT0E09
3JDYgvGm5drX+Y3hsmMn7IaG4e/53qm7TiVjFGAFVwd+3K6apdMUabVaz5oQ161I
tgcXvdk4RvVOdFL/ZSC+PsPyhZrwyXFQF9C494P7utu4Lnqc/Ke5buWeHTz5
-----END CERTIFICATE-----

 Validating input
 Please enter a short name for this certificate: ldaps_ca
 Installing certificate
 Finished adding LDAPS certificate
You will need to restart the Tanium Server service for this change to take effect.
Do you wish to restart the service now? [Yes|No]:
```

4. Restart the Tanium Server service. For more information, see Start, stop, and restart Tanium services on Tanium Appliances on page 313.

©2026 Tanium Inc. All Rights Reserved

Import the LDAP server root CA certificate files

About this task

> **Note:** To add multiple CA certificate files, put all certificates in one file and use the **Add Certificate** option to paste them in together. For more information, see Paste the LDAP server root CA contents on page 356.

1. Use SFTP to copy the file to the /incoming directory of the Tanium Server Appliance.
2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `A-A-A` (Appliance Configuration > Security > LDAP CA Certificate Management).
4. Enter `2` and follow the prompts to import the LDAP server root CA certificate file.
   - For the file ID, enter a short, unique string that you can use to reference the certificate.
5. Restart the Tanium Server service. For more information, see Start, stop, and restart Tanium services on Tanium Appliances on page 313.

Enable/Disable the LDAPS or StartTLS configuration

About this task

You can toggle the LDAPS or StartTLS configuration on and off. When disabled, the connection is unencrypted LDAP.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-A-A` (Appliance Configuration > Security > LDAP CA Certificate Management).
3. Enter `3` to enable or disable the LDAPS configuration.

Enable/Disable TLS certificate validation

About this task

If necessary during troubleshooting, you can disable TLS certificate validation to help you determine if there is a problem with the certificate. After troubleshooting, re-enable certificate validation.

©2026 Tanium Inc. All Rights Reserved

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A`-`A`-`A` (Appliance Configuration > Security > LDAP CA Certificate Management).
3. Enter `4` and then `E` to enable or `D` to disable TLS certificate validation for connections with the LDAP server, and follow the prompt to restart the Tanium Server service.

```
------------------------------------------------------

>>> Appliance Configuration -> LDAP Sync CA Cert Mgmt -> Validation <<<

Ignore certificate validity when using LDAPS or StartTLS.

Certificate Validation: Enabled

  E: Enable Certificate Validation
  D: Disable Certificate Validation

  R: Return to previous menu  RR: Return to top

Please select: D

You will need to restart the Tanium Server service for this change to
take effect.
Do you wish to restart the service now? [Yes|No]: Yes

Press enter to continue
```

View and manage LDAPS certificates

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A`-`A`-`A` (Appliance Configuration > Security > LDAP CA Certificate Management).
3. Enter `5` to list the LDAPS certificates that have been imported.

```
------------------------------------------------------

>>> Appliance Configuration -> LDAP Sync CA Cert Mgmt -> List Certificate <<<
```

©2026 Tanium Inc. All Rights Reserved

```
  1: subject= /O=Certificate Authority/OU=user.name@localdomain (User Name) / Lab
     e36063435f55542df19191d85105784d / Nov 25 17:42:29 2024 GMT

  R: Return to previous menu  RR: Return to top

------------------------------------------------------
```

4. Enter the number of a certificate to view its details, delete it, or copy it to a secondary Tanium Server.

```
------------------------------------------------------

>>> Appliance Configuration -> LDAP Sync CA Cert Mgmt -> List Certificates <<<



Common Name: Certificate Authority
Expiration:  Nov 25 17:42:29 2024 GMT
Fingerprint: e36063435f55542df19191d85105784d

  V: View Cert Details
  D: Delete Cert
  C: Copy Cert to ts2.localdomain (10.0.1.11)

  R: Return to previous menu  RR: Return to top

-------------------------------------------------------------------------------
```

Copy the LDAPS configuration and certificates to another Tanium Server in a Cluster

1. Sign in to a Tanium Server Appliance as a user with the `tanadmin` role.
2. Enter `A`-`A`-`A` (Appliance Configuration > Security > LDAP CA Certificate Management).
3. Enter `S` to go to the **Sync Configuration to Peer TS** screen, and follow the prompts to copy the configuration to the other Tanium Server Appliance.

©2026 Tanium Inc. All Rights Reserved

Tip:

The LDAPS configuration and certificates are copied automatically when you add a new Tanium Server to the Array.

To copy only an individual certificate, follow the steps in View and manage LDAPS certificates on page 359.

Configure security policy rules

About this task

The TanOS user access security policy has the following factory settings.

TanOS user access security policy factory settings

Setting	Factory default	Description
Password Lifetime	Minimum: 0 days Maximum: 36500 days	The minimum sets the minimum number of days between password changes. A value of 0 indicates the password can be changed at any time. The maximum sets the age at which a current password expires. A value of 36500 (the default) effectively disables password expiration.
Password History	4 most recent	The number of most recent passwords to disallow reuse. A setting of 0 allows reuse of any previous passwords. This setting does not apply to the `tanadmin` account.
Password Minimum Length	10 characters	The minimum number of characters allowed in a password. Valid range is 6–32 characters.
Password Minimum Characters Changed	0 (disabled)	The minimum number of characters in the new password that must not be present in the previous password. 5 is a common practice. STIG requires a minimum of 8. A setting of 0 allows reuse of any character. This setting does not apply to the `tanadmin` account.

©2026 Tanium Inc. All Rights Reserved

Setting	Factory default	Description
Login Failure Delay	0 seconds	The time, in seconds, between a failed sign in attempt and the next time the prompt is returned to prompt the user for the password.
Expired Passwords Effect	Force Password Change	Determine the effect on a user account when a password expires. Two options: • Disable the user account • Force password change on next sign in
Account Lockout Time	900 seconds after 3 failures	The number of seconds to lock an account after three consecutive unsuccessful sign in attempts. Valid range is 0-604800 seconds.
Maximum Concurrent Logins	10	The number of concurrent sign in sessions for a user account. Valid range is 2–1000.

To modify security policy settings:

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-A-P` (Appliance Configuration > Security > Appliance Configuration Security Policy).
3. Use the menu to view and edit password, sign in, and lockout rules.

Result

Note: After you modify password policy settings, it is expected that password prompts in TanOS menus provide users with guidance on the updated requirements.

Enable FIPS 140-3 mode

About this task

Enabling FIPS mode causes the Appliance to use a FIPS-validated cryptographic module for all cryptographic operations. It also ensures that services like SSH use only cryptographic algorithms that FIPS 140-3 allows.

©2026 Tanium Inc. All Rights Reserved

Best Practice:

- Enable FIPS mode only if you are required to do so for your organization.
- If FIPS mode is required for your organization, enable it before initial setup so that the password and keys that you configure during setup are FIPS-compliant. For more information, see one of the following sections:
  - Enable FIPS 140-3 mode before initial setup (physical Tanium Appliance) on page 60
  - Enable FIPS 140-3 mode before initial setup (virtual Tanium Appliance) on page 93
  - Enable FIPS 140-3 mode before initial setup (cloud-based Tanium Appliance) on page 130

Important:

- To use FIPS mode on a virtual Tanium Appliance, the VM on which the Appliance is installed must use a CPU type that supports the RDSEED instruction.
- Changing the FIPS mode affects the available ciphers and keys used while connecting to the Appliance over SSH. After you change the FIPS mode, the Appliance reboots immediately, and you might not be able to use SSH to access the TanOS console until you regenerate SSH keys. Before you change the FIPS mode, make sure you can access the Appliance another way, such as through iDRAC or the VM console.

Note: Enabling FIPS mode in TanOS also puts the Tanium Platform in FIPS mode.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-A-X` (Appliance Configuration > Security > Advanced Security).

©2026 Tanium Inc. All Rights Reserved

3. Enter `1` and follow the prompts to enable FIPS 140-3 mode and reboot for the changes to take effect.

```
-----------------------------------------------------

>>> Appliance Configuration -> Security -> Advanced <<<

        Setting     Current         Persistent
     FIPS 140-3:    disabled        disabled
        SELinux:    permissive      permissive

           AIDE:    not initialized
     AIDE Check:    unscheduled
    SSH Ciphers:    chacha20-poly1305@openssh.com,aes256-ctr,aes256-gcm@openssh.com

          1: FIPS 140-3 mode (disabled/enabled)
          2: AIDE
          4: Toggle SELinux mode (permissive/enforcing)
          5: Set Menu Timeout

          R: Return to previous menu  RR: Return to top

 -----------------------------------------------------

 TanOS Version:1.9.1

 Please select: 1

WARNING: Changing the FIPS mode affects the available ciphers and keys used
while connecting to the appliance over SSH. It is recommended that you ensure
you have an alternate means of connecting before continuing -- e.g. iDRAC
or VM console.

The appliance will immediately reboot for the FIPS mode change to take effect.

Are you sure you want to continue? [Yes|No]:
```

©2026 Tanium Inc. All Rights Reserved

To confirm that FIPS 140-3 mode is enabled after rebooting the Appliance, return to the Advanced Security menu (`A`-`A`-`X`).

```
-----------------------------------------------------


>>> Appliance Configuration -> Security -> Advanced <<<


        Setting     Current         Persistent
     FIPS 140-3:    enabled         enabled
        SELinux:    permissive      permissive


           AIDE:    not initialized
     AIDE Check:    unscheduled
    SSH Ciphers:    chacha20-poly1305@openssh.com,aes256-ctr,aes256-gcm@openssh.com


          1: FIPS 140-3 mode (disabled/enabled)
          2: AIDE
          4: Toggle SELinux mode (permissive/enforcing)
          5: Set Menu Timeout


          R: Return to previous menu  RR: Return to top


 -----------------------------------------------------
```

If necessary, regenerate SSH keys for users who access the TanOS console using SSH. For more information, see Manage SSH keys for TanOS users on page 227.

Use AIDE reporting

Advanced Intrusion Detection Environment (AIDE) is a host-based intrusion detection system (HIDS) for checking the integrity of files. The AIDE solution runs an initialization scan over a set of files and directories in the system and generates a reference snapshot of the environment state. Subsequent scans can be run, and the differences between initial and current scans are reported as differences to be investigated.

The set of files and directories over which the scans are run can be customized in a configuration file. If needed, contact Tanium Support on page 510 for assistance.

©2026 Tanium Inc. All Rights Reserved

Important: AIDE reports will be very noisy following TanOS upgrades, Tanium role installations, and Tanium solution module or content pack imports or reimports. To mitigate the noise and allow you to track real intrusions, the following workflow is recommended:

1. Before you perform an upgrade or installation, run an AIDE check report.
2. Then perform the upgrade or installation.
3. After the upgrade or installation, run AIDE initialization to reset the AIDE reference. A fresh AIDE report is run automatically at the end of the initialization process.

Enable AIDE

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-A-X-2` (Appliance Configuration > Security > Advanced Security > AIDE).
3. Enter `1` to initialize AIDE, enable a weekly check report, and run a test check report. Note that after initialization, the AIDE menu shows status, schedule, and recent report information.

```
------------------------------------------------------

>>> Appliance Configuration -> Security -> Advanced -> AIDE <<<

         Advanced Intrusion Detection Environment

        AIDE Status: initialized Mon Apr 06, 2020  14:58:56 UTC
     Check Schedule: enabled to run 02:10 each Sunday
     Recent Reports: none

          1: Reinitialize AIDE, enable weekly check report, run a test check report
          2: Run AIDE check report now
          3: Disable weekly AIDE check
          4: Enable weekly AIDE check report
          5: Copy AIDE check reports to outgoing directory
```

©2026 Tanium Inc. All Rights Reserved

```
         R: Return to previous menu  RR: Return to top


-----------------------------------------------------
```

Run an AIDE check report

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-A-X-2` (Appliance Configuration > Security > Advanced Security > AIDE).
3. Enter `2` to run an AIDE check report.
   Note that after the report has been run, the report status is updated.

```
-----------------------------------------------------

>>> Appliance Configuration -> Security -> Advanced -> AIDE <<<

         Advanced Intrusion Detection Environment

        AIDE Status: initialized Mon Apr 06, 2020  14:58:56 UTC
     Check Schedule: enabled to run 02:10 each Sunday
     Recent Reports: aide_check_20200406_1458_UTC.log

          1: Reinitialize AIDE, enable weekly check report, run a test check report
          2: Run AIDE check report now
          3: Disable weekly AIDE check
          4: Enable weekly AIDE check report
          5: Copy AIDE check reports to outgoing directory

          R: Return to previous menu  RR: Return to top


-----------------------------------------------------
```

Disable the weekly AIDE check report

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-A-X-2` (Appliance Configuration > Security > Advanced Security > AIDE).

©2026 Tanium Inc. All Rights Reserved

3. Enter `3` to disable the weekly AIDE check report.
   Note that after the disable report operation has been run, the scheduled report status is updated.

```
-----------------------------------------------------

>>> Appliance Configuration -> Security -> Advanced -> AIDE <<<

         Advanced Intrusion Detection Environment

        AIDE Status: initialized Mon Apr 06, 2020  14:58:56 UTC
     Check Schedule: unscheduled
     Recent Reports: aide_check_20200406_1458_UTC.log

          1: Reinitialize AIDE, enable weekly check report, run a test check report
          2: Run AIDE check report now
          3: Disable weekly AIDE check
          4: Enable weekly AIDE check report
          5: Copy AIDE check reports to outgoing directory

          R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

Enable the weekly AIDE check report

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-A-X-2` (Appliance Configuration > Security > Advanced Security > AIDE).
3. Enter `4` to enable the weekly AIDE check report.
   Note that after the enable report operation has been run, the scheduled report status is updated.

Export the weekly AIDE check report

1. Sign in to the TanOS console as a user with the `tanadmin` role.

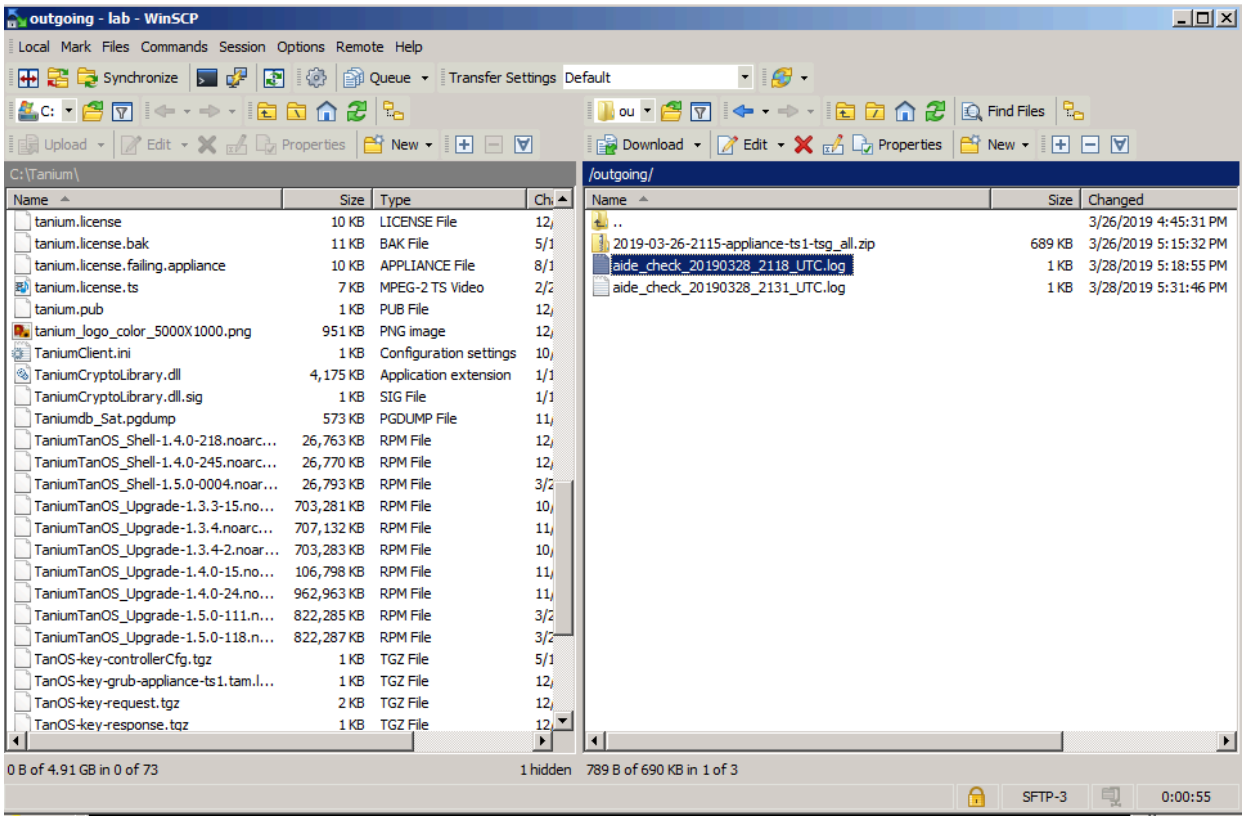
©2026 Tanium Inc. All Rights Reserved

2. Enter `A-A-X-2` (Appliance Configuration > Security > Advanced Security > AIDE).
3. Enter `5` to export the weekly AIDE check report to the /outgoing directory.

```
------------------------------------------------------

>>> Appliance Configuration -> Security -> Advanced -> AIDE <<<

         Advanced Intrusion Detection Environment

        AIDE Status: initialized Mon Apr 06, 2020  14:58:56 UTC
     Check Schedule: enabled to run 02:10 each Sunday
     Recent Reports: aide_check_20200406_1458_UTC.log

         1: Reinitialize AIDE, enable weekly check report, run a test check report
         2: Run AIDE check report now
         3: Disable weekly AIDE check
         4: Enable weekly AIDE check report
         5: Copy AIDE check reports to outgoing directory

         R: Return to previous menu  RR: Return to top

 ------------------------------------------------------

TanOS Version:1.9.1

Please select: 5

3 reports copied to outgoing directory.

Press enter to continue
```

4. Use SFTP to copy the report from /outgoing to your management computer.
   Figure 45. Copying the AIDE report file over SFTP

©2026 Tanium Inc. All Rights Reserved



Toggle SELinux mode

About this task

Security-Enhanced Linux (SELinux) is a set of kernel modifications and user-space tools that make a Linux-based OS more secure.

By default, the SELinux setting is set to `enforcing`.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-A-X` (Appliance Configuration > Security > Advanced Security).
3. Enter `4` to toggle the SELinux setting—permissive or enforcing. A reboot is not required.

Set menu timeout

About this task

The menu timeout is the amount of time that the TanOS menu system waits for user input. Enable this feature to cancel user sessions after a period of inactivity. The timeout applies to SSH sessions,

©2026 Tanium Inc. All Rights Reserved

but not to Tanium Console sessions. This setting takes effect when a user signs in to the Appliance. By default, menus do not time out.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A`-`A`-`X` (Appliance Configuration > Security > Advanced Security).
3. Enter `5` to set a menu timeout, in seconds. If you want to disable menu timeouts, set the value to `0`.

```
------------------------------------------------------


>>> Appliance Configuration -> Security -> Advanced <<<

        Setting     Current         Persistent
     FIPS 140-3:    disabled        disabled
        SELinux:    permissive      permissive

           AIDE:    not initialized
     AIDE Check:    unscheduled
    SSH Ciphers:    chacha20-poly1305@openssh.com,aes256-ctr,aes256-gcm@openssh.com

          1: FIPS 140-3 mode (disabled/enabled)
          2: AIDE
          4: Toggle SELinux mode (permissive/enforcing)
          5: Set Menu Timeout

          R: Return to previous menu  RR: Return to top

------------------------------------------------------

 TanOS Version:1.9.1

 Please select: 5

 The menu timeout is the amount of time in seconds the menu system will wait
 for user input. Enabling this feature will result in user sessions being
 cancelled after a period of inactivity. The timeout is applied to SSH
```

©2026 Tanium Inc. All Rights Reserved

```
sessions, but not to console sessions. This setting takes effect on login.


The timeout is expressed in seconds, minimum 60. 0 disables the feature.
Enter the desired timeout: 0
```

Manage the Disk Encryption Key

Export the Disk Encryption Key (physical Tanium Appliance only)

About this task

The Disk Encryption Key is used by the Appliance to lock and unlock access to the encrypted disks. You can export the key and store it in a safe location. You must provide the key to recover data after a hardware failure. When you run a Health Check, you might see messages alerting you to export the Disk Encryption Key.

```
Boot Check: Pass (EFI Boot)
Active partition: pass (VolGroup1-root)

>>> Hardware health (will take 1-12 seconds) <<<
hardware type: pass (TV-220)
RAID controller RAID.Integrated.1-1 Security Key: pass
disk encryption: pass


>>> Disk Encryption Key <<<

Disk Encryption Key check: fail (key has NOT been exported)  <--------

>>> Tanium Application file Permissions <<<

executed checks: 48
failed checks: 4
new health status setting: warning
```

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A`-`X`-`5` (Appliance Configuration > Advanced Configuration > Export Disk Encryption Key).
3. Follow the prompts to export the Disk Encryption Key to the /outgoing directory.

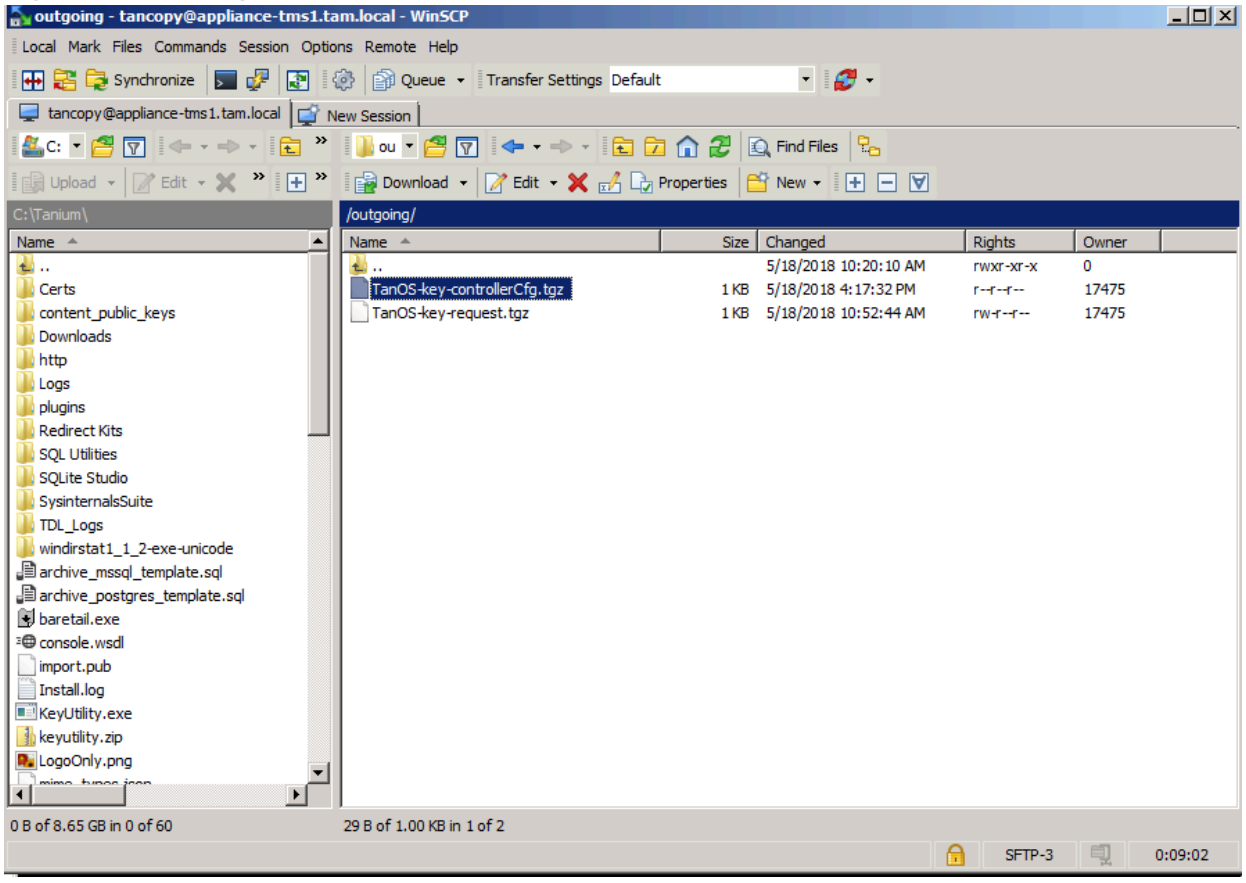
```
           >>> Appliance Configuration -> Advanced Menu -> Export Security Key <<<


Once the security key has been placed in the outgoing directory it
```

©2026 Tanium Inc. All Rights Reserved

```
will remain until the nightly cleanup job is run. After this time it
will be deleted and must be exported again.
Please be sure to download it and save in a secure location.

Would you like to export the security key? [Yes|No]: yes

The security key has been placed in the sftp outgoing directory.
This location will be cleaned daily at 02:00am appliance time!

Press enter to continue
```

4. Use SFTP to copy the file from the /outgoing directory to your local computer.

Figure 46. Copying the Disk Encryption Key file over SFTP



Change the Disk Encryption Key (physical Tanium Appliance only)

You can change the Disk Encryption Key in the event of a failure, but you need to have the existing key decrypted to do so.

©2026 Tanium Inc. All Rights Reserved



CAUTION: This is a lengthy process and can take 10 minutes or more to complete.

BEFORE YOU BEGIN

The passphrase that is associated with the existing key must be decrypted by Tanium. [Contact Tanium Support on page 510] for assistance.

CHANGE THE KEY WITH THE DECRYPTED PREVIOUS KEY

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-X-4` (Appliance Configuration > Advanced Configuration > Change Disk Encryption Key).
3. Type **Yes** to proceed, enter your decrypted previous key, and then enter a new key that meets the password policy requirements. The Disk Encryption Key cannot contain spaces or tabs.

```
           >>>  Appliance Configuration -> Advanced -> Disk Encryption Key <<<
           WARNING

The active Disk Encryption Key is used by the appliance to access data
on the appliance's disks. A backup copy of the key would be required in the
event of a hardware failure. Without the backup key you will NOT be able to
recover any data from the appliance's disks.

This option is used to change the Disk Encryption Key. To change the
key you will need the existing key. The key would have been exported and stored
in a safe location when your appliance was initially configured. The backup key
is encrypted before export, and may only be decrypted with the assistance of
Tanium Support.

CAUTION:
This is a lengthy process and can take 10 minutes or more to complete.

Would you like to change the Disk Encryption Key? [Yes|No]: Yes
Please enter the CURRENT Disk Encryption Key or enter to quit:
```

©2026 Tanium Inc. All Rights Reserved

```
The password policy requires meeting these rules:
 - Minimum 20 characters long
 - Maximum 32 characters long
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
 - At least 1 other character
 - Must not be based on a dictionary word
 - Must not contain part of the username

Please enter password (will not be displayed):
Password score: 100 out of 100 (strong)
Please enter password again:

WARNING: SECURELY SAVE THIS PASSWORD SO YOU CAN RECOVER FROM A FAILURE
Starting the process to replace the Disk Encryption Key.
This can take 10 minutes or more to complete.
```

4. Export the new Disk Encryption Key and download the key immediately from the /outgoing folder through SFTP.
   For export steps, see Export the Disk Encryption Key (physical Tanium Appliance only) on page 372.

Manage the GRUB key (physical Tanium Appliance or virtual Tanium Appliance only)

Export the GRUB key

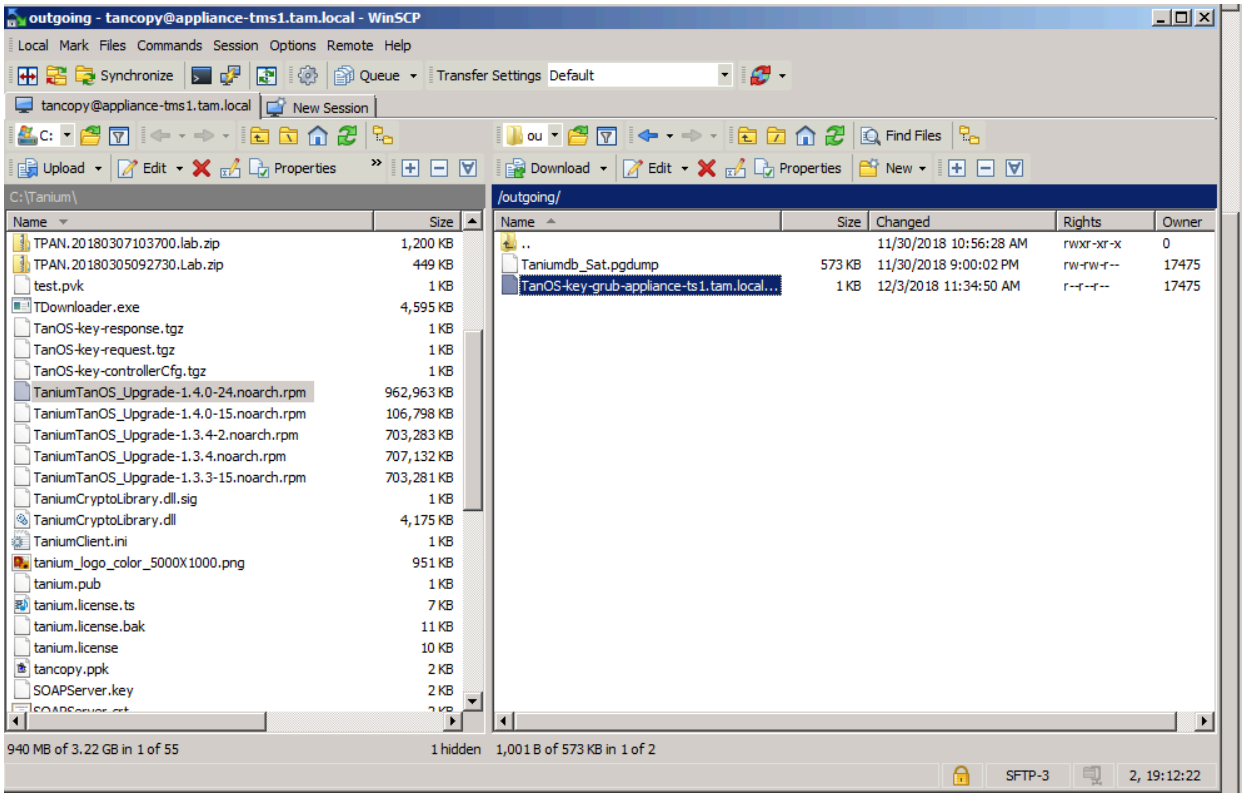
1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-X` (Appliance Configuration > Advanced Configuration).
3. Enter `6` and follow the prompts to export the GRUB key to the /outgoing folder.

```
>>> Appliance Configuration -> Advanced Menu -> Export Security Key <<<
```

©2026 Tanium Inc. All Rights Reserved

```
Once the security key has been placed in the outgoing directory it
will remain until the nightly cleanup job is run. After this time it
will be deleted and must be exported again.
Please be sure to download it and save in a secure location.

Would you like to export the security key? [Yes|No]: yes

The security key has been placed in the sftp outgoing directory.
This location will be cleaned daily at 02:00am appliance time!

Press enter to continue
```

4. Use SFTP to copy the file from the /outgoing directory to your local computer.
   Figure 47. Copying the GRUB key file over SFTP



Next steps

Important: If you need the GRUB password during recovery, you must provide the key to Tanium Support on page 510 for a technician to extract the GRUB password.

©2026 Tanium Inc. All Rights Reserved

Change the GRUB key password

About this task

If necessary, you can regenerate the GRUB key and password.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-X` (Appliance Configuration > Advanced Configuration).
3. Enter `7` and follow the prompts to generate a new GRUB key and export it to the /outgoing folder.

```
            >>> Appliance Configuration -> Advanced Menu -> Generate New Grub Key
<<<

Attention:

Generating new GRUB key will invalidate prior key and any emergency
recovery access it would have provided.  A system administrator must
export newly generated GRUB key file for emergency recovery use.

Are you sure you want to generate a new GRUB key? [Yes|No]: yes

Generating new GRUB password ...
Generating new GRUB key ...

Success.

Press enter to continue
```

   For export steps, see Export the GRUB key on page 375.

4. Use SFTP to copy the file from the /outgoing directory to your local computer.

Next steps

©2026 Tanium Inc. All Rights Reserved

Important: If you need the GRUB password during recovery, you must provide the key to Tanium Support on page 510 for a technician to extract the GRUB password.

©2026 Tanium Inc. All Rights Reserved

Tanium Appliance redundancy, backup, and recovery

Use multiple layers of redundancy and backup so that you can recover from issues as quickly as possible, from a routine failover through to a full restoration.

The subsequent topics in this section provide information about redundancy and backup best practices, using a Tanium Server cluster and a standby Module Server for redundancy, and using image-based backups, partition sync, and core and comprehensive backups for backup and restoration.

Tanium Appliance redundancy and backup best practices and considerations

The following sections describe standard guidance for redundancy and backups. You can reference these as standard best practices. Your overall redundancy and backup strategy depends on your disaster recovery plan and the specific needs of your organization.

Use multiple layers of redundancy and backup for Tanium Appliances

Multiple layers of redundancy and backup provide multiple recovery options to recover from issues as quickly as possible:

- For resiliency in case of most hardware failures and other issues that have a limited impact, configure a Tanium Server Cluster and a standby Module Server to provide redundancy. For more information, see Use a Tanium Server cluster for redundancy on page 383 and Use a standby Module Server for redundancy on page 386.

- For fast recovery from more significant issues, use the following backup methods:

    - Virtual Tanium Appliances and cloud-based Tanium Appliances: Use virtual infrastructure data protection tools to create image-based backups. For more information, see Use image-based backups for backup and restoration (cloud-based Tanium Appliance or virtual Tanium Appliance only) on page 390.

©2026 Tanium Inc. All Rights Reserved

- Physical Tanium Appliances: Use the partition sync feature of TanOS to backup the active partition to the inactive partition. For more information, see Use partition sync for backup and restoration (physical Tanium Appliance and test-environment virtual Tanium Appliance only) on page 391.

> **Note:**
>
> - Tanium does not allow third-party backup agents on the Appliance. However, you can use any data protection tool provided by your hypervisor, your cloud provider, or a third party that performs image-based backups.
> - Though partition sync is available on virtual Tanium Appliances, it is intended to be used only in a virtual environment that replicates a physical Appliance Array for testing purposes. The partition sync feature is not recommended as a backup solution for production virtual Tanium Appliances.

- For recovery from database-related issues, use *core backups* in TanOS. Perform a core backup of the active Module Server daily. If you choose not to perform a daily comprehensive backup of the primary Tanium Server, perform a core backup daily. For more information, see Use core and comprehensive backups for backup and restoration on page 397.

> **Note:**
>
> - Core backups do not require stopping Tanium Server or Module Server services.
> - Database restoration from core backups requires assistance from Tanium Support on page 510.
> - On virtual Tanium Appliances or cloud-based Tanium Appliances that are protected by a virtual infrastructure data protection tool, core backups are optional.

- As a last line of defense for disaster recovery, use *comprehensive backups* in TanOS. Use a comprehensive recovery bundle to perform a full restoration of the TanOS and Tanium environment.

©2026 Tanium Inc. All Rights Reserved

- **Tanium Server:** Perform a comprehensive backup of the primary Tanium Server daily or weekly.

  > **Note:**
  >
  > - Comprehensive backups do not require stopping Tanium Server services.
  > - The comprehensive backup includes the Tanium Server Downloads directory, which can be large. If disk space on your backup server is a concern, you might choose to run the comprehensive backup once weekly.

- **Module Server:** Perform a comprehensive backup of the active Module Server weekly.

  > **Note:**
  >
  > - The comprehensive backup stops all Tanium Module Server services. Make sure to run the backup during an appropriate maintenance window.

For more information, see Use core and comprehensive backups for backup and restoration on page 397.

> **Note:** On virtual Tanium Appliances or cloud-based Tanium Appliances that are protected by a virtual infrastructure data protection tool, comprehensive backups are optional.

Define a disaster recovery plan

Tanium recommends that you define a disaster recovery (DR) plan early during deployment. The restoration and backup options that fit your disaster recovery plan vary depending on your specific needs and requirements.

©2026 Tanium Inc. All Rights Reserved

To properly define a DR plan, define specific restore time objectives (RTO) and restore point objectives (RPO).

- **RPO**: The expected point of recovery. For example, an RPO of 1 month means recovery point within 30 days of the time of failure.
- **RTO**: What is the amount of downtime that is acceptable to recover the system.

Your schedule for each type of backup and the versions or copies of each type of backup that you store depend on your RPO and RTO.

Additional best practices

- Perform a partition sync on a physical Tanium Appliance or make sure that you have a recent image-based backup on a cloud-based Tanium Appliance or virtual Tanium Appliance before any major changes, including TanOS upgrades and Tanium Core Platform upgrades.
- Use any additional options for disaster recovery and redundancy that are provided by your cloud provider (for cloud-based Tanium Appliances) or your hypervisor or data center environment (for virtual Tanium Appliances).
- For better resiliency in a cloud-based environment, separate Tanium Server, Tanium Module Server, and Tanium Zone Server Appliances between two zones so that each zone contains each Appliance type.

Considerations after a recovery

- Make sure to update the DNS records in your domain configuration for any Appliances that have new IP addresses after a recovery. For the specific steps, review the documentation from your domain provider.
- Perform any configuration that was not included in the restoration. For example, after a restoration from a comprehensive recovery bundle, you must reconfigure the items listed in Items excluded from backups on page 399.
- After you perform any type of recovery, test the functionality of the Tanium solutions in your environment. Some solutions have settings that might need be changed if server addresses change. For more information, see the user guide for each solution. For example, if you perform a Module Server failover or recover a Module Server with a new IP address, and the

©2026 Tanium Inc. All Rights Reserved

Fully Qualified Domain Name configured for the Module Server in the **Endpoint Connection** settings for Direct Connect is set to only the IP address of the old Module Server, you must update that setting in Direct Connect before you can connect to an endpoint using Direct Connect functionality. (For more information about that specific setting, see Configure Endpoint Connection settings.)

Use a Tanium Server cluster for redundancy

You can configure Tanium Appliances into a Tanium cluster, where the Tanium Server is active-active, and the database component is active-passive. The Tanium Servers read and write to the database located on the primary Tanium Server Appliance.

- The *primary Server* is the Server that hosts the read/write database.
- The *secondary Server* contains a read-only database that replicates from the database on the primary Server.

For information about how to set up a Tanium cluster, see Configuring a Tanium cluster on page 168. For information about managing database replication, see Manage a Tanium cluster on page 328.

Testing a planned Tanium Server failover

About this task

As part of a planned failover exercise, you might want to failover to your secondary Appliance and then fail back.



Important: Before you begin any planned failover activities, check that database replication is healthy by running a health check (`3 -5`) on both Appliances.

In the following scenario, TS1 is a TanOS Appliance with the primary database and TS2 is a TanOS Appliance with a replicated database from TS1.

1. Follow the planned failover steps:
    - On TS1, stop the Tanium Server service (`2-1-`<line number of taniumserver service>`-2`).

©2026 Tanium Inc. All Rights Reserved

- On TS2, initialize database failover (`2-B-F`).
- On TS1, reinitialize replication (`2-B-E`).

2. Follow the planned failback steps:
   - On TS2, stop the Tanium Server service (`2-1-`<line number of taniumserver service>`-2`).
   - On TS1, initialize database failover (`2-B-F`).
   - On TS2, reinitialize replication (`2-B-E`).

Recover a failed member of a redundant TS cluster

If you have a Tanium cluster set up with multiple Tanium Servers, you can perform the following steps to recover the cluster.

PREREQUISITES

- One member of the cluster must be in good working order.
- Replication and communication must be healthy within the cluster prior to failure.

(PRIMARY SERVER FAILURE ONLY) INITIATE THE DATABASE SERVER FAILOVER

About this task

If the primary Tanium Server is down, you must perform the following steps to restore Tanium functionality:

This procedure promotes this Tanium Server to primary. Deploy a new secondary Server by following the steps in Restore a secondary Tanium Server on page 385.

1. Sign in to the TanOS console of the Appliance with the secondary database as a user with the `tanadmin` role.
2. Enter `2-B-F` (Tanium Operations > Cluster Configuration > Database Server Failover).
3. Follow the prompts to initiate the failover.

©2026 Tanium Inc. All Rights Reserved

RESTORE A SECONDARY TANIUM SERVER

About this task

If your secondary Tanium Server is no longer available and your environment is operational but in a state of reduced redundancy, perform the following steps to restore a secondary Tanium Server to the cluster:

1. Set up a new Appliance. For more information, see Getting started with the Tanium Appliance on page 41.
2. Perform the initial configuration for the new Appliance:
   - For a physical Tanium Appliance, see Completing the initial setup (physical Tanium Appliance) on page 60.
   - For a virtual Tanium Appliance, see Completing the initial setup (virtual Tanium Appliance) on page 93.
   - For a cloud-based Tanium Appliance, see Completing the initial setup (cloud-based Tanium Appliance) on page 130.

   Best Practice: Use the same FQDN and IP address as the backup to prevent extra steps during restoration.
3. Add the newly configured Appliance to the Array. For more information, see Add members to the Array on page 162.
4. Assign the Appliance the Tanium Server role and install new roles. For more information, see Assign roles on page 165 and Install Tanium roles on page 170.

   Important: Make sure that you match the platform version of the primary Server.
5. In a web browser, Sign in to Tanium Console on the new Appliance and reimport all modules to ensure they match the same version as the primary Tanium Server. Be careful not to accidentally upgrade modules on the secondary Tanium Server.
   After each module import, verify that the module loads and that service accounts and other settings are restored.
6. Manually reconfigure TanOS settings and backup schedules as necessary.

©2026 Tanium Inc. All Rights Reserved

Tip: If you are using an LDAPS or StartTLS configuration, the configuration and stored root CA certificates are automatically copied to the new secondary Tanium Server when you add it to the Array and install the role.

7. Verify the deployment on the new Appliance. For more information, see Verifying the deployment.

Use a standby Module Server for redundancy

If you add two Module Servers to an Appliance Array, you can schedule a Module Server sync to use the second Module Server as a standby. For information about managing synchronization of the secondary Module Server, see Manage the standby Module Server on page 329.

Test a planned Module Server failover or recover a failed Module Server with a standby Module Server

Perform the following procedure to test a planned Module Server failover or to recover a failed Module Server with a standby Module Server and provide a new standby Module Server.

PREREQUISITES

- The most recent TMS sync must be successful and meet your RPO.

PREPARE FOR PROMOTION OF THE STANDBY MODULE SERVER

1. Sign in to the standby Module Server Appliance as a user with the `tanadmin` role and perform a health check (`3-5`). Resolve any issues presented in the health check. For more information, see Run the Health Check on page 488.
2. If you are testing or otherwise conducting a planned failover in which both Module Servers are still operational, perform the following additional steps:
    a. Sign in to the active Module Server Appliance as a user with the `tanadmin` role and perform a health check (`3-5`). Resolve any issues presented in the health check. For more information, see Run the Health Check on page 488.
    b. On the active Module Server Appliance, review the Module Server sync status (`2-D`), and verify that the **Role** is `Active sync (source)` and the **Database**

©2026 Tanium Inc. All Rights Reserved

Replication status is `Active (streaming)`.

c. On the standby Module Server Appliance, review the Module Server sync status (`2-D`), and verify that the **Role** is `Standby (target)` and the **Database Replication** status is `Active (streaming)`.

d. On the active Module Server Appliance, perform a Module Server sync (`2-D-4`), and then verify that the **Last file sync status** is `OK` with the expected time stamp.

PROMOTE THE STANDBY MODULE SERVER TO ACTIVE

1. Sign in to the Tanium Server Appliance as a user with the `tanadmin` role.
2. Enter `2-A` (Tanium Operations > Configure Module Server(s)).
3. Enter `P` to **Promote TMS**.

```
           >>> Tanium Operations ->  Configure Module Server(s) ->  Promote TMS <<<

Active Module Server: tms1.test.tanium.local

Module Server 1:
  Name: tms1.test.tanium.local
  TMS Sync Role:        Active sync (source)
  TMS Sync File Ready:  Yes
  TMS Sync Replication: Active

Module Server 2:
  Name: tms2.test.tanium.local
  TMS Sync Role:        Target
  TMS Sync File Ready:  Yes
  TMS Sync Replication: Active

Note: Promoting TMS requires sync to be re-enabled.
Which Module Server should be promoted to active?

         1: tms1.test.tanium.local
         2: tms2.test.tanium.local
```

©2026 Tanium Inc. All Rights Reserved

```
         R: Return to previous menu  RR: Return to top


Please select:
```

4. Enter the line number of the standby Module Server that you want to promote.
5. Enter the administrative user name for the web-based Tanium Console. This is different from TanOS console tanadmin users.
6. Enter the password for the Tanium Console administrative user and press **Enter**.

Result

Important: After you perform this procedure, the formerly standby Module Server becomes active and registered with the Tanium Server, but Module Server sync is not configured, and the newly non-active Module Server is not automatically a standby Module Server, even if it was still operational (such as during a failover test). You will reconfigure Module Server sync in a later step.

MAKE SURE PLUGIN SCHEDULES ARE IN PLACE AND PERFORM STANDARD CHECKOUT STEPS

1. Import, reimport, or upgrade a module. You can safely upgrade modules in this state.
2. Make sure modules can load without errors.
3. Make sure package files are cached.
4. Make sure packages, sensors, users, computer groups, and other objects are restored.

Result

Your environment is now fully operational with a single, active Module Server.

(TESTING OR PLANNED FAILOVER ONLY) REASSIGN SYNC ROLES

About this task

If you are testing or otherwise conducting a planned failover in which both Module Servers are still operational, reassign sync roles to re-enable Module Server sync on the existing Module Servers:

1. Sign in to the Tanium Server Appliance as a user with the `tanadmin` role.
2. Enter `2`-`A`-`S` (Tanium Operations > Configure Module Server(s)). > Assign TMS Sync Role

©2026 Tanium Inc. All Rights Reserved

3. Enter the number of the newly active Module Server, and then enter `S` to enable TMS sync with the active Module Server as a source.
4. Enter the number of the newly non-active Module Server, and then enter `T` to enable TMS sync with the non-active Module Server as a target.
5. Restart the module services on the newly active Module Server.
    a. Sign in to the newly active Module Server Appliance as a user with the `tanadmin` role.
    b. Enter `2-1` (Tanium Operations > Tanium Service Control).
    c. For each module service, enter the line number of the service, and then enter `3` to restart it. For more information, see Start, stop, and restart Tanium services on Tanium Appliances on page 313.
    d. Make sure modules can load without errors and that module functions work, such as importing assets.

(FAILED MODULE SERVER ONLY) REPLACE FAILED MODULE SERVER

About this task

If you are replacing a failed Module Server, remove the failed Module Server and deploy a new Module Server to be configured as a standby.

1. Remove the failed Module Server:
    a. Sign in to the Tanium Server Appliance as a user with the `tanadmin` role.
    b. Enter `1-M` (Tanium Installation > Appliance Array).
    c. Enter the number of the failed Module Server.
    d. Enter `D` to delete the Module Server from the array.
2. Deploy a new Appliance:
    - For a physical Tanium Appliance, see Completing the initial setup (physical Tanium Appliance) on page 60.
    - For a virtual Tanium Appliance, see Completing the initial setup (virtual Tanium Appliance) on page 93.
    - For a cloud-based Tanium Appliance, see Completing the initial setup (cloud-based Tanium Appliance) on page 130.
3. Add the Appliance to the Array. For more information, see Add members to the Array on page

©2026 Tanium Inc. All Rights Reserved

162.

4. Assign the Appliance the Tanium Module Server role and install new roles. For more information, see Assign roles on page 165 and Install Tanium roles on page 170.

SCHEDULE MODULE SERVER SYNC AND OPTIONALLY PERFORM A FAILBACK

1. Schedule a Module Server sync to use the newly non-active or newly installed Module Server as a standby. For more information, see Schedule sync jobs on page 329.
2. (Optional) If you are testing, perform a failback by completing the steps in this section again with the Module Servers reversed.

Use image-based backups for backup and restoration (cloud-based Tanium Appliance or virtual Tanium Appliance only)

On a cloud-based Tanium Appliance or virtual Tanium Appliance, use virtual infrastructure data protection tools to create image-based backups. Though Tanium does not allow third party backup agents on the Appliance, you can use any data protection tool to perform image-based backups that is provided by your hypervisor, your cloud provider, or a third party. On a cloud-based Tanium Appliance or virtual Tanium Appliance, perform an image-based backup before you upgrade TanOS or Tanium Core Platform, so that you have an alternate partition in case issues occur during the upgrade process.



Important: Produce image-based backups of the Tanium Server and Module Server from snapshots taken at the same time.

Restore TanOS using a VM image (cloud-based Tanium Appliance or virtual Tanium Appliance only)

These steps are only available for cloud-based Tanium Appliances or virtual Tanium Appliances as these steps require an available image for restoration.

PREREQUISITES

- A known good image.

©2026 Tanium Inc. All Rights Reserved

- The restore point must have Tanium Module Server and Tanium Server images that are at the same time.

STEPS

1. Turn off all Appliances (Tanium Server, Tanium Module Server).
2. Restore the Appliances to the image or snapshot state.
3. Start the Tanium Servers first, followed by the Tanium Module Server.

Use partition sync for backup and restoration (physical Tanium Appliance and test-environment virtual Tanium Appliance only)

On a physical Tanium Appliance or virtual Tanium Appliance, TanOS can have a primary and secondary partition. The primary partition is by default the active partition, on which TanOS runs, and when the secondary partition is present, it is by default the inactive partition, available in case of failover or troubleshooting. A physical Tanium Appliance contains both partitions by default.

A partition sync is a backup procedure that uses the rsync utility to copy the active partition to the inactive partition, and it provides the quickest way to restore to a known good restore point. On a physical Tanium Appliance, perform a partition sync before you upgrade TanOS or Tanium Core Platform, so that you have an alternate partition in case issues occur during the upgrade process. You can also use the inactive partition if the active partition fails to boot. During the TanOS boot process, you have the option to select the inactive partition if needed.

©2026 Tanium Inc. All Rights Reserved

Note:

- Though partition sync is available on virtual Tanium Appliances, it is intended to be used only in a virtual environment that replicates a physical Appliance Array for testing purposes. The partition sync feature is not recommended as a backup solution for production virtual Tanium Appliances.
- A virtual Tanium Appliance contains only one partition by default. Appliances with only one partition do not contain the option to perform a partition sync. You can add a secondary partition to perform a partition sync. For more information, see Enable alternate partitions (test-environment virtual Tanium Appliance only) on page 392.

Manage partitions

ENABLE ALTERNATE PARTITIONS (TEST-ENVIRONMENT VIRTUAL TANIUM APPLIANCE ONLY)

About this task

A virtual Tanium Appliance contains only one partition set by default. Before you perform a partition sync, you must enable an alternate (inactive) partition.

Note: On a virtual Tanium Appliance, the option to enable partitions appears only if you have a single partition.

CAUTION: Enabling an alternate partition is a long-running operation. This operation performs an initial partition sync, which may take a long time depending on the configuration of your storage subsystem.

1. If needed, modify the virtual image to add disk storage.

   CAUTION: This action is not reversible. Storage that you add to the Appliance is permanently allocated. Do not attempt to remove disk storage from an Appliance, as the Appliance becomes unusable.

©2026 Tanium Inc. All Rights Reserved

2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `B` (Appliance Maintenance).
4. Enter `E` and follow the prompts to enable alternate partitions.
   If your virtual Tanium Appliance does not have enough space to enable the alternate partition, the TanOS console displays the minimum amount of space needed.

DISABLE ALTERNATE PARTITIONS (VIRTUAL TANIUM APPLIANCE ONLY)

About this task

Use this option on virtual Tanium Appliances to remove the alternate (inactive) partition set. Use this option if you do not need the alternate partition. After you remove the alternate partition set, you can allocate the unused storage to the primary partition of the Appliance.



CAUTION:

- Do not disable the alternate partition set with the intent to reclaim disk storage for the host computer or other virtual machines. Disk storage on the Appliance is permanently allocated, and space from alternate partitions can be reallocated only to the primary partition of the Appliance. Do not attempt to remove disk storage from an Appliance, as the Appliance becomes unusable.
- Disabling an alternate partition used for a partition sync removes the partition sync backup.



Note: A virtual Tanium Appliance contains only one partition by default. This menu option appears only if you have enabled an alternate partition.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B` (Appliance Maintenance).
3. Enter `D` and follow the prompts to remove all alternate partitions.

©2026 Tanium Inc. All Rights Reserved

```
------------------------------------------------------

            >>> Appliance Maintenance <<<

         1: Backup
         2: Alerting
         3: Upgrade TanOS
         5: Shell Keys

         A: Clean directories
         B: Reboot/Shutdown
         C: Maintenance mode
         D: Discard alt partitions
         I: Increase storage

         X: Advanced Maintenance

         R: Return to previous menu  RR: Return to top

------------------------------------------------------

TanOS Version:        1.9.1

 Please select: D
 This will remove all data on all alt partitions. While it is possible to
 recreate alt partitions, doing so will NOT recover any data on the current alt
 partitions.  You may need to add an additional disk to the VM if you want to
 create new alt partitions.
 This action is IRREVERSIBLE!

 CAUTION: Do not disable the alternate partition set with the intent to reclaim
 disk storage. Disk storage on the appliance is permanently allocated.
 Do not attempt to remove disk storage from an appliance, as the appliance will
 become unusable.

 Do you wish to continue with this irreversible action? [Yes|No]: yes
```

©2026 Tanium Inc. All Rights Reserved

```
 Logical volume "altroot" successfully removed
 Logical volume "altopt" successfully removed
 Logical volume "alttmp" successfully removed
 Logical volume "althome" successfully removed
 Logical volume "altvarlogaudit" successfully removed
 Logical volume "altvarlog" successfully removed
 Logical volume "altvar" successfully removed


Press enter to continue
```


Tip: Use the Increase storage on page 445 option to reallocate the storage from the deleted partition set.

BOOT FROM THE ACTIVE OR INACTIVE PARTITION

When the Tanium Appliance boots, you are prompted to select a partition. Your choices are **TanOS Active** and, if an inactive partition is present, **TanOS Inactive**.

- The **TanOS Active** option boots into the *active partition*. By default, the primary partition is the active partition.
- The **TanOS Inactive** option boots into the *inactive partition*. By default, the secondary partition is the inactive partition.

Perform a partition sync

About this task

In an Array, start the partition sync on the primary Appliance only. The Array automatically performs the sync on all other Servers in the Array.

©2026 Tanium Inc. All Rights Reserved

Note:

- Though partition sync is available on virtual Tanium Appliances, it is intended to be used only in a virtual environment that replicates a physical Appliance Array for testing purposes. The partition sync feature is not recommended as a backup solution for production virtual Tanium Appliances.
- A virtual Tanium Appliance contains only one partition by default. Appliances with only one partition do not contain the option to perform a partition sync. You can add a secondary partition to perform a partition sync. For more information, see Enable alternate partitions (test-environment virtual Tanium Appliance only) on page 392.

Important: To protect data consistency, the partition sync job disables (shuts down) the Tanium Server, Tanium database server, and other related services for the duration of the partition sync. Make sure to perform a partition sync at a time that does not disrupt solution processes.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-1-P` (Appliance Maintenance > Backup > Partition Sync).
3. Follow the prompts to complete the backup. After the partition sync completes, TanOS displays a message indicating whether the sync was successful or encountered errors.

   Important: If the partition sync encounters errors, resolve any issues before attempting a TanOS or Tanium Core Platform upgrade. TanOS alerts you if the most recent partition sync was unsuccessful when you attempt an upgrade.

   For information about how to change the active partition to the inactive partition, see Perform a partition swap to restore TanOS from a partition sync on page 396.

Perform a partition swap to restore TanOS from a partition sync

Important: If you are performing a partition swap on all Appliances, start with all Tanium Servers followed by the Tanium Module Servers.

©2026 Tanium Inc. All Rights Reserved

PREREQUISITES

- A previous partition sync that is within your RPO
- The password that was used on the previous partition sync (if the TanOS password was changed after partition sync)
- Access to a user with the `tanadmin` role

STEPS

1. Sign in to the TanOS console as a user with the `tanadmin` role. Make sure the Appliance is booted to the primary partition in normal mounting mode.
2. Initiate a partition swap (`A-X-3`). TanOS automatically reboots.

   Note: When you change the active partition, the partition that was set as the inactive partition becomes the active partition, and the partition that was set as the active partition becomes the inactive partition. For example, in the default configuration, the primary partition is the active partition and the secondary partition is the inactive partition. After you change the active partition, the secondary partition becomes the active partition and the primary partition becomes the inactive partition.
3. Boot into the **TanOS Active** partition.
4. Perform a partition sync (`B-1-P`). This syncs your secondary partition (which is active) to your primary partition (inactive).

   Important: Changes on the primary partition are overwritten.
5. If necessary, repeat these steps for all Tanium Servers and Tanium Module Servers in the Array.

Use core and comprehensive backups for backup and restoration

Core backups and comprehensive backups produce recovery bundles that help rebuild the Appliance Array and the Tanium environment in the event of major issues.

©2026 Tanium Inc. All Rights Reserved

Important: Store backup files in a location that is protected from unauthorized access,and protect them from intentional and accidental modification. A modified or corrupted backup file could cause the restoration to fail or leave the restored system in an unstable or insecure state.

Best Practice: Regularly perform core and comprehensive backups for protection from major issues, but for the fastest recovery from minor incidents or misconfigurations, use redundancy, partition sync (for physical and virtual Tanium Appliances), and snapshots or other image backups (for cloud-based or virtual Tanium Appliances). For more information, see Tanium Appliance redundancy and backup best practices and considerations on page 379.

- A **comprehensive backup** produces a *comprehensive recovery bundle*, which includes the full set of files that are necessary to recover a Tanium Core Platform Server. With assistance from Tanium, you can fully restore TanOS and the complete Tanium environment from this backup.

  Important: A comprehensive backup stops services on the Tanium Module Server to capture the module data. During this time, users can still access Tanium and ask questions, but the module workbenches are unavailable until the backup completes. A comprehensive backup also backs up significantly more data than a core backup. Performing this backup on secondary Servers minimizes the impact of the backup on performance and avoids downtime in most cases.

- A **core backup** produces a *core recovery bundle*, which includes essential files to restore a Tanium Server or Module Server to the point that Tanium Clients can register. It omits the Tanium Server downloads used by custom packages and file data from Tanium modules. Because this backup does not require stopping Tanium services and it backs up less data, the performance impact is minimal.

  Note: Database restoration from core backups requires assistance from Tanium Support on page 510.

The following tables detail the contents of each recovery bundle:

©2026 Tanium Inc. All Rights Reserved

Contents of core and comprehensive backups on a Tanium Server or Zone Server

Contents	Included in Core Backup	Included in Comprehensive Backup
Appliance, Array and network settings	✓	✓
LDAP database contents (locally managed Tanium accounts)	✓	✓
Critical Tanium Server or Tanium Zone Server configuration and key material	✓	✓
LDAP and root CA certificates	✓	✓
Tanium Server database contents	✓	✓
Tanium Server downloads	✗	✓

Contents of core and comprehensive backups on a Module Server

Contents	Included in Core Backup	Included in Comprehensive Backup
Appliance, Array and network settings	✓	✓
Critical Tanium Module Server configuration and key material	✓	✓
LDAP and root CA certificates	✓	✓
Module Server database contents	✓	✓
File data from Tanium modules	✗	✓

Items excluded from backups

Certain items are excluded from backups:

- Generally, any TanOS configuration that is specific to that Appliance. This includes:

©2026 Tanium Inc. All Rights Reserved

    - Auth key file (SSH keys)
    - FQDN, IP, routes
- TanOS local user accounts and their account policies (such as password policy)
- Scheduled jobs (such as backups)

You can transfer the backup file to a remote location using SCP, or copy the backup into the /outgoing directory for manual collection.

Sample contents of a core recovery bundle

```
$ ls -laR
total 40
drwxr-xr-x@ 12 john.doe  staff   384 Nov  2 14:18 .
drwxrwxrwx@ 45 john.doe  staff  1440 Nov  2 14:17 ..
-rw-r--r--@  1 john.doe  staff  6148 Nov  2 14:19 .DS_Store
-rw-r--r--@  1 john.doe  staff  2238 Nov  2 14:05 README.txt
drwxr-xr-x  11 john.doe  staff   352 Nov  2 14:18 TaniumServer
drwxr-xr-x   4 john.doe  staff   128 Nov  2 14:18 TaniumZoneServer
drwxr-xr-x  13 john.doe  staff   416 Nov  2 14:06 config
drwxr-xr-x   3 john.doe  staff    96 Nov  2 14:05 database
-rwxr-xr-x   1 john.doe  staff  1493 Nov  2 14:05 decrypt-payload.sh
drwxr-xr-x   5 john.doe  staff   160 Nov  2 14:05 enc_ssl
-rw-r--r--   1 john.doe  staff  1067 Nov  2 14:06 manifest.txt

./TaniumServer:
total 288
drwxr-xr-x  11 john.doe  staff    352 Nov  2 14:18 .
drwxr-xr-x@ 11 john.doe  staff    352 Nov  2 14:24 ..
drwxr-x---   4 john.doe  staff    128 Nov  2 10:31 Backup
-r--------   1 john.doe  staff   1111 Oct  9 14:55 SOAPServer.crt
-r--------   1 john.doe  staff   1704 Oct  9 14:55 SOAPServer.key
drwxr-x---   5 john.doe  staff    160 Oct 24 18:10 content_public_keys
-rw-r-----   1 john.doe  staff  90112 Nov  2 14:05 pki.db
-rw-r-----   1 john.doe  staff  20480 Nov  2 10:31 server.db
-rw-r-----   1 john.doe  staff    158 Oct  9 14:55 tanium.pub
-rw-r-----   1 john.doe  staff  20480 Oct  9 14:55 tdownloader.db
-rw-r-----   1 john.doe  staff   1133 Oct  9 15:01 trusted-module-servers.crt

./TaniumServer/Backup:
total 352
drwxr-x---   4 john.doe  staff    128 Nov  2 10:31 .
drwxr-xr-x  11 john.doe  staff    352 Nov  2 14:18 ..
-rw-r-----   1 john.doe  staff  90112 Nov  2 10:31 pki-backup.db
-rw-r-----   1 john.doe  staff  90112 Oct  9 15:12 pki.db

./TaniumServer/content_public_keys:
total 0
drwxr-x---   5 john.doe  staff  160 Oct 24 18:10 .
drwxr-xr-x  11 john.doe  staff  352 Nov  2 14:18 ..
drwxr-x---   3 john.doe  staff   96 Nov  2 10:31 console
drwxr-x---   3 john.doe  staff   96 Nov  2 10:31 content
drwxr-x---   3 john.doe  staff   96 Nov  2 10:31 manifest
```

©2026 Tanium Inc. All Rights Reserved

```
./TaniumServer/content_public_keys/console:
total 8
drwxr-x---  3 john.doe  staff   96 Nov  2 10:31 .
drwxr-x---  5 john.doe  staff  160 Oct 24 18:10 ..
-r--r-----  1 john.doe  staff  586 Oct 24 18:10 console-release.pub

./TaniumServer/content_public_keys/content:
total 8
drwxr-x---  3 john.doe  staff   96 Nov  2 10:31 .
drwxr-x---  5 john.doe  staff  160 Oct 24 18:10 ..
-r--r-----  1 john.doe  staff  586 Oct 24 18:10 content-release.pub

./TaniumServer/content_public_keys/manifest:
total 8
drwxr-x---  3 john.doe  staff   96 Nov  2 10:31 .
drwxr-x---  5 john.doe  staff  160 Oct 24 18:10 ..
-r--r-----  1 john.doe  staff  586 Oct 24 18:10 manifest-release.pub

./TaniumZoneServer:
total 208
drwxr-xr-x   4 john.doe  staff    128 Nov  2 14:18 .
drwxr-xr-x@ 11 john.doe  staff    352 Nov  2 14:24 ..
-rw-r-----   1 john.doe  staff  86016 Nov  2 14:05 pki.db
-rw-r-----   1 john.doe  staff  20480 Nov  2 10:31 zoneserver.db

./config:
total 104
drwxr-xr-x  13 john.doe  staff   416 Nov  2 14:06 .
drwxr-xr-x@ 11 john.doe  staff   352 Nov  2 14:24 ..
-rw-r--r--   1 john.doe  staff    36 Nov  2 14:06 .tanium-user-key-encryption.key
-rw-r--r--   1 john.doe  staff   171 Nov  2 14:05 TaniumServer-TDL-config.txt
-rw-r--r--   1 john.doe  staff   994 Nov  2 14:05 TaniumServer-config.txt
-rw-r--r--   1 john.doe  staff   122 Nov  2 14:05 TaniumZoneServer-config.txt
-r-xr-xr-x   1 john.doe  staff  8041 Nov  2 14:05 Appliance_array.json
drwxr-xr-x   3 john.doe  staff    96 Nov  2 14:06 certs
-rw-r--r--   1 john.doe  staff  1299 Nov  2 14:05 fstab
-rw-r--r--   1 john.doe  staff   126 Nov  2 14:05 ifcfg-ens160
-rw-r--r--   1 john.doe  staff    78 Nov  2 14:05 ifcfg-lo
-rw-r--r--   1 john.doe  staff  4701 Nov  2 14:06 slapd.ldif
-rw-r--r--   1 john.doe  staff  4563 Nov  2 14:05 tanos_environment

./config/certs:
total 0
drwxr-xr-x   3 john.doe  staff   96 Nov  2 14:06 .
drwxr-xr-x  13 john.doe  staff  416 Nov  2 14:06 ..
drwxr-xr-x   3 john.doe  staff   96 Nov  2 14:06 root

./config/certs/root:
total 16
drwxr-xr-x  3 john.doe  staff    96 Nov  2 14:06 .
drwxr-xr-x  3 john.doe  staff    96 Nov  2 14:06 ..
-rw-r--r--  1 john.doe  staff  7732 Nov  2 14:06 redhat-uep.pem

./database:
total 7360
drwxr-xr-x   3 john.doe  staff       96 Nov  2 14:05 .
drwxr-xr-x@ 11 john.doe  staff      352 Nov  2 14:24 ..
-rw-r--r--   1 john.doe  staff  3764562 Nov  2 14:06 tsdb.pgdump

./enc_ssl:
total 16
drwxr-xr-x   5 john.doe  staff  160 Nov  2 14:05 .
drwxr-xr-x@ 11 john.doe  staff  352 Nov  2 14:24 ..
-rw-r--r--   1 john.doe  staff   33 Nov  2 14:05 iv.txt
```

©2026 Tanium Inc. All Rights Reserved

```
drwxr-xr-x   3 john.doe  staff   96 Nov  2 14:05 pubkeys
-rw-r--r--   1 john.doe  staff  384 Nov  2 14:05
symmetric.enc.24cc7840d640bbcc6a15a756c49428e50323c2d9

./enc_ssl/pubkeys:
total 8
drwxr-xr-x  3 john.doe  staff   96 Nov  2 14:05 .
drwxr-xr-x  5 john.doe  staff  160 Nov  2 14:05 ..
-rw-r--r--  1 john.doe  staff  624 Nov  2 14:05 24cc7840d640bbcc6a15a756c49428e50323c2d9.pub
```

Sample contents of a comprehensive recovery bundle

```
$ ls -laR
total 40
drwxr-xr-x@ 11 john.doe  staff   352 Nov  2 14:31 .
drwxrwxrwx@ 46 john.doe  staff  1472 Nov  2 14:29 ..
-rw-r--r--@  1 john.doe  staff  6148 Nov  2 14:30 .DS_Store
-rw-r--r--   1 john.doe  staff  2238 Nov  2 14:06 README.txt
drwxr-xr-x  12 john.doe  staff   384 Nov  2 14:31 TaniumServer
drwxr-xr-x   4 john.doe  staff   128 Nov  2 14:31 TaniumZoneServer
drwxr-xr-x  13 john.doe  staff   416 Nov  2 14:06 config
drwxr-xr-x   3 john.doe  staff    96 Nov  2 14:06 database
-rwxr-xr-x   1 john.doe  staff  1493 Nov  2 14:06 decrypt-payload.sh
drwxr-xr-x   5 john.doe  staff   160 Nov  2 14:06 enc_ssl
-rw-r--r--   1 john.doe  staff  1090 Nov  2 14:07 manifest.txt

./TaniumServer:
total 288
drwxr-xr-x   12 john.doe  staff    384 Nov  2 14:31 .
drwxr-xr-x@  11 john.doe  staff    352 Nov  2 14:31 ..
drwxr-x---    4 john.doe  staff    128 Nov  2 10:31 Backup
drwxr-x---  999 john.doe  staff  31968 Nov  2 11:59 Downloads
-r--------    1 john.doe  staff   1111 Oct  9 14:55 SOAPServer.crt
-r--------    1 john.doe  staff   1704 Oct  9 14:55 SOAPServer.key
drwxr-x---    5 john.doe  staff    160 Oct 24 18:10 content_public_keys
-rw-r-----    1 john.doe  staff  90112 Nov  2 14:05 pki.db
-rw-r-----    1 john.doe  staff  20480 Nov  2 10:31 server.db
-rw-r-----    1 john.doe  staff    158 Oct  9 14:55 tanium.pub
-rw-r-----    1 john.doe  staff  20480 Oct  9 14:55 tdownloader.db
-rw-r-----    1 john.doe  staff   1133 Oct  9 15:01 trusted-module-servers.crt

./TaniumServer/Backup:
total 352
drwxr-x---   4 john.doe  staff    128 Nov  2 10:31 .
drwxr-xr-x  12 john.doe  staff    384 Nov  2 14:31 ..
-rw-r-----   1 john.doe  staff  90112 Nov  2 10:31 pki-backup.db
-rw-r-----   1 john.doe  staff  90112 Oct  9 15:12 pki.db

./TaniumServer/Downloads:
total 1815088
drwxr-x---  999 john.doe  staff      31968 Nov  2 11:59 .
drwxr-xr-x   12 john.doe  staff        384 Nov  2 14:31 ..
-rw-r-----    1 john.doe  staff         56 Nov  2 11:50
005a3cd39f819b3392cc39f99e62f7831c1011c95d971f9
c23d8cbadc00642a9
-rw-r-----    1 john.doe  staff      15738 Nov  2 11:59
00dbf6a76715a7c3d4005b7ca451d23985a6e060300b241
29f7a7933c73a3fb1
-rw-r-----    1 john.doe  staff       4068 Nov  2 11:29
027e5bf6248a58f3f73e6f51a72bd9e0d21cf6de75c6e6c
f27ead0b62514fe52
drwxr-x---  281 john.doe  staff       8992 Nov  2 11:57 DownloadAttempts
```

©2026 Tanium Inc. All Rights Reserved

```
-rw-r-----    1 john.doe  staff        269 Oct  9 15:08 DownloadProgress_1
-rw-r-----    1 john.doe  staff         76 Oct  9 15:08 DownloadProgress_1.modified
-rw-r-----    1 john.doe  staff        205 Oct  9 15:08 DownloadProgress_10
-rw-r-----    1 john.doe  staff        269 Nov  2 11:48 DownloadProgress_100
-rw-r-----    1 john.doe  staff         85 Nov  2 11:15 DownloadProgress_100.error
-rw-r-----    1 john.doe  staff         76 Nov  2 11:48 DownloadProgress_100.modified
-rw-r-----    1 john.doe  staff        269 Nov  2 11:48 DownloadProgress_101
-rw-r-----    1 john.doe  staff         85 Nov  2 11:15 DownloadProgress_101.error
-rw-r-----    1 john.doe  staff         76 Nov  2 11:48 DownloadProgress_101.modified
-rw-r-----    1 john.doe  staff      13461 Nov  2 11:37
a06ce519c0b087489a32c4d4cac24fbc914ec7ca085b0dc
a53fd49a222e5cf1d
-rw-r-----    1 john.doe  staff      99192 Nov  2 11:56
a0cfcbfcfbf9d28f07e10c209df01b35e48e65ab77b3985
eb30eb74b7112f0e6
-rw-r-----    1 john.doe  staff        262 Nov  2 11:37
a144a623d5d8019c8628d020189a74df67d4a06c5d43bf8
b3f9dbbf70f9bf4f7
-rw-r-----    1 john.doe  staff  102047744 Nov  2 11:18 tdl-crls.db
drwxr-x---    2 john.doe  staff         64 Nov  2 11:59 tmp
-rw-r-----    1 john.doe  staff         68 Nov  2 10:31 upload_hosts.txt

./TaniumServer/Downloads/DownloadAttempts:
total 2232
drwxr-x---  281 john.doe  staff   8992 Nov  2 11:57 .
drwxr-x---  999 john.doe  staff  31968 Nov  2 11:59 ..
-rw-r-----    1 john.doe  staff    257 Oct  9 15:08 1.json
-rw-r-----    1 john.doe  staff    266 Oct  9 15:04 10.json
-rw-r-----    1 john.doe  staff    268 Oct  9 15:06 11.json
-rw-r-----    1 john.doe  staff    284 Oct  9 15:06 12.json
-rw-r-----    1 john.doe  staff    284 Oct  9 15:06 13.json
-rw-r-----    1 john.doe  staff    278 Oct  9 15:06 14.json
-rw-r-----    1 john.doe  staff    274 Oct  9 15:06 15.json
-rw-r-----    1 john.doe  staff    276 Oct  9 15:06 16.json
-rw-r-----    1 john.doe  staff    280 Oct  9 15:06 17.json
-rw-r-----    1 john.doe  staff    293 Oct  9 15:09 18.json
-rw-r-----    1 john.doe  staff    268 Oct  9 15:09 19.json
-rw-r-----    1 john.doe  staff    265 Oct  9 15:08 2.json
-rw-r-----    1 john.doe  staff    266 Oct  9 15:08 20.json
-rw-r-----    1 john.doe  staff    276 Oct  9 15:08 21.json
-rw-r-----    1 john.doe  staff    286 Oct  9 15:08 22.json
-rw-r-----    1 john.doe  staff    283 Oct  9 15:08 23.json
-rw-r-----    1 john.doe  staff    274 Oct  9 15:08 24.json
-rw-r-----    1 john.doe  staff    279 Oct  9 15:08 25.json
-rw-r-----    1 john.doe  staff    277 Oct  9 15:08 26.json
-rw-r-----    1 john.doe  staff    268 Oct  9 15:08 27.json
-rw-r-----    1 john.doe  staff    286 Oct  9 15:08 28.json
-rw-r-----    1 john.doe  staff    284 Oct  9 15:08 29.json
-rw-r-----    1 john.doe  staff    271 Oct  9 15:08 3.json
-rw-r-----    1 john.doe  staff    269 Oct  9 15:08 30.json
-rw-r-----    1 john.doe  staff    268 Oct  9 15:08 31.json
-rw-r-----    1 john.doe  staff    258 Oct  9 15:08 32.json
-rw-r-----    1 john.doe  staff    271 Oct  9 15:08 33.json
-rw-r-----    1 john.doe  staff    268 Oct  9 15:08 4.json
-rw-r-----    1 john.doe  staff    266 Oct  9 15:08 43.json
-rw-r-----    1 john.doe  staff    260 Oct  9 15:08 5.json
-rw-r-----    1 john.doe  staff    280 Oct  9 15:08 6.json
-rw-r-----    1 john.doe  staff    276 Oct  9 15:08 7.json
-rw-r-----    1 john.doe  staff    276 Oct  9 15:08 8.json
-rw-r-----    1 john.doe  staff    263 Oct  9 15:08 9.json

./TaniumServer/Downloads/tmp:
total 0
drwxr-x---    2 john.doe  staff     64 Nov  2 11:59 .
```

©2026 Tanium Inc. All Rights Reserved

```
drwxr-x---  999 john.doe  staff  31968 Nov  2 11:59 ..

./TaniumServer/content_public_keys:
total 0
drwxr-x---   5 john.doe  staff  160 Oct 24 18:10 .
drwxr-xr-x  12 john.doe  staff  384 Nov  2 14:31 ..
drwxr-x---   3 john.doe  staff   96 Nov  2 10:31 console
drwxr-x---   3 john.doe  staff   96 Nov  2 10:31 content
drwxr-x---   3 john.doe  staff   96 Nov  2 10:31 manifest

./TaniumServer/content_public_keys/console:
total 8
drwxr-x---  3 john.doe  staff   96 Nov  2 10:31 .
drwxr-x---  5 john.doe  staff  160 Oct 24 18:10 ..
-r--r-----  1 john.doe  staff  586 Oct 24 18:10 console-release.pub

./TaniumServer/content_public_keys/content:
total 8
drwxr-x---  3 john.doe  staff   96 Nov  2 10:31 .
drwxr-x---  5 john.doe  staff  160 Oct 24 18:10 ..
-r--r-----  1 john.doe  staff  586 Oct 24 18:10 content-release.pub

./TaniumServer/content_public_keys/manifest:
total 8
drwxr-x---  3 john.doe  staff   96 Nov  2 10:31 .
drwxr-x---  5 john.doe  staff  160 Oct 24 18:10 ..
-r--r-----  1 john.doe  staff  586 Oct 24 18:10 manifest-release.pub

./TaniumZoneServer:
total 208
drwxr-xr-x   4 john.doe  staff    128 Nov  2 14:31 .
drwxr-xr-x@ 11 john.doe  staff    352 Nov  2 14:31 ..
-rw-r-----   1 john.doe  staff  86016 Nov  2 14:06 pki.db
-rw-r-----   1 john.doe  staff  20480 Nov  2 10:31 zoneserver.db

./config:
total 104
drwxr-xr-x  13 john.doe  staff   416 Nov  2 14:06 .
drwxr-xr-x@ 11 john.doe  staff   352 Nov  2 14:31 ..
-rw-r--r--   1 john.doe  staff    36 Nov  2 14:06 .tanium-user-key-encryption.key
-rw-r--r--   1 john.doe  staff   171 Nov  2 14:06 TaniumServer-TDL-config.txt
-rw-r--r--   1 john.doe  staff   994 Nov  2 14:06 TaniumServer-config.txt
-rw-r--r--   1 john.doe  staff   122 Nov  2 14:06 TaniumZoneServer-config.txt
-r-xr-xr-x   1 john.doe  staff  8041 Nov  2 14:06 Appliance_array.json
drwxr-xr-x   3 john.doe  staff    96 Nov  2 14:06 certs
-rw-r--r--   1 john.doe  staff  1299 Nov  2 14:06 fstab
-rw-r--r--   1 john.doe  staff   126 Nov  2 14:06 ifcfg-ens160
-rw-r--r--   1 john.doe  staff    78 Nov  2 14:06 ifcfg-lo
-rw-r--r--   1 john.doe  staff  4701 Nov  2 14:06 slapd.ldif
-rw-r--r--   1 john.doe  staff  4563 Nov  2 14:06 tanos_environment

./config/certs:
total 0
drwxr-xr-x   3 john.doe  staff   96 Nov  2 14:06 .
drwxr-xr-x  13 john.doe  staff  416 Nov  2 14:06 ..
drwxr-xr-x   3 john.doe  staff   96 Nov  2 14:06 root

./config/certs/root:
total 16
drwxr-xr-x  3 john.doe  staff    96 Nov  2 14:06 .
drwxr-xr-x  3 john.doe  staff    96 Nov  2 14:06 ..
-rw-r--r--  1 john.doe  staff  7732 Nov  2 14:06 redhat-uep.pem

./database:
```

©2026 Tanium Inc. All Rights Reserved

```
total 7360
drwxr-xr-x   3 john.doe  staff       96 Nov  2 14:06 .
drwxr-xr-x@ 11 john.doe  staff      352 Nov  2 14:31 ..
-rw-r--r--   1 john.doe  staff  3764519 Nov  2 14:06 tsdb.pgdump

./enc_ssl:
total 16
drwxr-xr-x   5 john.doe  staff  160 Nov  2 14:06 .
drwxr-xr-x@ 11 john.doe  staff  352 Nov  2 14:31 ..
-rw-r--r--   1 john.doe  staff   33 Nov  2 14:06 iv.txt
drwxr-xr-x   3 john.doe  staff   96 Nov  2 14:06 pubkeys
-rw-r--r--   1 john.doe  staff  384 Nov  2 14:06
symmetric.enc.24cc7840d640bbcc6a15a756c49428e50323c2d9

./enc_ssl/pubkeys:
total 8
drwxr-xr-x  3 john.doe  staff   96 Nov  2 14:06 .
drwxr-xr-x  5 john.doe  staff  160 Nov  2 14:06 ..
-rw-r--r--  1 john.doe  staff  624 Nov  2 14:06 24cc7840d640bbcc6a15a756c49428e50323c2d9.pub
```

Configure automatic core or comprehensive backups

About this task

Use TanOS to schedule automatic core and comprehensive backups for the Tanium Appliance.

Tip: After you perform the initial setup for an Appliance, a core backup is scheduled by default.

The TanOS health check reports an error that automatic backups cannot complete until you set up an encryption key. To remove the error from the health check, you can either add an encryption key or disable the scheduled core backup. For more information about the TanOS health check, see Run the Health Check on page 488.

The general process to set up an automatic backup includes the following steps:

1. Add an encryption key for all backups.
2. Configure a core or comprehensive backup.
3. Test the automatic backup.
4. Schedule the automatic backup.

Result

When you schedule an automatic backup, TanOS prompts you to select a remote host to which to save the recovery bundle. TanOS also saves the recovery bundle to the /outgoing directory, where

©2026 Tanium Inc. All Rights Reserved

you can use SFTP to download the recovery bundle.

ADD ENCRYPTION KEY FOR THE BACKUPS

About this task

Encrypt all core and comprehensive backup recovery bundles with a key pair. Encryption is required for both automatic and manual backups.

1. Use OpenSSL to generate a public/private key pair in a PEM file. Enter a passphrase when prompted.
   ```
   openssl genrsa -aes256 -out ssl-pvk.pem 3072
   ```
2. (FIPS mode only) For customers that need to decrypt backup bundles on a FIPS-enabled Appliance, encrypt your backup key using the following command:
   ```
   openssl pkcs8 -topk8 -in OLD_FILENAME.pem -v2 aes-256-cbc -out NEW_FILENAME.pem
   ```
3. Extract the public key from the PEM file. Enter your passphrase when prompted.
   ```
   openssl pkey -in ssl-pvk.pem -pubout -out ssl-pub.pem
   ```
4. Extract the identifier for the public key. This identifier is visible in the backup file and can be useful to find a particular public key.
   ```
   openssl pkey -pubin -in ssl-pub.pem -outform DER | openssl dgst -sha1
   ```
5. Copy the contents of the ssl-pub.pem file (the public key) to the clipboard.
6. Sign in to the TanOS console as a user with the `tanadmin` role.
7. Enter `B`-`1` (Appliance Maintenance > Backup).
8. Enter `E`, paste the public key from the clipboard, and press **Ctrl**-**D**.

```
-----------------------------------------------------

       >>> Appliance Maintenance -> Backup <<<

           Automatic Backups

         E: Set Encryption Key
         C: Configure Automatic Backup
```

©2026 Tanium Inc. All Rights Reserved

```
          A: Run Automatic Backup Now
          S: Schedule Automatic Backup

            Manual Backups

          P: Partition Sync
          N: Core Backup
          F: Comphrehensive Backup
          L: List Database Backups

          R: Return to previous menu  RR: Return to top

 ------------------------------------------------------

 TanOS Version:1.9.1

 Please select: E
Paste the PEM public key then press Ctrl-D
-----BEGIN PUBLIC KEY-----
MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAxlgJIiY7Lxq0OtQYP1ic
l6QKvpiLTiMFprfGx5HpvjED8ea90k3NLs4gqKCnNfqzoflBDam12jdtqm0XM7TD
ythv8tPL2qoCk8HRilJzRQqk8YpAw0tz2tgvl9WqZfjIrRgN/CReTPxXg08OTr8g
8v/P8NY/IHs2xEQttC3ALgwlUpjEnIfZIYvGX/sFLioTCiuntIEDZqDRd086FC8K
6Zrdz6z8Rb9iCZu//Usc5o+uNpVJT2iOjXsSt5ZnWZzF6LlgwI/RPB1UZ+loCRQP
/A8vpp3FcyjcE04XYgMRFJI1/fiGI9MzZC0V2Ki2dAWJERN37+11CeLZip0AXf5T
q7psBQwu9I85q681F/aGZ9vsJuX0JTkEKzKJdoGiWsmuUVNUX3gUrLQHNf0OBtx2
7yivtj2dQAdjE8qGFKoZ/ndUqX/BYg6FCktMvwqmMtVVlKyWTl4g/h75tvmMBKOS
H3iCa4S+jag34+D1J8q9YAU0t7m9EY3uXzQIdvkCJWAFAgMBAAE=
-----END PUBLIC KEY-----
Successfully imported key 24cc7840d640bbcc6a15a756c49428e50323c2d9
 Press enter to continue
```

9. Press **Enter** to go to the **Backup** menu.
10. To test the encryption, perform a manual core backup using the steps described in Manually run a core or comprehensive backup on page 412.
    a. After the backup completes, download the recovery bundle. Note that you are not prompted to set a password.

©2026 Tanium Inc. All Rights Reserved

b. Extract the recovery bundle. The folder contains a README.txt file that describes how to decrypt the recovery bundle.

CONFIGURE AN AUTOMATIC BACKUP

About this task

In a new installation with a Tanium role installed, an automatic core backup is scheduled to run nightly at 2:01 AM UTC. You can edit the backup, disable the backup, or configure an automatic comprehensive backup.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-1-C` (Appliance Maintenance > Backup > Configure Automatic Backup).
3. Select the type of backup to configure:

```
 ------------------------------------------------------


       >>> Maintenance -> Backup -> Configure <<<


Type                    Enabled         Export (SCP)    Scheduled
===============         =======         ============    =========
Core                    no              no              yes
Comprehensive           no              no              no


          N: Configure Core Backup
          F: Configure Comprehensive Backup


          R: Return to previous menu  RR: Return to top


 ------------------------------------------------------
```

   - To configure a core backup, enter `N`.
   - To configure a comprehensive backup, enter `F`.

4. Follow the prompts to enable the backup and to specify file transfer options.
   - Automatic backups always save the recovery bundles to the /outgoing directory for download with SFTP.

©2026 Tanium Inc. All Rights Reserved

- You can specify a username and IP address for a destination server to reach with secure copy protocol (SCP). If you set up a file transfer with SCP, copy the public SSH key of the TanOS user that you are using to configure and run the backup to the remote user's ~/.ssh/authorized_keys file on the remote system. Ensure proper privileges on the remote system; you may need to run CHMOD 600 on the ~/.ssh/authorized_keys file.

  To locate a TanOS user's public SSH key to copy and store in the remote user's authorized keys file, sign in to the TanOS menu and navigate to **User Administration**`C` > **TanOS**`U` > **user**`#` > **Key Pair**`P`. The public SSH key is presented for copying.

  The backup files are stored on the remote system at /home/<remote user>/ .

  For information about managing TanOS user SSH keys, see Manage SSH keys for TanOS users on page 227.

TEST AN AUTOMATIC BACKUP

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B`-`1`-`A` (Appliance Maintenance > Backup > Run Now).
3. Select the type of backup to run.
4. Verify the backup settings and enter `Yes` to run the backup.
5. Verify the backup completes successfully.
   - If the backup exports the recovery bundle to a remote server with SCP, sign in to the remote server and verify the recovery bundle exists.
   - Extract the recovery bundle. The folder contains a README.txt file that describes how to decrypt the recovery bundle.

```
          >>> Maintenance -> Backup -> Run Core Now <<<

Current Backup Configuration

Enabled:                  yes
TanOS User:               tanadmin
```

©2026 Tanium Inc. All Rights Reserved

```
 Export via SCP:           no
 Remote SCP Host:
 Remote SCP User:
 Remote SCP Directory:

 Run automatic backup now with these settings? [Yes|No]: yes

Searching for files to include in the Recovery Bundle
Capturing TaniumServer database snapshot
Packaging and encrypting Recovery Bundle
Backup file copied to outgoing
Finished processing core Recovery Bundle.
 Successfully completed the scheduled backup

 Press enter to continue
```

SCHEDULE AN AUTOMATIC BACKUP

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-1-S` (Appliance Maintenance > Backup > Schedule).
3. Select the type of backup to view the schedule settings. The schedule settings include the current settings and the pending settings.

```
            >>> Maintenance -> Backup -> Schedule Core <<<

Current time: Thu 2022-03-07 20:09:55 UTC
Active : Disabled
Every Day          | 02:01 UTC
Crontab formatted time string: 01 02 * * *

Pending: Disabled
Day of Month | 1             | 00:00 UTC
Crontab formatted time string: 00 00 1 * *
```

©2026 Tanium Inc. All Rights Reserved

```
        1: Disable Schedule
        2: Enable Schedule

        4: Schedule by Day of Month
        5: Schedule by Day of Week
        6: Select Time of Day

        7: Activate Schedule Settings

        R: Return to previous menu  RR: Return to top

--------------------------------------------------------
```

- Enter `1` to disable the backup.
- Enter `2` to enable the backup.
- Enter `4` to enter the days of the month to run the backup. You can enter a date range or comma-separated days.
- Enter `5` to enter the days of the week to run the backup. You can enter a range or comma-separated values.
- Enter `6` to select the time to run the backup. Enter the hours and minutes in UTC time.
- To confirm the pending settings, enter `7` to activate the settings. The active settings update to match the pending settings.



Important: If you enter `R` and do not activate the settings, the changes do not save.

VIEW LOG FILES AFTER A BACKUP

About this task

If a backup fails, you can review the TanOS log file for additional information.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-1-1-1` (Tanium Support Menu > Tanium Log Files > TanOS Appliance > TanOS Log).
3. Enter `V` to view the current log file, or enter the line number of a previous log file if the relevant log entries have been rotated out of the current log file.

©2026 Tanium Inc. All Rights Reserved

Manually run a core or comprehensive backup

About this task

> **Note:** You must encrypt all backups with a key pair. Encryption is required for both automatic and manual backups. For information about how to set up encryption, see Add encryption key for the backups on page 406.

Complete the following steps to perform a manual backup of the Tanium Appliance:

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-1` (Appliance Maintenance > Backup).
3. Use the menu to create a backup:
   - Enter `N` to go to the **Backup off-box Core** menu.
   - Enter `F` to go to the **Backup off-box Comprehensive** menu.
4. Follow the prompts to confirm the backup and to specify file transfer options. You can save the backup file to the /outgoing directory for download with SFTP, and you can specify a username and IP address for a destination server that can be reached with secure copy protocol (SCP).

```
           >>> Appliance Maintenance -> Backup/Restore -> Backup off-box
Comprehensive <<<

 The remote backup will:
 - stop services during file collection (TMS comprehensive only)
 - create an archive with appropriate files
 - encrypt the archive using the pre-arranged public key
 - transfer the backup via scp (optional)
 - provide the backup for sftp download (optional)

 The backup will be deleted at the end; a transfer option MUST be chosen.

 Would you like to continue with a Comprehensive backup? [Yes|No]: yes
```

©2026 Tanium Inc. All Rights Reserved

```
Would you like to make this backup available for download via sftp? [Yes|No]: yes

If you'd like to copy this backup file to a remote system via scp, ensure
that the public key of tanadmin has been added to the authorized keys of
the user on the target system. The file will be placed in the home directory
of that user.

Would you like to transfer the file via scp to a remote location? [Yes|No]: no
Searching for files to include in the Recovery Bundle
Capturing TaniumServer database snapshot
Packaging and encrypting Recovery Bundle
Backup file copied to outgoing
Finished processing comp Recovery Bundle.
Press enter to continue
```

5. After the backup completes, press **Enter** to go to the **Backup** menu.

REVIEW THE TANOS LOG FILE

About this task

If a backup fails, you can review the TanOS log file for additional information.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-1-1-1` (Tanium Support Menu > Tanium Log Files > TanOS Appliance > TanOS Log).
3. Enter `V` to view the current log file, or enter the line number of a previous log file if the relevant log entries have been rotated out of the current log file.

Use a comprehensive recovery bundle to perform a full restoration of the TanOS or Tanium environment

You can perform a full restoration of the Tanium environment using a comprehensive recovery bundle.

©2026 Tanium Inc. All Rights Reserved

Note: Each environment presents unique considerations, and the restoration process may vary depending on your specific needs. A full restoration rebuilds the TanOS environment, similar to the initial setup or a migration, and it might take significant time to complete. To engage the appropriate Tanium resources for additional guidance and support during restoration, contact Tanium Support on page 510.

Tip: To perform a limited restoration to recover from database issues using a core recovery bundle, contact Tanium Support on page 510.

PREPARE A NEW INSTALLATION FOR RESTORATION

1. If you are using any existing Appliances, reset TanOS. For more information, see Perform a TanOS reset on page 463.
2. Follow the initial configuration steps relevant to your TanOS environment for each new or reset Appliance:
   - Completing the initial setup (physical Tanium Appliance) on page 60
   - Completing the initial setup (virtual Tanium Appliance) on page 93
   - Completing the initial setup (cloud-based Tanium Appliance) on page 130

   Important: Install the same version of TanOS that was installed in the environment that was backed up. If you plan to upgrade, do so only after completing the restoration.
3. Create an Appliance Array, following these specific steps:
   a. Create the Array, and add all Appliances. (Do not assign roles yet.) For more information, see Create the Array on page 161 and Add members to the Array on page 162.
   b. Assign and install roles for *only* the primary Tanium Server and active Module Server. For more information, see Assign roles on page 165 and Install Tanium roles on page 170.

   Important: Install the same version of the Tanium Core Platform that was installed in the environment that was backed up. If you plan to upgrade, do so only after completing the restoration.
4. Completing and verifying the Tanium Core Platform installation on Tanium Appliances on

©2026 Tanium Inc. All Rights Reserved

page 196, including uploading your Tanium license.

5. Import your licensed solutions in Tanium Console. For more information, see Managing Tanium solutions.

   Important: Install a version of each solution from the same semiannual release that was installed in the environment that was backed up. If you encounter issues or need assistance obtaining the appropriate version of a solution, contact Tanium Support on page 510.

RESTORE THE MODULE SERVER

1. Use SFTP to copy the recovery bundle file backed up from the previous Module Server to the /incoming directory on the new Module Server Appliance.
2. Sign in to the TanOS console on the Module Server Appliance as a user with the `tanadmin` role.
3. Enter `B-1-O` (Appliance Maintenance Menu > Backup > Restore from Backup).
4. Enter the line number of the recovery bundle to use and follow the prompts to perform the restoration.

   CAUTION: This procedure overwrites your current configuration. Make sure you want to restore the environment to a backup before you proceed.

RESTORE THE TANIUM SERVER AND REGISTER THE RESTORED MODULE SERVER

1. Use SFTP to copy the recovery bundle file backed up from the previous Tanium Server to the /incoming directory on the Tanium Server Appliance.
2. Sign in to the TanOS console on the Tanium Server Appliance as a user with the `tanadmin` role.
3. Enter `B-1-O` (Appliance Maintenance Menu > Backup > Restore from Backup).
4. Enter the line number of the recovery bundle to use and follow the prompts to perform the restoration.

©2026 Tanium Inc. All Rights Reserved

> **CAUTION:** This procedure overwrites your current configuration. Make sure you want to restore the environment to a backup before you proceed.

5. Follow the steps in Promote the standby Module Server to active on page 387 to register the restored Module Server with the restored Tanium Server.

   > **Note:** Even though the Module Server is currently the only one in the Array and is not a standby Module Server, these steps automatically register it with the Tanium Server.

6. Sign in to Tanium Console on the Tanium Server and verify that the Tanium environment has been restored.

RESTORE THE REMAINING ARRAY MEMBERS

1. Assign and install roles for the secondary Tanium Server, the standby Module Server, and any Zone Servers, and then complete final tasks to configure the Array. For more information, see Assign roles on page 165, Install Tanium roles on page 170, and What to do next on page 171.
2. Sign in to Tanium Console on the secondary Tanium Server and import licensed modules. For more information, see Managing Tanium solutions.

Result

> **Note:** If you use SNMP, the SNMP configuration settings are restored from the backup, but the SNMP service is not re-enabled. To restart the SNMP service, enter `A-5-S` (Appliance Configuration > SNMP Configuration > Set Password and Start the SNMP Service) and re-enter the SNMP password.

VIEW THE LOG FOR THE BACKUP RESTORATION

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-1-1-10` (Tanium Support Menu > Tanium Log Files > TanOS Appliance > Backup Restore Log).
3. Enter `V` to view the current log file, or enter the line number of a previous log file if the relevant log entries have been rotated out of the current log file.

©2026 Tanium Inc. All Rights Reserved

Monitoring and maintaining the Tanium Appliance

Perform regular maintenance tasks to ensure that the Tanium Appliance infrastructure remains in good health. For maintenance tasks to be performed on a routine basis, see Perform monthly maintenance on page 418 and Perform quarterly maintenance on page 419. If an Appliance is not performing as expected, you might need to troubleshoot issues or change settings. For more information, see Tanium Appliance support and troubleshooting on page 487.

Use the **Appliance Maintenance** menu to perform most maintenance tasks, such as backups, system resets, TanOS upgrades, and system reboots or shutdowns. The **Appliance Configuration** menu contains some of the configuration options for ongoing monitoring and maintenance. The **Tanium Support** menu contains several tools to monitor status and run diagnostics.

The subsequent topics in this section provide details about the tasks to monitor and maintain the Tanium Appliance.

Configure monitoring and perform routine maintenance for Tanium Appliances

The subsequent topics in this section provide information about configuring Tanium Appliance monitoring, performing monthly and quarterly maintenance, and an overview of backups.

Configure Tanium Appliance monitoring

Perform any of the following tasks to facilitate monitoring the health of your Tanium deployment and Appliance infrastructure. For example, if your organization has a syslog server or SNMP manager, you can integrate it with the Appliance for monitoring. If these monitoring solutions reveal issues that require resolution, see Tanium Appliance support and troubleshooting on page 487.

CONFIGURE TANOS ALERTS

TanOS can send alerts to a syslog server or to an email recipient. For optimal results, configure an

©2026 Tanium Inc. All Rights Reserved

SMTP email recipient. If the syslog server fails, the SMTP recipient receives a failure notification every 15 minutes until either the failure is resolved or syslog forwarding is disabled. For more information, see Configure syslog alerts on page 436.

CONFIGURE SYSLOG FORWARDING

You can forward Appliance logs to a remote syslog server. The syslog forwarding configuration is separate from the syslog alert configuration. For the differences, and the steps to configure syslog forwarding, see Configure syslog forwarding on page 429.

CONFIGURE SNMP

You can configure integration with an SNMP manager to collect and analyze Appliance information. After you configure credentials, the user `tansnmp` can make a remote SNMP connection to the Appliance or to the Integrated Dell Remote Access Controller (iDRAC) interface of a physical Appliance to conduct SNMP polling from a remote host or SNMP manager. For more information, see Configuring SNMP on page 439.

Perform monthly maintenance

If these tasks reveal issues that require resolution, see Tanium Appliance support and troubleshooting on page 487.

REVIEW THE HEALTH CHECK REPORT

About this task

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

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

MONITOR APPLIANCE PERFORMANCE (OPTIONAL)

©2026 Tanium Inc. All Rights Reserved

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

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

Perform quarterly maintenance

VERIFY THE GRUB KEY BACKUP

About this task

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

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

   Note: A new backup is required whenever the key password is regenerated. For more information, see Change the GRUB key password on page 377.

2. Export the key and save it in a safe location if no backup exists or if the current backup is not the latest. For more information, see Export the GRUB key on page 375.

REVIEW AND UPDATE TANOS USER ACCOUNTS

1. On each Appliance, review the TanOS system users to ensure that they can access the Appliance operating system and that they have the appropriate authentication settings. For example, users who authenticate through passwords must comply with the password policy of your organization. For more information, see Configure security policy rules on page 361.

©2026 Tanium Inc. All Rights Reserved

> **Tip:** The health check reports any TanOS user password that has expired or that expires within 14 days, so you do not need to check expiration dates manually during this review.

The predefined roles for TanOS system users include:

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

For more information, see Managing TanOS users on page 225.

2. Verify that the predefined `tanremote` user account is present if you configured an Integrated Dell Remote Access Controller (iDRAC) interface on the physical Appliance. The account provides remote access to the iDRAC virtual console. This is useful for diagnosing hardware and network interface issues if the TanOS system becomes unavailable. For more information, see Manage the iDRAC interface (physical Tanium Appliances only) on page 420.

Backup overview

TanOS contains the options to perform *core* and *comprehensive* backups. Physical Tanium Appliances and virtual Tanium Appliances with inactive partitions also have the option to back up the active partition to the inactive partition. On virtual Tanium Appliances and cloud-based Tanium Appliances, you can also take a snapshot of the Appliance image. For core and comprehensive backups, you can schedule automatic backups or perform a manual backup.

> **Tip:** For more information and steps, see Tanium Appliance redundancy, backup, and recovery on page 379.

Manage the iDRAC interface (physical Tanium Appliances only)

Use the `tanremote` user account to sign in to the iDRAC virtual console to diagnose hardware and

©2026 Tanium Inc. All Rights Reserved

network interface issues in the event the TanOS system becomes unavailable. The `tanremote` user is not a TanOS user or a Tanium Console user.

Before you begin

You must use a cable to connect the iDRAC interface to your network and use TanOS to configure the iDRAC interface before you enable the `tanremote` user.

Configure the iDRAC interface

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-I` (Appliance Configuration > Manage iDRAC).
3. Enter `N` and follow the prompts to configure the iDRAC interface.

Set password for the tanremote user

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-I` (Appliance Configuration > Manage iDRAC).
3. Enter `P` and follow the prompts to change the password of the `tanremote` user.

```
            >>> Appliance Configuration -> Manage iDRAC -> Set iDRAC Password <<<

 This will change the iDRAC user tanremote password.
 Access to the iDRAC is via the specific iDRAC IP.

Would you like to change the tanremote password? [YES/NO]: yes



The password policy requires meeting these rules:
 - Minimum 10 characters long
 - Maximum 20 characters long
 - At least 1 upper case character
 - At least 1 lower case character
 - At least 1 numeric character
```

©2026 Tanium Inc. All Rights Reserved

```
- At least 1 other character
- Must not be based on a dictionary word
- Must not contain part of the username


Please enter password (will not be displayed):
```

Enable the tanremote user

About this task

Best Practice: Set the password for the `tanremote` user before you enable the user.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-I` (Appliance Configuration > Manage iDRAC).
3. Enter `E` and follow the prompts to enable the `tanremote` user.

Disable the tanremote user

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-I` (Appliance Configuration > Manage iDRAC).
3. Enter `D` and follow the prompts to disable the `tanremote` user.

Close all iDRAC sessions

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-I` (Appliance Configuration > Manage iDRAC).
3. Enter `C` and follow the prompts the close all iDRAC sessions.

Reset iDRAC

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-I` (Appliance Configuration > Manage iDRAC).

©2026 Tanium Inc. All Rights Reserved

3. Enter `K` and follow the prompts to reset the iDRAC interface.

Import a custom certificate for the iDRAC interface

About this task

You can import your own server authentication certificate and key for encrypting communication with the iDRAC interface on a Tanium Appliance.

1. Use SFTP to copy the certificate and private key files to the /incoming directory of the Tanium Server Appliance.

   Note:

   - The private key file must be unencrypted.
   - You cannot import a PFX directly. To extract the necessary files, see Extract a certificate and key from a PFX file on page 424.

2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `A`-`A`-`C` (Appliance Configuration > Security > iDRAC Certificate Management).
4. Enter `1` and follow the prompts to import the iDRAC certificate file.

```
            >>> Select iDRAC Certificate <<<

Pick a certificate (*.pem or *.crt) to import. Press ENTER to re-scan the
incoming directory.

    1: mycert.pem                          4.5K
       subject=C = US, ST = CA, L = Emeryville, O = domain.com, CN = tanos-lab,
emailAddress = user@domain.com

    R: Return to previous menu  RR: Return to top

Please select: 1

Examining mycert.pem
```

©2026 Tanium Inc. All Rights Reserved

```
MD5: 9e64a1b36a326e030a37090413cae2c4

Valid through: May 26 22:13:36 2024 GMT
Subject: C=US, ST=CA, L=Emeryville, O=domain.com, CN=tanos-lab/
emailAddress=user@domain.com
Valid through: Jul  7 00:12:49 2030 GMT
Subject: C=US, ST=CA, O=domain.com, OU=domain.com Certificate Authority,
CN=domain.com Intermediate CA/emailAddress=user@domain.com



Use this file? [Yes|No]: y

Uploading the selected key
SSL key successfully uploaded to the RAC.
Uploading the selected certificate
Web server is restarting to complete the certificate update. Please wait for
a few minutes for this process to complete.

Press enter to continue
```



Best Practice: After you successfully import the certificate and key, delete the private key file from you local computer.

EXTRACT A CERTIFICATE AND KEY FROM A PFX FILE

About this task

Though you cannot use a PFX file directly to supply a certificate and key, you can extract them from the file using the OpenSSL utility.

1. Use OpenSSL to extract the certificate file. When prompted, enter the passphrase that was used to encrypt the PFX file.

```
openssl pkcs12 -in mycert.pfx -nokeys -out idracpublic.pem
```

2. Use OpenSSL to extract the encrypted private key. When prompted, enter the passphrase that was used to encrypt the PFX file and a new password to temporarily encrypt the private

©2026 Tanium Inc. All Rights Reserved

key.

```
openssl pkcs12 -in mycert.pfx -nocerts -out idracprivateencrypted.key
```

3. Decrypt the private key. When prompted, enter the passphrase that you used to encrypt the private key file in the previous step.

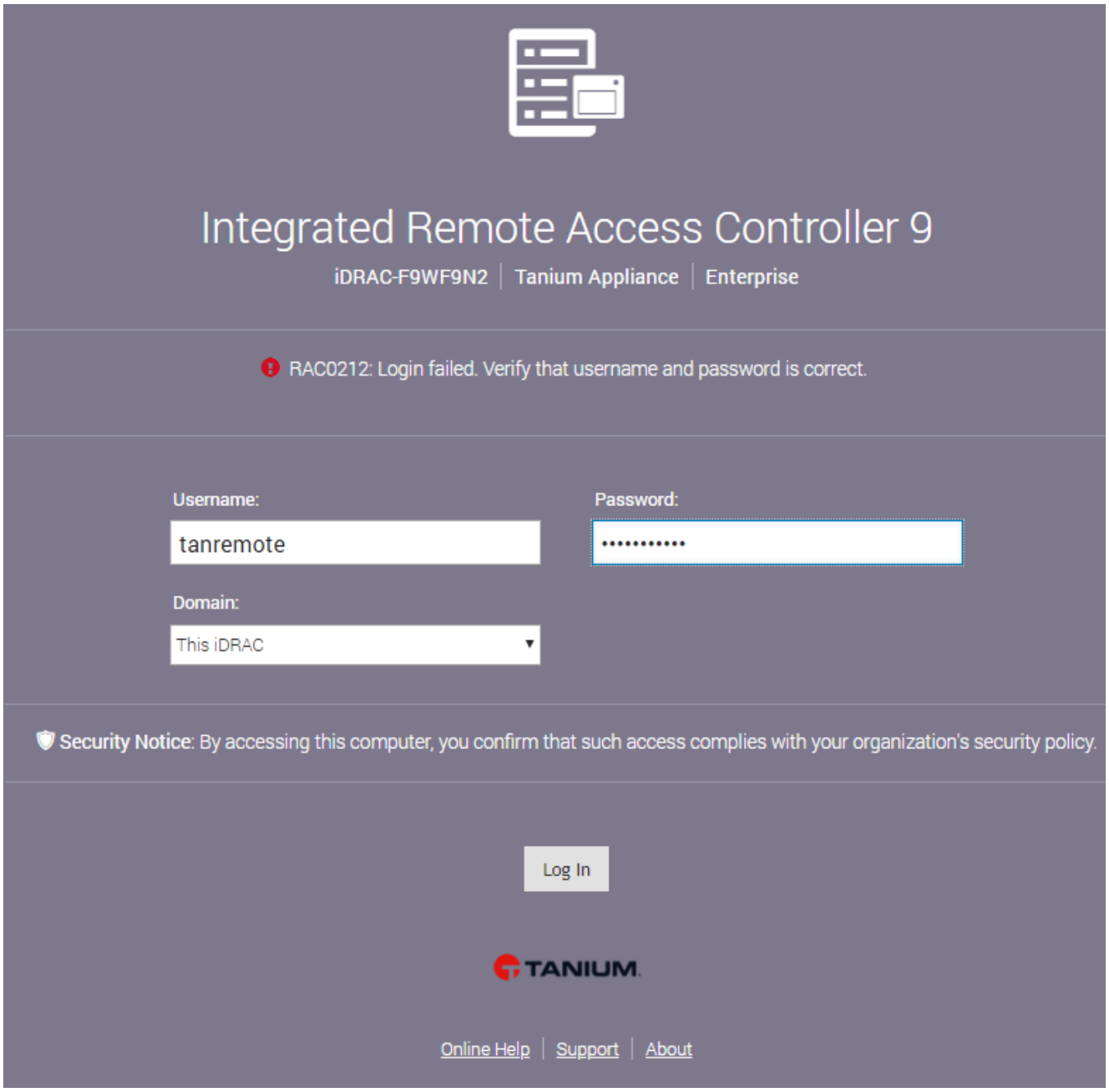
```
opensslrsa -in idracprivateencrypted.key -out idracprivate.key
```

Access the iDRAC virtual console

You can access the iDRAC virtual console at `http://<iDRAC interface IP address>`. Sign in with username `tanremote` and the password that was set with this procedure.

Figure 48. iDRAC virtual console sign-in

©2026 Tanium Inc. All Rights Reserved



Troubleshoot the Lifecycle Controller job queue

Important: The following procedures are typically necessary only at the direction of Tanium Support.

CLEAR QUEUED FIRMWARE UPDATES

©2026 Tanium Inc. All Rights Reserved

About this task

If a firmware update failed to schedule or run and did not remove itself from the Lifecycle Controller job queue, you can manually clear firmware updates from the Lifecycle Controller.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-I-F` (Appliance Configuration > Manage iDRAC > Flush Pending Firmware Entries).

CLEAR THE LIFECYCLE CONTROLLER JOB QUEUE

About this task

If failed jobs remain in the Lifecycle Controller job queue, you can force the queue to clear. This procedure also clears any queued firmware updates.

Important: This procedure requires an iDRAC reset and prompts you to perform the reset after allowing three minutes for the Lifecycle Controller to sync the clearing of the job queue.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-I-X` (Appliance Configuration > Manage iDRAC > Clear iDRAC job queue (FORCE)).

VIEW THE IDRAC LOG

About this task

The iDRAC log provides information about system events and firmware updates in the iDRAC interface.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-I-V` (Appliance Configuration > Manage iDRAC > View iDRAC Logs).

Configure syslog forwarding or alerts

TanOS supports syslog forwarding, which sends all Appliance log messages to a remote syslog server, and alerting, which sends Appliance alerts to a syslog server, an SMTP email recipient, or both.

©2026 Tanium Inc. All Rights Reserved

Note: Severity level is a global setting that applies to both Syslog and SMTP alerts.

Syslog alerts versus forwarding

The syslog forwarding configuration under **Appliance Configuration** is separate from the syslog alert configuration in the **Appliance Maintenance** menu. Note these key differences:

- Syslog configuration for alerts sends events that match the specified alert threshold severity (info, warn, and error).
- Syslog forwarding configuration sends all messages located in /var/log/messages to a syslog destination.

Check the syslog status

About this task

The syslog status shows the last five log entries and the current syslog forwarding configuration.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-4` (Appliance Configuration > Syslog Configuration).
3. Enter `1` to view the status.

```
-----------------------------------------------------

>>> Appliance Configuration -> Syslog Configuration -> Check Status <<<

 Checking existing syslog configuration

 ###
 Found TanOS syslog configuration with destination logfile Kernel

 Current size of /var/log/tanos :76924

 Last 5 entries in /var/log/tanos:
2020-05-22T14:00:01.756970+00:00 appliance-160 TanOS_Shell:
```

©2026 Tanium Inc. All Rights Reserved

```
privileged_support_health_check.sh:
DEBUG called by root -b
2020-05-22T14:15:01.908001+00:00 appliance-160 TanOS_Shell:
privileged_support_health_check.sh:
DEBUG called by root -b
2020-05-22T14:30:01.962601+00:00 appliance-160 TanOS_Shell:
privileged_support_health_check.sh:
DEBUG called by root -b
2020-05-22T14:31:19.706181+00:00 appliance-160 TanOS_Shell:
privileged_appliance_configuration_
ntp.sh: DEBUG called by tanadmin
2020-05-22T14:33:36.632542+00:00 appliance-160 TanOS_Shell:
privileged_appliance_sub_configurat
ion_syslog.sh: DEBUG called by tanadmin

 ###
 No existing TanOS syslog forwarding configuration found

 Press enter to continue
```

Configure syslog forwarding

ACCESS THE SYSLOG CONFIGURATION MENU

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-4` (Appliance Configuration > Syslog Configuration).

MANAGE THE SYSLOG SERVER TRUST CERTIFICATE

About this task

If you use a trust certificate for TLS communication with your syslog server, import the certificate before you enable and configure server settings for syslog forwarding.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-4` (Appliance Configuration > Syslog Configuration).

©2026 Tanium Inc. All Rights Reserved

3. From the **Syslog Configuration** menu:
    - Enter `2` to view the previously imported trust certificate.
    - Enter `3` to paste the trust certificate in PEM format for import.
    - Enter `4` to remove the previously imported trust certificate.

MANAGE THE KEY PAIR FOR CERTIFICATE AUTHENTICATION

If you use certificate authentication with your syslog server, add the necessary public-private key pair before you enable and configure server settings for syslog forwarding.

A key pair is required only for destinations that use **TLS Auth**, which authenticates this Appliance to the syslog server. A TLS destination with **TLS Auth** disabled needs only the syslog server trust certificate.

Import a key pair

1. Use SFTP to copy the key file to the /incoming directory of the Tanium Server Appliance.
2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `A-4-8` (Appliance Configuration > Syslog Configuration > Load Key Pair for TLS Auth from SFTP incoming).

View or remove the previously imported key pair

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-4` (Appliance Configuration > Syslog Configuration).
3. From the **Syslog Configuration** menu:
    - Enter `7` to view the key pair.
    - Enter `9` to remove the key pair.

CONFIGURE SYSLOG FORWARDING DESTINATIONS

About this task

Syslog forwarding sends the same data that gets logged in /var/log/messages to each configured destination. TanOS supports multiple syslog forwarding destinations. If no destinations are

©2026 Tanium Inc. All Rights Reserved

configured, syslog forwarding is disabled.

Note:

- If you do not enable RFC5424 output format, TanOS defaults to RFC3164 syslog output.
- You must have imported a valid trust certificate for the syslog server to enable TLS communication with the server. For more information, see Manage the syslog server trust certificate on page 429.
- You must have imported a key pair to enable certificate-based authentication with the server. For more information, see Manage the key pair for certificate authentication on page 430.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-4-5` (Appliance Configuration > Syslog Configuration > Configure Forwarding).

```
------------------------------------------------------

>>> Appliance Configuration -> Syslog Configuration -> Configure Forwarding <<<

TLS certificate: No
TLS key pair: No

  1: 10.10.10.10  tcp  514

  A: Add syslog destination

  R: Return to previous menu  RR: Return to top

------------------------------------------------------

 TanOS Version: 1.9.1
```

©2026 Tanium Inc. All Rights Reserved

```
Please select:
```

3. Manage forwarding destinations:
    - **Add a destination:** Enter `A` to open the **Add Destination** menu.

```
-----------------------------------------------------


>>> Add Destination <<<


                 Current    Pending
Host             -
Protocol         -
├─Port           -
├─TLS Auth       n/a        n/a
└─TCP Framing    n/a        n/a
RFC 5424         no         no


     Configure Syslog Destination Settings
  H: Hostname
  P: Protocol


  O: Port Number
  T: [DISABLED] TLS Auth
  F: [DISABLED] TCP Framing (Octet-Counted)
  C: RFC 5424 Output Format


  S: Save Entry


  R: Return to previous menu  RR: Return to top


-----------------------------------------------------


 TanOS Version: 1.9.1
```

      Use the menu options to configure the settings for the remote syslog server and then enter `S` to save the destination.

    - **Edit a destination:** Enter the line number of the destination to open the **Edit**

©2026 Tanium Inc. All Rights Reserved

Destination menu.

```
-----------------------------------------------------


>>> Edit Destination <<<

                 Current                    Pending
Host             10.10.10.10                10.10.10.10
Protocol         tcp                        tcp
├─Port           514                        514
├─TLS Auth       n/a                        n/a
└─TCP Framing    yes                        yes
RFC 5424         no                         no

     Configure Syslog Destination Settings
  H: Hostname
  P: Protocol

  O: Port Number
  T: [DISABLED] TLS Auth
  F: TCP Framing (Octet-Counted)
  C: RFC 5424 Output Format

  S: Save Entry
  X: Delete Entry

  R: Return to previous menu  RR: Return to top


-----------------------------------------------------


 TanOS Version: 1.9.1
```

Modify the settings and enter `S` to save.

- **Delete a destination:** Enter the line number of the destination to open the **Edit Destination** menu and then enter `X` to delete the entry.

©2026 Tanium Inc. All Rights Reserved

(Optional) Force the full FQDN to appear in syslog messages

About this task

By default, the internal syslog server determines whether the fully qualified domain name (FQDN) or only the host name appears in syslog messages. You can optionally force the FQDN to always appear.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-4-10` (Appliance Configuration > Syslog Configuration > Configure FQDN Behavior).
3. Enter `E` to enable the setting and force the FQDN to always appear in syslog messages, or `D` to disable the setting and allow the internal server to decide whether the FQDN or only the host name should appear in syslog messages.

(Optional) Forward entries from other log files

About this task

You can forward entries to the configured syslog destination from other logs, including any custom logs you have created. You can associate a tag with each selected log file to identify the forwarded entries from that log.

Tip: For information about creating a custom log, see Tanium Core Platform troubleshooting and logs in an Appliance deployment on page 512.

You can forward logs only from the following directories on the Appliance:

- /var/log
- /opt/Tanium/TaniumServer/Logs
- /opt/Tanium/TaniumServer/TDL_Logs
- /opt/Tanium/TaniumModuleServer/Logs
- /opt/Tanium/TaniumModuleServer/TDL_Logs

©2026 Tanium Inc. All Rights Reserved

- /opt/Tanium/TaniumZoneServer/Logs
- /opt/Tanium/TaniumModuleServer/services/*-files/logs

For more information about available logs, see Overview of Tanium Appliance logs, reports, and troubleshooting features on page 493.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-4-6` (Appliance Configuration > Syslog Configuration > Custom File Forwarding).
3. Use the following options to manage the forwarded log files:
   - **Add a log file:** Enter `A` to add a line, and then follow the prompts to specify the path and file name of a log file to forward and a tag to apply to forwarded entries from that log.

     ```
     ------------------------------------------------------


     >>> Custom File Forwarding <<<


     List files (one file per line) to forward out to syslog
       1: /opt/Tanium/TaniumServer/Logs/log0.txt TS-log0
       2: /opt/Tanium/TaniumZoneServer/Logs/log0.txt TZS-log0


       A: Add a line
       X: Remove the file


       R: Return to previous menu  RR: Return to top


     ------------------------------------------------------------------------
     --


     Please select: a
     Enter the filename: /var/log/secure
     Enter the tag: secure
     ```

   - **Edit the file name and tag for a previously entered log file:** Enter the line number of the log file to edit, enter `E` to edit the line, and then follow the prompts to edit the path and file name and tag.

©2026 Tanium Inc. All Rights Reserved

- **Remove a log file from the list:** Enter the line number of the log file to edit, enter `X` to delete the line.
- **Remove all log files from the list:** Enter `X`.

Configure syslog alerts

You can send Appliance alerts to a syslog server, an SMTP email recipient, or both. Syslog servers and SMTP are independent alerting destinations and receive the same alerts.

Tip: If you configure both a syslog destination and an SMTP destination, the SMTP destination provides an additional benefit: if TanOS cannot deliver alerts to the syslog destination, it sends a failure notification to the SMTP destination every 15 minutes until the issue is resolved.

ENABLE OR DISABLE ALL ALERTS

About this task

The **Global alert status** setting controls whether TanOS sends alerts to any destination. When global alerts are disabled, TanOS sends no alerts to the syslog destination or the SMTP destination, however those destinations are configured.



Important: On TanOS 1.9.0 or earlier, disabling global alerts suppressed only syslog alerts, and TanOS continued to send SMTP alerts. If you rely on SMTP alerts and global alerts are disabled, enable global alerts after you upgrade.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-2-3` (Appliance Maintenance > Alerting > Configure Alerts).
3. Enter `1` to enable or disable global alerts. The menu updates to show the current **Global alert status**.

SET THE ALERT SEVERITY LEVEL

©2026 Tanium Inc. All Rights Reserved

About this task

Use the **Configure Alerts** menu to set the alert severity threshold to info, warn, or error.

- Info: Includes all alerts
- Warn: Includes all error and warning alerts
- Error: Includes error alerts

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-2-3` (Appliance Maintenance > Alerting > Configure Alerts).
3. Use the menu to set a severity level and enable/disable alerting.

CONFIGURE A SYSLOG SERVER DESTINATION FOR ALERTS

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-2-1` (Appliance Maintenance > Alerting > Configure Syslog Destination).
3. Enter `2` and follow the prompts to configure a syslog destination.

```
            >>> Appliance Maintenance -> Alerting -> Configure Syslog Destination
<<<

Please enter the destination host: 10.10.10.10
Please enter the destination port: 514
Please enter the destination protocol [tcp/udp]: udp

Alert syslog destination updated.
```

4. Enter `1` to enable syslog alerts. The **Configure Syslog Destination** menu updates to show the current status.

```
            >>> Appliance Maintenance -> Alerting -> Configure Syslog Destination
<<<
```

©2026 Tanium Inc. All Rights Reserved

```
Current destination status: Enabled
Current server address: 10.10.10.10
Current server port: 514
Current server protocol: udp

         1: Enable/Disable syslog alerts
         2: Edit Syslog Destination
         3: Send Syslog Test Alert

         R: Return to previous menu  RR: Return to top

--------------------------------------------------------
```

5. Enter `3` to send a test alert to the syslog server.

Result

The test alert appears in the syslog server logs.

Figure 49. Test alert in the syslog server logs



CONFIGURE AN SMTP DESTINATION FOR ALERTS

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-2-2` (Appliance Maintenance > Alerting > Configure SMTP Destination).
3. Enter `2` and follow the prompts to configure the SMTP destination.

```
           >>> Appliance Maintenance -> Alerting -> Configure SMTP Destination <<<

Please enter the SMTP host: 10.10.10.10
Please enter the destination port: 25
Please enter the recipient email address: admin@tam.local
```

©2026 Tanium Inc. All Rights Reserved

```
Alert SMTP destination updated.
```

4. Enter `1` to enable SMTP alerts. The **Configure SMTP Destination** menu updates to show the current status.

```
            >>> Appliance Maintenance -> Alerting -> Configure SMTP Destination <<<

Current destination status: Enabled
Current server address: 10.10.10.10
Current server port: 25
Current recipient address: admin@tam.local

         1: Enable/Disable SMTP alerts
         2: Edit SMTP Destination
         3: Send SMTP Test Alert

         R: Return to previous menu  RR: Return to top

--------------------------------------------------------
```

5. Enter `3` to send a test alert to the mail recipient.

Configuring SNMP

Tanium Appliances support SNMP v3, though the SNMP service is not enabled by default. You can configure SNMP credentials and start the service to allow remote SNMP connections to the Appliance or to the iDRAC interface of a physical Tanium Appliance. The default user name for SNMP connections is `tansnmp`. A remote host or SNMP manager can use the configured credentials to conduct SNMP polling on the Appliance. Tanium Appliances only respond to SNMP requests; they do not send SNMP traps.

There is not a Tanium-specific MIB. Tanium Appliances report a specific SNMPv2 `sysObjectID` and include the following standard MIBs:

- SNMPv2-MIB: Contains system information, such as up time, contact information, and basic system configuration

©2026 Tanium Inc. All Rights Reserved

- IP-MIB: Contains objects for managing IP address tables, IP forwarding information, and related statistics
- IF-MIB: Contains information about each network interface, including configuration parameters, traffic statistics, and status
- TCP-MIB: Contains objects for managing TCP connection states and statistics, such as active connections, retransmissions, and errors
- UDP-MIB: Contains objects related to UDP traffic statistics and configurations, such as active sockets and datagram counts
- HOST-RESOURCES-MIB: Contains objects for managing and monitoring system resources, such as storage and device status
- UCD-SNMP-MIB: Contains additional system monitoring and network interface statistics. This MIB includes monitoring objects for CPU, memory, and system load, which are not covered by other MIBs.

Note: For a physical Tanium Appliance, see Dell Technologies: SNMP Reference Guide for iDRAC and Chassis Management Controller for information about the MIB used with iDRAC. Some limitations apply for the iDRAC implementation in the Tanium Appliance. For example, the Tanium Appliance does not support SNMP v1 or v2, nor does it send SNMP traps.

Figure 50. Example of SNMP polling using snmpwalk

©2026 Tanium Inc. All Rights Reserved

```
[user@localhost ~]# snmpwalk -v 3 -u tansnmp -A password -X password -a sha -x AES -l authPriv tanos-server.lab.tanium.local
SNMPv2-MIB::sysDescr.0 = STRING: Linux tanos-server 3.10.0-1160.80.1.el7.x86_64 #1 SMP Tue Nov 8 15:48:59 UTC 2022 x86_64
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.49011.2.1.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (363770) 1:00:37.70
SNMPv2-MIB::sysContact.0 = STRING: user@domain.com
SNMPv2-MIB::sysName.0 = STRING: tanos-server
SNMPv2-MIB::sysLocation.0 = STRING: lab
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORID.1 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance
SNMPv2-MIB::sysORID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.2 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.3 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.8 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.9 = STRING: The MIB modules for managing SNMP Notification, plus filtering.
SNMPv2-MIB::sysORDescr.10 = STRING: The MIB module for logging SNMP Notifications.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORUpTime.9 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORUpTime.10 = Timeticks: (5) 0:00:00.05
```

Set password and start the SNMP service

About this task

Note:

- Passwords must be 8–20 characters.
- After restoring from a backup, SNMP settings such as user name, location, contact, and authentication type are automatically restored. However, the SNMP service is not re-enabled after a restore. Enter `S` and re-enter the SNMP password to restart the service.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-5` (Appliance Configuration > SNMP Configuration).
3. Enter `S`, enter the desired SNMP password at the prompt, and press Enter to save the

©2026 Tanium Inc. All Rights Reserved

password and enable the SNMP service.

```
-----------------------------------------------------


>>> Appliance Configuration -> SNMP Configuration <<<


State:     Enabled
Username:  tansnmp
Location:  New York, NY
Contact:   user@company.com
EngineID:  0x80001f8880d6736914ae15e56000000000
Auth Type: SHA
Priv Type: AES


Sample:
snmpwalk -v3 -u tansnmp -A 'password' -X 'password' -a SHA -x AES -l authPriv
10.10.10.61


          U: Change the Username
          L: Change the Location
          C: Change the Contact
          A: Change the Authentication Type
          P: Change the Privacy Type
          V: View SNMP Service Status
          D: Stop the SNMP Service
          S: Set Password and Start the SNMP Service


          R: Return to previous menu  RR: Return to top


-----------------------------------------------------


 TanOS Version:        1.9.1


        Please select: s
        Enter the desired SNMP password:


        Successfully saved and enabled the SNMP service
```

©2026 Tanium Inc. All Rights Reserved

```
Press enter to continue
```

Change the SNMP user name, location, or contact

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-5` (Appliance Configuration > SNMP Configuration).
3. Enter `U` to change the user name, `L` to change the location, or `C` to change the contact and follow the prompts to enter the new value.

Change the SNMP authentication or privacy type

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-5` (Appliance Configuration > SNMP Configuration).
3. Enter `A` to change the authentication type or `P` to change the privacy type, and follow the prompts to select the new value.

   Note: Supported authentication types are SHA, SHA-256, SHA-384, and SHA-512. Supported privacy types are AES and AES-256. The defaults are SHA and AES.
4. Enter `S` and re-enter the SNMP password to apply the changes and restart the service.

View SNMP service status

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-5` (Appliance Configuration > SNMP Configuration).
3. Enter `V` to view the SNMP service status details.

Stop the SNMP service

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-5` (Appliance Configuration > SNMP Configuration).
3. Enter `D` to stop and disable the SNMP service.

©2026 Tanium Inc. All Rights Reserved

Clean up generated files

About this task

Clean directories to clear up disk space or clear logs to make it easier to work with new entries in the log viewer.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-A` (Appliance Maintenance > Clean directories).
3. Use the menu to delete files that have been generated in the SFTP /incoming and /outgoing directories, core dump files, application logs, and so on.

Reboot or shut down

Tasks that you complete with TanOS menus typically do not require you to reboot the system. A reboot might be required during troubleshooting workflows.

Shutdown turns off the system and powers down the Appliance.

> **Important:** On a physical Tanium Appliance, you must have physical or iDRAC access to the Appliance to power it on. Do not perform a system shutdown unless you are prepared to power the Appliance back on.

Reboot

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-B-1` (Appliance Maintenance > Reboot/Shutdown > Reboot).
3. Follow the prompts to reboot the Appliance.

Shut down

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-B-2` (Appliance Maintenance > Reboot/Shutdown > Shutdown).

©2026 Tanium Inc. All Rights Reserved

3. Follow the prompts to shut down the Appliance.

Increase storage

About this task

On cloud-based Tanium Appliances and virtual Tanium Appliances, you can add a disk to the virtual image or increase the size of the existing virtual disk to increase the amount of storage that is available to TanOS.

CAUTION:

- This action is not reversible. Storage that you add to the Appliance is permanently allocated. Do not attempt to remove disk storage from an Appliance, as the Appliance becomes unusable.
- On an Appliance that has been upgraded over time from TanOS 1.7.1 or earlier, you cannot increase the size of existing virtual disks. Attempting to do so might result in unusable storage on the virtual disk that cannot be reallocated. If you need to increase storage in this case, add a virtual disk.

1. Modify the virtual image to add a disk or increase the size of the existing virtual disk.
2. Sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `B-I` (Appliance Maintenance > Increase Storage).
4. Follow the prompts to add the disk storage.

```
          >>> Maintenance -> Increase Storage <<<

Utilize unused disks or free disk space to expand the TanOS /opt partition.

This space can be additional storage that has been added through the hypervisor
or reclaimed space from discarding alternate paritions.
```

©2026 Tanium Inc. All Rights Reserved

```
 Be advised: This action is permanent!

 Current space
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/VolGroup1-opt  349G   14G  318G   4% /opt

 Additional space available: 445.41 GiB

Would you like to add this additional space to TanOS? [Yes|No]: yes
  Size of logical volume VolGroup1/opt changed from 354.34 GiB (90712 extents) to
<799.76 GiB (204
738 extents).
  Logical volume VolGroup1/opt successfully resized.
resize2fs 1.42.9 (28-Dec-2013)
Filesystem at /dev/mapper/VolGroup1-opt is mounted on /opt; on-line resizing required
old_desc_blocks = 45, new_desc_blocks = 100
The filesystem on /dev/mapper/VolGroup1-opt is now 209651712 blocks long.

Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/VolGroup1-opt  788G   14G  739G   2% /opt
 Press enter to continue
```

Note: If your virtual Tanium Appliance has an inactive partition set, any new storage is evenly allocated across the active (/OPT) and inactive (/ALTOPT) partitions.

Manage OS services

About this task

Use this menu to start, stop, restart, enable, and view status details for the network time protocol daemon (chronyd) and SSH daemon (sshd) services.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B`-`S` (Appliance Maintenance > OS Services).
3. Select a service to open the **Service Control** menu:

©2026 Tanium Inc. All Rights Reserved

- To manage chronyd, enter `1`.

```
-----------------------------------------------------

           >>> Service Control -> chronyd <<<

   Service        State      Status
   chronyd        enabled    running

   NOTE: Cannot disable OS services

         1: Start service
         2: Stop service
         3: Restart service
         4: [DISABLED] Disable service
         5: Enable service
         6: Status Details

         R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

- To manage sshd, enter `2`.

```
-----------------------------------------------------

           >>> Service Control -> sshd <<<

   Service        State      Status
   sshd           enabled    running

   NOTE: Cannot disable OS services

         1: Start service
         2: Stop service
         3: Restart service
         4: [DISABLED] Disable service
```

©2026 Tanium Inc. All Rights Reserved

```
          5: Enable service
          6: Status Details


          R: Return to previous menu  RR: Return to top


--------------------------------------------------
```

4. Use the menu to select an action to start, stop, restart, enable, or view status details for the service.
5. Follow the prompts to perform the action.

View the overall status for TanOS, Tanium, and the Appliance

The subsequent topics in this section provide information about viewing OS status and partition information, network status, Tanium component status, and Appliance status.

View OS status and partition information

View OS status and partition information from the **System Status** menu. This information includes the list of partitions with space used, as provided by the `df -h` command.

VIEW OS STATUS AND PARTITION INFORMATION WITH THE TANADMIN ROLE

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `4-1-1` (Status > System Status > OS Status).

TANUSER: VIEW OS STATUS AND PARTITION INFORMATION WITH THE TANUSER ROLE

1. Sign in to the TanOS console as a user with the `tanuser` role.
2. Enter `1-1` (System Status > OS Status).

View network status

View network status from the **System Status** menu.

©2026 Tanium Inc. All Rights Reserved

VIEW NETWORK STATUS WITH THE TANADMIN ROLE

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `4-1-2` (Status > System Status > Network Status).

TANUSER: VIEW NETWORK STATUS WITH THE TANUSER ROLE

1. Sign in to the TanOS console as a user with the `tanuser` role.
2. Enter `1-2` (System Status > Network Status).

View Tanium component status

VIEW TANIUM STATUS WITH THE TANADMIN ROLE

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `4-2` (Status > Tanium Status).

VIEW TANIUM STATUS WITH THE TANUSER ROLE

1. Sign in to the TanOS console as a user with the `tanuser` role.
2. Enter `2` (Tanium Status).
3. Use the menu to view Tanium service status.

View Appliance status

Appliance status shows Appliance version information, OS status, or hardware status.

VIEW APPLIANCE STATUS WITH THE TANADMIN ROLE

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `4-3` (Status > Appliance Status).
3. Use the menu to view Appliance version information, OS status, or hardware status.

©2026 Tanium Inc. All Rights Reserved

VIEW APPLIANCE STATUS WITH THE TANUSER ROLE

1. Sign in to the TanOS console as a user with the `tanuser` role.
2. Enter `3` (Appliance Status).
3. Use the menu to view Appliance version information, OS status, or hardware status.

Perform database operations

If you encounter issues with the Tanium deployment, Tanium Support might direct you to perform database operations.

> **Note:** Database operations are available on the Tanium Server and Tanium Module Server. In an All-In-One deployment, database operations apply only to the Tanium Server.

View the Postgres log file

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-3-1` (Tanium Support > Database Operations > Select File).
3. Enter the line number for the postgres.log file, and use the menu to view the log or copy it to the /outgoing folder.

```
 ------------------------------------------------------
>>> Tanium Support -> Postgres -> Logs -> postgres.log <<<

        Size: 80   Last Update: 2020-10-25 06:11:39

          V: View the file
          F: Follow log file growth
          E: Export to outgoing (sftp)

          R: Return to previous menu  RR: Return to top

 ------------------------------------------------------
```

©2026 Tanium Inc. All Rights Reserved

View Postgres configuration files

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-3-2` (Tanium Support > Database Operations > Select File).
3. Use the menu to review or modify the configuration.

View Postgres control data

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-3` (Tanium Support > Database Operations).
3. Enter `3` to view Postgres control data.

```
pg_control version number:            942
Catalog version number:               201510051
Database system identifier:           6813452830717815614
Database cluster state:               in production
pg_control last modified:             Thu 09 Apr 2020 02:31:02 PM UTC
Latest checkpoint location:           0/2384610
Prior checkpoint location:            0/2381B90
Latest checkpoint's REDO location:    0/23845D8
Latest checkpoint's REDO WAL file:    000000010000000000000002
Latest checkpoint's TimeLineID:       1
Latest checkpoint's PrevTimeLineID:   1
Latest checkpoint's full_page_writes: on
Latest checkpoint's NextXID:          0/3498
Latest checkpoint's NextOID:          27854
Latest checkpoint's NextMultiXactId:  1
Latest checkpoint's NextMultiOffset:  0
Latest checkpoint's oldestXID:        1825
Latest checkpoint's oldestXID's DB:   1
Latest checkpoint's oldestActiveXID:  3498
Latest checkpoint's oldestMultiXid:   1
Latest checkpoint's oldestMulti's DB: 1
Latest checkpoint's oldestCommitTsXid:0
Latest checkpoint's newestCommitTsXid:0
```

©2026 Tanium Inc. All Rights Reserved

```
Time of latest checkpoint:            Thu 09 Apr 2020 02:31:02 PM UTC
Fake LSN counter for unlogged rels:   0/1
Minimum recovery ending location:     0/0
Min recovery ending loc's timeline:   0
Backup start location:                0/0
Backup end location:                  0/0
End-of-backup record required:        no
wal_level setting:                    hot_standby
wal_log_hints setting:                off
max_connections setting:              256
max_worker_processes setting:         8
max_prepared_xacts setting:           0
max_locks_per_xact setting:           64
track_commit_timestamp setting:       off
Maximum data alignment:               8
Database block size:                  8192
Blocks per segment of large relation: 131072
WAL block size:                       8192
Bytes per WAL segment:                16777216
Maximum length of identifiers:        64
Maximum columns in an index:          32
Maximum size of a TOAST chunk:        1996
Size of a large-object chunk:         2048
Date/time type storage:               64-bit integers
Float4 argument passing:              by value
Float8 argument passing:              by value
Data page checksum version:           0


 Press enter to continue
```

Enable full Postgres audit log

About this task

Postgres logs are very rarely useful in troubleshooting Appliance or platform issues. Audit logging is disabled by default. When enabled, Postgres logging can consume inordinate disk space. For best results, enable audit logging only when debugging.

©2026 Tanium Inc. All Rights Reserved

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-3` (Tanium Support > Database Operations).
3. Enter `4` and follow the prompts to enable audit logging.

```
-----------------------------------------------------


>>> Tanium Support menu -> Enable Postgres Full Audit Logging <<<



 Do you want to Enable Full Postgres audit logging ? [Yes|No]: yes


 Enabling Postgres audit logging
 Reloading Postgres configuration


 Press enter to continue
```

Manage the database memory plan

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-3-D` (Tanium Support > Database Operations > DB Tuning).
3. Review the available memory plans and enter the letter for the plan you want to select.

   Tip: For more information about Appliance sizing and specifications, see Reference: Tanium Appliance sizing and specifications on page 644.

4. Enter `A` to apply the new memory plan.

   Note: You must apply the same database memory plan for both Tanium Servers in a cluster, or for both an active and standby Module Server. A Tanium Server and a Module Server are not required to have the same memory plan.

Run the Postgres top command

1. Sign in to the TanOS console as a user with the `tanadmin` role.

©2026 Tanium Inc. All Rights Reserved

2. Enter `3-3` (Tanium Support > Database Operations).
3. Enter `M` to view results of the top command.

```
last pid: 29609;  load avg:  0.08,  0.03,  0.05;       up 0+03:02:11
14:45:53
3 processes: 1 running, 2 sleeping
CPU states: 34.5% user,  0.0% nice, 15.0% system, 50.5% idle,  0.0% iowait
Memory: 924M used, 67M free, 46M buffers, 560M cached
DB activity:  17 tps,  0 rollbs/s,   0 buffer r/s, 100 hit%,     38 row r/s,    0 row
w/s
DB I/O:     0 reads/s,     0 KB/s,    27 writes/s,   210 KB/s
DB disk: 348.7 GB total, 328.3 GB free (5% used)
Swap: 10M used, 4086M free, 924K cached

  PID USERNAME PRI NICE  SIZE   RES STATE   TIME   WCPU    CPU COMMAND
23453 postgres  20    0 4426M   50M sleep   0:08  0.20%  0.60% postgres: postgres
tanium 10.10.10.55(60908) idle
29610 postgres  20    0 4421M 6496K run     0:00  0.00%  0.00% postgres: postgres
postgres [local] idle
```

4. Enter `Q` to return to the **Database Operations** menu.

Query the tanium database

About this task

The **Manage Queries** menu includes predefined queries that can be useful during troubleshooting.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-3-Q-S` (Tanium Support > Database Operations > Manage Queries > Select Query).
3. Use the menu to select a predefined query and return to the **Manage Queries** menu.
4. Enter `X` to run the query and save the results to the /outgoing folder.

```
           >>> Tanium Support menu -> Database Operations -> Execute Query <<<

Running Query DBsizes
```

©2026 Tanium Inc. All Rights Reserved

```
Query results saved to outgoing in DBsizes.results


Press enter to continue
```

5. Enter `Q` to view query results.

```
  datname   |  size
------------+---------
 template1 | 7145 kB
 template0 | 7145 kB
 postgres  | 7264 kB
 tanium    | 16 MB
(4 rows)


/tmp/tmp.G2h8V4Iab2 (END)
```

6. Enter `Q` to return to the **Manage Queries** menu.

View database replication status and history

About this task

View the database replication status and history to help troubleshoot replication issues between the primary and secondary Tanium Server or between the active and inactive Module Server. The replication status is captured every 15 minutes at the same time as the automatic health check, and, additionally, when you view the current status. The status is recorded as a new entry in the history if the server role changes or if there is an important change in the replication status; otherwise the status overwrites the previous entry in the history. The **Postgres Replication History** screen displays the 10 most recent history entries.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-3` (Tanium Support > Database Operations).
3. Enter `S` to view the Postgres replication history.

```
 ------------------------------------------------------
>>> Postgres Replication History <<<


    C: Show Current Status
```

©2026 Tanium Inc. All Rights Reserved

```
     Timestamp                 Status          Role
   1: 2024-04-23 20:00:33       Fail            Secondary
   2: 2024-04-16 07:45:32       Fail            Secondary
   3: 2024-04-16 07:30:13       Pass            Secondary
   4: 2024-04-15 22:00:13       Pass            Secondary
   5: 2024-04-15 21:45:12       Fail            Secondary
   6: 2024-04-15 20:15:13       Pass            Secondary

   R: Return to previous menu  RR: Return to top

-------------------------------------------------------
```

4. Enter `C` to view the current replication status, or enter the number of the historical status to view.

```
Viewing previously captured replication status

Status Timestamp:         2024-04-16 07:30:13
Service Type:             TS

>>> Local Database Replication Status <<<
Cluster Address:          10.10.110.236
Postgres TS service:      Pass (Running)
Cluster Role:             Secondary
Last WAL LSN:             0/51806B8
Last Xact Replay:         2024-04-16 07:30:06.291924+00
Streaming Status:         Pass (streaming)
Written LSN:              0/51806B8
Last Msg Send:            2024-04-16 07:30:06.292087+00
Last Msg Receipt:         2024-04-16 07:30:06.292141+00
Replication Lag:          00:00:07.872822

>>> Remote Database Replication Status <<<
Cluster Address:          10.10.110.205
Network Access:           Pass (Responding)
Remote DB Net Latency:    1ms
```

©2026 Tanium Inc. All Rights Reserved

```
Cluster Role:             Primary
Replication Slot:         Pass (Active)
Slot Restart LSN:         0/51806B8
Current Log Location:     0/51806B8
Streaming Status:         Pass (streaming)
In Recovery Mode:         Pass (No)
Sync State:               async
Backend Start:            2024-04-15 21:59:44.180481+00
Sent Log Location:        0/51806B8
Write Log Location:       0/51806B8
Replay Log Location:      0/51806B8
Flush Log Location:       0/51806B8

Overall Status:           Pass



Press enter to continue
```


Tip: The Tanium Support Gatherer report includes the latest 50 replication history entries, in the postgres-repl-ts.json log file for each Tanium Server, or the postgres-repl-tms.json file for each Module Server. For more information, see Run Tanium Support Gatherer on page 500.

Initiate database server failover

1. Sign in to the TanOS console of the Appliance with the secondary database as a user with the `tanadmin` role.
2. Enter `2-B-F` (Tanium Operations > Cluster Configuration > Database Server Failover).
3. Follow the prompts to initiate the failover.

Collect database replication statistics (Module Server only)

About this task

When troubleshooting a replication issue on a Module Server, you can temporarily enable replication

©2026 Tanium Inc. All Rights Reserved

statistics that indicate the amount of data recorded in the database on the primary Module Server that has not yet been replicated to the secondary Module Server. When you enable this collection, TanOS records statistics once per minute, in the replstats_yyyy-mm-dd.json file in the outgoing folder. TanOS creates one log file for each day while collection is enabled.

Important: Keep database replication statistics disabled when you are not troubleshooting a replication issue. The **TMS Database Stats Collection** health check indicates that collection of database replication statistics is enabled.

1. Enter `3-3-C` (Tanium Support > Database Operations > Collect Replication Stats).
2. Follow the prompts to enable or disable collection of database replication statistics.

Monitor performance

Use the Performance Monitoring menu to view resource usage.

Run a SAR command

1. Sign in to the TanOS console of the Appliance with the primary database server as a user with the `tanadmin` role.
2. Enter `3-P-1` (Tanium Support > Performance Monitoring > SAR command).
3. Use the menu to issue a command. The results of the command are returned to the screen.

```
Linux 3.10.0-1160.53.1.el7.x86_64 (ts1)     04/20/2022      _x86_64_     (2 CPU)


19:57:03        CPU     %user     %nice   %system   %iowait    %steal     %idle
19:57:04        all      0.50      0.00      0.50      0.00      0.00     99.00
19:57:05        all      2.00      0.00      1.00      0.00      0.00     97.00
19:57:06        all      1.50      0.00      0.50      0.00      0.00     98.00
19:57:07        all      0.50      0.00      0.00      0.00      0.00     99.50
19:57:08        all      0.50      0.00      0.50      0.00      0.00     98.99
Average:        all      1.00      0.00      0.50      0.00      0.00     98.50


 Available options
```

©2026 Tanium Inc. All Rights Reserved

```
 1  - CPU utilization        8  - Swap Space utilization
 2  - Individual CPU usage   9  - Swap statistics
 3  - Memory utilization    10  - Task/Switch activity
 4  - Memory statistics     11  - I/O Xfer statistics
 5  - Pageing statistics    12  - Block device Activity
 6  - Hugepages statistics  13  - Network statistics
 7  - Queue/Load            14  - Power Management

Please select an option or enter to quit:
```

Export a SAR snapshot

1. Sign in to the TanOS console of the Appliance with the primary database server as a user with the `tanadmin` role.
2. Enter `3-P` (Tanium Support > Performance Monitoring).
3. Enter `2` to take a five second snapshot of SAR data and export it to the /outgoing folder.

```
           >>> Collecting SAR performance snapshot <<<

Performance snapshot has been completed

Snapshot file is appliance-160_perfstats_040920_1522.txt
You may now download it from the sftp outgoing directory

Press enter to continue
```

4. Use SFTP to copy the snapshot file from the /outgoing directory on the Appliance to your management computer.

Export a SAR performance data

1. Sign in to the TanOS console of the Appliance with the primary database server as a user with the `tanadmin` role.
2. Enter `3-P` (Tanium Support > Performance Monitoring).

©2026 Tanium Inc. All Rights Reserved

3. Enter `3` to collect the complete set of SAR data files for the last 30 days and export it to a ZIP file in the /outgoing folder.

```
           >>> Creating zip file with SAR performance data <<<


Performance data was saved to file appliance-160_perfdata_040920_1526.zip.
You may now download it from the sftp outgoing directory


Press enter to continue
```

4. Use SFTP to copy the snapshot file from the /outgoing directory on the Appliance to your management computer.

Export all SAR files

1. Sign in to the TanOS console of the Appliance with the primary database server as a user with the `tanadmin` role.
2. Enter `3-P` (Tanium Support > Performance Monitoring).
3. Enter `4` to collect all SAR files into a single file and export it to the /outgoing folder.

```
           >>> Collecting Complete SAR performance output <<<


Performance snapshot has been completed


Snapshot file is appliance-156_perfstats_040920_1534.txt
You may now download it from the sftp outgoing directory


Press enter to continue
```

4. Use SFTP to copy the snapshot file from the /outgoing directory on the Appliance to your management computer.

Run the iotop command

1. Sign in to the TanOS console of the Appliance as a user with the `tanadmin` role.

©2026 Tanium Inc. All Rights Reserved

2. Enter `3-P` (Tanium Support > Performance Monitoring).
3. Enter `I` to monitor input/ouput usage for the Appliance.
4. Enter `Q` to return to the **Performance Monitoring** menu.

Run the perf top command

1. Sign in to the TanOS console of the Appliance as a user with the `tanadmin` role.
2. Enter `3-P` (Tanium Support > Performance Monitoring).
3. Enter `P` to monitor CPU usage for the Appliance.
4. Enter `Q` to return to the **Performance Monitoring** menu.

Run the htop command

1. Sign in to the TanOS console of the Appliance as a user with the `tanadmin` role.
2. Enter `3-P` (Tanium Support > Performance Monitoring).
3. Enter `T` to monitor processes for the Appliance.
4. Enter `Q` to return to the **Performance Monitoring** menu.

Perform advanced maintenance tasks for Tanium Appliances

Important: Consult with Tanium Support before you use advanced options. For more information, see Support for Tanium Appliances on page 510.

Install a firmware update

About this task

When you Run the Health Check on page 488 , you might see messages alerting you to perform a firmware update.

Use the Advanced Maintenance menu to stage and apply firmware updates. On a physical Tanium

©2026 Tanium Inc. All Rights Reserved

Appliance, the updates include iDRAC firmware updates, PERC firmware updates, NIC firmware updates, and BIOS firmware updates.

Important: Updating a firmware update is a major task. The process can take from 10-30 minutes, depending on model. Allow the firmware update to complete before attempting any other tasks with the Appliance. Do NOT manually power off or reboot the Appliance.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-X-1` (Appliance Maintenance > Advanced Maintenance > Firmware Update).
3. Follow the prompts to update the iDRAC, PERC, NIC, and BIOS firmware.

```
          >>> Appliance Maintenance -> Advanced Menu -> Firmware Update <<<

Firmware Type          Current Version   Target Version    Status
====================   ===============   ==============    ==============

iDRAC                  1.11.11.11        2.22.22.22        Ready to Apply
PERC                   33.3.3-3333       44.4.4-4444       Ready to Apply
NIC: Intel Copper      55.5.55           66.6.66           Ready to Apply
NIC: Broadcom Copper   77.7.7            88.8.8            Ready to Apply
BIOS                   9.9.9             10.10.10          Ready to Apply

Note that the system may need to reboot to apply changes. In general iDRAC
does not require reboot; BIOS and PERC do require reboot. If any selected
firmware upgrade requires a reboot, the system will reboot immediately after
all firmwares have been staged or applied.

Gathering information to perform bulk upgrades...

Upgrade 'iDRAC' to 2.22.22.22 [Yes|No]: yes
Upgrade 'PERC' to 44.4.4-4444 [Yes|No]: yes
Upgrade 'NIC: Intel Copper' to 66.6.66 [Yes|No]: yes
Upgrade 'NIC: Broadcom Copper' to 88.8.8 [Yes|No]: yes
Upgrade 'BIOS' to 10.10.10 [Yes|No]: yes
```

©2026 Tanium Inc. All Rights Reserved

```
Proceed with selected upgrades now? [Yes|No]
```

Perform a TanOS reset

About this task

The **Appliance Reset** menu allows you to perform a software reset which erases the Tanium application software and data.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B`-`X`-`2` (Appliance Maintenance > Advanced Maintenance > Reset).
3. Enter `1` to perform a software reset.
4. Follow the prompts to initiate the reset.

```
------------------------------------------------------


  >>> Appliance Maintenance -> Reset -> Software <<<


Removing Tanium Software from this appliance
The appliance will be rebooted after the removal

Would you like to continue with the software reset? [Yes|No]: yes
Starting removal of software

Removing installed software
Working on Module Server and Modules...
Removed Tanium Module Server
Working on Tanium Server...
Removed Tanium Server
Removed database configuration
Finished removing software
Finished reset of software!


Rebooting appliance
```

©2026 Tanium Inc. All Rights Reserved

Re-install ACLs

About this task

If you experience issues copying to or from the `tancopy`/incoming or /outgoing directories, you can use this menu to reapply the access control lists (ACL) for those directories.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B`-`X` (Appliance Maintenance > Advanced Maintenance).
3. Enter `3` to reapply the ACLs.

Overwrite Module ACLs (Module Server only)

About this task

Use this option to reset the file ownership and permissions for a Tanium module service directory on the Module Server. Use this option only if directed to do so by Tanium Support.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B`-`X`-`4` (Appliance Maintenance > Advanced Maintenance > Overwrite Module ACLs).
3. Enter the line number of the module service for which you want to reset permissions.
4. Confirm the prompt to apply the changes.

View the TanOS partition sync log

About this task

Note: This menu only appears if the Appliance contains an active partition and an inactive partition. This menu is not available on cloud-based Tanium Appliances.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B`-`X` (Appliance Maintenance > Advanced Maintenance).
3. Enter `5` to view the TanOS partition sync log file.

©2026 Tanium Inc. All Rights Reserved

Upgrading TanOS and Tanium Core Platform

Specific versions of TanOS and Tanium Core Platform are bundled together in the semiannual release. Upgrade these components at the same time so that your deployment remains in a supported configuration.

The subsequent topics in this section provide information about upgrading to a new semiannual release or maintenance release, upgrading TanOS on Tanium Appliances, and upgrading the Tanium Core Platform in an Appliance deployment.

Upgrading to a new semiannual release or maintenance release

©2026 Tanium Inc. All Rights Reserved

Tip:

TanOS periodically checks the TanOS manifest for available upgrades and informs you on the **tanadmin** menu screen when an upgrade is available.

```
Welcome tanadmin last login to tanos-server at 2022-08-25 21:35
Current system time: 2022-08-26 21:49:25 UTC
Latest Available Prod Version: Upgrade available to 1.9.1.1234


------------------------------------------------------

                >>> tanadmin menu <<<

         1: Tanium Installation Menu
         2: Tanium Operations Menu
         3: Tanium Support Menu
         4: Status Menu

         A: Appliance Configuration Menu
         B: Appliance Maintenance Menu
         C: User Administration Menu

         P: Password change (current user)
         Q: View End User License Agreement (EULA)

         @: About this Appliance

         Z: Log out

------------------------------------------------------
```

Additionally, a health check reports when an upgrade is available. For more information, see Run the Health Check on page 488.

Note: When Tanium Appliances query the TanOS manifest for available updates at content.tanium.com, Tanium might collect non-identifiable metadata about the Appliance, including version and feature usage information, to further support, develop, and improve its products.

Tanium™ Semiannual Release 2026H2

Tanium™ Semiannual Release 2026H2 includes new versions of the following components:

- Tanium Operating System (TanOS): The operating system that runs on each Appliance

©2026 Tanium Inc. All Rights Reserved

- Tanium Core Platform: The software that runs on Tanium Core Platform Servers, including the Tanium Server, Tanium Module Server, Tanium Zone Server, and Tanium Zone Server Hub
- Tanium solutions: The solutions that you have licensed to provide specific functionality in your Tanium environment, including modules, shared services, and content-only solutions
- Tanium Client: The service that runs on endpoints to discover and report data in the Tanium environment
- Tanium™ Endpoint Configuration Toolset: A collection of tools, such as Tanium™ Client Extensions, that are deployed to endpoints to enable functionality for Tanium solutions

For version and support information, see 2026H2 release notes.

For more information about Tanium releases, see Tanium releases.

Maintenance releases

Maintenance releases provide security and bug fixes for currently supported semiannual releases. These upgrades are typically released monthly, and the support window remains based on the semiannual release. The maintenance release provides new versions only for the components that have fixes since the last update and might or might not contain upgrades for

Tanium Core Platform, Tanium solutions, Tanium Client, and the Tanium Endpoint Configuration Toolset.

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



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

Upgrade process

©2026 Tanium Inc. All Rights Reserved

Upgrading TanOS, Tanium Core Platform, and Tanium solutions

You must use the versions of TanOS, Tanium Core Platform, and Tanium solutions that are provided in a semiannual release together, or the later versions of each component that are provided in maintenance releases that upgrade the semiannual release. When upgrading to a new semiannual release, you must upgrade these components at the same time, beginning with TanOS. To begin the upgrade, see Upgrade TanOS on Tanium Appliances.

Important:

- After you start the upgrade process for a new semiannual release, you cannot access Tanium solutions until you finish upgrading both the platform and solutions. Make sure to plan a maintenance window with enough time to complete all upgrades.
- As a best practice, upgrade to the latest maintenance release available for semiannual release 2026H2. Do not upgrade to a maintenance release that has an earlier release date than the currently installed maintenance release. For example, if you have a maintenance release from February 1 currently installed, install a maintenance release of the 2026H2 semiannual release from February 1 or later.

Note: If you are installing a maintenance release that does not include a TanOS upgrade, begin the upgrade process with Tanium Core Platform. For more information, see Upgrade Tanium Core Platform in an Appliance deployment.

UPGRADING THE TANIUM ENDPOINT CONFIGURATION TOOLSET AND TANIUM CLIENT

You deploy the Tanium Endpoint Configuration Toolset and, optionally, the Tanium Client to endpoints using the change management feature of Tanium Endpoint Configuration. For more information, see Managing endpoint tool upgrade rollouts. If you do not enable Client upgrades in the change management feature, or if you need to upgrade the Tanium Client in upgrade rings for which Client upgrades are not yet enabled, you must upgrade the Tanium Client on endpoints using Client Management or other means to maintain a supported configuration. For more information, see Upgrading Tanium Clients. Tanium Semiannual Release 2026H2 supports all Tanium Client versions that the Tanium Core Platform supports. Each semiannual release supports the current endpoint

©2026 Tanium Inc. All Rights Reserved

configuration toolset and the two previous toolset releases.

Best Practice:

To ensure that all the features and fixes are available to endpoints, upgrade the Tanium Client to the version provided in the release, and deploy the Endpoint Configuration Toolset to all endpoints as soon as possible.

Note:

You cannot install the Tanium Client on a Tanium Appliance.

Upgrade TanOS on Tanium Appliances

The subsequent topics in this section provide information about preparing for the upgrade, understanding the upgrade process and upgrade paths, performing the upgrade, and viewing the TanOS upgrade log.

©2026 Tanium Inc. All Rights Reserved

Important:

- If you are upgrading to a semiannual release, or if you are upgrading to a maintenance release that includes upgrades for both TanOS and Tanium Core Platform, you must upgrade Tanium Core Platform immediately after upgrading TanOS, followed by all Tanium solutions. After you start the upgrade process for a new semiannual release, you cannot access Tanium solutions until you finish upgrading both the platform and solutions. For more information, see Upgrading TanOS and Tanium Core Platform on page 465.
- The TanOS upgrade does not automatically upgrade Tanium Core Platform. You must upgrade Tanium Core Platform after the TanOS upgrade is complete. The necessary steps are linked from this topic as you complete the TanOS upgrade steps.
- You must provide the Tanium Core Platform binaries to the Appliance before upgrading TanOS to a new semiannual release. The necessary steps are included in this topic.
- As a best practice, upgrade to the latest maintenance release available for semiannual release 2026H2. Do not upgrade to a maintenance release that has an earlier release date than the currently installed maintenance release. For example, if you have a maintenance release from February 1 currently installed, install a maintenance release of the 2026H2 semiannual release from February 1 or later.

Best Practice: Do not upgrade directly to TanOS 1.9.1 from a version earlier than 1.9.0. If you are upgrading from a version earlier than 1.9.0, you must perform intermediate upgrades to follow the path for the version from which you are upgrading as indicated in Upgrade paths on page 473.

Before you begin

1. Read the release notes for the TanOS versions that were released after your current version to stay informed about expected behavior.
2. If your current deployment does not use an Appliance Array, create an Array. For more information, see Installing and managing an Appliance Array on page 158.

©2026 Tanium Inc. All Rights Reserved

3. Plan a maintenance window that accounts for all necessary upgrade tasks. If you manage a Zone Server separately from the Appliance Array, you must also upgrade it separately during the same maintenance window in which you upgrade the Appliance Array. The procedure is the same, but it must be done separately on each Zone Server that is not an Array member. For more information about Zone Servers installed outside of an Array, see Installing individual Zone Servers on page 176.

4. Verify the current deployment is working as expected, including all Tanium Core Platform and solutions.

5. Run a health check on page 488 on each Appliance to check the status of network services and Tanium services.

6. Create a backup of the Appliance. If you have an inactive partition on a physical Tanium Appliance or virtual Tanium Appliance, you can choose to perform a partition sync on page 395 to back up the active partition to the inactive partition. Alternatively, for virtual or cloud Appliances, you can create a snapshot of the virtual image before you upgrade.

   > **Important:** Though a normal upgrade does not require you to restore from a backup, the backup lets you quickly restore the Appliances to a known functional state if you encounter issues during an upgrade.

7. Cloud-based Tanium Appliances hosted by Microsoft Azure: Make sure that the Accelerated Networking feature is disabled on the network interfaces that are connected to Tanium Appliances.

8. Virtual Tanium Appliances: Verify that the VM uses a CPU type that exposes the x86-64-v2 microarchitecture level. If the CPU does not expose this level, the pre-upgrade check prevents the upgrade. Hypervisor settings that determine the exposed microarchitecture level include **EVC Mode** for VMware vSphere, **Processor Compatibility Mode** in Microsoft Hyper-V, and **CPU Type** in Proxmox VE. For more information, see the documentation for your hypervisor.

9. Make sure you have the installation package or a token URL for each Tanium Core Platform version you will need during the upgrade process. You can use the token URL to download the installation package directly to the Appliance; for token URLs, Contact Tanium Support on page 510. You can download the installation package from the **Artifacts** section of your Tanium Account. For more information, see View Tanium artifacts. However, you must upload

©2026 Tanium Inc. All Rights Reserved

the files to the Appliance using SFTP after you download them on a separate computer.

> **Note:** You must download the installation packages if you are in an air-gapped environment.

Carefully follow the prescribed upgrade paths for the steps to provide each package at the appropriate time. The necessary packages include the following:

- For upgrading to TanOS 1.9.1 as part of Tanium Semiannual Release 2026H2, the Tanium Core Platform installation package file is 7.9.3.xxxx_linux_server_package_8.zip, where xxxx is the build number for the maintenance release. See the release notes for the semiannual release for the latest available maintenance release.
- If your upgrade path includes an intermediate upgrade to TanOS 1.9.0, the Tanium Core Platform installation package file is 7.8.4.xxxx_linux_server_package_8.zip, where xxxx is the build number for the maintenance release. See the release notes for the semiannual release for the latest available maintenance release.

Understand the upgrade process

Use the primary Tanium Server Appliance to perform the upgrade. This automatically manages the upgrade on all Appliances in the Appliance Array. The upgrade process runs pre-upgrade checks on all Appliances in the Array in parallel before upgrading any of the Appliances. If you see the message `Pre-upgrade checks failed, not upgrading`, fix the issue that is reported with the message before attempting the upgrade again.

> **Tip:** When upgrading to a new semiannual release, the pre-upgrade checks include verifying that you have uploaded the Tanium Core Platform installation package from the semiannual release bundle. For more information, see Provide the Tanium Core Platform installation package on page 474

When you upgrade TanOS, the appliances are upgraded in the following order:

1. The primary Tanium Server

©2026 Tanium Inc. All Rights Reserved

2. Any secondary Tanium Server, and the active Module Server, in parallel

3. All other Appliances, including any inactive Module Server and Zone Servers, in parallel

During an upgrade, TanOS stops all Tanium services, and resumes services after rebooting the Appliance. The upgrade runs independently of the session that starts it, so the upgrade continues if you lose your SSH connection to the Appliance. Sign in again and view the TanOS upgrade log on page 481 to follow the progress.

It is safe to restart the Tanium Appliance upgrade if it is interrupted. The upgrade checks the status of all Appliances in the Array before proceeding from where the interruption occurred. If you have problems restarting an upgrade that was interrupted, contact Tanium Support on page 510.

Note: On an Appliance that uses NIC teaming, TanOS moves the team IP addresses to a single member interface during the upgrade and rebuilds the team when the Appliance reboots. NIC redundancy is unavailable until the reboot finishes.

To troubleshoot TanOS upgrade issues, review the upgrade log from the Appliance that had an issue. For more information, see View the TanOS upgrade log on page 481.

Important:

- If your current deployment does not use an Appliance Array, create an Array before upgrading. For more information, see Installing and managing an Appliance Array on page 158.
- If you manage a Zone Server separately from the Appliance Array, you must also upgrade it separately during the same maintenance window in which you upgrade the Appliance Array. The procedure is the same, but it must be done separately on each Zone Server that is not an Array member. For more information about Zone Servers installed outside of an Array, see Installing individual Zone Servers on page 176.

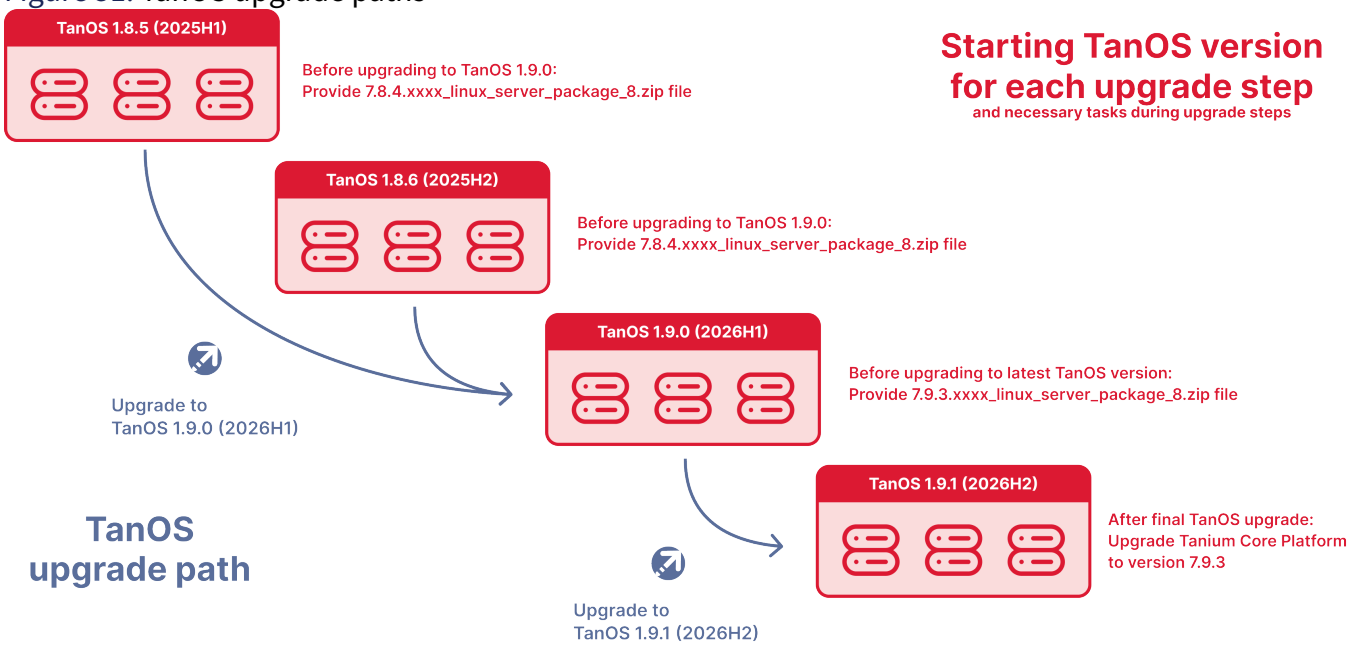
Upgrade paths

If you are upgrading from TanOS 1.9.0, you can upgrade directly to version 1.9.1. If you are upgrading

©2026 Tanium Inc. All Rights Reserved

from a version earlier than 1.9.0, perform one or more intermediate upgrades before upgrading to version 1.9.1. The following diagram provides an overview of upgrade paths from recent versions of TanOS. Repeat the steps in Perform the upgrade on page 474 to follow the appropriate path for the version from which you are upgrading.

Figure 51. TanOS upgrade paths



Note: If you are upgrading from a version of TanOS earlier than 1.8.5, you must perform additional intermediate upgrades in stages. For more information about upgrading to earlier versions of TanOS before completing an upgrade to TanOS 1.9.0, see the Tanium Appliance User Guide version 1.9.0, the Tanium Appliance User Guide version 1.8.5, or the Tanium Appliance User Guide for another applicable version in the PDF archive.

Perform the upgrade

Repeat the steps in this section for each upgrade that is necessary to follow the appropriate upgrade path for the version from which you are initially upgrading. For more information, see Upgrade paths on page 473.

PROVIDE THE TANIUM CORE PLATFORM INSTALLATION PACKAGE

Before upgrading to a new version, you must provide the correct Tanium Core Platform installation package to the primary Tanium Server in the Appliance Array:

©2026 Tanium Inc. All Rights Reserved

- For upgrading to TanOS 1.9.1 as part of Tanium Semiannual Release 2026H2, the Tanium Core Platform installation package file is 7.9.3.xxxx_linux_server_package_8.zip, where xxxx is the build number for the maintenance release. See the release notes for the semiannual release for the latest available maintenance release.
- If your upgrade path includes an intermediate upgrade to TanOS 1.9.0, the Tanium Core Platform installation package file is 7.8.4.xxxx_linux_server_package_8.zip, where xxxx is the build number for the maintenance release. See the release notes for the semiannual release for the latest available maintenance release.

Note: If you provide an installation package that this version of TanOS cannot install, TanOS leaves the file in the /incoming directory and lists the file name in the menu under `Left in /incoming, not usable by this TanOS`. If no usable package is available, the menu reports `No installable Tanium Core Platform version is available`.

Important: If you manage a Zone Server separately from the Appliance Array, you must also provide the installation package to the Zone Server separately. For more information about Zone Servers installed outside of an Array, see Installing individual Zone Servers on page 176. As a best practice, do not upload the entire upgrade package to the Zone Server or use the tokens download steps. To avoid copying Tanium Server and Module Server files onto a host in a separate network, download the package from the **Artifacts** section of your Tanium Account, extract only the Zone Server RPM from ZIP file, and use SFTP to copy only that file to the /incoming folder of the Zone Server Appliance.

Use a downloaded installation package

1. If you did not already do so, download the Tanium Core Platform installation package from the **Artifacts** section of your Tanium Account. For more information, see View Tanium artifacts.
2. Use SFTP to copy the TanOS upgrade file to the /incoming directory on the primary Tanium Server Appliance. For more information, see Reference: Transfer files to and from the Appliance on page 621.

Use a tokens download

©2026 Tanium Inc. All Rights Reserved

1. If you did not already do so, contact Tanium Support on page 510 to obtain a token URL for the Tanium Core Platform package file.
2. On the primary Tanium Server, sign in to the TanOS console as a user with the `tanadmin` role.
3. Enter `B` to go to the **Appliance Maintenance** menu.
4. Enter `T` to go to the **Tokens Download** menu, and follow the prompts to download the package.

(INTERNET-CONNECT ENVIRONMENTS) UPGRADE FROM THE TANOS MANIFEST

About this task

In an internet-connected environment, you can download the latest available version that appears in the TanOS manifest directly from Tanium.

1. On the primary Tanium Server, sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-3` (Appliance Maintenance > Upgrade TanOS).
3. At the prompt, enter `Yes` to upgrade all Appliances in the Array.

```
>>> Appliance Maintenance -> Upgrade TanOS <<<

Updating Array Information

 Getting update from ts2 (10.70.197.248)
 Sending update to ts2 (10.70.197.248)
 Getting update from tms1 (10.70.197.249)
 Sending update to tms1 (10.70.197.249)

 Array Upgrade Progress Report
 =============================
     Name                      Role                      Version
     ts1                       TaniumServer              1.9.0
     ts2                       TaniumServer              1.9.0
```

©2026 Tanium Inc. All Rights Reserved

```
    tms1                    Tanium Module Server      1.9.0

 This appliance is ready to perform a full-array Tanium upgrade.
 You should choose to upgrade all appliances in the array even if some of
 them happen to already be on the desired version.


Do you want to upgrade all appliances in the array? [Yes|No]:
```

4. Enter `D` to download the version available from the manifest.

```
>>> Appliance Maintenance -> Upgrade TanOS <<<

Updating Array Information

 Getting update from ts2 (10.70.197.248)
 Sending update to ts2 (10.70.197.248)
 Getting update from tms1 (10.70.197.249)
 Sending update to tms1 (10.70.197.249)

 Array Upgrade Progress Report
 =============================
    Name                    Role                    Version
    ts1                     TaniumServer            1.9.0
    ts2                     TaniumServer            1.9.0
    tms1                    Tanium Module Server    1.9.0

 This appliance is ready to perform a full-array Tanium upgrade.
 You should choose to upgrade all appliances in the array even if some of
 them happen to already be on the desired version.


Do you want to upgrade all appliances in the array? [Yes|No]: Yes
Fetching latest upgrade information from Tanium
```

©2026 Tanium Inc. All Rights Reserved

```
Select an Upgrade RPM (must be at least 1.9.1.1234 )

         T: Download from Tokens
         D: Download 1.9.1.1234 from Tanium

         R: Return to previous menu  RR: Return to top
```

5. After TanOS downloads the upgrade RPM, enter the number for the downloaded file, and follow the prompts to perform the upgrade.

```
>>> Appliance Maintenance -> Upgrade TanOS <<<

Updating Array Information

 Getting update from ts2 (10.70.197.248)
 Sending update to ts2 (10.70.197.248)
 Getting update from tms1 (10.70.197.249)
 Sending update to tms1 (10.70.197.249)

 Array Upgrade Progress Report
 =============================
     Name                      Role                      Version
     ts1                       TaniumServer              1.9.0
     ts2                       TaniumServer              1.9.0
     tms1                      Tanium Module Server      1.9.0

 This appliance is ready to perform a full-array Tanium upgrade.
 You should choose to upgrade all appliances in the array even if some of
 them happen to already be on the desired version.



Do you want to upgrade all appliances in the array? [Yes|No]: Yes
Fetching latest upgrade information from Tanium

 Select an Upgrade RPM (must be at least 1.9.1.1234 )
```

©2026 Tanium Inc. All Rights Reserved

```
T: Download from Tokens
D: Download 1.9.1.1234 from Tanium

1: TaniumTanOS_Upgrade-1.9.1-1234.noarch.rpm                991M
   Size:   990,636,286 SHA1: d0711017c773a05c0b9dfc0b8e33b66c0a8208df

R: Return to previous menu  RR: Return to top
```

Note: When prompted to back up the active partition to the inactive partition, enter `Yes`.

The TanOS Console displays the upgrade process for each Appliance in the Array during the upgrade.

(AIR-GAPPED ENVIRONMENTS) UPGRADE BY MANUALLY UPLOADING AN RPM FILE

About this task

In an air-grapped environment, you can manually upload the TaniumTanOS_Upgrade-<version>.noarch.rpm upgrade package downloaded from your Tanium Account to upgrade to TanOS 1.9.1. Make sure that you follow the appropriate Upgrade paths on page 473 for the version from which you are upgrading.

1. Download the TanOS upgrade package from the **Artifacts** section of your Tanium Account. For more information, see View Tanium artifacts.
2. Use SFTP to copy the TanOS upgrade file to the /incoming directory on the primary Tanium Server Appliance. For more information, see Reference: Transfer files to and from the Appliance on page 621.
3. On the primary Tanium Server, sign in to the TanOS console as a user with the `tanadmin` role.
4. Enter `B-3` (Appliance Maintenance > Upgrade TanOS).
5. At the prompt, enter `Yes` to upgrade all Appliances in the Array.

```
>>> Appliance Maintenance -> Upgrade TanOS <<<
```

©2026 Tanium Inc. All Rights Reserved

```
Updating Array Information


 Getting update from ts2 (10.70.197.248)
 Sending update to ts2 (10.70.197.248)
 Getting update from tms1 (10.70.197.249)
 Sending update to tms1 (10.70.197.249)

 Array Upgrade Progress Report
 ============================
     Name                      Role                      Version
     ts1                       TaniumServer              1.9.0
     ts2                       TaniumServer              1.9.0
     tms1                      Tanium Module Server      1.9.0

 This appliance is ready to perform a full-array Tanium upgrade.
 You should choose to upgrade all appliances in the array even if some of
 them happen to already be on the desired version.



Do you want to upgrade all appliances in the array? [Yes|No]:
```

6. Enter the line number of the RPM file to use, and follow the prompts to perform the upgrade. When prompted to back up the active partition to the inactive partition, enter `Yes`.

   The TanOS Console displays the upgrade process for each Appliance in the Array during the upgrade.

WHAT TO DO NEXT

Perform the following steps after each TanOS upgrade.

1. If you manage any Zone Servers separately from the Appliance Array, repeat the upgrade process on these Zone Servers. For more information about Zone Servers installed outside of an Array, see Installing individual Zone Servers on page 176.

2. Run a health check on page 488 to check the status of network services and Tanium services.

©2026 Tanium Inc. All Rights Reserved

3. Verify the components in the deployment on page 198. If verification fails, see Tanium Appliance support and troubleshooting on page 487.

4. Upgrade Tanium Core Platform to the version in the same semiannual release. For more information, see Upgrade Tanium Core Platform in an Appliance deployment on page 481.

    - If you completed an intermediate upgrade to TanOS 1.9.0, upgrade Tanium Core Platform to version 7.8.4.
    - If you completed the upgrade to TanOS 1.9.1, upgrade Tanium Core Platform to version 7.9.3.
    - If you completed an upgrade to a later build of TanOS 1.9.1 from a maintenance release, upgrade Tanium Core Platform 7.9.3 to the build from the same maintenance release.

5. If you completed an intermediate upgrade, repeat all steps in Perform the upgrade on page 474 to continue the appropriate upgrade path. For more information, see Upgrade paths on page 473.

View the TanOS upgrade log

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-1-1-2` (Tanium Support > Tanium Log Files > TanOS Appliance > Upgrade Log).
3. Enter `V` to view the current TanOS upgrade log file, or enter the line number of a previous log file if the relevant log entries have been rotated out of the current log file.

Upgrade Tanium Core Platform in an Appliance deployment

The subsequent topics in this section provide information about preparing for the upgrade, upgrading the Tanium Core Platform, and installing solution updates and verifying the upgrade.

Important: You must upgrade TanOS before upgrading Tanium Core Platform, and you must upgrade all Tanium solutions after upgrading Tanium Core Platform. After you start the upgrade process, you cannot access Tanium solutions until you finish upgrading both the platform and solutions. For more information, see Upgrading TanOS and Tanium Core Platform on page 465.

©2026 Tanium Inc. All Rights Reserved

Tip: In Tanium Console, the **Solutions** page (**Administration** > **Configuration** > **Solutions**) indicates at the top-right if Tanium Core Platform Servers are up-to-date or if an update is available.

Note: For air-gapped environments, install a full air gap update, which includes updates to solution modules, production content packs, and lab content packs. For more information, see Install a full update on page 207.

Important:

- If your current deployment does not use an Appliance Array, create an Array before upgrading. For more information, see Installing and managing an Appliance Array on page 158.
- If you manage a Zone Server separately from the Appliance Array, you must also upgrade it separately during the same maintenance window in which you upgrade the Appliance Array. The procedure is the same, but it must be done separately on each Zone Server that is not an Array member. For more information about Zone Servers installed outside of an Array, see Installing individual Zone Servers on page 176.

Before you begin

- Read the release notes for all of the Tanium Core Platform versions that were released after your current version to stay informed about expected behavior.
- If you are upgrading to a new semiannual release or maintenance release that includes a Tanium Core Platform upgrade, the appropriate upgrade package file is included in the semiannual release bundle or maintenance release bundle. If you upgraded TanOS, you have already supplied the Tanium Core Platform installation package to the Appliance.
- Make sure the current deployment is working as expected, including all Tanium Core Platform Servers and solutions.
- Perform a backup of the Appliance. For more information, see Tanium Appliance redundancy,

©2026 Tanium Inc. All Rights Reserved

backup, and recovery on page 379.

- If you are upgrading from Tanium Core Platform 7.5.6 or earlier to a semi-annual release for the first time (including Tanium Core Platform 7.6.2 or later), upgrade all solutions before you install the release bundle that includes Tanium Core Platform 7.6.2 or later. For information about upgrading solutions, see Import, re-import, or update specific solutions. When you upgrade to subsequent semi-annual releases, a separate upgrade of solutions is not necessary or possible. You can optionally use the change management feature in Endpoint Configuration to manage a staged rollout of the endpoint tools that enable upgraded solution functionality on endpoints. For more information, see Managing Tanium Client and endpoint tool upgrade rollouts.

Upgrade the Tanium Core Platform

About this task

Use the following steps to upgrade all Appliances within an Array. This procedure upgrades all Tanium Servers, Tanium Module Servers, Tanium Zone Servers, and Tanium Zone Server Hubs within the Array. If you are upgrading to a new semiannual release, you already provided the Tanium Core Platform installation package to the primary Tanium Server.



Best Practice: If you are upgrading an individual Zone Server that is not part of the Appliance Array, do not upload the entire upgrade package to the Zone Server or use the tokens download in TanOS during the upgrade. To avoid copying Tanium Server and Module Server files onto a host in a separate network, download the package from the **Artifacts** section of your Tanium Account, extract only the Zone Server RPM from ZIP file, and use SFTP to copy only that file to the /incoming folder of the Zone Server Appliance. For more information about Zone Servers installed outside of an Array, see Installing individual Zone Servers on page 176.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `1-U` (Tanium Installation > Upgrade Tanium Software).
3. Enter `Yes` to upgrade Tanium Core Platform on all Appliances in the Array.

```
--------------------------------------------------


   >>> Tanium Installation -> Upgrade Software <<<
```

```
Use this menu to upgrade already installed Tanium Software.
Note: Tanium Modules must be upgraded from the Web UI

Please install a TanOS Upgrader which contains new Tanium versions.

Currently installed Tanium software:

TaniumServer                    7.9.3.1234
Note: Upgrading a TaniumServer requires packages of the same version for all
three platform variants: TaniumServer, TaniumModuleServer, TaniumZoneServer
Updating Array Information
Getting update from ts1 (10.70.197.248)
Sending update to ts1 (10.70.197.248)
Getting update from ts1 (10.70.197.249)
Sending update to ts1 (10.70.197.249)

Array Upgrade Progress Report
=============================
    Name                        Role                        Version
    ts1                         TaniumServer                7.8.4.1234
    ts2                         TaniumServer                7.8.4.1234

This appliance is ready to perform a full-array Tanium upgrade.
You should choose to upgrade all appliances in the array even if some of
them happen to already be on the desired version.

Do you want to upgrade Tanium on all appliances in the array? [Yes|No]: yes

As part of SAR2026H2, TanOS 1.9.1 supports only Tanium Core Platform 7.9.3.1234.
You cannot install any other version of Tanium Core Platform.

Available Upgrades:

         1: 7.9.3.1234
         T: Download from Tanium
```

©2026 Tanium Inc. All Rights Reserved

```
         R: Return, do not upgrade


Please select:
```

4. Enter the line number of the upgrade package that you uploaded to the /incoming directory.

Install solution updates and verify the upgrade

If you encounter issues during verification, see Tanium Appliance support and troubleshooting on page 487.

SIGN IN TO TANIUM CONSOLE AND UPDATE SOLUTIONS

Sign in to Tanium Console as an administrator. You are redirected to the **Solutions** page, where each installed solution upgrades to the version included in the semiannual release bundle.

> **Note:** You cannot access Tanium solutions until all solutions are upgraded.

VERIFY THE BASIC DEPLOYMENT

1. From the Tanium **Home** page, ask the following question to verify that endpoints with the Tanium Client respond:
   `Get Computer Name and Tanium Server Name from all machines`
2. Click **Search** and review the results grid to verify that all endpoints with the Tanium Client report successfully.
3. You can also go to the **Client Status** page to review recent Client registration details. Go to **Administration** > **Configuration** > **Client Status** to go to the page.

VERIFY THE ZONE SERVER DEPLOYMENT

1. Use the Tanium Client Management service to deploy the Tanium Client to an endpoint in your environment. In the configuration for Tanium Server, specify the Zone Server FQDN (appliance-zs.tam.local in this example).
2. In Interact, ask `Get Computer Name and Tanium Server Name from all`

©2026 Tanium Inc. All Rights Reserved

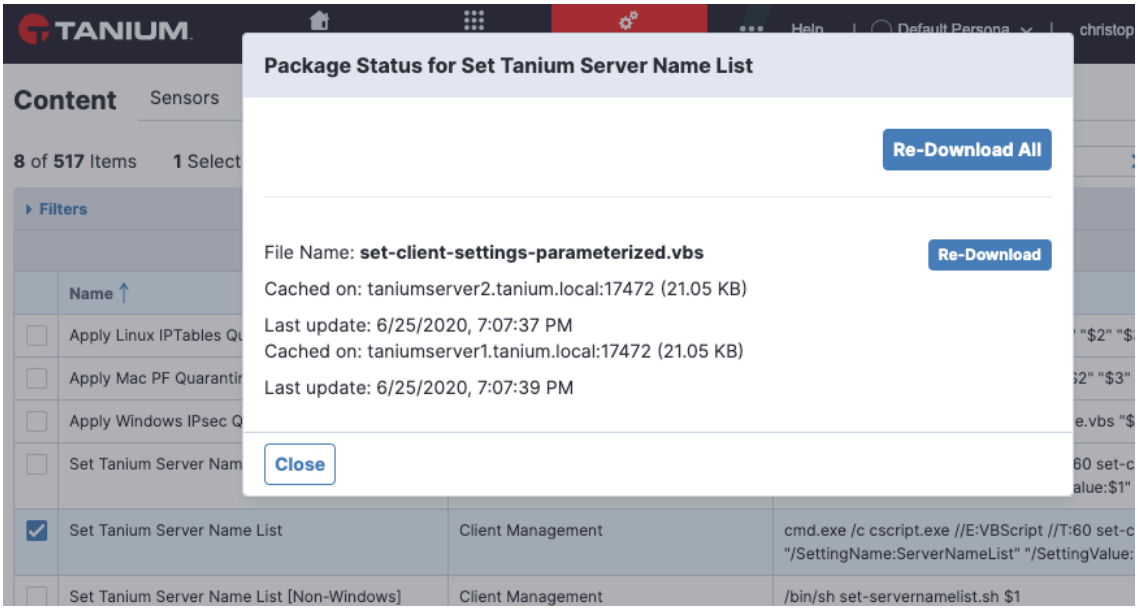
`machines` and verify that the Tanium Client on the Zone Server reports through the Tanium Zone Server.

VERIFY A TANIUM CLUSTER DEPLOYMENT

About this task

Perform the following additional verifications if you installed a Tanium Cluster through an Appliance Array on page 158.

1. In Interact, ask `Get Tanium Server Name List from all machines`. Verify that both Tanium Servers are active.
2. Verify that both Servers can download packages with URL-specified files when such a package is created or imported. The **Set Tanium Server Name** package is an example of a package with URL-specified files:
    a. Go to **Administration** > **Content** > **Packages**.
    b. Select the row for **Set Tanium Server Name List**.
    c. Click **Status** and check that the files have been downloaded and are now cached on both Servers.
    Figure 52. Verifying package cache status on both Tanium Servers



©2026 Tanium Inc. All Rights Reserved

Tanium Appliance support and troubleshooting

The subsequent topics in this section provide information about viewing version information and running the health check, restarting services and networking, recovering from errors, reviewing logs, running diagnostics and gathering support information, and contacting Tanium Support.

View version information

About this task

When discussing issues, it is important to communicate precise version information with colleagues and with Tanium Support. This screen also provides other important information, such as system time, uptime, and basic network configuration details.

1. Sign in to the TanOS console as a user with the `tanadmin` or `tanuser` role.
2. Enter `@` to go to the **About this Appliance** menu that shows version information, system time, uptime, and basic network configuration details.

```
------------------------------------------------------------


             >>> About this Appliance <<<


Hostname:                          ts1
Domain Name:                       test.tanium.local

System Time (MM/DD/YY):            08/30/22-20:50:06-UTC
Uptime:                            up 6 days, 5 hours, 16 minutes

TanOS Version:                     1.9.1.1234

Appliance Model:                   TV-110
Serial Number:                     421d22ac4b1f4ea5-901ea65b30d6b6fc
```

©2026 Tanium Inc. All Rights Reserved

```
IP Address:                         10.10.10.162
Gateway address:                    10.10.10.2

Name Servers:                       10.10.10.10
NTP Servers:                        0.pool.ntp.org

Tanium Version:                     7.9.3.1234
Server Role:                        Tanium Server (Primary DB)
Server Addons:                      Zone Server Hub
Tanium Cluster Role:                Primary Node
Cluster Member IP:                  10.10.10.163

Appliance Type:                     Linux KVM
Number of Processors:               2 x 2304 MHz
Total Memory:                       64G

Tanium Server Pub Key MD5:          88da5655a7f03950077d9e3681dffba7
Tanium Server Init Key MD5:         78fc1a51b0779f89f13d341f633f1f9e
TZS Hub Registration Fingerprint: 47:fa:27:96:94:54

-----------------------------------------------------------------



Press enter to continue
```

Run the Health Check

About this task

After initial configuration, TanOS automatically runs a health check every 15 minutes. The results for the latest health check are stored in the health.log file in the /outgoing directory.

©2026 Tanium Inc. All Rights Reserved

Best Practice:

The health check sends alerts if they are enabled. As a best practice:

- Enable alerts.
- Configure a severity level for alerts that matches the checks for which you want to receive alerts. For information about specific alerts, including severity levels, see Reference: TanOS health check results on page 538.
- Configure an SMTP destination to send email alerts.
- (Optional) Configure a syslog destination.

For information about configuring alerts, see Configure syslog alerts on page 436.

To run a health check manually:

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3` (Tanium Support).
3. Enter `5` to run the health check.

```
           >>> Tanium Support -> Run Health Check <<<

Report time: 2020-10-29 14:44:29 UTC
Report Uptime:  14:44:29 up  8:10,  1 user,  load average: 0.00, 0.01, 0.05

>>> Is EULA Accepted <<<
   automated@none.com accepted June2019 EULA on Thu Oct 29 06:29:33 UTC 2020
Is EULA Accepted: pass

>>> Operating System health (will take 7-10 seconds) <<<
CPU: pass
Memory: pass (70% avail >= 10%)
Swap: pass (100% avail >= 50%)
```

©2026 Tanium Inc. All Rights Reserved

```
Partition /: pass (8%)
Partition /boot: pass (24%)
Partition /var: pass (3%)
Partition /var/log/audit: pass (2%)
Partition /opt: pass (2%)
Partition /tmp: pass (1%)
Partition /home: pass (1%)
Partition /cores: pass (1%)
Partition /var/log: pass (1%)
Boot Check: Pass (BIOS Boot with virtual machine)
Active partition: pass (VolGroup1-root)

>>> Hardware health (will take 1-12 seconds) <<<
hardware type: pass (TV-110)

>>> User health <<<
user tanium: pass
user tanadmin: pass
user tancopy: pass
user tanfactory: pass (disabled)
system user shells: pass
system user policies: pass

>>> Network health (will take 5-7 seconds) <<<
default gateway: pass
generic name resolution: pass
own hostname resolution: pass (Hosts)
no stats available
L2 check eth0: pass
mount /opt/mounts/connect: pass (not configured)
mount /opt/mounts/detect: pass (not configured)
mount /opt/mounts/trends: pass (not configured)
Connection tracking: pass

>>> Service health <<<
chronyd service: pass (running)
```

©2026 Tanium Inc. All Rights Reserved

```
chronyd service: pass (time synced)
rsyslog service: pass
syslog delivery: N/A (syslog delivery is disabled)
iptables service: pass
ip6tables service: pass
sshd service: pass
ipsec service: pass
local auth service: pass

>>> Application health <<<
taniumserver.service: pass (service is running)
taniumserver.service: pass (iptables)
taniumserver.service: pass (database connected)
taniumserver.service: pass (database size: 1 GB)
TMS connectivity: fail (127.0.0.1:17477)
taniummoduleserver.service: pass (does not exist/not installed)
taniumzoneserver.service: pass (does not exist/not installed)

>>> TanOS <<<
BIOS Version: pass (not checked)
PERC Version: pass (not checked)
iDRAC Version: pass (not checked)
Backup: fail (Backup schedule cannot run without key)
TanOS key material: pass

>>> Miscellaneous <<<
misc 1: pass
core files: pass
shell keys: pass

>>> Database Replication Health <<<

Database Replication: pass (Not configured)

>>> Disk Encryption Key <<<
```

©2026 Tanium Inc. All Rights Reserved

```
Disk Encryption Key check: N/A (no iDRAC)

>>> Tanium Application file Permissions <<<
TaniumServer file permissions: pass

>>> Postgres SSL Health Check <<<
Postgres SSL: pass
SSL CRL file: root.crl.pem

>>> OVA Health (TV-2xx) <<<
RAM Requirements: fail (1837)
CPU Requirements: fail (2)

executed checks: 58
failed checks: 4

>>> End Health Check <<<
Press enter to continue
```

Results appear on screen, and the results are also stored in the health.log file in the /outgoing directory. For more information about each check, see Reference: TanOS health check results on page 538.

Note: If your health check report prompts you to accept the end-user license agreement (EULA), go to the **tanadmin** menu and enter Q to view the EULA. Follow the prompts to accept the license agreement.

Note: The TanOS health check provides a warning when the available space is 70% full on any partition. When the available space is 95% full, TanOS stops all Tanium services to preserve TanOS functionality.

©2026 Tanium Inc. All Rights Reserved

Tip: After you perform the initial configuration for an Appliance, a core backup is scheduled by default. The health check reports an error that automatic backups cannot complete until you set up an encryption key. To remove the error from the health check, you can either add an encryption key or disable the scheduled core backup. For information about how to disable the core backup, see Configure an automatic backup on page 408.

Overview of Tanium Appliance logs, reports, and troubleshooting features

The following logs, reports, and troubleshooting features can help diagnose issues with the Appliance itself. For additional information about logs and troubleshooting for Tanium Core Platform Servers, see Tanium Core Platform troubleshooting and logs in an Appliance deployment on page 512.

- About this Appliance screen on page 487: This screen provides information about the Tanium Appliance version, system time, uptime, and basic network configuration details.
- Advanced Support menu on page 501: This menu provides options for exporting core files, generating process dumps, and viewing directory space usage.
- Array roles log on page 497: This log records events that relate to installation of roles on Appliances.
- Airgap log on page 222: This log records events that relate to an air gap installation.
- Backup Restore log on page 416: This log records events that relate to the restoration of a core or comprehensive backup.
- Cloud Access Point log on page 195: This log records access information for Tanium Clients that connect to Tanium Cloud through an Appliance with the Cloud Access Point role.
- Database Operations menu on page 450: This menu provides options for viewing information about Tanium database operations.
- Health Check report on page 488: This report provides information on the health of the Appliance operating system, hardware, users, network, services, applications, database replication, disk encryption, Postgres SSL, and the virtual machine (if applicable).

©2026 Tanium Inc. All Rights Reserved

- iDRAC log: on page 427 The iDRAC log provides information about system events and firmware updates in the iDRAC interface.
- Measure data transfer rate on page 158: You can measure the data transfer rate between an Array Manager and an Array member to help diagnose network issues between Appliances.
- Network Diagnostics menu on page 503: This menu provides options for running network diagnostic procedures, viewing networking information, and viewing firewall details.
- Network Latency log on page 505: This log records periodic tests of network latency to help monitor and diagnose network issues between Appliances.
- Performance Monitoring menu on page 458: This menu provides options for viewing information about system activity, processes, input/output usage, CPU usage, and other resource usage.
- Read-only restricted shell on page 506: Opening an RO shell enables you to view files on the Appliance file system, including logs that are not accessible through the TanOS console.
- SNMP walk on page 439: You can configure integration with a Simple Network Management Protocol (SNMP) manager for collecting and analyzing Appliance information.
- Status menu on page 448: This menu provides options for viewing information about system activity, processes, input/output usage, CPU usage, and other resource usage.
- Syslog forwarding on page 429: You can forward Appliance logs to a remote syslog server.
- Tanium Support Gatherer on page 500: The Tanium Support Gatherer (TSG) provides information on the status of the Appliance system, processes, and network interfaces.
- TanOS event log on page 497: This log records major events on the Appliance, such as Server installations, upgrades, initial configuration, software resets, backups, partition synchronization, Tanium Module Server synchronization, Tanium Core Platform services stopped due to lack of disk space, Tanium Server or Module Server failover, and restricted or unrestricted shell access.
- TanOS partition sync log on page 464: This log records events that relate to partition synchronization on Appliances with active and inactive partitions.
- TanOS upgrade log on page 481: This log records events that relate to Appliance upgrades.

©2026 Tanium Inc. All Rights Reserved

- TCP dump on page 501: Running a TCP dump creates a packet capture (PCAP) file for the network interface that you select. PCAP files capture real-time data packets that traverse a network. You can use the files to analyze network traffic and troubleshoot network issues.

Restart services or networking

Check whether a Tanium service needs to be restarted. You can use the TanOS menu to stop a service whether the service is enabled, and you can use TanOS to start a service if the service is enabled.

Restart services

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-1` (Tanium Operations > Tanium Service Control).
3. Enter the line number of the service you want to manage to view the service commands.

```
          >>> Tanium Operations -> Tanium Service Control -> Service <<<

   Service         State      Status
   taniumserver     enabled    running

        1: Start service
        2: Stop service
        3: Restart service
        4: Disable service
        5: Enable service
        6: Status Details

        R: Return to previous menu

-------------------------------------------------------
```

4. Type the number of a service control command to issue the command.

Restart networking

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `A-2` (Appliance Configuration > Networking Configuration).
3. Enter `4` to restart networking.

Exit maintenance mode after an error

About this task

Some maintenance procedures that you perform in TanOS automatically enter maintenance mode to ensure Tanium services are not affected by the maintenance operation. When the operation completes, TanOS automatically exits maintenance mode and resumes normal operations. However, if an error occurs during a maintenance operation, TanOS can sometimes stay in maintenance mode. If TanOS indicates that you are unable to perform an operation due to maintenance activity, you can manually exit maintenance mode.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-C` (Appliance Maintenance > Maintenance Mode).
3. Enter `1` to clear any maintenance actions.

Reinitialize replication

About this task

Use this procedure after the secondary database server has been promoted to primary, or to reinitialize a broken Tanium cluster.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-B` (Tanium Operations > Cluster Configuration).
3. Enter `E` and follow the prompts to reinitialize replication.

Reindex databases

About this task

©2026 Tanium Inc. All Rights Reserved

Use this procedure to reindex databases as directed by Tanium Support, or if you encounter database-related issues in solution logs after a TanOS upgrade.

Important: This operation stops most Tanium services while it is running, and it might take several minutes to complete.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-3-I` (Tanium Support > Database Operations > Reindex Databases), and follow the prompt to reindex all databases.

Review TanOS Appliance logs

About this task

TanOS Appliance logs record events related to TanOS operations, such as Appliance configuration, installation of roles, TanOS upgrades, status and failures from previous health checks, and other operations at the OS level.

Tip: When you view a log, you can use commands similar to ex editor commands to search for patterns (keywords).

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-1-1` (Tanium Support > Logs > TanOS Appliance).
3. Select a log from the menu.
4. Select an item to view the log, follow its growth, delete it, or export it to the /outgoing directory.

Review Tanium Core Platform logs

About this task

If you are diagnosing issues with the Tanium Core Platform installation, review the logs. For

©2026 Tanium Inc. All Rights Reserved

additional information about logs and troubleshooting for Tanium Core Platform Servers, see Tanium Core Platform troubleshooting and logs in an Appliance deployment on page 512.

Tip: When you view a log, you can use commands similar to ex editor commands to search for patterns (keywords).

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-1` (Tanium Support > Logs).
3. Enter `2` for Tanium Server, `3` for Tanium Module Server, or `4` for Tanium Zone Server, depending on the role of the Appliance.

```
------------------------------------------------------


     >>> Tanium Support -> Logs -> taniumserver <<<


          1: Tanium Server Log (log0.txt)
          2: Tanium Server TDL Log (log0.txt)
          3: Tanium Server RBAC Log (rbac0.txt)
          4: Tanium Server PAM4 Log (tanium_pam4.log)
          5: Tanium Server Workbenches (workbenches_manager.log)
          6: Tanium Server Signature Verifier (signature_verifier.log)
          7: Tanium Server DB Upgrade Log (database-upgrade0.txt)
          8: Tanium Server Auth0 Log (auth0.txt)
          8: Tanium Module History Log (module-history0.txt)


          R: Return to previous menu  RR: Return to top


------------------------------------------------------
```

4. Select an item to view the log, follow its growth, delete it, or export it to the /outgoing directory.

```
------------------------------------------------------


>>> Tanium Support -> Logs -> TaniumServer -> log0.txt <<<
```

©2026 Tanium Inc. All Rights Reserved

```
      Size: 538   Last Update: 2022-03-11 14:10:40

         V: View file
         F: Follow log file growth
         T: Delete content of logfile
         E: Export to outgoing (sftp)

        R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

Review Tanium solution module logs

About this task

If you are diagnosing issues with expected behavior for solution modules, examine the module logs on the Module Server.

Tip: When you view a log, you can use commands similar to vi editor commands to search for patterns (keywords).

1. Sign in to the TanOS console on the Module Server as a user with the `tanadmin` role.
2. Enter `3-2` (Tanium Support > Module Log Files Access).
3. Select a log from the menu.
4. Select an item to view the log, follow its growth, delete it, or copy it to the /outgoing directory.

Review the configuration

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2-2` (Tanium Operations > Configuration Settings).

©2026 Tanium Inc. All Rights Reserved

3. Use the menu to view and edit Tanium Core Platform Server configuration files.

Run Tanium Support Gatherer

About this task

The Tanium Support Gatherer (TSG) collects system status, process status, network interface status, the scheduled tasks in the /etc/cron.d directory, and so on, to help Tanium Support evaluate possible Appliance or Tanium Core Platform Server issues.

Each Tanium Core Platform Server has a predefined list of files and commands to gather relevant data. The TSG output files are placed in the SFTP outgoing directory. The output files are ZIP archives, named with their collection or module name and a datestamp. The files remain in the outgoing directory until a daily cleanup task removes them. From the TSG menu, you specify a single item (a module or collection of files) or a comma-separated list of items.



Note: The ZIP files are password-protected. The password is the fully-qualified domain name of the Appliance from which the TSG was run.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3`-`A` (Tanium Support > Tanium Support Gatherer).
3. Enter `A` to run the Tanium Support Gatherer.
   TanOS runs the report and indicates the name of the zipped report file.

```
Generating Appliance TSG: tsg-tms1-vc-appliance-2022-04-19-2033
Gathering OS files
Gathering Network files
Gathering Database files
Gathering Tanium Server files
Creating zip file
Exporting zip file
Exported tsg-tms1-vc-appliance-2022-04-19-2033.zip
Password for the file is the appliance's FQDN
 Press enter to continue
```

4. Use SFTP to copy the zipped report to your local machine.

©2026 Tanium Inc. All Rights Reserved

Copy core files

About this task

> **Note:** To upload the Core Files directly to an SFTP destination from the /outgoing directory, you must add the tanadmin user's public SSH key to the SFTP user's authorized keys on the remote host. For more information, see Manage SSH keys for TanOS users on page 227.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-X-1` (Tanium Support > Advanced Support > Copy Core Files).
3. Enter the line number of the core files to copy.
   TanOS generates a ZIP file containing the compressed core files and uploads it to the /outgoing directory.
4. To upload the generated file to an SFTP location using TanOS, enter `Yes` and follow the prompts to enter the SFTP host IP or fully qualified domain name (FQDN), remote user name, and destination directory and file name.

Run tcpdump

About this task

Running a TCP dump creates a packet capture (PCAP) file for the network interface that you select. PCAP files capture real-time data packets that traverse a network. You can use the files to analyze network traffic and troubleshoot network issues.

You can add filters to the report to control how much data is captured. You can also see a preview of the report before you run the command.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `3-B` (Tanium Support > TcpDump).
3. Choose the network interface on which you want to run the command.
4. To limit the results, add filters such as IP/FQDN, port numbers, file size, or time range.

©2026 Tanium Inc. All Rights Reserved

```
-----------------------------------------------------

>>> Tanium Support -> TcpDump -> ens32 <<<

 About to launch a tcpdump for interface ens32
 Attention: If Host/IP and port filters are supplied, both will be applied

 Valid IP/Host filters include single FQDN's OR IPv4/6 addresses,
 e.g. 172.30.20.10 OR time.customer-a.internal OR 0123:4567:89ab:cdef::1
 Please provide a IP/FQDN filter (empty for none):
 No IP/Host capture filter supplied...

 Valid port number filters include a single port number between 1 and 65535
 Please provide a port number (1-65535) filter (empty for none):
 No port capture filter provided...

 Please provide a maximum size for the pcap file (1-512) in MB.: 512
 Please provide a maximum time in minutes (1-60) for the capture: 1
 Time option accepted: 1 minutes

 Run details:
   Interface: ens32
   Host filter:
   Port filter:
   PCAP size (packets): 426666
   Capture time (seconds): 60

 Would you like a preview? [Yes|No]:
```

5. Enter `yes` or `no` to accept or decline a preview of the file.
6. Enter `yes` to launch TCP dump and create the file.

```
-----------------------------------------------------
 Would you like to launch tcpdump? [Yes|No]: y
 tcpdump running, please be patient (might take up to 60 seconds)...
 tcpdump finished
 Please connect via sftp using tancopy to retrieve the file from outgoing
```

©2026 Tanium Inc. All Rights Reserved

```
(tcpdump_ens32.pcap)

 Warning - please keep in mind that this location is cleaned every night at 2:00 am
appliance time!

 Press enter to exit
```

7. Use SFTP to copy the file from the /outgoing directory to your local computer.

Run network diagnostics

Use the Network Diagnostics menu to run basic diagnostic procedures.

Ping a remote system

1. Sign in to the TanOS console of the Appliance as a user with the `tanadmin` role.
2. Enter `3-4-F` (Tanium Support > Run Network Diagnostics > Ping Remote System).
3. Enter the IP address or fully qualified domain name (FQDN) of the system to ping to view connection information.

Test a connection using a remote port

About this task

The **Test Remote Port** screen allows you to attempt a connection to a given destination and port using TCP.

1. Sign in to the TanOS console of the Appliance as a user with the `tanadmin` role.
2. Enter `3-4-2` (Tanium Support > Run Network Diagnostics > Test Remote Port (TCP)).
3. Enter the IP address or FQDN of the destination to test.
4. Enter the port number for the connection. The TanOS console indicates whether the Appliance can successfully connect using the specified port.

Trace the connection path to a destination

©2026 Tanium Inc. All Rights Reserved

About this task

Use the Trace Path screen to run a traceroute command to a remote destination using a specified connection protocol.

1. Sign in to the TanOS console of the Appliance as a user with the `tanadmin` role.
2. Enter `3-4-3` (Tanium Support > Run Network Diagnostics > Trace Path).
3. Enter the protocol to use for the connection, the FQDN or IP address of the destination, and the port to view the connection path between the Appliance and the destination.

Resolve a host name

1. Sign in to the TanOS console of the Appliance as a user with the `tanadmin` role.
2. Enter `3-4-4` (Tanium Support > Run Network Diagnostics > Resolve Name).
3. Enter the FQDN to find its IP address.

Check IPSEC

1. Sign in to the TanOS console of the Appliance with the secondary database as a user with the `tanadmin` role.
2. Enter `3-4` (Tanium Support > Run Network Diagnostics).
3. Enter `5` to view information about any active IPsec tunnels.

Listening ports

1. Sign in to the TanOS console of the Appliance with the secondary database as a user with the `tanadmin` role.
2. Enter `3-4` (Tanium Support > Run Network Diagnostics).
3. Enter `6` to view a list of all detected listening ports.

Show firewall

1. Sign in to the TanOS console of the Appliance with the secondary database as a user with the

©2026 Tanium Inc. All Rights Reserved

`tanadmin` role.

2. Enter `3-4` (Tanium Support > Run Network Diagnostics).
3. Enter `7` to view firewall details.

View network latency between Array members

VIEW CURRENT NETWORK LATENCY

1. Sign in to the TanOS console of the Appliance with the secondary database as a user with the `tanadmin` role.
2. Enter `3-4` (Tanium Support > Run Network Diagnostics).
3. Enter `8` to view the latency between the current Appliance and other Array members.

VIEW NETWORK LATENCY HISTORY

1. Sign in to the TanOS console of the Appliance with the secondary database as a user with the `tanadmin` role.
2. Enter `3-1-1-11` (Tanium Support Menu > Tanium Log Files > TanOS Appliance > Network Latency Log).
3. Enter `V` to view the current log file, or enter the line number of a previous log file if the relevant log entries have been rotated out of the current log file.

MEASURE THE DATA TRANSFER RATE BETWEEN AN ARRAY MANAGER AND AN ARRAY MEMBER

About this task

You can measure the data transfer rate between an Array Manager and another Appliance in the Array to help diagnose network issues between Appliances.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `1-M` (Tanium Installation > Appliance Array).
3. Enter the line number for the Appliance with which to measure the data transfer rate.

©2026 Tanium Inc. All Rights Reserved

4. Enter `N` to begin the measurement.

Examine Tanium and TanOS files

In rare cases, you or Tanium Support might need to examine Tanium and TanOS files written to the file system.

Important: Any unauthorized access of the Appliance operating system outside of the Tanium provided system UI (TanOS Menu system) voids the warranty of the Appliance.

Note: From read-only and read-write shells, you can access the /incoming directory at /xfer/incoming and the /outgoing directory at `/xfer/outgoing`.

Open read-only restricted shell

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-5` (Appliance Maintenance > Shell Keys).
3. Enter `O` to open a read-only shell.

```
           >>> Appliance Maintenance -> Launch Read Only Restricted Shell <<<

A read only restricted shell will be opened.

The shell will be forcibly closed after 10 minutes of inactivity.

Use /xfer/ subdirectories to move files on/off the appliance.

Are you sure you want to open RO shell? [Yes|No]: yes
(tanium@appliance-160.tam.local)/
(0 13:43:24 1) ->
```

4. Enter `exit` to close the shell.

©2026 Tanium Inc. All Rights Reserved

Request read-write restricted shell or full shell access

About this task

You must follow a special procedure to request read-write restrictive shell access or full shell access.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `B-5` (Appliance Maintenance > Shell Keys).
3. Enter `W` or `F`, and follow the prompts to generate a shell access request package. The package is written to the /outgoing folder.

```
All previous keys or requests have been deactivated.


The request file TanOS-key-request.tgz has been copied to tancopy outgoing.


Provide the request file to Tanium Support for verification and processing.
A response file will be returned; both files expire in seven days.
Once the response is loaded, shell access is granted for the duration it
specifies.



Press enter to continue
```

4. Use SFTP to copy the request file from the /outgoing directory to your local computer.
5. Email the file and TanOS version information to Tanium Support. For more information, see Support for Tanium Appliances on page 510.
   Tanium Support sends you a response file. For multiple Appliances, you might receive multiple files named with serial numbers.
6. Use SFTP to copy the response file to the /incoming directory. The file name must be in the format TanOS-key-response*.tgz or TanOS-key-serialNo*.tgz.
7. At the **Appliance Maintenance** > **Shell Keys** menu prompt, enter `1`, and then enter the number of a response file to validate the response.

```
          >>> Appliance Maintenance -> Feature Request -> Validate Response <<<
```

©2026 Tanium Inc. All Rights Reserved

```
  1: TanOS-key-serialNo-e121-1.tgz                                  890
  2: TanOS-key-serialNo-e121-2.tgz                                  896

  R: Return to previous menu  RR: Return to top

Please select: 1

Filename   = TanOS-key-serialNo-e121-1.tgz
User       = tanadmin
KeyID      = 1ea29a3fce9a7a1f4cf7270cb831d4c7fddaa75560e9154d6f5d971daa46241d
Start Time = Fri Aug 26 17:32:30 UTC 2022
Expiration = Fri Aug 26 21:09:17 UTC 2022

Signature verified, genuine response

Verifying DB matches
DB Match has been found
Request is still valid
Shell access timeout has been updated.
Return to the menu to open a shell session.

Press enter to continue
```

The **Shell Keys** menu now has additional options.

```
------------------------------------------------------


   >>> Appliance Maintenance -> Shell Keys <<<

     Current shell authorization type is Read Write Restricted Shell
     Current shell authorization expires in 1 hour 59 minutes

         1: Validate Response
         2: Remove shell access
         3: Launch Read Write Restricted Shell

         O: Open Read Only Restricted Shell
```

©2026 Tanium Inc. All Rights Reserved

```
        W: Request Read Write Restricted Shell Activation
        F: Request Full Shell Activation

        L: Shell Key Listing
        A: Revoke All Shell Keys

        R: Return to previous menu  RR: Return to top

-------------------------------------------------------
```

8. Enter `3` to launch the shell.

```
           >>> Appliance Maintenance -> Shell Access -> Launch Unrestricted Shell
<<<

Access is still valid. A unrestricted access shell will be opened

All connections (regardless of shell access) will be forcibly closed
after 60 minutes.

(tanadmin@appliance-ts1.tam.local)~
(0 20:02:08 1) ->
```

9. Enter `exit` to close the shell.
10. When you are finished troubleshooting, go to the **Shell Keys** menu and enter `2` to remove shell access.



Note: Shell keys expire seven days after they are created by Tanium Support.

Security of Tanium Appliances

Tanium prioritizes security in all of its products, and the Appliance is no exception. Appliances are built on a minimal OS and include only the packages and services needed to support the Tanium Platform. Appliances are configured with secure defaults, most of which cannot be reduced or disabled. A Security Technical Implementation Guide (STIG) is available from the U.S. Defense Information Systems Agency (DISA) that you can use to validate that all exposed configuration

©2026 Tanium Inc. All Rights Reserved

settings are in a secure state.

Tanium releases appliance updates on a regular basis to ensure that packages are up to date and contain the latest fixes. Software bills of material (SBOMs) are available for Tanium Appliance and the Tanium Platform.

Tanium performs regular penetration tests and secure code reviews as part of our overall product security strategy. An attestation document, verifying the penetration tests performed on Tanium Appliances by a third party, is available on request.

Security scanners and antivirus tools are not allowed on Tanium Appliances

The Tanium Appliance is a closed, hardened system intended to run only Tanium software and supporting services. To maintain performance, stability, and security of the Tanium Platform, installation and execution of third-party software is not allowed. Access to the underlying operating system is restricted.

If your compliance, security, or audit process requires information that is not available in the UI, APIs, or menu system, contact Tanium Support on page 510 and provide information about your requirements so that we can understand enhancements that you might need in the Tanium Appliance. Accessing the underlying operating system to run manual or automated scans or audits is not supported.

Support for Tanium Appliances

Contact Tanium Support

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

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

TanOS support lifecycle

Tanium routinely provides security patches, feature improvements and bug fix repairs to TanOS Appliances via in-place upgrades, incrementing TanOS versions forward. These upgrades are the only way to ensure your Tanium Appliance is patched against the latest security vulnerabilities and known software issues, since Tanium only releases versions forward and does not release patches against previously released versions. Tanium offers a fixed date lifecycle policy for Tanium Appliances.

©2026 Tanium Inc. All Rights Reserved

Physical hardware support terms are different and can be found in the Hardware Terms and Conditions.

In order to be able to provide support for Tanium Appliances, the TanOS version must not be older than 18 months from the date of release. Customers are required to upgrade TanOS versions that have reached end of support prior to Tanium working on a support case. Customers are strongly encouraged to stay on the latest release of TanOS to ensure they are using the most secure and functional Tanium Appliance product available.

For TanOS versions that are beyond the support lifecycle term, Tanium offers commercially reasonable support as follows:

- Commercially reasonable support incidents will be provided through Tanium Support. If the support incident requires escalation to development for further guidance or requires a non-security or a security update, then customers will be asked to upgrade to a fully supported TanOS version.
- Commercially reasonable support does not include an option to engage Tanium product development resources; technical workarounds may be limited or not possible.

Tanium customers are expected to use the provided upgrade paths on page 469 to maintain TanOS at a supported version on an ongoing basis. Previous TanOS release dates can be viewed in the release notes to determine if a given version is still within the Tanium support window.

Support information for physical Tanium Appliances

For detailed information about support for physical Tanium Appliances, review your hardware support terms with Tanium. To receive ongoing support services for physical Appliances, renew the annual support and maintenance services on each Appliance. Customers can renew support and maintenance services for a maximum of 6 years from the original purchase date. Tanium Support is always the primary contact for all Tanium Appliance concerns, including hardware issues.

All physical Tanium Appliances include self-encrypting hard drives that are FIPS 140-2 Validated. During initial setup, each Appliance creates a unique encryption key, stored on the RAID controller of the Appliance and not the individual drives. Only you the customer can access, export, or change this key. Because the data on the drive remains encrypted if a drive is removed from an Appliance, no other system can access the data on the drive, and the drive must be reformatted before reuse. Failed hard drives are typically returned to the Appliance hardware OEM. If you choose to keep a failed drive, additional charges might apply.

©2026 Tanium Inc. All Rights Reserved

Tanium Core Platform troubleshooting and logs in an Appliance deployment

Tanium Core Platform Servers generate several predefined logs that you can use to diagnose issues and unexpected behavior. You can also configure custom logs that copy specific content from the predefined logs based on filters.

Note:

For information about Tanium Client logs, see Tanium Client Management User Guide: Troubleshooting.

Contact Tanium Support on page 510 if you need help to analyze logs.

Tip: You can optionally forward entries from any available logs to a syslog destination. For more information, see Configure syslog forwarding on page 429.

Logging levels

The logging level determines how much detail Tanium Core Platform Servers and Tanium Clients record in logs, from 0 (no logging) to 99 (the highest level of detail). Select a level that provides just enough detail for you to understand what happened during an event. If you set the level too high, logs might contain so much detail that finding a particular event becomes difficult, especially if the logs roll over quickly and you must search across multiple files. Furthermore, when the number of log files reaches the maximum, the oldest files are deleted and you lose their record of events. For more information, see Log rollover on page 530.

The following logging levels are best practices for specific scenarios with all Tanium components except TDownloader:

©2026 Tanium Inc. All Rights Reserved

- 1: Normal (default) logging level. At this level, logs typically record error conditions (such as failed operations) but few informational messages (such as successful operations).
- 11: Best practice value for long-term troubleshooting. At this level, logs generally record enough information to help you understand the history of issues that occur. You can leave the level at 11 indefinitely without the logs being cluttered with less useful information or rolling over too quickly.
- 41: Best practice value for temporary troubleshooting. At this level, logs record details that are useful for diagnosing specific issues. When you finish troubleshooting the issue, the best practice is to revert to a lower logging level.
- 91 or higher: Most detailed logging level for advanced debugging. Because this level causes logs to roll over quickly and include details that are excessive for most scenarios, use it only for short periods and then revert to a lower logging level.



Note:

A value of **0** disables logging. As a best practice, do not disable logging.

In the case of TDownloader, which typically records fewer log messages than other components, it is a best practice to set the logging level at **41** for typical use.

The logging level that you set on a platform Server or Tanium Client applies to all the log types on that Server or Client, except for custom logs. You can also set the TDownloader log on page 528 to a different level than other logs on the same Tanium Server or Module Server. You have the following options for changing the logging level:

- Tanium Server and Tanium Module Server: Change the logging level through Tanium Console. For more information, see Configure Server logging levels.
- All Tanium Core Platform Servers: Configure the **LogVerbosityLevel** settings through the Console (see Reference: Deployment-related settings on page 632) or the TanOS menus on the Appliance (see Manage Tanium Core Platform settings).
- TDownloader: Configure the **LogVerbosityLevel** setting through the TanOS menus on the Appliance (see Manage the TDownloader configuration).

©2026 Tanium Inc. All Rights Reserved

- Custom logs: For more information about the logging level impact on custom logs, or to change the level, see CLI command executables and options for custom logs on page 532.
- Tanium Client: Configure the **LogVerbosityLevel** setting on the Tanium Client. For more information, see LogVerbosityLevel and Modify Client settings.

Troubleshooting workflow

Before you begin

As a best practice, configure the Tanium Platform Analyzer (TPAN) report with the following settings. The report can facilitate future troubleshooting regardless of whether your deployment currently has issues. For the specific steps, see Configuring Health Check.

- **Number of reports to keep on disk**: Enter `12`.
- **Metrics collection schedule**: Select **Every 15 minutes**.

  > **Note:** To see the current metrics, use your browser to navigate to https://<Tanium Server URL>/metrics and sign in as a user with the **Administrator** reserved role.

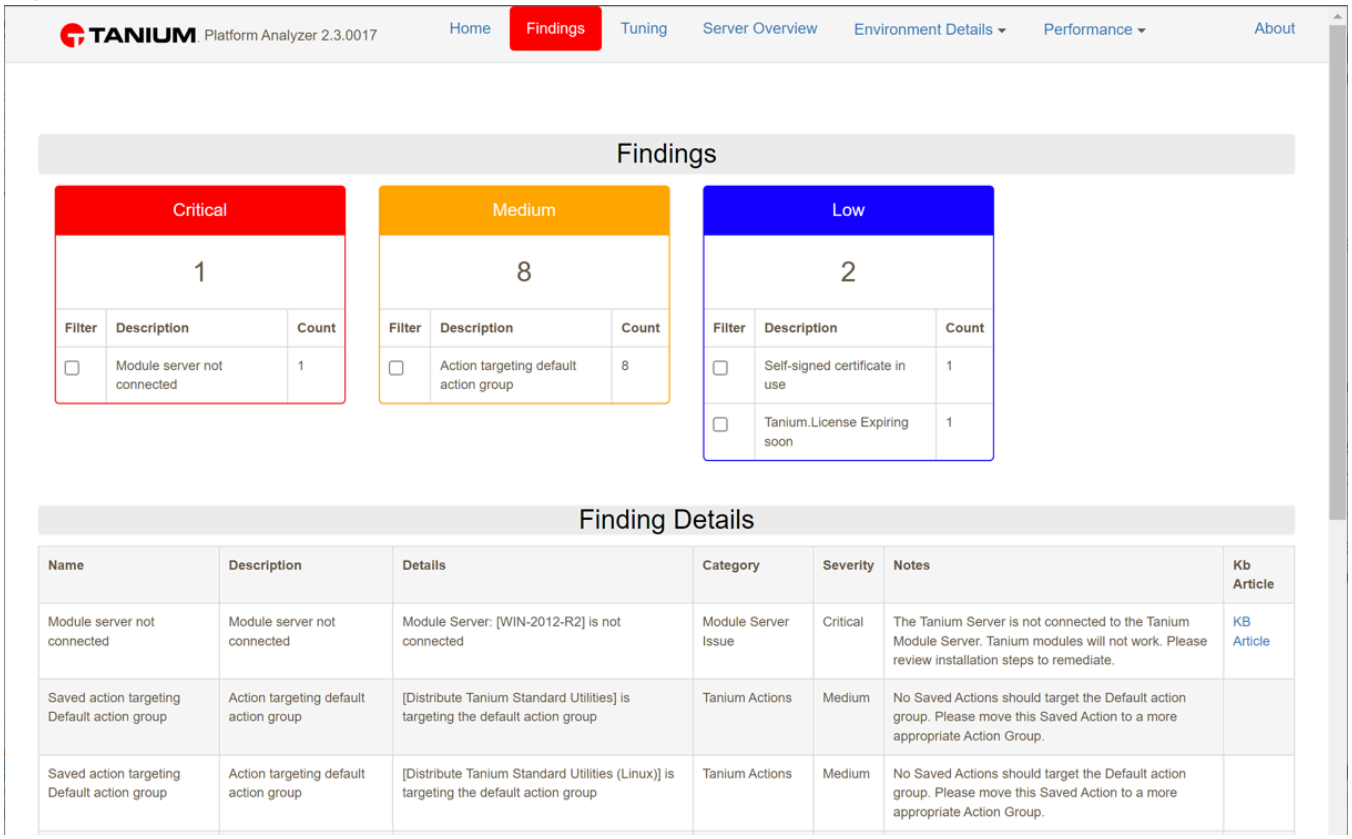
- **Enable Collection**: Select **Enabled**.
- **Set Collection Schedule**: Run the report at least once per week.
- **Log Level**: Select **Debug**.
- **VDI in use**: Select **Yes** if any Tanium Clients run on virtual desktop infrastructure (VDI) endpoints.
- **Active-Active 50/50?**: Select **Yes** if the Tanium Servers have an active-active configuration.

> **Note:** You can use the default values for other settings.

Tanium Support might ask you to send TPAN reports if you request troubleshooting assistance. You can manually download the reports and manually or automatically share them with Tanium. For more information, see Generating reports.

©2026 Tanium Inc. All Rights Reserved

Figure 53. TPAN report



Troubleshoot issues during Server deployment or solution operations

About this task

The following steps represent an overview of the tasks to perform if issues occur during the installation or upgrade of Tanium Core Platform Servers, or during the regular operation of Tanium solutions:

1. Perform troubleshooting tasks that are specific to the activity during which the issue occurred, as described in the following guides. First perform the tasks that do not require reviewing logs. If those initial tasks do not resolve the issue, perform the remaining tasks in this workflow to review reports and logs.

Activity	User Guide
Installing or upgrading the Tanium Appliance	Tanium Appliance Support and Troubleshooting on page 487
Deploying and managing Tanium Clients	Tanium Client Management User Guide: Troubleshooting

©2026 Tanium Inc. All Rights Reserved

Activity	User Guide
Performing regular operations in Tanium Console or Interact	Tanium Console User Guide: Troubleshooting
Performing regular operations in other Tanium modules or shared services	Tanium Console User Guide: Troubleshoot solution-specific issues

2. Run and review the TPAN report on page 529 for a comprehensive view of the issues, risks, and performance of your Tanium environment.
3. If Tanium Console displays error messages, review them in the Console local error log on page 519.
4. Review the Tanium Core Platform Server logs on page 525. These are the most comprehensive logs in terms of recording the broadest range of events.
5. Review any other log types based on the activity during which the issue occurred. For example, if users encounter role permission errors during Console operations, review the RBAC log. For more information, see Log and report types on page 516.
6. (Optional) If the logs do not have enough detail for you to understand an issue, raise the logging level to 41 (see Logging levels on page 512) and repeat the operation that triggered the issue. For example, import a solution if the previous attempt to import it failed.

   Best Practice: After you finish troubleshooting, set the logging level to 11 or lower.
7. If analyzing logs on your own is insufficient to diagnose the issue, create a support package to send to Tanium Support and then Contact Tanium Support on page 510 for additional help. The issue that you are troubleshooting determines which support package to send:
   - Issues with specific Tanium solutions: For more information, see Solution logs and support packages on page 526.
   - Issues with the Tanium Appliance: To run and export a on the status of the Tanium Appliance system, processes, and network interfaces, see Run Tanium Support Gatherer on page 500.

Log and report types

You can view the **Local Error Log** through Tanium Console. The requirements for viewing other log types vary by infrastructure:

©2026 Tanium Inc. All Rights Reserved

- Platform Server logs: You must sign in to the TanOS console as a user with the `tanadmin` role to access most logs. However, some logs require you to open a read-only (RO) restricted shell. For more information, see Open read-only restricted shell.
- Tanium Client logs: You require access to the endpoint hosts.

Tip: In addition to viewing action logs directly on individual endpoints, you can use the Console to view the action logs of up to 50 endpoints. For more information, see Investigate action-related issues.

The following Tanium Core Platform Server logs are available.



Note:

For log types that are available on Tanium Clients, see Troubleshooting.

For logs that apply specifically to TanOS and the Tanium Appliance, see Overview of Appliance logs, reports, and troubleshooting features on page 493.

- Action scheduler log on page 518
- Authentication log on page 519
- Console local error log on page 519
- Database upgrade log on page 519
- Download catalog cleaner log on page 519
- HTTP connection log on page 520
- LDAP log on page 520
- Module plugin history log on page 521
- Module-provided privileges log on page 521

©2026 Tanium Inc. All Rights Reserved

- Package cache cleaner log on page 522
- Package download log on page 522
- PKI log on page 523
- PKI TLS log on page 523
- PostgreSQL installation log on page 524
- RBAC log on page 524
- Server logs on page 525
- Solution logs and support packages on page 526
- Tanium Downloader log on page 528
- TPAN report on page 529
- Workbenches manager log on page 530

Note: Platform Servers do not generate certain log types unless errors occur or you raise the logging level beyond a specific threshold.

In the following sections, variables such as *<Tanium Server>* represent Server installation directories.

Tip: To find specific events in a log, you can open it in a text editor or use CLI commands to search for keywords. For examples of useful search strings, see Filter regex on page 532.

Action scheduler log

- Access: Open read-only restricted shell and view the log /opt/Tanium/TaniumServer/Logs/action-scheduler<#>.txt.
- Content: This log records events that relate to scheduled actions, such as why the Tanium

©2026 Tanium Inc. All Rights Reserved

Server did or did not deploy actions. For example, the log records Tanium Client connection failures. At logging levels between 1 (default) and 41, the Server generates the log only if errors occurred, such as actions failing to deploy. To record additional details for normal (successful) operations of scheduled actions, set the logging level to 91.

Authentication log

- Access: Sign in to the TanOS console as a user with the `tanadmin` role and enter the following sequence of menu options: `3` (**Tanium Support** menu), `1` (**Tanium Log Files** menu), `2` (**Tanium Server** menu), and `8` (**Auth0 Log**).
- Content: This log records user and service account access to Tanium Console or the Tanium API through all authentication methods, including SAML SSO, Lightweight Directory Access Protocol (LDAP), Active Directory (AD), Windows authentication, TanOS local authentication service, and API tokens.

Console local error log

- Access: Sign in to Tanium Console, click expand the **<user name>** drop-down menu in the Main menu (header), and select **Local Error Log**.
- Content: 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. The Console maintains a separate log for each browser that you use. For more information, see Work with the Console error log.

Database upgrade log

- Access: Sign in to the TanOS console as a user with the `tanadmin` role and enter the following sequence of menu options: `3` (**Tanium Support** menu), `1` (**Tanium Log Files** menu), `2` (**Tanium Server** menu), and `7` (**DB Upgrade Log**).
- Content: This log records actions that the Tanium Server installer performs on Tanium database schemas when you upgrade the Tanium Core Platform.

Download catalog cleaner log

©2026 Tanium Inc. All Rights Reserved

About this task

- Access: Open read-only restricted shell and view the log /opt/Tanium/TaniumServer/Logs/download-catalog-cleaner<#>.txt.
- Content: This log records events that relate to the periodic removal of files from the Tanium Server downloads directory. These are files that Tanium Clients request from Internet URLs upon executing certain content, such as action packages or sensors that require the files. The downloads cleaning process removes files only if they are associated with an allowed URL that has an expiration configured (default is seven days) and the files have expired. For more information about allowed URL settings, see Managing allowed URLs.

Tip: Review the following logs for similar issues:

- Package download log on page 522: This log records events that relate to the downloads queue for package files.
- Package cache cleaner log on page 522: This log records events that relate to the removal of package files from the Tanium Server chunk cache (a sub-directory of the downloads directory).
- Tanium Downloader log on page 528: This log records download events on the Tanium Server.

HTTP connection log

- Access: Open read-only restricted shell and view the log /opt/Tanium/TaniumServer/Logs/http-access<#>.txt.
- Content: This log records all HTTP requests that are sent to port 443 on the Tanium Server. For example, the log records registration attempts by Tanium Clients or the Zone Server and Tanium API access attempts. The log includes timing information for the requests, such as date-time and duration.

LDAP log

- Access: Open read-only restricted shell and view the log /opt/Tanium/TaniumServer/Logs/

©2026 Tanium Inc. All Rights Reserved

ldap<#>.txt.

- Content: This log records LDAP synchronization and authentication events for interactions between the Tanium Server and LDAP servers.

> **Note:** At any given time in an active-active deployment, only one Tanium Server performs synchronization and records synchronization events in its LDAP log.
>
> The Authentication log on page 519 can also help you troubleshoot LDAP authentication issues.

Module plugin history log

- Access: Open read-only restricted shell and view the log on each Server:
  - Tanium Server: *<Tanium Server>*/Logs/module-history<#>.txt
  - Module Server: *<Module Server>*/Logs/module-history<#>.txt
- Content: This log records all HTTP requests from the Tanium Server to any solution on the Module Server. For example, if a Tanium Console user tries to access the **Endpoints by Compliance Rule Failures** chart, the user browser sends the request to the Tanium Server, which forwards the request to the Module Server, which forwards the request to the Tanium™ Risk service. The log also records *plugin* executions. A plugin is an extension to a Tanium Core Platform component or solution. Plugin operations are usually transparent to users. However, Tanium Support might instruct you to review plugin details when troubleshooting unexpected behavior.

Module-provided privileges log

- Access: Open read-only restricted shell and view the log /opt/Tanium/TaniumServer/Logs/module-provided-privileges<#>.txt.
- Content: This log records events that relate to dependencies among Tanium solutions with respect to implicitly provided permissions. For example, if Tanium™ Deploy references a content set in Tanium™ Trends, an error occurs if you import Deploy but not Trends. As another example, the log records an error if you delete a content set that is associated with role permissions that are assigned to users. The Tanium Server generates this log only if the

©2026 Tanium Inc. All Rights Reserved

logging level is at least 40.

Package cache cleaner log

- Access: Open read-only restricted shell and view the log /opt/Tanium/TaniumServer/Logs/package-cleaner<#>.txt.
- Content: The Tanium Server uses cache storage for packages and associated files that actions reference. To conserve disk space, the Server periodically removes packages and files that are no longer referenced by an action that has an issue date-time in the future. Before removing the package and files, the Server waits until they have aged past the expiration interval (default 120 days) since the last issue date-time.

Tip: Review the following logs for similar issues:

- Download catalog cleaner log on page 519: This log records events that relate to the removal of files that the Tanium Server downloads to serve Tanium Client requests.
- Package download log on page 522: This log records events that relate to the downloads queue for package files.
- Tanium Downloader log on page 528: This log records all download events on the Tanium Server.

Package download log

- Access: Open read-only restricted shell and view the log /opt/Tanium/TaniumServer/Logs/package-download<#>.txt.
- Content: This log records events that relate to the download queue for package files that the Tanium Server downloads and deploys to Tanium Clients through actions. For example, the log might indicate why certain packages are not in the download queue. The Server generates this log only if the logging level is at least 20.

©2026 Tanium Inc. All Rights Reserved

Tip: Review the following logs for similar issues:

- Download catalog cleaner log on page 519: This log records events that relate to the removal of files that the Tanium Server downloads to serve Tanium Client requests.
- Package cache cleaner log on page 522: This log records events that relate to the removal of package files from the Tanium Server chunk cache.
- Tanium Downloader log on page 528: This log records all download events on the Tanium Server.

PKI log

- Access: Open read-only restricted shell and view the log on each Server:
  - Tanium Server: *<Tanium Server>*/Logs/pki<#>.txt
  - Module Server: *<Module Server>*/Logs/pki<#>.txt
  - Zone Server: *<Tanium Zone Server>*/Logs/pki<#>.txt
- Content: This log records events that relate to changes in the set of digital keys that Tanium Core Platform components use to prove their identity to each other. For example, the log records key generation and revocation events. The log also records events that relate to trust approvals and denials among Tanium Servers, Zone Server Hubs, and Zone Servers.

PKI TLS log

- Access: Open read-only restricted shell and view the log on each Server:
  - Tanium Server: *<Tanium Server>*/Logs/pki-tls<#>.txt
  - Module Server: *<Module Server>*/Logs/pki-tls<#>.txt
  - Zone Server: *<Tanium Zone Server>*/Logs/pki-tls<#>.txt
- Content: This log records events that relate to Transport Layer Security (TLS) connections

©2026 Tanium Inc. All Rights Reserved

among Tanium Core Platform Servers and Tanium Clients. For example, the log records TLS handshake failures that occur due to expired certificates.

PostgreSQL installation log

- Access: Sign in to the TanOS console as a user with the `tanadmin` role and enter the following sequence of menu options: `3` (**Tanium Support** menu), `3` (**Database Operations** menu), `1` (**Display Postgre log file**), and `2` (**postgres.log**).
- Content: This log records events that relate to the PostgreSQL database that the Module Server installer creates locally as the storage system for Tanium solutions.

RBAC log

- Access: Sign in to the TanOS console as a user with the `tanadmin` role and enter the following sequence of menu options: `3` (**Tanium Support** menu), `1` (**Tanium Log Files** menu), `2` (**Tanium Server** menu), and `3` (**Tanium Server RBAC Log**).
- Content: This log records events that relate to Tanium role-based access control (RBAC). If users attempt operations that their assigned roles do not allow, the log indicates which permissions are missing. These operations include viewing, editing, reassigning, creating, or deleting configuration objects that are associated with permissions. Some examples are viewing persona configurations, editing sensors, reassigning computer groups for a user, moving filter groups to other content sets, or deleting platform settings.

©2026 Tanium Inc. All Rights Reserved

Tip:

Tanium Console displays an alert when you attempt an operation that fails due to missing permissions. You can then view the Console error log to find the reference number (`Ref# <hash>`) for that error. To see more details for the error, use the same reference number to find the corresponding entry in the RBAC log. The following entry is an example from the Console error log:

```
ERROR: 400 Bad Request RBAC Exception (Ref# 1f14e8215610cf72):
RBACInsufficientPrivilege
```

The corresponding entry in the RBAC log might resemble the following record:

```
2020-10-02T19:22:24.076Z[00:001652:] RBAC Exception (Ref# 1f14e8215610cf72) thrown
during SOAP request processing: RBACInsufficientPrivilege
- Operation: add question
- Privileges: Any of these privileges ('administrator', 'write sensor', 'write
action', 'write action for saved question', 'approve action', 'content
administrator', 'write package', 'define question')
```

For more information, see Work with the Console error log.

Server logs

- Access:
  - Tanium Server: Sign in to the TanOS console as a user with the `tanadmin` role and enter the following sequence of menu options: `3` (**Tanium Support** menu), `1` (**Tanium Log Files** menu), `2` (**Tanium Server** menu), and `1` (**Tanium Server Log**).
  - Module Server: Sign in to the TanOS console as a user with the `tanadmin` role and enter the following sequence of menu options: `3` (**Tanium Support** menu), `1` (**Tanium Log Files** menu), and `3` (**Tanium Module Server**).
  - Zone Server: Sign in to the TanOS console as a user with the `tanadmin` role and enter the following sequence of menu options: `3` (**Tanium Support** menu), `1`

©2026 Tanium Inc. All Rights Reserved

(**Tanium Log Files** menu), and `4` (**Tanium Zone Server**).

- Content: Each Tanium Core Platform Server has a main log that is the most comprehensive in terms of which events it records. The Server log includes all the events that other log types do not record. For example, the Tanium Server log records Tanium database access errors that result from incorrect credentials or permissions.

Solution logs and support packages

- Log access: Sign in to the TanOS console as a user with the `tanadmin` role and enter the following sequence of menu options: `3` (**Tanium Support** menu), `2` (**Module Log files Access** menu), and `<solution>`.
- Log content: Each Tanium solution generates a log that records events that relate to the activities of that solution. Solutions include modules (such as Comply), shared services (such as Client Management), and platform services (such as Tanium Data Service).
- Support packages: Tanium solutions enable you to create packages that collect all the logs and files that are relevant for troubleshooting. Tanium Support might request that you provide these packages to help you troubleshoot. See:
    - Asset
    - Automate
    - Benchmark
    - Certificate Manager
    - Client Management
    - Comply
    - Connect
    - Console
    - Criticality
    - Deploy

©2026 Tanium Inc. All Rights Reserved

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

©2026 Tanium Inc. All Rights Reserved

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

TDownloader log

- Access: Sign in to the TanOS console as a user with the `tanadmin` role and enter the following sequence of menu options for the corresponding Server:
  - Tanium Server: `3` (**Tanium Support** menu), `1` (**Tanium Log Files** menu), `2` (**Tanium Server** menu), and `2` (**Tanium Server TDL Log**)
  - Module Server: `3` (**Tanium Support** menu), `1` (**Tanium Log Files** menu), `3` (**Tanium Module Server** menu), and `2` (**Tanium Module Server TDL Log**)
- Content: This log records a history of the actions that the TDownloader service performs when it downloads files from Tanium and other Internet locations. If your deployment includes a proxy server, the log records connection status events on the proxy. The log might help you troubleshoot when importing or updating Tanium modules, shared services, content packs, and content configurations (such as package definitions).

Best Practice: The TDownloader log has its own logging level setting that you can configure independently of other logs on the same Server. The default logging level is **1**. However, because TDownloader typically records fewer log messages than other components, you can set it to **41** indefinitely for improved troubleshooting without the TDownloader log becoming cluttered with less useful information or rolling over too quickly. Configure the **LogVerbosityLevel** setting for TDownloader through the CLI (see Reference: Command-line interface on page 587) or the TanOS menus on the Appliance (see Manage the TDownloader configuration).

©2026 Tanium Inc. All Rights Reserved

Tip:

If the TDownloader log indicates certificate errors, you might resolve the errors by updating the certificates that the service uses for downloads authentication. For more information, see Managing remote authentication.

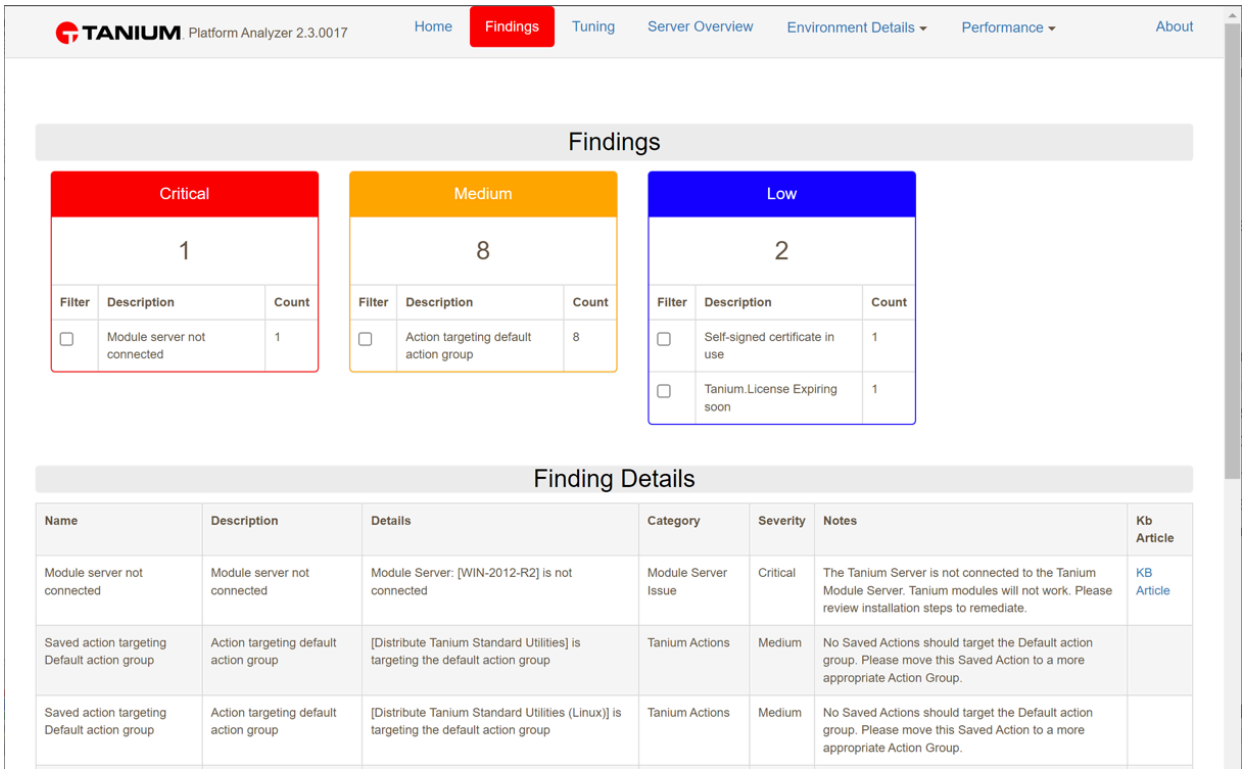
Review the following logs for similar issues:

- Download catalog cleaner log on page 519: This log records events that relate to the removal of files that the Tanium Server downloads to serve Tanium Client requests.
- Package cache cleaner log on page 522: This log records events that relate to the removal of package files from the Tanium Server chunk cache.
- Package download log on page 522: This log records events that relate to the downloads queue for package files.

TPAN report

- Access: Generate TPAN reports through Tanium Health Check. For more information, see Generating reports.
- Content: Provides a comprehensive view of the issues, risks, and performance of your Tanium environment. You can download reports locally to share with Tanium Support. Regularly collecting and sharing these reports can help Tanium provide you with the best support.

©2026 Tanium Inc. All Rights Reserved



Workbenches manager log

- Access: Sign in to the TanOS console as a user with the `tanadmin` role and enter the following sequence of menu options: `3` (**Tanium Support** menu), `1` (**Tanium Log Files** menu), `2` (**Tanium Server** menu), and `5` (**Tanium Server Workbenches**).
- Content: This log records events that relate to the installation and uninstallation of workbenches for Tanium solutions (modules and shared services). A *workbench* is the user interface that you use to perform solution operations.

Log rollover

To clear space for new logs, Tanium Core Platform Servers roll over and compress existing logs when they exceed the maximum log size (10 MB) and maximum number of logs. The maximum number of log files varies by log type and format. By default, custom log types have a maximum of 10 plain text logs and 10 ZIP logs.

©2026 Tanium Inc. All Rights Reserved

Number of log files

Log File Name	Plain Text	ZIP
action-scheduler<#>.txt	10	10
auth<#>.txt	10	10
database-upgrade<#>.txt	10	10
download-catalog-cleaner<#>.txt	10	10
http-access<#>.txt	2	3
Install_postgres.log	1	0
ldap<#>.txt	10	10
log<#>.txt (main Server log for each Tanium Core Platform Server)	10	10
log<#>.txt (TDownloader log)	10	0
module-history<#>.txt	2	3
module-provided-privileges<#>.txt	10	10
package-cleaner<#>.txt	10	10
package-download<#>.txt	10	10
pki<#>.txt	10	10
pki-tls<#>.txt	10	10
rbac<#>.txt	10	10
tanium-data.log<#>.txt	10	10
workbenches_manager.log	1	0

The following sections describe the rollover process. The variable <log_type#>.txt represents a log file name (such as log0.txt):

©2026 Tanium Inc. All Rights Reserved

Rollover for plain text logs

When the first log file <log_type>0.txt reaches 10 MB in size, it is renamed <log_type>1.txt and a new <log_type>0.txt is created. When <log_type>0.txt again reaches 10 MB, <log_type>1.txt is renamed <log_type>2.txt, <log_type>0.txt is again renamed <log_type>1.txt, and <log_type>0.txt is again recreated. The process of rolling logs whenever <log_type>0.txt reaches 10 MB continues until the maximum number of plain-text logs exist. For example, each Tanium Core Platform Server log has a maximum of 10 plain-text logs: log0.txt to log9.txt.

Rollover for ZIP logs

After recording the maximum number of plain-text logs, the oldest log is compressed. For example, log9.txt is saved as log10.zip. When <log_type>0.txt again reaches 10 MB, the file name of the first ZIP log is incremented (for example, log10.zip becomes log11.zip and the oldest plain-text log is again compressed and replaces the first ZIP log. The ZIP file rollover process continues until the maximum number of ZIP files exist. For example, each Tanium Core Platform Server log has a maximum of 10 ZIP files: log10.zip to log19.zip. When <log_type>0.txt reaches 10 MB again after that, the first ZIP log is created again (such as log10.zip) but the oldest ZIP log (such as log19.zip) is not renamed and is effectively dropped because the second oldest ZIP file replaces it (for example, log18.zip becomes the new log19.zip).

Create a custom log for Tanium Core Platform Servers

About this task

If you want to troubleshoot only specific information in predefined Tanium logs, you can configure a Tanium Core Platform Server to filter the logs based on a regular expression and to copy the matching content to a custom log. Custom logs are especially useful if you set a high logging level for the predefined logs such that they roll over too quickly and record too much information for you to easily find specific issues. You can create as many custom logs as necessary and base each one on a different filter. After you configure a new log type, the Tanium Core Platform Server creates a custom log file upon recording an event in a predefined log that matches the regular expression. Thereafter, whenever the predefined logs record additional events that match the filter, the server copies those records to the custom log.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Log filtering can consume significant resources on a server, especially if you set a high logging level. Therefore, the best practice is to remove custom logs after you finish a troubleshooting session. For more information, see the logging level setting in the CLI command executables and options for custom logs on page 532 table.

Tip: You can also configure custom logs on a Tanium Client. For more information, see Create a custom log for a Tanium Client.

Perform the following procedure with the options listed in the CLI command executables and options for custom logs on page 532 table, using the TanOS console on the applicable Server.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2` to go to the **Tanium Operations** menu.

```
>>> Tanium Operations Menu <<<

1: Tanium Service Control
2: Tanium Configuration Settings
4: Install Custom SOAP Cert
5: Manage Custom Signing Keys
7: Download SOAP Certificate
9: Import CAC Certificate

A: Configure Module Server(s)
B: Configure Tanium Cluster
C: Manage Content
M: Module Operations

I: Import public key to Tanium Zone Server

X: Advanced Operations

R: Return to previous menu  RR: Return to top
```

3. Enter `2` to go to the **Configuration Settings** menu.

©2026 Tanium Inc. All Rights Reserved

```
>>> Tanium Operations -> Configuration Settings <<<

Note: Some settings may require a service restart to take effect.

1: Edit Tanium Server Settings
2: Edit Tanium Server TDL Settings
3: Add Tanium Server TDL Auth User
4: Add Tanium Server TDL Auth Cert

5: Edit Tanium Module Server Settings
6: Edit Tanium Module Server TDL Settings
7: Add Tanium Module Server TDL Auth User
8: Add Tanium Module Server TDL Auth Cert

9: Edit Tanium Zone Server Settings
11: Edit isolated subnets list
12: Edit separated subnets list

13: Control Root CA Certs

R: Return to previous menu  RR: Return to top
```

4. Enter `1` to go to the **Tanium Server Config Settings** menu.

```
>>> Tanium Operations -> Configuration Settings -> Edit <<<
Editing: Tanium Server Config Settings

1: AddressMask 16777215
2: AllowedHubs 127.0.0.1
3: AuthPluginTimeoutSeconds 60
4: AuthenticationPlugin InternalPython:tanium_pam4/pam_workflow.py
5: ClientCertificateAuth /opt/Tanium/TaniumServer/cac.pem
6: ClientCertificateAuthField X509v3 Subject Alternative Name
7: ClientCertificateAuthRegex .*:\s(\d+)@.*
8: ConsoleSettingsJSON /opt/Tanium/TaniumServer/http/config/console.json
9: EnforceAllowedHubs 1
10 ForceSOAPSSLClientCert 1
```

©2026 Tanium Inc. All Rights Reserved

```
11: LogPath /opt/Tanium/TaniumServer/Logs
12: LogVerbosityLevel 1
13: ModuleServer 10.10.10.103,appliance-tms1.tam.local:17477
14: ModuleServerPort 17477
15: ReportingTLSCertPath /opt/Tanium/TaniumServer/reporting.crt
16: ReportingTLSKeyPath /opt/Tanium/TaniumServer/reporting.pvk
17: SQLConnectionString postgres:10.70.164.248@user=postgres dbname=tanium
sslmode=require sslcert=/opt/Tanium/.postgresql/postgresql.crt sslkey=
/opt/Tanium/.postgresql/postgresql.key sslcompression=1
18: ServerPort 17472
19: ServerSOAPPort 8443
20: TrustedCertPath /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
21: TrustedHostList host1.example.com,192.168.0.1
22: Version 7.9.3.1234

A: Add a line
R: Return to previous menu  RR: Return to top
```

5. For each log setting (`LogVerbosityLevel`, `LogPrefix`, and `FilterRegex`), enter `A` to add the setting and then enter its value. The Table 15. CLI options for custom logs on page 536 table describes the settings. For the <log subject>, specify any text string to identify the purpose of the log.

   ```
   Logs.<log subject>.LogVerbosityLevel

   Logs.<log subject>.LogPrefix

   Logs.<log subject>.FilterRegex
   ```

   For example, if the log is for troubleshooting common access card (CAC) authentication, you might specify the following values:

   ```
   Logs.CAC.LogVerbosityLevel = 41

   Logs.CAC.LogPrefix = CACAuthLog

   Logs.CAC.FilterRegex = .*Client Certificate auth.*
   ```

6. To review the log after the Appliance generates messages that match the filter:
   a. Open a read-only (RO) restricted shell. For more information, see Open read-only

©2026 Tanium Inc. All Rights Reserved

restricted shell on page 506.

b. Go to the Logs directory:

```
cd /opt/Tanium/TaniumServer/Logs
```

c. List the directory contents:

```
ls -la
```

The following is an example of the output, including the custom log `CACAuthLog`:

```
total 1264
drwxr-x---. 2 tanium tanium 4096 Nov 16 21:24 .
drwxr-x---. 20 tanium tanium 4096 Nov 16 22:15 ..
-rw-r-----. 1 tanium tanium 685 Nov 16 21:28 CACAuthLog0.txt
-rw-r-----. 1 tanium tanium 2805 Oct 26 19:39 auth0.txt
-rw-r-----. 1 tanium tanium 322930 Oct 26 18:41 database-upgrade0.txt
-rw-r-----. 1 tanium tanium 857760 Nov 16 19:36 http-access0.txt
-rw-r-----. 1 tanium tanium 31873 Nov 16 20:01 log0.txt
-rw-r-----. 1 tanium tanium 27082 Nov 16 19:36 module-history0.txt
-rw-r-----. 1 tanium tanium 17223 Nov 16 19:33 package-cleaner0.txt
-rw-r-----. 1 tanium tanium 3300 Oct 26 18:46 pki0.txt
```

d. Display the custom log contents using standard UNIX commands such as `more`, `cat`, or `tail`:

```
more CACAuthLog0.txt
```

e. When you finish viewing the log contents, enter `exit` to close the shell.

Next steps

CLI options for custom logs

Executable/ Option	Description
Log prefix	The log file prefix. The server automatically appends a number to the prefix and adds the suffix (.txt) upon generating the log. For example, if you enter `CertificateAuthentication` as the prefix for a custom server log, the first file that the Client generates for that log type is CertificateAuthentication0.txt .
Filter regex	The regular expression to use for filtering the predefined logs. The Server or Client copies log entries that match

©2026 Tanium Inc. All Rights Reserved

Executable/ Option	Description
	the filter to the custom log. **Note:** The filter applies only to log messages, not to thread names, thread IDs, or timestamps. The following are examples of useful filter expressions for the Tanium Server Install.txt log: • `.*Begin MiniDumper.*` records messages about application crashes. • `.*Failing to sync sensors.*` identifies sensor synchronization failures. • `.*msg=NoMaxAgeFound.*` records instances where the Tanium Server issues a question that uses deleted sensors. • `.*Client Certificate auth.*` records authentication messages relating to Tanium Client certificates. This is useful for troubleshooting smart card (common access card) authentication issues. For more information, see Troubleshoot smart card authentication. The following are examples of useful filter expressions for Tanium Server or Zone Server Install.txt logs: • `.*Begin registration.*` identifies Tanium Clients that are trying to register. • `.*Registration complete.*` identifies Clients that successfully registered.
Logging level	The logging level of the custom log. For more information, see Logging levels on page 512. **Important:** Higher logging levels consume more resources on the server. If different custom log types have different levels, the server generates all log types at the highest level that is set for any custom log type. This ensures that filter matching applies to all log messages at the highest configured level. However, in this case, each log file still contains only the level of detail that corresponds to the level you set for its log type. For example, you might set the logging level to 1 for predefined logs on the Tanium Server and set the level to 91 for a custom log. In this case, the server generates log messages at level 91 for all log types and the custom log contains messages at level 91, but the predefined logs contain messages only at level 1.

©2026 Tanium Inc. All Rights Reserved

Reference: TanOS health check results

The TanOS health check provides an overview of the health of the TanOS environment on a Tanium Appliance. After initial configuration, TanOS automatically runs a health check every 15 minutes. The results for the latest health check are stored in the health.log file in the /outgoing directory. For information about manually running a health check, see Run the Health Check on page 488.

Best Practice:

The health check sends alerts if they are enabled. As a best practice:

- Enable alerts.
- Configure a severity level for alerts that matches the checks for which you want to receive alerts. For information about specific alerts, including severity levels, see Reference: TanOS health check results on page 538.
- Configure an SMTP destination to send email alerts.
- (Optional) Configure a syslog destination.

For information about configuring alerts, see Configure syslog alerts on page 436.

Is EULA accepted

TanOS EULA acceptance health check results

Check	Description	Severity	Condition	Remediation
`Is EULA Accepted`	Checks whether the end-user license agreement (EULA) has been accepted. Reports the user who accepted the EULA and the	WARN	EULA not accepted	From the main menu, enter `Q` to view the EULA. Follow the prompts to review and accept the EULA.

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
	time at which it was accepted.			

Operating System health

TanOS operating system health check results

Check	Description	Severity	Condition	Remediation
`CPU`	Checks for excessive processor usage across all cores. The reported value is snapshot of a single point in time. **Best Practice:** Use SNMP polling for continuous monitoring of processor utilization. For more information, see Configuring SNMP on page 439 .	WARN	>90% average CPU usage across all processors	• Review the CPU usage of running processes to determine whether certain processes might be consuming excessive processor time. Contact Tanium Support on page 510 for assistance in troubleshooting such processes. **Tip:** You can use the htop command on page 461 to monitor processes and resource usage. • After determining the cause of the issue, you can, as a temporary measure, restart Tanium services on page 313 or reboot the Appliance on page 444. If possible, determine the cause before restarting to avoid delaying a diagnosis. • For a virtual Tanium Appliance or cloud-based Tanium Appliance, increase system resources.
`Memory`	Checks for low available RAM. Because of the way Linux	ERROR	No available memory	• If the Swap check on page 539 is `2` or lower, low available RAM is

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
	manages memory, it is common for available RAM to be below 10% in production. However, if the RAM is full and the Appliance uses a significant amount of swap space, performance might degrade.	WARN	<10% available memory	usually not a cause for concern. • If an ERROR condition is frequent for the Memory check, or if the Swap check on page 539 is 3 or higher, review the following remediation recommendations: • Review the memory usage of running processes to determine whether certain processes might be using excessive memory. Contact Tanium Support on page 510 for assistance in troubleshooting such processes. **Tip:** You can use the htop command on page 461 to monitor processes and resource usage. • After determining the cause of the issue, you can, as a temporary measure, restart Tanium services on page 313 or reboot the Appliance on page 444. If possible, determine the cause before restarting to avoid delaying a diagnosis. • For a virtual Tanium Appliance or cloud-based Tanium Appliance, increase available RAM.

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
`Swap`	Indicates the concurrent I/O pages swapped per second.	INFO	N/A	
`Partition <partition name>`	Checks the used space on disk partitions **Important:** When disk usage exceeds 95% on a critical partition (/ , /var , /log , or /opt), TanOS stops all Tanium services to preserve TanOS functionality.	ERROR	>95% disk usage on a critical partition (/ , /var , /log , or /opt)	• If any partition reports a WARN condition, determine what is using the space and reduce the size before filling up the partition. If necessary, contact Tanium Support on page 510 for assistance. • For a virtual Tanium Appliance or cloud-based Tanium Appliance, increase available storage for the virtual machine or cloud instance, and then increase storage on page 445 on the Appliance. • For a physical Tanium Appliance, contact Tanium Support on page 510 for assistance.
		WARN	>75% disk usage on any partition	
`Boot Check`	Checks the boot type configured for the Appliance. TanOS must be configured for EFI boot on a physical Tanium Appliance . On a virtual Tanium Appliance or cloud-based Tanium Appliance , both EFI and BIOS boot are allowed.	INFO	BIOS boot with a physical Appliance	Contact Tanium Support on page 510 for assistance.
`GRUB key`	Checks whether the GRUB key in use on the Appliance is valid.	WARN	Invalid GRUB key	Generate a new GRUB key. For more information, see Change the GRUB key password on page 377 .
`Active partition`	Reports which partition set TanOS is using. This can be useful information when	N/A	N/A	N/A

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
	alternate partitions on page 392 are in use for a physical Tanium Appliance or virtual Tanium Appliance. This check is informational and always reports a "pass" condition.			
`Upgrade`	Checks whether a TanOS upgrade has failed	ERROR	Upgrade failed	Reattempt the TanOS upgrade on page 469. If the upgrade fails repeatedly, collect a Tanium Support Gatherer (TSG) bundle on page 500 and contact Tanium Support on page 510.

Hardware health

TanOS hardware health check results

Check	Description	Severity	Condition	Remediation
`hardware type`	Physical Tanium Appliance: Reports the hardware Appliance code Virtual Tanium Appliance or cloud-based Tanium Appliance: Reports the virtual Appliance code This check is informational and always reports a "pass" condition.	N/A	N/A	N/A
`RAID controller <#> security key`	Physical Tanium Appliance only: Checks whether the RAID controller security key is set,	WARN	RAID controller security key is not properly set	Contact Tanium Support on page 510 for assistance.

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
	which is necessary for proper encryption of the RAID array.			
`disk encryption`	Physical Tanium Appliance only: Checks the status of disk encryption in the RAID array.	WARN	Disk encryption not configured correctly	Contact Tanium Support on page 510 for assistance
`hardware SEL`	Physical Tanium Appliance only: Checks the usage of the hardware system event log	ERROR	>90% of log space used	Sign in to the iDRAC virtual console on page 425 as the `tanremote` user, and clear the hardware system event log.

User health

TanOS user health check results

Check	Description	Severity	Condition	Remediation
`user <username>`	Checks that each TanOS user has the correct level of privileges for the role assigned to that user	ERROR	User privileges do not match the assigned role	Contact Tanium Support on page 510 for assistance.
`admin users`	Checks that at least two users have been given the `tanadmin` role	INFO	Only one user has the `tanadmin` role assigned	Create another TanOS user on page 233 with the `tanadmin` role.
`system user policies`	Checks that the security policies for each TanOS user match the user security policies that are configured for the Appliance	ERROR	A security policy for a user does not match the policy configured for the Appliance	Reapply the security policy on page 361 that is not properly applied.

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
`password expiration`	Checks the password expiration date for each local TanOS user that can authenticate with a password. Reports a warning for a password that expires within 14 days or that must be changed at the next sign-in.	ERROR	A user password has expired	Change the password for the affected user. To change your own password, see Change the password for the current TanOS user on page 225 . To reset the password for another user, see Reset a user password or enable password access on page 237 .
`MFA Policy`	Checks that more than one authentication method is globally enabled for all users	WARN	Only one authentication method is configured globally	Require at least two of the available authentication methods on page 242 : key authentication, password authentication, or multifactor (TOTP) authentication.

Network health

TanOS network health check results

Check	Description	Severity	Condition	Remediation
`own hostname resolution`	Checks that the Appliance can resolve its own host name	INFO	DNS timeout or an unknown error occurred	Check that the DNS configuration on page 337 is correct. Work with your network administrator to resolve DNS or other network issues, and perform another health check.
		ERROR	Own host name cannot be resolved	Check that the host name and DNS configuration on page 337 is correct. If the resolution relies on DNS, work with your network administrator to resolve DNS issues.
`mount <module share>`	Checks whether a configured module share is disconnected	ERROR	Module share is configured but not mounted	List and test module file share mounts. If necessary delete the mount and re-create it. For more information, see

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
				Configure solution module file share mounts on page 333 .
`Connection tracking`	Checks the ratio of network connections to the maximum number allowed for the Appliance	INFO	>70% of available network connections in use	Contact Tanium Support on page 510 to assist in determining the cause of the high number of connections.

Service health

TanOS service health check results

Check	Description	Severity	Condition	Remediation
`chronyd service`	Checks that the time synchronization service is running and that the time is synchronized	ERROR	Service is not running or status cannot be determined	Check the status of the chronyd service on page 446 , and attempt to start or restart it. If the service fails to start, review Status Details for more information about the failure.
		WARN	Time not synchronized	• Make sure that a valid time synchronization source is provided for the NTP configuration on page 351. • Restart the chronyd service on page 446.
`host time`	Virtual Tanium Appliance only: Checks the time difference between the host and virtual Appliance	WARN	Time difference >5s	• Make sure that a valid time synchronization source is provided for the NTP configuration on page 351. • Make sure a valid time synchronization source is provided

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
				for the NTP configuration on your hypervisor host. • Restart the chronyd service on page 446.
`rsyslog service`	Checks that the rsyslog service is running	ERROR	Service is not running or status cannot be determined	Reboot the Appliance on page 444 or reconfigure syslog forwarding on page 429 to restart the rsyslog service.
`syslog delivery`	Checks whether the rsyslog service is successfully forwarding syslog messages to the configured destination **Note:** This check can occasionally produce a false positive WARN condition due to a temporary increase in the outgoing message queue. Typically, remediation is necessary only if you observe a repeated or persistent WARN condition.	WARN	Messages have not been delivered (indicates number of failed messages)	• Make sure that syslog forwarding on page 429 is properly configured and that the remote syslog server is reachable. • Reboot the Appliance on page 444 or reconfigure syslog forwarding on page 429 to restart the rsyslog service.
`syslog forwarding TLS`	Checks whether certificate enforcement is properly configured for syslog forwarding if TLS is enabled for syslog forwarding	WARN	A misconfiguration exists that is preventing certificate enforcement for syslog forwarding with TLS enabled	Reconfigure syslog forwarding on page 429 to resolve the misconfiguration.
`iptables service`	Checks whether the iptables service is running	ERROR	Service is not running or status cannot be	Reboot the Appliance on page 444 . If the problem persists, contact Tanium Support on page 510 for assistance.

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
			determined	
`ip6tables service`	Checks whether the ip6tables service is running	ERROR	Service is not running or status cannot be determined	Reboot the Appliance on page 444 . If the problem persists, contact Tanium Support on page 510 for assistance.
`sshd service`	Checks whether the sshd service is running	ERROR	Service is not running or status cannot be determined	Check the status of the sshd service on page 446 , and attempt to start or restart it. If the service fails to start, review Status Details for more information about the failure.
`ipsec`	Checks whether the ipsec service is running **Important:** The ipsec service is required for an active-activeTanium Server or active passive Tanium Module Server configuration.	ERROR	Service is not running or status cannot be determined	Use the Tanium Service Control menu on page 313 to check the status of the ipsec service , and attempt to start or restart it. If the service fails to start, review Status Details for more information about the failure.
`sssd service`	Checks whether the sssd service is running, and whether debug logging is enabled **Note:** Running the sssd service with debug logging enabled could cause performance issues.	ERROR	Service is not running or status cannot be determined	From the main menu, enter `C - A - T - S` to check the status of the sssd service , and attempt to start or restart it. If the service fails to start, review Status Details for more information about the failure. For configuration information, see Configure LDAP authentication for TanOS system users on page 252 .
		INFO	Debug logging enabled	Contact Tanium Support on page 510 for assistance.
`local auth service`	Checks whether the slapd service is running. The slapd service provides the local	ERROR	Service is not running or status cannot be	Use the Tanium Service Control menu on page 313 to check the status of the slapd service , and attempt to start or

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
	authentication service on page 294 for Tanium Console users. Additionally, it always manages the default user `tanium`, even if you use LDAP authentication and do not otherwise use the local authentication service in TanOS.		determined	restart it. If the service fails to start, review Status Details for more information about the failure.
`Local LDAP config`	Performs internal checks to evaluate the health of the local authentication service on page 294.	ERROR	Internal checks failed	
`Remote LDAP config`	Performs internal checks to evaluate the health of the local authentication service on page 294 on the remote Appliance in a clustered environment	ERROR	Internal checks failed	• From the main menu, enter `C-L-C` for more details about the LDAP content mismatch. • From the main menu, enter `1-M-E` to restart replication, which resolves most LDAP configuration errors.
`LDAP contents`	Checks that the local LDAP contents for the local authentication service on page 294 match the remote LDAP contents in a clustered environment	ERROR	Local contents do not match remote contents	

Application health

TanOS application health check results

Check	Description	Severity	Condition	Remediation
`TS`	Tanium Server only: Checks whether the taniumserver	ERROR	Service is not running or	Use the Tanium Service Control menu on page 313 to check the

Check	Description	Severity	Condition	Remediation
	service is running		status cannot be determined	status of the taniumserver service , and attempt to start or restart it. If the service fails to start, review Status Details for more information about the failure.
`TS database connection`	Tanium Server only: Checks the Tanium Server connection to the database	ERROR	The Tanium Server cannot connect to the database	Contact Tanium Support on page 510 for assistance.
`TS database`	Tanium Server only: Checks the size of the Tanium Server database	INFO	Database size >50GB	Contact Tanium Support on page 510 for assistance.
`TS database pg_wal`	Tanium Server only: Checks the size of the PostgreSQL write-ahead log (WAL) directory	ERROR	pg_wal directory missing	Contact Tanium Support on page 510 for assistance.
		ERROR	pg_wal directory >50% of partition size	
`LDAP Sync`	Tanium Server only: Checks LDAPS or StartTLS certificate configuration	WARN	LDAPS or StartTLS certificate validation is disabled	Check the LDAP configuration for the Tanium Server.
		WARN	In a clustered environment, the LDAPS or StartTLS certificate configuration	

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
			does not match the configuration on a peer	
		INFO	LDAPS or StartTLS certificates exist but are not in use	
`TMS`	Primary Tanium Module Server only: Checks whether the taniummoduleserver service is running	ERROR	Service is not running or status cannot be determined	Use the Tanium Service Control menu on page 313 to check the status of the taniummoduleserver service , and attempt to start or restart it. If the service fails to start, review Status Details for more information about the failure.
`Secondary TMS`	Secondary Tanium Module Server only: Checks whether the taniummoduleserver service is running. The service should be stopped on a secondary Module Server.	ERROR	Service is running or status cannot be determined	Use the Tanium Service Control menu on page 313 to check the status of the taniummoduleserver service and stop it.
`tanium-<solution-name>`	Tanium Module Server only: Checks whether each installed solution service is running	ERROR	Service is not running or status cannot be determined	Use the Tanium Service Control menu on page 313 to check the status of the service for the solution, and attempt to start or restart it. If the service fails to start, review Status Details for more information about the failure.
`TMS database pg_wal`	Tanium Module Server only: Checks the size of the	ERROR	pg_wal directory	Contact Tanium Support on page 510 for assistance.

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
	PostgreSQL write-ahead log (WAL) directory		missing	
		ERROR	pg_wal directory >50% of partition size	
`IPsec`	Tanium Server in an active-active configuration or Tanium Module Servers in an active passive configuration: Checks that there is a secure connection between Tanium Servers in an active-active configuration	ERROR	Secure connection failed between Tanium Servers or Tanium Module Servers	Use the Tanium Service Control menu on page 266 to restart the ipsec service if it is already running, or attempt to start it if it is not. If the service fails to start, review Status Details for more information about the failure.
`Memory Plan`	Tanium Server or Tanium Module Server only: Checks that the memory plan for the local database instance is set appropriately	WARN	Configured memory plan is not the preferred plan for the Appliance model (physical Tanium Appliance) or the available memory (virtual Tanium Appliance or cloud-based Tanium Appliance)	Configure the memory plan on page 453 to the indicated preferred plan.

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
`TZS`	Tanium Zone Server only: Checks whether the taniumzoneserver service is running	ERROR	Service is not running or status cannot be determined	Use the Tanium Service Control menu on page 313 to check the status of the taniumzoneserver service , and attempt to start or restart it. If the service fails to start, review Status Details for more information about the failure.
`Zone Hub`	Tanium Zone Server Hub only: Checks whether taniumzoneserver service is running	ERROR	Service is not running or status cannot be determined	Use the Tanium Service Control menu on page 313 to check the status of the taniumzoneserver service , and attempt to start or restart it. If the service fails to start, review Status Details for more information about the failure.
`TaniumServer file permissions`	Tanium Server only: Checks for proper file permissions and ownership on Tanium Server files	WARN	Specified files do not have the proper permissions or ownership	Reinstall access control lists (ACLs). on page 464
`TaniumModuleServer file permissions`	Tanium Module Server only: Checks for proper file permissions and ownerships on Tanium Module Server files	WARN	Specified files do not have the proper permissions or ownership	Reinstall access control lists (ACLs). on page 464
`TaniumZoneServer file permissions`	Tanium Zone Server only: Checks for proper file permissions and ownership on Tanium Zone Server files	WARN	Specified files do not have the proper permissions or ownership	Reinstall access control lists (ACLs). on page 464

©2026 Tanium Inc. All Rights Reserved

TanOS

TanOS system health check results

Check	Description	Severity	Condition	Remediation
`BIOS Version`	Physical Tanium Appliance only: Checks whether the installed BIOS firmware version is up to date with the version available with the installed version of TanOS	WARN	Old version of firmware installed	Install the available firmware update on page 461 .
`PERC Version`	Physical Tanium Appliance only: Checks whether the installed RAID controller firmware version is up to date with the version available with the installed version of TanOS	WARN	Old version of firmware installed	Install the available firmware update on page 461 .
`iDRAC Version`	Physical Tanium Appliance only: Checks whether the installed iDRAC firmware version is up to date with the version available with the installed version of TanOS	WARN	Old version of firmware installed	Install the available firmware update on page 461 .
`NIC Version`	Physical Tanium Appliance only: Checks whether the installed NIC firmware version is up to date with the version available with the installed version of TanOS	WARN	Old version of firmware installed	Install the available firmware update on page 461 .
`Backup`	Tanium Server or primary Tanium Module Server only: Checks whether a system backup is scheduled to run	ERROR	Backup is scheduled, but an encryption key is not	Configure the encryption key on page 406 for the backup.

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
			properly configured	
		INFO	No backup is scheduled	Configure an automatic backup. on page 405
`Partition sync`	Appliances with an inactive partition set: Checks whether a partition sync has been performed in the last 90 days	WARN	The fstab configuration file used to mount the inactive partition is missing	Perform a partition sync. on page 395
		WARN	The partition sync time stamp is missing	
		INFO	>90 days since last partition sync	
`TanOS key material`	Checks for issues with the cryptographic keys on the Appliance	ERROR	A required key is invalid, obsolete, or missing	Generate a new key for any keys that are indicated by the error.
`TanOS version`	Internet-connected Appliances: Checks whether a newer version of TanOS is available	INFO	A newer version of TanOS is available for upgrade	Upgrade TanOS on page 469 to the new version.
`TanOS version match`	Appliances in an Array: Checks whether the TanOS version matches for all Array members	WARN	TanOS versions do not all match	Upgrade TanOS on page 469 to the new version on all Array members.

©2026 Tanium Inc. All Rights Reserved

Miscellaneous

Miscellaneous TanOS health check results

Check	Description	Severity	Condition	Remediation
`Core Files`	Checks for core dumps that are stored on the Appliance from process crashes  **Best Practice:** Copy core files from the Appliance to share with Tanium Support on page 510 when requesting troubleshooting assistance. To save disk space, clean up core files that have been copied or are no longer needed.	WARN	Core files exist on the Appliance	• Copy core files on page 501 for troubleshooting. • Use the Clean directories on page 444 menu to clean the Cores directory after core files have been copied or are no longer needed.
`Shell Keys`	Checks whether a TanOS shell key on page 507 is active for read-write restricted shell or full shell access	INFO	Shell key is active	Use the Shell Keys on page 507 menu to remove shell access or revoke all shell keys when read-write restricted shell or full shell access is no longer needed.
`Auth plugin`	Tanium Server only: Checks whether the proper authentication plugin is in use	INFO	Deprecated or unsupported authentication plugin in use	Contact Tanium Support on page 510 for assistance.

Database replication health

TanOS database replication health check results

Check	Description	Severity	Condition	Remediation
`Database Replication`	Tanium Server or Tanium Module Server only: Checks the status of database replication	ERROR	Database replication failed	• Review replication status. on page 455 • From the main menu on the

©2026 Tanium Inc. All Rights Reserved

Check	Description	Severity	Condition	Remediation
				secondary Tanium Server or Module Server, enter `3-3-B` to reinitialize the replication.
		WARN	Database replication is in a start-up, catch-up, back-up, or stopping state	Allow time for the replication state to clear and then perform another health check.
`TMS Database Stats Collection`	Tanium Module Server only: Checks whether collection of database replication statistics is enabled	INFO	Collection of database replication statistics enabled	Disable collection of database replication statistics. on page 457 Keep database replication statistics disabled when you are not troubleshooting a replication issue.

TMS sync health

TanOS TMS sync health check results

Check	Description	Severity	Condition	Remediation
`Tanium Module Server Sync Health`	Tanium Module Server only: Checks whether Module Server synchronization is successful. If a Module Server file sync is in progress, the error is not reported until the sync has been running for more than 24 hours.	ERROR	Module Server synchronization failed, or a Module Server file sync has been running for more than 24 hours	• Review the detailed status for Module Server sync. on page 330 • Check the Module Server sync configuration on page 329.

Disk Encryption Key

TanOS Disk Encryption Key health check results

Check	Description	Severity	Condition	Remediation
`Disk Encryption Key check`	Physical Tanium Appliance only: Checks whether the Disk Encryption Key has been exported **Important:** The Disk Encryption Key is required to decrypt drives after a hardware failure.	WARN	Disk Encryption Key has not been exported	Export the Disk Encryption Key on page 89 and store it in a safe location.

Postgres SSL health check

TanOS Postgres SSL health check results

Check	Description	Severity	Condition	Remediation
`Postgres SSL`	Tanium Server only: Checks the TLS configuration of the local PostgreSQL database	ERROR	Missing DB Directory	Contact Tanium Support on page 510 for assistance.
		ERROR	TLS disabled for PostgreSQL database	
`SSL CRL file`	Tanium Server only: Reports the name of the certificate revocation list (CRL) file if in use. This check is informational only.	N/A	N/A	N/A

©2026 Tanium Inc. All Rights Reserved

OVA health

TanOS OVA health check results

Check	Description	Severity	Condition	Remediation
`Client Count`	Virtual Tanium Appliance only: Reports the count of Tanium Clients that have connected during the current or prior day and checks whether the number exceeds the maximum recommended with current virtual machine resources	INFO	Number of connected Clients exceeds the recommended maximum	• To determine whether the RAM and CPU are adequate, see each of those checks in this section. • Increase virtual machine resources. For more information, see Cloud-based Tanium Appliance and virtual Tanium Appliance specifications on page 648
`RAM Requirements`	Virtual Tanium Appliance only: Checks whether the RAM configured for the virtual machine is less than the RAM recommended for the number of connected Clients	INFO	RAM less than recommended minimum	Increase virtual machine RAM. For more information, see Cloud-based Tanium Appliance and virtual Tanium Appliance specifications on page 648
`CPU Requirements`	Virtual Tanium Appliance only: Checks whether the number of CPU cores configured for the virtual machine is less than the CPU cores recommended for the number of connected Clients	INFO	CPU cores less than recommended minimum	Increase virtual machine CPU cores. For more information, see Cloud-based Tanium Appliance and virtual Tanium Appliance specifications on page 648

©2026 Tanium Inc. All Rights Reserved

Reference: TanOS menu map

The following tables list the available options in the TanOS menus.

> **Note:** Not all menu paths are available on every Tanium Core Platform server type or in every deployment.

TanOS menu

The main TanOS console menu contains the following options.

TanOS menu structure and options

Option	Menu
1	Tanium Installation Menu on page 561
2	Tanium Operations Menu on page 563
3	Tanium Support Menu on page 568
4	Status Menu on page 573
A	Appliance Configuration Menu on page 573
B	Appliance Maintenance Menu on page 579
C	User Administration Menu on page 583
P	Password change (current user) on page 225
Q	View end user license agreement (EULA)
@	About this Appliance on page 487
Z	Log out

Common menu options

The following table lists menu items that apply to most screens in the TanOS console.

©2026 Tanium Inc. All Rights Reserved

Common menu options in TanOS

Option	Menu
`R`	Return to previous menu
`RR`	Return to top

Log menu options

The following table lists menu items that apply to most logs in the TanOS console.

Log menu options in TanOS

Option	Menu
`V`	View current file
`F`	Follow current file growth
`T`	Delete content of current file
`E`	Export current and rotated files to outgoing (sftp)
`x`	Line number of recent rotated log files

Service menu options

The following table lists menu items that apply to most services in the TanOS console.

Service menu options in TanOS

Option	Menu
`1`	Start service
`2`	Stop service
`3`	Restart service

©2026 Tanium Inc. All Rights Reserved

Option	Menu
`4`	Disable service
`5`	Enable service
`6`	Status details

Tanium Installation Menu

Enter `1` to access the Tanium Installation Menu.

- `M` - Manage Appliance Array on page 158
    - `C` - Create Appliance Array on page 161
    - `A` - Add Member on page 162
    - `F` - Refresh Appliance Array on page 174
    - `I` - Install Pending Role Changes on page 170
    - `E` - Restart Replication on page 545
    - `X` - Reset Appliance Array on page 175
    - `n` - line number of Array member
        - `A` - Assign Role: All-in-One on page 165
        - `T` - Assign Role: Tanium Server on page 165
        - `M` - Assign Role: Tanium Module Server on page 165
        - `Z` - Assign Role: Tanium Zone Server on page 165
        - `U` - Cancel pending role change
        - `P` - Promote member to manager on page 172

©2026 Tanium Inc. All Rights Reserved

        - `D` - Delete member on page 173
        - `I` - Update IP Address on page 340
        - `N` - Measure Data Transfer Rate on page 158
    - `1` - Install Tanium Server (All-in-one) on page 187
    - `2` - Install Tanium Server Service
    - `3` - Install Tanium Module Server Service
    - `4` - Install Tanium Zone Server Service on page 176
    - `5` - Install Tanium Cloud Access Point Service on page 191
- `U` - Upgrade Tanium Software on page 481[1]
- `A` - Install Tanium Zone Server Hub Add-On on page 179[1]
- `E` - Remove Tanium Zone Server Hub Add-On on page 179[1]
- `D` - Tanium Direct Connect Zone Proxy on page 183
    - `T` - Download from Tanium on page 183
    - `L` - List Installed DEC Proxy Versions on page 185[1]
    - `V` - View DEC Provision Instructions[3]
    - `X` - Remove DEC Proxy on page 187[3]

©2026 Tanium Inc. All Rights Reserved

Note:

[1] Specific to Tanium Server

[3] Specific to Zone Server

Tanium Operations Menu

Enter `2` to access the Tanium Operations Menu.

- `1` - Tanium Service Control on page 313
    - `x` - service name
        - For options, see Service menu options on page 560.
    - `A` - Restart ALL enabled Tanium services
    - `B` - Stop ALL Tanium services
    - `C` - Start ALL Tanium services
    - `D` - Disable ALL Tanium services
    - `E` - Enable ALL Tanium services
    - `J` - Display journal
- `2` - Tanium Configuration Settings on page 314
    - `1` - Edit Tanium Server Settings on page 314[1]
    - `2` - Edit Tanium Server TDL Settings on page 316[1]
    - `3` - Add Tanium Server TDL Auth User on page 315[1]

©2026 Tanium Inc. All Rights Reserved

    - `4` - Add Tanium Server TDL Auth Cert on page 321 [1]
    - `5` - Edit Tanium Module Server Settings on page 314[2]
    - `6` - Edit Tanium Module Server TDL Settings on page 316[2]
    - `7` - Add Tanium Module Server TDL Auth User on page 315[2]
    - `8` - Add Tanium Module Server TDL Auth Cert on page 321[2]
    - `9` - Edit Tanium Zone Server Settings on page 314[1,3]
    - `10` - Edit Zone Server List on page 176[1,3]
    - `11` - Edit Isolated Subnets List on page 324[1,3]
    - `12` - Edit Separated Subnets List on page 324[1,3]
    - `13` - Control Root CA Certs on page 315
- `4` - Install custom SOAP certificates on page 266[1]
- `5` - Manage Custom Signing Keys on page 325[1,2]
    - `L` - List content signing keys
    - `A` - Add content signing key
    - `D` - Delete content signing key
- `7` - Download SOAP Certificate on page 266[1]
- `9` - Import CAC Certificate on page 300[1]
- `A` - Configure Module Server(s) on page 329[2] / Register Module Server on page 266[1,5]
    - `P` - Promote TMS on page 332[2]

©2026 Tanium Inc. All Rights Reserved

        - `S` - Assign TMS Role[2]
            - `x` - TMS line number[2]
                - `S` - Enable TMS Sync as Source[2]
                - `T` - Enable TMS Sync as Target[2]
                - `D` - Disable TMS Sync[2]
        - `1` - Step 1 - Configure Module Server Address[1,5]
        - `2` - Step 2 - Register Module Server[2,5]
        - `3` - Read about Remote Module Server configuration[2]
- `B` - Configure Tanium cluster on page 328[1]
    - `I` - Initialize Cluster as Primary[6]
    - `C` - Read about cluster operations
    - `X` - Remove Cluster[6]
    - `F` - Database Server Failover on page 328
    - `E` - Reinitialize Replication on page 329
    - `S` - Replication Status on page 328
    - `D` - IPsec management[6]
- `C` - Manage content on page 201[1]
    - `1` - Install Airgap Content on page 208
    - `2` - Airgap Usage Report on page 221

©2026 Tanium Inc. All Rights Reserved

        - `3` - Prune Airgap Content on page 222
        - `4` - Manage Web Server Content on page 223
        - `B` - Set Manifest on page 332
- `D` - Configure Module Server sync on page 329[2]
    - `1` - Show Detailed Status
    - `2` - Configure IPSEC
        - `1` - Display Local IPSEC host key
        - `2` - Display IPSEC
        - `3` - Configure IPSEC
        - `4` - Delete IPSEC
        - `5` - Restart IPSEC
        - `6` - Test IPSEC
    - `3` - Disable TMS Sync
    - `4` - Sync Now
    - `5` - Schedule Sync on page 329
    - `V` - View Sync Log
- `I` - Import Public Key to Tanium Zone Server on page 178[3]
- `M` - Module Server SSL Certificate on page 266[2]
- `S` - Install SAMLEncryption Cert on page 266[1]
- `P` - Manage Cloud Access Point on page 191[4]

©2026 Tanium Inc. All Rights Reserved

    - `C` - Configure Cloud Access Point on page 194
    - `S` - Manage Cloud Access Point Service on page 194
        - For options, see Service menu options on page 560.
- `X` - Advanced operations on page 335[1,2]
    - `2` - Toggle UseTBBAllocatorStats on page 335
    - `3` - Generate new keys (tanium.pub)
    - `4` - Manage HTML banner on page 336
    - `5` - Generate reporting keys (Zone Server to Server)
    - `6` - Generate reporting keys (Client to Server)
    - `7` - Disable SAML SSO

©2026 Tanium Inc. All Rights Reserved

Note:

[1] Specific to Tanium Server

[2] Specific to Module Server

[3] Specific to Zone Server

[4] Specific to Tanium Cloud Access point

[5] Manual registration of the Tanium Module Server with a Tanium Server is unnecessary in an Array, except when you replace the SSL certificate on the Module Server. These functions are provided only for that process and for legacy installations. Use an Array on page 165 to manage Tanium Core Platform Server roles.

[6] Manual cluster management is deprecated, and these functions are provided only for legacy installations. Use an Array on page 168 to configure a Tanium Server cluster.

Tanium Support Menu

Enter `3` to access the Tanium Support Menu.

- `1` - Tanium Log Files
    - For all logs listed in the following menus, see Log menu options on page 560.
    - `1` - TanOS Appliance on page 497
        - `1` - TanOS Log on page 411
        - `2` - Upgrade Log on page 481
        - `3` - Health Log
        - `4` - Health Failure Log

©2026 Tanium Inc. All Rights Reserved

- `5` - Messages Log
- `6` - License Log
- `7` - TanOS Event Log
- `8` - TanOS Disk Re-sizing Log
- `9` - Airgap Log on page 222
- `10` - Backup Restore Log on page 416
- `11` - Array Latency Log on page 505
- `12` - Array Roles Log

- `2` - Tanium Server on page 497[1]
  - `1` - Tanium Server Log (log0.txt)
  - `2` - Tanium Server TDL Log (log0.txt)
  - `3` - Tanium Server RBAC Log (rbac0.txt)
  - `4` - Tanium Server PAM4 Log (tanium_pam4.log)
  - `5` - Tanium Server Workbenches (workbenches_manager.log)
  - `6` - Tanium Server Signature Verifier (signature_verifier.log)
  - `7` - Tanium Server DB Upgrade Log (database-upgrade0.txt)
  - `8` - Tanium Server Auth0 Log (auth0.txt)
  - `9` - Tanium Module History Log (module-history0.txt)

- `3` -Tanium Module Server on page 497[2]
  - `1` - Tanium Module Server log

    (log0.txt)

©2026 Tanium Inc. All Rights Reserved

        - `2` - Tanium Module Server TDL log (log0.txt)
        - `3` - TMS PluginsManager log (plugins_manager.log)
        - `4` - Tanium Module Server Sync Log (module_sync.log)
        - `5` - Tanium Module History Log (module-history0.txt)
    - `4` - Tanium Zone Server on page 497[3]
        - `1` - Tanium Zone Server Log (log0.txt)
        - `2` - DEC Proxy Log (proxy.log)
    - `5` - PostgreSQL[1,2]
        - `x` - PostgreSQL log file name
- `2` - Tanium Module log files on page 499[2]
    - `x` - Module name
        - For options, see Log menu options on page 560.
- `3` - Database Operations on page 450[1,2]
    - `1` - Display Postgres log file on page 450
    - `2` - View Postgresql config files on page 451
    - `3` - Display Postgres control data on page 451
    - `4` - Enable full Postgres Audit logs on page 452
    - `D` - Database Memory Plan on page 453
        - `T` - Select Tiny Plan
        - `D` - Select Dev Plan

©2026 Tanium Inc. All Rights Reserved

        - `S` - Select Small Plan
        - `M` - Select Medium Plan
        - `L` - Select Large Plan
        - `X` - Select X-Large Plan
        - `A` - Apply Memory Plan
    - `M` - Monitor Database on page 453
    - `Q` - Manage Database Queries on page 454
        - `S` - Select query
        - `X` - Execute query
        - `V` - View query
        - `Q` - View query results
    - `S` - Replication Status on page 455
    - `F` - Database Server Failover on page 457
    - `B` - Reinitialize Replication on page 496
    - `I` - Reindex Databases on page 496
- `4` - Run Network Diagnostics on page 503
    - `1` - Ping Remote System on page 503
    - `2` - Test Remote Port (TCP) on page 503
    - `3` - Trace Path on page 503
    - `4` - Resolve Name on page 504
    - `5` - Check IPSEC on page 504

©2026 Tanium Inc. All Rights Reserved

        - `6` - Listening Ports on page 504
        - `7` - Show Firewall on page 504
        - `8` - Show Array Network Latency on page 505
- `5` - Run Health Check on page 488
- `6` - Display Last Scheduled Health Check Results
- `7` - Appliance Hardware Report
- `A` - Run TSG (Tanium Support Gatherer) on page 500
- `B` - Run TCPdump on page 501
- `P` - Performance Monitoring on page 458
        - `1` - Run SAR command on page 458
        - `2` - Export SAR snapshot on page 459
        - `3` - Export SAR performance data on page 459
        - `4` - Combine all SAR files on page 460
        - `I` - Run iotop command on page 458
        - `P` - Run perf top command on page 461
        - `T` - Run htop command on page 461
- `X` - Advanced Support
        - `1` - Copy Core Files on page 501
        - `2` - Generate Process Memory Dump
        - `3` - Directory Space Usage
        - `V` - Internal Tanium VPN Connection

©2026 Tanium Inc. All Rights Reserved

Note:

[1] Specific to Tanium Server

[2] Specific to Module Server

[3] Specific to Zone Server

Status Menu

Enter `4` to access the Status Menu.

- `1` - System Status Menu
  - `1` - OS Status on page 448 *(includes partition information)*
  - `2` - Network Status on page 448
- `2` - Tanium Status Menu on page 449
  - `x` - *service name*
    - For options, see Service menu options on page 560.
- `3` - Appliance Status Menu on page 449
  - `1` - Appliance Version Details
  - `2` - Appliance Status (OS)
  - `3` - Appliance Status (HW)

Appliance Configuration Menu

Enter `A` to access the Appliance Configuration Menu.

©2026 Tanium Inc. All Rights Reserved

- `1` - Hostname/DNS configuration on page 337
    - `1` - Manage Hostname/Domain Name on page 337
    - `2` - Manage DNS Server on page 338
    - `3` - Edit manual hosts entries on page 339
- `2` - Networking Configuration
    - `1` - Network Interfaces on page 340
        - `x` - Network interface name
            - `I` - Manage IP Address
            - `M` - Manage MTU Size
            - `U` - Set Interface Up
            - `D` - Set Interface Down
            - `S` - Set Advertised Speeds on page 343[8]
            - `X` - Reset Interface on page 345
    - `2` - IPSEC Configuration on page 345
    - `3` - Routing Configuration on page 349
    - `4` - Restart Networking on page 495
    - `T` - NIC Teaming on page 350
        - `A` - Create a Network Team on page 350
- `3` - NTP Configuration on page 351
    - `x` - NTP server name
    - `A` - Add NTP server

©2026 Tanium Inc. All Rights Reserved

- `4` - Syslog Configuration on page 429
    - `1` - Check current status on page 428
    - `2` - View Trust Certificate on page 429
    - `3` - Paste Trust Certificate on page 429
    - `4` - Remove Trust Certificate on page 429
    - `5` - Configure syslog forwarding on page 430
    - `6` - Custom File Forwarding on page 434
    - `7` - View Public Key for TLS Auth on page 430
    - `8` - Load Key Pair for TLS from SFTP incoming on page 430
    - `9` - Remove Key Pair for TLS Auth on page 430
    - `10` - Configure FQDN Behavior on page 434
- `5` - SNMP configuration on page 439
    - `U` - Change the Username on page 443
    - `L` - Change the Location on page 443
    - `C` - Change the Contact on page 443
    - `A` - Change the Authentication Type on page 443
    - `P` - Change the Privacy Type on page 443
    - `V` - View SNMP Service Status on page 443
    - `D` - Stop the SNMP Service on page 443
    - `S` - Set Password and Start the SNMP Service on page 441
- `6` - Module file share configuration on page 333[2]

©2026 Tanium Inc. All Rights Reserved

        - `1` - Create a new Connect mount on page 333
        - `2` - Create a new Detect mount on page 333
        - `4` - Delete an existing Connect mount
        - `5` - Delete an existing Detect mount
        - `A` - List existing mounts on page 334
        - `B` - Test existing mounts on page 334
        - `C` - Re-attempt mounts
- `7` - Reset all NICs to DHCP on page 353[7]
- `A` - Security on page 354
    - `2` - Manage SSH on page 354
        - `A` - Add Rule *(to allow inbound SSH)*
        - `x` - *Delete existing rule*
    - `3` - Configure SSH Banner on page 354
    - `4` - Display SSH Fingerprints on page 355
    - `5` - Regenerate SSH Host keys
    - `6` - Manage HTTPS on page 355
        - `A` - Add Rule *(to allow inbound HTTPS)*
        - `x` - *Delete existing rule*
    - `A` -LDAP CA certificate management on page 356[1,2]
        - `1` - Add Certificate on page 356
        - `2` - Import Certificate on page 358

©2026 Tanium Inc. All Rights Reserved

        - `3` - Toggle LDAPS or StartTLS Configuration on page 358
        - `4` - Toggle TLS Certificate Validation on page 358
        - `5` - List Certificates on page 359
        - `S` - Sync Configuration to Peer TS on page 360
    - `B` -Database Certificate Management[1,2]
        - `1` - Import DB Server and Client certificate
        - `2` - Export DB Server Certificate
        - `3` - Import DB Client Certificate
        - `L` - List Certificates
    - `C` - iDRAC Certificate Management on page 423
        - `1` - Replace iDRAC Cert and Key
    - `P` - Security Policy on page 361
        - `1` - Password Lifetime
        - `2` - Password History Reuse Limit
        - `3` - Password Minimum Length
        - `4` - Password Minimum Characters Changed
        - `D` - Login Failure Delay
        - `E` - Expired Passwords Effect
        - `L` - Account Lockout Time
        - `M` - Maximum Concurrent Logins
        - `T` - Login Timeout

©2026 Tanium Inc. All Rights Reserved

- `X` - Advanced security
    - `1` - FIPS 140-3 mode (disabled/enabled) on page 362
    - `2` - AIDE on page 365
        - `1` - Initialize AIDE, enable weekly check report, run check report on page 366
        - `2` - Run AIDE check report now on page 367
        - `3` - Disable weekly AIDE check on page 367
        - `4` - Enable weekly AIDE check report on page 368
        - `5` - Copy AIDE check reports to outgoing directory on page 368
    - `4` - Toggle SELinux mode (permissive/enforcing) on page 370
    - `5` - Set Menu Timeout on page 370
- `I` - iDRAC Management on page 420[8]
    - `N` - iDRAC network configuration on page 421
    - `P` - Set `tanremote` password on page 421
    - `E` - Enable `tanremote` password on page 422
    - `D` - Disable `tanremote` password on page 422
    - `C` - Close all iDRAC sessions on page 422
    - `K` - Reset iDRAC on page 422
    - `F` - Flush Pending Firmware Entries on page 426
    - `X` - Clear iDRAC job queue (FORCE) on page 427
    - `V` - View iDRAC Logs on page 427

©2026 Tanium Inc. All Rights Reserved

- `X` - Advanced configuration
    - `3` - Change Active Partition on page 396[9]
    - `4` - Change Disk Encryption Key on page 373[8]
    - `5` - Export Disk Encryption Key on page 372[8]
    - `6` - Export Grub Key on page 375
    - `7` - Generate New Grub Key on page 377
    - `8` - Set Virtual Console Keymap on page 96

Note:

[1] Specific to Tanium Server

[2] Specific to Module Server

[7] Virtual Tanium Appliances only

[8] Physical Tanium Appliances only

[9] Available only when alternate partition is enabled

Appliance Maintenance Menu

Enter `B` to access the Appliance Maintenance Menu.

- `1` - Backup on page 379
    - Automatic Backups
    - `E` - Set Encryption Key on page 406

©2026 Tanium Inc. All Rights Reserved

- `C` - Configure Automatic Backup on page 408
    - `N` - Configure Core Backup
    - `F` - Configure Comprehensive Backup
- `A` - Run Automatic Backup Now on page 409
- `S` - Schedule Automatic Backup on page 410
    - `N` - Schedule Core Backup
    - `F` - Schedule Comprehensive Backup
- Manual Backups
- `P` - Partition Sync on page 379[9]
- `N` - Core Backup on page 412
- `F` - Comprehensive Backup on page 412
- `O` - Restore from Backup on page 413

- `2` - Alerting on page 436
    - `1` - Configure Syslog Destination on page 437
    - `2` - Configure SMTP Destination on page 438
    - `3` - Configure Alerts on page 436
    - `4` - Status
- `3` - Upgrade TanOS on page 469
- `5` - Shell keys on page 506
    - `1` - Validate Response on page 507
    - `2` - Remove Shell Access on page 507

©2026 Tanium Inc. All Rights Reserved

    - `3` - Launch Shell on page 507
    - `O` - Open Read Only Restricted Shell on page 506
    - `W` - Request Read Write Restricted Shell Activation on page 507
    - `F` - Request Full Shell Activation on page 507
    - `L` - Shell Key Listing on page 507
    - `A` - Revoke All Shell Keys on page 507
- `A` - Clean directories on page 444
    - `1` - SFTP (IN/OUT)
    - `2` - Cores
    - `3` - Tanium Application Logs
    - `4` - Tanium TSG HTTP files
    - `5` - Tanium Connect output logs
    - `T` - /tmp directory
- `B` - Reboot/Shutdown on page 444
    - `1` - Reboot the Appliance
    - `2` - Shutdown the Appliance
- `C` - Maintenance mode on page 496
    - `1` - Clear maintenance action
- `D` - Discard alt partitions on page 393[7,9]
- `E` - Enable alt partitions on page 392[7,10]
- `I` - Increase storage on page 445

©2026 Tanium Inc. All Rights Reserved

- `S` - OS services on page 446
    - `1` - ntpd
        - For options, see Service menu options on page 560.
    - `2` - sshd
        - For options, see Service menu options on page 560.
- `T` - Tokens download
- `X` - Advanced maintenance on page 461
    - `1` - Install Firmware Updates on page 461[8]
    - `2` - Appliance Reset on page 463
        - `1` - Software reset
    - `3` - Re-Apply ACLs on page 464
    - `4` - Overwrite Module ACLs on page 464[2]
    - `5` - View TanOS Partition Sync Log File on page 464

Note:

[2] Specific to Module Server

[7] Virtual Tanium Appliances only

[8] Physical Tanium Appliances only

[9] Available only when alternate partition is enabled

[10] Available only when alternate partition is disabled

©2026 Tanium Inc. All Rights Reserved

User Administration Menu

Enter `C` to access the User Administration Menu.

- `U` - TanOS User Management on page 225
    - `x` - individual user
        - `A` - Manage SSH Authorized Keys on page 229
        - `P` - Manage SSH Key Pair on page 231
        - `L` - Reset SSH Lockout
        - `C` - Change/Enable Password on page 237
        - `N` - Disable password access on page 235
        - `M` - Multifactor Authentication on page 245
        - `E` - Enable Account on page 238
        - `D` - Disable Account on page 238
        - `T` - Manage Account Protection on page 239
        - `X` - Delete User on page 239
        - `F` - Edit known hosts file on page 240
    - `A` - Add system user on page 234
- `I` - Recent login information on page 242
    - `A` - View Last 20 Successful Logins
    - `B` - View Last 20 Failed Logins
    - `C` - View Login Statistics

©2026 Tanium Inc. All Rights Reserved

- `M` - Multifactor Global Settings on page 242
    - `K` - Require Key Authentication on page 243
    - `P` - Require Password Authentication on page 244
    - `M` - Require Multifactor Authentication on page 244
    - `X` - Reset ALL Multifactor Settings
- `A` - AD/LDAP TanOS Authentication on page 252
    - `M` - Manage AD/LDAP Certificate on page 253
        - `I` - Import Certificate on page 255
        - `P` - Paste Certificate on page 254
        - `E` - Export Certificate on page 255
        - `V` - View Certificate and Details on page 255
        - `D` - Delete Certificate on page 255
    - `C` - Configure AD/LDAP TanOS Authentication on page 257
        - `E` - Enable
        - `D` - Domain
        - `H` - Host
        - `P` - Port
        - `C` - Bind Credentials
        - `B` - Base Search DN
        - `S` - Schema
        - `Q` - Referrals

©2026 Tanium Inc. All Rights Reserved

        - `K` - SSH Public Key Attribute
        - `U` - Users Filter
        - `G` - Groups Filter
        - `M` - TanOS Roles Mapping
            - `A` - tanadmin Mappings
                - `A` - Add Mapping
                - `I` - Manually Input Mapping
                - `X` - Remove ALL tanadmin Mappings
            - `U` - tanuser Mappings
                - `A` - Add Mapping
                - `I` - Manually Input Mapping
                - `X` - Remove ALL tanuser Mappings
        - `V` - Validate Configuration
        - `A` - Activate Configuration Changes
- `W` - Walkthrough Configuration on page 256
- `S` - Detailed Status on page 262
- `V` - Verify AD/LDAP User or Group
    - `U` - Verify AD/LDAP User on page 263
    - `G` - Verify AD/LDAP Group on page 264
- `T` - Troubleshooting
    - `S` - Manage System Security Services Daemon (sssd)

©2026 Tanium Inc. All Rights Reserved

        - For options, see Service menu options on page 560.
    - `D` - Enable Debug Logging
    - `V` - View Domain Log File
    - `L` - Logoff User
- `E` - Export configuration to SFTP outgoing on page 264
- `I` - Import configuration from SFTP incoming on page 265
- `X` - Reset ALL AD/LDAP TanOS Auth Settings

- `L` - Local Tanium User Management on page 294
    - `1` - Add Local User on page 295
    - `2` - Manage Local Users on page 296
    - `A` - Enable/Disable Local Authentication Service on page 298
    - `B` - Security Policy Local Authentication Service on page 299
    - `C` - Check Local Authentication Contents

©2026 Tanium Inc. All Rights Reserved

Reference: TanOS command line interface

Tanium Appliances contain a command line interface (CLI) that you can access from SSH.

Requirements

To access all CLI commands, you must access the CLI as a user with the `tanadmin` role. Some CLI commands are available to users with the `tanuser` role, as noted in Tanium platform commands on page 588.

Best Practice: Configure an SSH key to authenticate the user account you use to run CLI commands. If you have not configured an SSH key, you are prompted for a password each time you run a command.

Syntax

```
ssh -q[t] <user>@<ip-or-fqdn> <command> [action/options] ...
```

Best Practice: Always include the `ssh -q` option for Appliance CLI commands to suppress unnecessary messages.

©2026 Tanium Inc. All Rights Reserved

Important: You must include the `ssh -t` option with interactive commands that prompt for information. This option is not necessary for commands that run silently or only return information.

Tanium platform commands

Tanium platform commands for Tanium Appliance CLI

Command	Description
add hub	Install the Tanium Zone Server Hub add-on to an existing Tanium Server role.
configure cap <action>	Configure the Tanium Cloud Access Point role. This command has the following options: • `show` - Show the current Cloud Access Point configuration. • `set <host1> <host2> <listen_port_client>` - Configure the host names from the Tanium Cloud Client edge URLs (host1 and host2) and the port that you want Tanium Clients to use to communicate with the Cloud Access Point (listen_port_client). Usage example: `ssh -q user@appliance configure cap set sample-zsb1 sample-zsb2 443`
configure ipsec <action>	Configure IPsec communication with a peer Appliance in an Array. Both Appliances must have the same Tanium role of either Tanium Server or Tanium Module Server. This command has the following actions: • `show` - Show the current IPsec configuration • `set <serial>` - Enable IPsec with the Appliance with the specified serial number

©2026 Tanium Inc. All Rights Reserved

Command	Description
	• `test` - Test the IPsec connection • `disable` - Clear the IPsec configuration and preserve the key • `reset` - Reset the IPsec configuration and generate a new key  **Important:** After you perform an IPsec reset, run `refresh array` on an Array Manager Appliance to distribute the updated IPsec key to the other Appliances in the Array.
configure tms sync <action>	Configure the Tanium Module Server synchronization feature, which copies content from an active Tanium Module Server to a standby Tanium Module Server. To use this feature, you must: • Install two Tanium Module Servers. • Add both Tanium Module Servers to the Array. For more information about Tanium Module Server synchronization, see Schedule sync jobs on page 329 . This command has the following actions: • `status` - Shows the current Tanium Module Server synchronization status `source` - Specifies the source, or active, Tanium Module Server from which data is copied `target` - Specifies the target, or standby, Tanium Module Server to which data is copied `disable` - Disables synchronization between the two Tanium Module Servers
dec proxy	Install, upgrade or remove the Direct Connect (DEC) Zone Proxy. Available options: • list: List the available DEC proxy versions. • install <version>: Install the selected version of DEC proxy. • remove: Uninstall the DEC proxy.

©2026 Tanium Inc. All Rights Reserved

Command	Description
	• show <item>: Show information about the installed DEC proxy. The following items are available: • `version` - Show the installed version. • `cert` - Show the TLS certificate. • `token` - Show the enrollment token. • `apipayload` - Show the API payload used to configure the connection on the Tanium platform. • `instructions` - Show the provisioning instructions.
help	Show a list of available commands. Add `help` to any command to show help for that particular command.
install aio [version]	Install the specified version of the Tanium All-in-One role. Run the command without a version to display the available versions found on the Appliance. Usage example: `ssh -qt user@appliance install aio` 7.9.3 `.1234` **Note:** Use Tanium Appliances configured with the All-in-One role only for evaluation purposes. Tanium does not support All-in-One deployments in production environments. Do not allow a Tanium Appliance that is configured with the All-in-One role to accept inbound connections from the internet.

©2026 Tanium Inc. All Rights Reserved

Command	Description
install airgap [<file>] [<console_uri>]	Install a Tanium Airgap content bundle that you copied to the /incoming directory as the `tancopy` user. For more information, see Reference: Transfer files to and from the Appliance on page 621 . This command supports the following files: • Tanium_Airgap_*.zip - A full Airgap bundle. • TaniumAirgap-*.rpm - A full Airgap bundle in RPM format. • Airgapped-*-Installer.zip - An installer for an individual solution. If you omit file and exactly one Airgap file is in the /incoming directory, TanOS uses that file. Use console_uri to set the local content and manifest URLs to a host other than the FQDN of this Appliance; specify the host name without a protocol prefix. On the Array Manager, TanOS creates the content signing key and distributes it to the peer Tanium Server and Module Server automatically. This command mirrors the `2` - `C` - `1` menu. Usage example `ssh -q user@appliance install airgap Tanium_Airgap_` 2026H2 `_Ux_yyyy-mm-dd.zip`
install cap	Install the Tanium Cloud Access Point role.
install tms [version]	Install the specified version of the Tanium Module Server role. Run the command without a version to display the available versions found on the Appliance. Usage example: `ssh -qt user@appliance install tms` 7.9.3 `.1234`
install ts [version]	Install the specified version of the Tanium Server role. Run the command without a version to display the available versions found on the Appliance. Usage example:

©2026 Tanium Inc. All Rights Reserved

Command	Description
	`ssh -qt user@appliance install ts 7.9.3 .1234`
install tzs [version]	Install the specified version of the Tanium Zone Server role. Run the command without a version to display the available versions found on the Appliance. Usage example: `ssh -qt user@appliance install tzs 7.9.3 .1234` **Important:** Make sure to import the public key to the Zone Server Appliance before you run this command (TanOS menu 2-I).The public keys are stored in the tanium-init.dat file. For detailed steps, see Import the Tanium Server public key file to the Zone Server on page 178 .
manage ldaps <action>	Manage the LDAPS or StartTLS CA certificates used by the Tanium Server. This command has the following actions: • `list` - List the installed certificates • `add` - Add a certificate or certificates. Provide the certificate contents on stdin. • `remove <SHA256>` - Remove the certificate with the specified SHA256 fingerprint. • `print <SHA256>` - Display details for the certificate with the specified SHA256 fingerprint. • `enable` - Enable the LDAPS configuration. • `disable` - Disable the LDAPS configuration. • `alwaysvalidate` - Enable certificate validation. • `nevervalidate` - Disable certificate validation. • `syncpeer` - Synchronize LDAPS settings and certificates to the peer Tanium Server in the cluster. • `copypeer <SHA256>` - Copy the certificate with the specified SHA256 fingerprint to the peer Tanium Server in

©2026 Tanium Inc. All Rights Reserved

Command	Description
	the cluster. • `status` - Display the LDAPS configuration status.
promote tms <user> <serial>	Promote a secondary Tanium Module Server to become the active Module Server in the Array, where `user` is the user name of a Tanium Console user with the Admin role and `serial` is the serial number of the Module Server to promote. You must supply the password of the Tanium Console user on stdin. **Important:** Run this command from an Array Manager Appliance. This command performs the following actions: 1. Stops the Tanium Module Server synchronization target from receiving data from the active Module Server 2. Updates all Tanium Servers in the Array to use the specified Tanium Module Server as the active remote Module Server 3. Registers the selected Tanium Module Server with all Tanium Servers in the Array Usage example: `ssh -q user@appliance promote tms MyAdminConsoleUser 8ca9c7bae2e8ec27-5484b887017201d5 <<< 'mypassword123'`
remove hub	Remove the Tanium Zone Server Hub add-on.
set manifest url { <type> <value> | defaults }	Set the URL of a Tanium manifest. For type, specify `main` or `labs`. For value, specify the URL for the corresponding manifest. To restore the default manifest URLs, use `set manifest url defaults`.
set trusted host list { <hosts> | auto | none }	Set the TrustedHostList on the Tanium Server, Module Server, or All-in-One Appliance, including the TDownloader for each service. This command mirrors the `2 - 2 - 1` menu.

©2026 Tanium Inc. All Rights Reserved

Command	Description
	This command has the following options: • `hosts` - A comma-separated list, with no spaces, of the FQDNs and IP addresses of all Tanium Servers and Module Servers, plus `localhost,127.0.0.1`. • `auto` - Derive the list from the Appliance Array membership. • `none` - Remove the TrustedHostList setting.  **Note:** The `none` option clears the TrustedHostList but does not restore the default. On a Tanium Server, the default is the list of Tanium Server FQDNs, which the Tanium Server regenerates when the `taniumserver` service restarts. To restore the default, use `none` and then restart the service. A Module Server has no default TrustedHostList, so `none` leaves it at its default.
show fingerprint { ts | tzs | hub | soap }	Show the Tanium fingerprint for the Tanium Server (`ts`), the Tanium Server SOAP certificate (`soap`), Tanium Zone Server (`tzs`), or Tanium Zone Server hub (`hub`). Usage example: `ssh -q user@appliance show fingerprint ts`
show manifest urls [json]	Show the URLs for the main and labs Tanium manifests. By default, the URLs are returned in plain text. Use the `json` option to return the URLs in JSON format.
show trusted host list	Show the configured Tanium TrustedHostList. Usage example `ssh -q user@appliance show trusted host list`
sync tms	Copy the contents of the active Tanium Module Server to the standby Tanium Module Server. Run this command in interactive mode using the `-t` option for ssh to ensure proper cleanup after canceling. You can send this command to

©2026 Tanium Inc. All Rights Reserved

Command	Description
	the Array Manager or the active Module Server. Usage example `ssh -qt user@appliance sync tms`
upgrade tanium [version]	Upgrade the Tanium software on the Appliance to the specified version . Run the command without a version to display the available versions found on the Appliance. `ssh -qt user@appliance upgrade tanium` 7.9.3 `.1234`

Appliance Array commands

Appliance Array commands for Tanium Appliance CLI

Command	Description
add array member <ip_address>	Add another Appliance with the specified IP address to the Appliance Array that is defined on the current Appliance.

©2026 Tanium Inc. All Rights Reserved

Command	Description
	Tip: When you run this command, it might include interactive prompts to trust the new Array member and to enter the password for the new Array member. If you are using this command in a script, you can avoid these prompts as follows: • To avoid a prompt that asks whether to trust the new Array member and continue connecting, you can use the following command to register the fingerprint of the new Array member before you use the `add array member` command to add it: `ssh -qt user@new_Array_member show ssh-host-fingerprints | \ ssh -qt user@Array_manager register ssh-host \ new_Array_member` • To avoid a password prompt when you add an Array member, you can use one of the following methods: • Copy the public key for the `tanadmin` user on the primary Appliance to the `tanadmin` user accounts on the remaining Appliances. For information about how to use TanOS menus to add a public key for a user account, see Manage SSH keys for TanOS users on page 227. For information about how to use the CLI to add a public key for a user account, see the `add pubkeys` command at TanOS management commands on page 600. • Configure separate public keys for the `tanadmin` user on each Appliance, and then use agent forwarding to authenticate with the added Array members by including the `-A` SSH option in the command.

©2026 Tanium Inc. All Rights Reserved

Command	Description
	`ssh -qtA user@appliance add array member <ip_address>` Agent forwarding requires an SSH agent (such as ssh-agent in OpenSSH) to be running on your local host. For more information, see the documentation for your SSH client.

array assign roles <action>	Use a JSON document to assign the desired roles to Array members and perform necessary setup steps.
	
	This command has the following actions:
	• `show` - Provides a template for the JSON configuration file on stdout.
	Usage example:
	`ssh -q user@appliance array assign roles show > config.json`
	• `dryrun` - Using a JSON configuration file supplied on stdin, display the actions.
	Usage example:
	`ssh -q user@appliance array assign roles dryrun < config.json`
	• `apply` - Using a JSON configuration file supplied on stdin, apply the requested changes.
	Usage example:
	`ssh -q user@appliance array assign roles apply < config.json`
	
	In the JSON configuration file template you retrieve from the `Array assign roles show` command, you must configure the following settings:
	• `password_b64`: The base64-encoded password for the Tanium Console admin user that is specified for the `tanium_username` setting.

©2026 Tanium Inc. All Rights Reserved

Command	Description
	Tip: You can use one of the following commands to base64-encode the password: • Windows: `powershell "[convert]::ToBase64String([Text.Encoding]::UTF8.GetBytes(\"password\"))"` • Non-Windows: `printf 'password' | base64` • `role`: The role to assign for each Array member, using one of the following numeric settings: • `1`: All-in-One • `2`: Tanium Server • `3`: Tanium Module Server • `4`: Tanium Zone Server
array create health-check	Generate a new health check report on each Array member. Any previous reports are deleted. After running this command, the results of the latest report are stored in the health.log file in the /outgoing directory on each Array member.

©2026 Tanium Inc. All Rights Reserved

Command	Description
array restart replication	Restart LDAP replication for the local authentication service to resolve internal LDAP errors.
array self test	Run a self-test on all Array members.
array set trusted host list { <hosts> | auto | none }	Set the TrustedHostList on every Appliance in the Array, including the Tanium Server and Module Server on each member and their TDownloaders. Run this command on the Array Manager. The options are the same as for the `set trusted host list` command; with `auto`, the Array Manager derives the list from Array membership and applies the same value to every member.
array sync partitions	Create backups of the active partitions by copying their contents to the inactive partitions for each affected Appliance in the Array. This may take a while to complete. Tanium services are stopped during the backup. Appliances that do not have alternate partitions are not affected.
array upgrade appliance [--interactive] [version]	Upgrade TanOS on all Appliances in the Array to the specified version. Run this command only on the primary Tanium Server in the Array. Run the command without a version to display the available versions found on the Appliance. Use the `--interactive` flag to respond to confirmation prompts during the upgrade rather than accepting default responses. Requires `ssh -t`. Usage example: `ssh -qt user@appliance array upgrade appliance` 1.9.1 `.1234`
array upgrade tanium [version]	Upgrade the Tanium software on all Appliances in the Array to the specified version. Run the command without a version to display the available versions found on the Appliance. **Important:** Load all RPMs to the incoming directory on the primary Tanium Server before running this command. Usage example: `ssh -qt user@appliance array upgrade tanium` 7.9.3 `.1234`

©2026 Tanium Inc. All Rights Reserved

Command	Description
create array <ip_address> <name of array>	Create an Appliance Array with the specified name (spaces accepted) and add the current Appliance as a member, using the specified IP address.
promote member <serial_number>	Promote an Array member with the Tanium Server role to be an Array Manager. Specify the serial number of the Tanium Server to promote.
demote member <serial_number>	Demote an Array Manager so it can no longer manage the Array. The Appliance remains an Array member. Specify the serial number of the Appliance to demote. To find the serial number of an Appliance, run `report info`. **Important:** Run this command from a different Array Manager, not from the Appliance you are demoting. The Array supports a maximum of two managers; do not demote the last manager, as this leaves the Array unmanageable.
refresh array	Retrieve current membership from the other Appliances in the Array. This information is refreshed on all Appliances in the Array.
reset array	Remove the current Appliance from the Appliance Array.

TanOS management commands

TanOS management commands for Tanium Appliance CLI

Command	Description
create backup <backup_type> [user@SCP_host]>	Create a core or comprehensive backup bundle, and copy it to the /outgoing directory and optionally an SCP destination. For backup_type, use `core` or `comprehensive`.
create health-check	Generate a new health check report. Any previous reports are deleted. After running this command, the results of the latest report are stored in the health.log

©2026 Tanium Inc. All Rights Reserved

Command	Description
	file in the /outgoing directory. If a health check is already running, the command outputs the cached report from the previous run and returns exit code 16. **Tip:** To generate a new health check report on all Array members, use the `array create health-check` command.

create tsg { -list | <tsg-type> } [sftp-destination]	Create a Tanium Support Gatherer (TSG) ZIP file and optionally upload it to an SFTP destination. Specify a `tsg-type`, typically `appliance` or a specific solution.
	
	Use the `--list` option to display the TSG types that are available in your environment.
	
	Optionally, specify the `sftp-destination` in the format `sftp-user@host:destination`. If you include only the user name and host, the TSG is uploaded to the SFTP server's home directory with the default generated file name. If you do not include an `sftp-destination`, the TSG is created in the /outgoing directory.
	
	Note: You can use the `A` option with the `ssh` command to use agent forwarding to authenticate with the SFTP destination. Agent forwarding requires an SSH agent (such as ssh-agent in OpenSSH) to be running on your local host. For more information, see the documentation for your SSH client. Alternatively, you can generate an SSH key pair using the TanOS console for the specified TanOS user and add the public key to the SFTP destination's authorized keys. For more information, see Manage SSH keys for TanOS users on page 227.
	
	Usage examples:
	
	`ssh -qt user@appliance create tsg connect`
	
	`ssh -qtA user@appliance create tsg appliance username@sftphost.example:newfilename.zip`

download package <URL|token>	Download a package from download.tanium.com to the /incoming directory. Specify either the full URL of the download or the token from the URL. **Tip:** No download URL or token is necessary to download an available upgrade package for TanOS. For more information, see command `download package Appliance-upgrade`. Usage examples:

©2026 Tanium Inc. All Rights Reserved

Command	Description

	`ssh -qt user@appliance download package https://download.tanium.com/hGAE28KOIAv0OYVtBIZk5IPv5o_iWBVeAhabcdefghi`
	`ssh -qt user@appliance download package hGAE28KOIAv0OYVtBIZk5IPv5o_iWBVeAhabcdefghi`
	Note:
	This command includes an interactive prompt to confirm the download. You can supply `yes` as a here string on stdin to skip the prompt automatically. For example:
	`ssh -qt user@appliance download package hGAE28KOIAv0OYVtBIZk5IPv5o_iWBVeAhabcdefghi <<< 'yes'`

download package appliance-upgrade <version>	Download an upgrade package for a specific version of TanOS to the `/incoming` directory. Usage example: `ssh -qt user@appliance download package appliance-upgrade` 1.9.1 **Note:** This command includes an interactive prompt to confirm the download. You can supply `yes` as a here string on stdin to skip the prompt automatically. For example: `ssh -qt user@appliance download package appliance-upgrade 1.9.1 <<< 'yes'`
export security key <key_type>	Export the Disk Encryption Key or the GRUB key to the `/outgoing` directory. For `key_type`, specify `raid` or `grub`.
netdiag <action>	View network diagnostics. This command has the following actions: • `check ipsec` - View information about active IPsec tunnels.

©2026 Tanium Inc. All Rights Reserved

Command	Description
	• `show listening ports` - View a list of all detected listening ports. • `show firewall` - View firewall details. • `show array latency` - View the latency between the current Appliance and other Array members.
network <subcommand>	Configure TanOS networking. This command mirrors the `A - 2` menu. This command has the following subcommands: • `interface help` - Show detailed help for the `interface` subcommands. • `interface list` - List the network interfaces. • `interface show` - Show the details for an interface. • `interface set` - Configure an interface. Because this subcommand replaces the configuration for the interface, you must specify every setting that you want to keep, not only the settings that you are changing. • `interface mtu` - Set the MTU for an interface. • `interface up` - Bring an interface up. • `interface down` - Bring an interface down. Use the `--force` option to bring down the interface that carries your session. • `interface reset` - Reset an interface to its default configuration. • `route help` - Show detailed help for the `route` subcommands. • `route list` - List the routes. • `route add` - Add a route. • `route delete` - Delete a route. • `restart` - Restart networking. • `confirm` - Confirm a pending change. • `revert` - Revert a pending change.

©2026 Tanium Inc. All Rights Reserved

Command	Description
	• `pending` - Show the status of a pending change. **Important:** Subcommands that change the configuration apply immediately and then revert automatically after 60 seconds unless you run `network confirm` within that time. This protects you from losing access to the Appliance. To skip the confirmation window, use the `--auto-confirm` option. **Note:** You cannot configure network interfaces on a cloud-based Tanium Appliance .

performance <tool> [options]	Manage performance data collection.
	
	The following tools are available:
	
	• perf record <duration> - Record performance data, where duration is the number of seconds to record.
	
	Usage example:
	
	`ssh -q user@appliance performance perf record 60 -t`
	
	• perf top - Monitor a performance counter in real-time. This command requires the ssh -t option. To exit, press `Q`.
	
	• vmstat <delay> [count] - Monitor virtual memory statistics, where delay is the number of seconds between updates, and count is the number of times to show statistics. For example, if you specify a delay of `3` and a count of `10`, the command shows statistics for ten intervals of three seconds, so the total duration is 30 seconds. If you omit the count, the command returns statistics according to the delay until you press `Ctrl-C`.
	
	Usage example:
	
	`ssh -qt user@appliance performance vmstat 3 10`
	
	• iostat <delay> [count] - Monitor I/O statistics, where delay is the number of seconds between updates, and count is the number of times to show statistics. For example, if you specify a delay of `3` and a count of `10`, the command shows statistics for ten intervals of three seconds, so the total duration is 30 seconds. If you omit the count, the command returns statistics according to the delay until you press `Ctrl-C`.
	
	• pidstat <delay> [count] - Monitor individual processes, where delay is the number of seconds between updates, and count is the number of times to show

©2026 Tanium Inc. All Rights Reserved

Command	Description
	statistics. For example, if you specify a delay of `3` and a count of `10`, the command shows statistics for ten intervals of three seconds, so the total duration is 30 seconds. If you omit the count, the command returns statistics according to the delay until you press Ctrl-C. • htop - Monitor process usage in real-time. This command requires the ssh -t option. To exit, press `Q`. Usage example: `ssh -qt user@appliance performance htop` • iotop - Monitor I/O usage in real-time. This command requires the ssh -t option. To exit, press `Q`. Options: • `-t` - Limit results to Tanium-related process. This option is unavailable for the iostat and pidstat tools. • `-D` - Data clean-up, for when a command is interrupted.
reboot appliance [--force]	Reboot the Appliance. This command includes an interactive prompt to confirm the reboot. You can supply yes as a here string on stdin to skip the prompt automatically. For example: `ssh -qt user@appliance reboot appliance <<< 'yes'` Use the `--force` flag to skip the confirmation prompt and stop any existing maintenance action before rebooting. The reboot runs in the background and the SSH session returns immediately.
report info [text|json]	Report basic information for the Appliance, including the serial number, Server name, TanOS version, role, and Tanium version. Specify `json` to output the report in JSON format. The default format is `text` . This command is available to users with the `tanuser` role.
reset software	Removes all Tanium Core Platform software from the Appliance, but preserves TanOS settings such as network and system user configuration.

©2026 Tanium Inc. All Rights Reserved

Command	Description
	Note: This command includes an interactive prompt to confirm the reset. You can supply `yes` as a here string on stdin to skip the prompt automatically. For example: `ssh -qt user@appliance reset software <<< 'yes'`
rotate security key grub	Generate a new GRUB key
security export aide	Export the last run Advanced Intrusion Detection Environment (AIDE) report to the `/outgoing` directory.
security initialize aide	Enable AIDE and weekly AIDE reports.
security run aide	Manually run an AIDE report.
security set <setting> <value>	Configure advanced security settings. Available settings, with the available values for each setting, are as follows: • fips - FIPS mode • enabled • disabled • aide - AIDE reporting • disabled To enable AIDE, use security initialize aide.

©2026 Tanium Inc. All Rights Reserved

Command	Description
	• selinux - Security-Enhanced Linux (SELinux) mode • enforcing • permissive **Note:** TanOS configures SELinux in enforcing mode with the targeted policy during initial startup. All TanOS user accounts are mapped to the `staff_u` SELinux user. • menu_timeout - The time TanOS menus wait for input before canceling user sessions • 0 (timeout disabled) • Timeout value in seconds **Note:** Enabling FIPS mode includes an interactive prompt. You can supply `yes` as a here string on stdin to skip the prompt automatically. For example: `ssh -q user@appliance security set fips enabled <<< 'yes'`
security show [json]	Show advanced security settings. To return settings in JSON format, specify `json`.
`service <action>`	Control Tanium Core Platform and TanOS services This command has the following actions:

©2026 Tanium Inc. All Rights Reserved

Command	Description
	• `list [service|alias] [service|alias] ...` - List controllable services with the basic status for each service. Specify an alias to list a specific group of services, or specify service names to view the basic status of those services. • `status <service|alias> [service|alias] ...` - Display detailed status and activity for each specified service or each service indicated by a specified alias. • `start <service|alias> [service|alias] ...` - Start each specified service or each service indicated by a specified alias. • `stop <service|alias> [service|alias] ...` - Stop each specified service or each service indicated by a specified alias. • `restart <service|alias> [service|alias] ...` - Restart each specified service or each service indicated by a specified alias. • `enable <service|alias> [service|alias] ...` - Enable each specified service or each service indicated by a specified alias. • `disable <service|alias> [service|alias] ...` - Disable each specified service or each service indicated by a specified alias. • `is-enabled <service|alias> [service|alias] ...` - Display whether each specified service or each service indicated by a specified alias is enabled. • `is-active <service|alias> [service|alias] ...` - Display whether each specified service or each service indicated by a specified alias is active. • `is-failed <service|alias> [service|alias] ...` - Display whether each specified service or each service indicated by a specified alias has failed. You can indicate multiple services using the following aliases: • `all` - All controllable services • `all_tanium` - All Tanium Core Platform services, except for database services • `all_db` - All database services • `all_os` - All TanOS services • `all_ts` - All Tanium Server services • `all_tms` - All Module Server and module services

©2026 Tanium Inc. All Rights Reserved

Command	Description

	Usage examples:
	`ssh -qt user@appliance service list`
	`ssh -qt user@appliance service status all_tanium`
	`ssh -qt user@appliance service restart taniumserver.service`

set backup key	Set the public key to encrypt backup files. The public key must be in PEM format. When the key is imported successfully, the command displays the key ID.
set fqdn	Set the FQDN for the Appliance. This command is available only when the Appliance does not have a role installed. Usage example: `ssh -q user@appliance set fqdn Appliance.example.com`
set nameservers	Set one or more DNS name servers for the Appliance. Any existing name servers are overwritten. Usage example: `ssh -q user@appliance set nameservers 8.8.8.8 9.9.9.9`
set ntp <server1> [server2]	Set NTP servers for the Appliance. To configure an NTP server that requires authentication, you can specify a colon-separated value for the argument that contains the server name, key ID, key type, and key value. Usage example: `ssh -q user@appliance set ntp ntp.secret.corp:42:SHA1:bfb7759a67daeb65410490b4d98bb9da7d1ea2ce`
show nameservers	Show the DNS name servers for the Appliance.
show ntp	Show the NTP servers that are configured and connection information. This command is available to users with the `tanuser` role.

©2026 Tanium Inc. All Rights Reserved

Command	Description
show ssh-host-fingerprints	Show the SSH host fingerprints.
sync partitions	Create a backup of the active partition by copying its contents to the inactive partition. This may take a while to complete. Tanium services are stopped during the backup.
upgrade appliance [--interactive] [version]	Upgrade TanOS to the specified version on the Appliance. Run the command without a version to display the available versions found on the Appliance. Use the `--interactive` flag to respond to confirmation prompts during the upgrade rather than accepting default responses. Requires `ssh -t`. Usage example: `ssh -qt user@appliance upgrade appliance` 1.9.1

TanOS user management commands

TanOS user management commands for Tanium Appliance CLI

Command	Description
add pubkeys	Add entries to the authorized_keys file for the user. The command prompts you to paste the contents of keys to add, or you can provide the key file or contents on stdin. This command is available to users with the `tanuser` role. Usage example: `ssh -qt user@appliance add pubkeys < ~/.ssh/my-key.pub`

©2026 Tanium Inc. All Rights Reserved

Command	Description
	Tip: You can use the `ssh-copy-id` command in OpenSSH to add an SSH public key from your local host to any TanOS user with the `tanadmin` role on the Tanium Appliance. For example: `ssh-copy-id -i public_key_file user@appliance`
configure mfa <action>	Configure authentication requirements and multifactor settings. This command has the following actions: • `show global [json]` - Show the global authentication requirements and multifactor settings. Specify `json` to output JSON format. • `enable global <auth_type>` - Enable global password requirement, key requirement, or multifactor authentication. For auth_type, specify `key`, `password`, or `mfa`. **Important:** To make sure an admin user can still sign in through SSH after you enable multifactor authentication, you must either exempt at least one admin user or configure multifactor authentication individually for at least one admin user before you enable multifactor authentication globally. • `disable global <auth_type>` - Disable global password requirement, key requirement, or multifactor authentication. For auth_type, specify `key`, `password`, or `mfa`. • exempt user <user_name> - Exempt the specified user from global multifactor authentication requirements. • reset global - Reset global password, key, and multifactor authentication requirements to optional. • show user <user_name> - Show the account requirements and multifactor settings for the specified user. • enable user gauth <user_name> - Configure Google Authenticator multifactor authentication for a user.

©2026 Tanium Inc. All Rights Reserved

Command	Description

	Note: You must use the `-t` option to run SSH in terminal mode for TanOS to display the QR code during MFA setup; otherwise, TanOS displays only the URL.
	• reset user <user_name> - Reset the multifactor authentication settings for the specified user.
	Usage examples:
	`ssh -q user@appliance exempt user backup-admin`
	`ssh -q user@appliance enable global mfa`

copy pubkeys tancopy	Copy the SSH keys for the current user to the authorized_keys file for the `tancopy` user account.

delete pubkeys	Remove entries from the authorized_keys file for the user. The command prompts you to paste the contents of keys to delete, or you can provide key contents on stdin.
	Tip:
	Use the following command to list the contents of the authorized_keys file. You can copy the contents of individual keys from the provided list.
	`ssh -qt user@appliance show pubkeys authorized_keys`
	This command is available to users with the `tanuser` role.
	Usage example:
	`ssh -qt user@appliance delete pubkeys < key-to-delete.pub`

ldap-auth <action>	Configure LDAP authentication for TanOS users. This command has the following actions:

©2026 Tanium Inc. All Rights Reserved

Command	Description

	• `config list` - Display the current TanOS LDAP configuration.
	• `config get <setting>` - Display the value of the specified setting on page 610.
	• `config set <setting> <value>` - Set the value of the specified setting on page 610.
	• `config enable` - Enable the TanOS LDAP configuration with the current settings.
	• `config disable` - Disable the TanOS LDAP configuration.
	• `config validate` - Validate whether the required settings are configured.
	Note: This action does not check the server connection.
	• `config password` - Set the password for the user used to sign in and query the directory. This command prompts you to enter the password, or you can provide the password on stdin.
	Usage example:
	`ssh -qt user@appliance ldap-auth config password <<< 'my_ldap_password'`
	Tip:
	Configure the user name in the `bind_dn` setting:
	`ssh -qt user@appliance ldap-auth config set bind_dn <user_name>`
	• `config import` - Import the TanOS LDAP configuration from the /incoming directory on the Appliance.
	• `config export` -Export the TanOS LDAP configuration from the /outgoing directory on the Appliance.
	• `config install` - Import a TanOS LDAP configuration supplied on stdin.
	• `config reset` - Reset the TanOS LDAP configuration.

©2026 Tanium Inc. All Rights Reserved

Command	Description
	• `cert install` - Install the LDAP server root CA certificate supplied on stdin. • `cert import` - Import a LDAP server root CA certificate from the /incoming directory on the Appliance. • `cert export` -Export the LDAP server root CA certificate to the /outgoing directory on the Appliance. • `verify group <groupname>` - Verify that an LDAP query returns a specific group. • `verify user <username>` - Verify that an LDAP query returns a specific user. • `status sssd` - Display the status of the sssd service. • `status counts` -Display counts of users and groups. • `status users` - Display the list of visible users. • `status groups` - Display the list of visible groups. • `status privileges` - Display roles for visible users. • `settings` - Display the list of available settings for the TanOS LDAP configuration. The following TanOS LDAP settings are configurable with the `ldap-auth config set` command: • `attribute_sshkey`- The LDAP attribute that contains the SSH public key for each user • `base_dn` - The base DN from which TanOS queries the directory • `bind_dn` - The user name used to sign in to and query the LDAP server in a format accepted by the server **Tip:** Configure the password using the `ldap-auth config password` command. • `debug_level` - The logging level for the configured domain (`0`-`9`) • `domain_name` - The domain by which the system and logs refer to the LDAP configuration. This setting does not affect the connection to the LDAP server. • `filter_groups` - The LDAP search filter to use to limit the groups that the LDAP server returns for the query. Leave this setting blank to return all groups under the base search DN.

©2026 Tanium Inc. All Rights Reserved

Command	Description
	• `filter_users` - The LDAP search filter to use to limit the users that the LDAP server returns for the query. Leave this setting blank to return all users under the base search DN. • `ldap_enabled` - Specifies whether LDAP authentication is enabled for authenticating TanOS system users (`true` or `false`) • `ldap_host` - The host name of the LDAP server • `ldap_port` - The port on which to connect to the LDAP server • `ldap_referrals` - Specifies whether TanOS allows the LDAP server to refer the query to other connected LDAP servers when you have multiple LDAP servers in your organization (`true` or `false`) • `ldap_schema` - The schema used by the LDAP server (`ad`, `rfc2307`, `rfc2307bis`, or `ipa`) • `mappings_tanadmin` - A pipe-delimited list of LDAP groups that are granted the `tanadmin` role • `mappings_tanuser` - A pipe-delimited list of LDAP groups that are granted the `tanuser` role
local-auth <action>	Manage Tanium Console user accounts in the local authentication service when it is enabled. For more information, see Configure the local authentication service for Tanium Console users on page 294 . This command has the following actions: • local-auth add user <user_name> <first_name> <last_name> - Add a Tanium Console user account with the specified user name, first name, and last name to the local authentication service. This command prompts for the password for the new user when run interactively, or you can supply the password on stdin. • local-auth delete user <user_name> - Delete the specified Tanium Console user account from the local authentication service. • local-auth list users - List Tanium Console user accounts in the local authentication service. • local-auth set password <user_name> - Change the password for the specified Tanium Console user account in the local authentication service. This command prompts for the new password when run interactively, or you can supply the new password on stdin. Usage example:

©2026 Tanium Inc. All Rights Reserved

Command	Description
	`ssh -q user@appliance local-auth set password SomeConsoleUser <<< 'new-console-password'` • local-auth unlock user <username> - Unlock a Tanium Console user account in the local authentication service.

register ssh-host <remote_host> [scan]	Add entries to SSH known_hosts file for the current user.
	You can provide fingerprints for the remote host on stdin, or you can use the scan option to automatically discover and add the fingerprints of a remote host.
	For example:
	`ssh -q user@Array_manager register ssh-host 192.168.15.115 < fingerprints.txt`
	`ssh -q user@Array_manager register ssh-host 192.168.15.253 scan`
	Best Practice: For a higher level of security, explicitly provide the fingerprints that you have verified to belong to the remote host on stdin instead of using the `scan` option.

show pubkeys <key_type>	Show the SSH public keys for the current user. Key types: • `identity` - Show the identity public key file for the user (id_rsa.pub). • `authorized_keys` - Show entries in the authorized_keys file for the user.
set password	Change the password for the current user. This command prompts for the new password when run interactively, or you can supply the new password on stdin. This command is available to users with the `tanuser` role. Usage example: `ssh -q user@appliance set password <<< 'my-new-password'`
`system-auth <action>`	Manage TanOS system users. This command has the following actions:

©2026 Tanium Inc. All Rights Reserved

Command	Description
	• list users - List all TanOS system users. • show user <user_name> - Show the details of the specified TanOS system user. • add user <user_name> <first_name> <last_name> [options] - Add a TanOS system user with the specifier user name, first name, and last name. The following options are available: • --role - Specify `tanadmin` or `tanuser`. The default is `tanadmin`. • --sshkey - Add an SSH key for the user. If you specify this option, you must provide a single SSH public key on stdin. • --nopassword - Disable password authentication for the user and require an SSH key for sign-in on SSH connections. Usage example: `ssh -q user@appliance add user NewUser John Smith --sshkey < pubkey.pub` • reset ssh lockout <user_name> - Reset a specified TanOS system user who is locked out from sign-in on SSH connections. • change password <user_name> - Reset the password for another TanOS system user. The command randomly generates and displays a new password for the specified user. **Note:** If you specify the user who is currently signed in rather than another user, the command behaves the same as set password, and you can either provide a new password on the standard input stream or set a password at the interactive prompt. You cannot specify a new password for another user. • disable password access <user_name> - Disable password authentication for the specified TanOS system user and require an SSH key for sign-in on SSH connections. • enable user <user_name> - Enable the specified TanOS system user.

©2026 Tanium Inc. All Rights Reserved

Command	Description
	• disable user <user_name> - Disable the specified TanOS system user. • protect user <user_name> - Protect a user account with the `tanadmin` role, which prevents it from being disabled or deleted. • unprotect user <user_name> - Unprotect a user account. • delete user <user_name> - Delete the specified TanOS system user.

Examples

Show a list of commands

Command:

```
ssh -q tanadmin@10.10.10.55 help
```

Example response:

```
The following commands are available in the TanOS CLI.

Tanium Platform
 install aio: Install the All-in-One role
 install ts: Install the Tanium Server role
 install tms: Install the Tanium Module Server role
 install tzs: Install the Tanium Zone Server role
 add hub: Add a Zone Server Hub to a TS or AiO
 remove hub: Remove the Tanium Zone Server Hub
 upgrade tanium: Upgrade Tanium software
 configure module service: Configure the Tanium Server to use a Module Server
 register module service: Register the Tanium Module Server

TanOS Appliance Array
```

©2026 Tanium Inc. All Rights Reserved

```
 create Array: Create a new Appliance Array
 reset Array: Reset this Appliance's Array configuration
 add Array member: Add a Member to the Array

TanOS Management
 report info: Report information about the Appliance
 reset software: Reset the software on the Appliance
 upgrade Appliance: Upgrade the Appliance
 set backup key: Set the Backup Encryption Key
 copy pubkeys tancopy: Copy the user's SSH keys to tancopy

To see more information about each command, run it with the option "help". E.g.
ssh -qt user@appliance install ts help
```

Show help for the install aio command

Command:

```
ssh -q tanadmin@10.10.10.55 install aio help
```

Example response:

```
Install the All-in-One role

Installs the All-in-One role (TaniumServer and TaniumModuleServer) onto the Appliance. This option requires the password to be
used for the 'tanium'
console user.

Usage:   install aio <version>
Example: ssh -qt user@appliance install aio 7.9.3.1234
Menu:    1-1
```

Install the Tanium Zone Server Hub add-on

Command:

©2026 Tanium Inc. All Rights Reserved

```
ssh -q tanadmin@10.10.10.55 add hub
```

Example response:

```
staging /opt/utils/installers/TaniumZoneServer-7.9.3.1234-1.x86_64.rpm
Checking RPM signatures
Signature verification succeeded.
Installing Tanium Zone Server
Preparing packages...
TaniumZoneServer-7.9.3.1234-1.x86_64
TaniumZoneServer service installed. Complete installation by:
1. Set ServerName with '/opt/Tanium/TaniumZoneServer/TaniumZoneServer config set ServerName <name>'
2. Set any desired optional settings (ServerPort, LogVerbosityLevel, etc) by running '/opt/Tanium/TaniumZoneServer/
TaniumZoneServer config set <key> <value>'
3. Copy tanium-init.dat file into /opt/Tanium/TaniumZoneServer/TaniumZoneServer
4. Enable the TaniumZoneServer with 'systemctl enable taniumzoneserver'
5. Start the TaniumZoneServer with 'systemctl start taniumzoneserver'
If you are configuring this to be a TaniumZoneServer Hub do the following:
1. '/opt/Tanium/TaniumZoneServer/TaniumZoneServer config set ZoneHubFlag 1'
2. Create a file named ZoneServerList.txt in the /opt/Tanium/TaniumZoneServer/ directory with the ip addresses/FQDNs of the
ZoneServers
Tanium Zone Server Installation completed
Configuring Zone Server Hub
 Add-On Zone Server Hub install - copied public key
Tanium Zone Server Installation completed
```

Retrieve Appliance information

Command:

```
ssh -q tanadmin@10.10.10.55 report info
```

Example response:

```
Serial Number:      5c7a65fd-2b96-4732-b2a1-fd9f56b8801e
Name:               ts1
TanOS Version:      1.9.1.1234
Role:               Tanium Server
TaniumServer:       7.9.3.1234
```

©2026 Tanium Inc. All Rights Reserved

Reference: Transfer files to and from the Appliance

During various operations that you perform on the Appliance, you might need to upload or download files. Operations that produce logs or other output place files in the /outgoing directory, from which you can download it. When you must supply a file, you upload it to the /incoming directory. You perform these file transfers using an SFTP client, such as WinSCP in Windows or the sftp utility in macOS or Linux, and connecting as the `tancopy` user. You must have an SSH key configured for the `tancopy` user and use it for authentication.

Configure the SSH key for the tancopy user

Tip: You typically configure this SSH key during initial setup of the Appliances. This information is provided as reference if you need to reconfigure the key.

1. Use an SSH key generator such as ssh-keygen to generate a public/private key pair. Note:
    - Specify an RSA key with 2048 bits (such as ssh-keygen -t rsa -b 2048).
    - Specify a passphrase that is easy to remember.
    - Save the private key to a location that you can access when you set up your SFTP client.
2. Copy the text in the public key file to the clipboard. If you use ssh-keygen, copy the contents of the .pub file that you created.

    Important: In an SSH key exchange, the keys must match exactly, including line endings.
3. Sign in to the TanOS console as a user with the `tanadmin` role.
4. Enter `C-U` (User Administration > TanOS User Management).

©2026 Tanium Inc. All Rights Reserved

5. Enter the line number for the `tancopy` user to go to the user administration menu for this user.

```
           >>> User Administration -> TanOS -> tancopy <<<

Username:         tancopy
Account Enabled:  Yes
Authentication:   SSH Key Only
Password Expires: N/A
SSH Lockout:      No (0)
Multifactor:      Not configured
Protected:        No

Notes:
  * This user account cannot be deleted
  * This user account cannot have a password
  * This user account cannot use multifactor

         A: Manage SSH Authorized Keys
         P: Manage SSH Key Pair
         L: Reset SSH Lockout
         C: [DISABLED] Change Password
         N: [DISABLED] Disable Password Access
         M: [DISABLED] Multifactor Authentication

         E: Enable Account
         D: Disable Account
         T: [DISABLED] Manage Account Protection
         X: [DISABLED] Delete User

         F: Edit known hosts file

         R: Return to previous menu  RR: Return to top

-----------------------------------------------------
```

©2026 Tanium Inc. All Rights Reserved

6. Enter `A` (Authorized Keys).

7. Enter `A` and follow the prompts to add the contents of the public key generated in Step 1.

```
            >>> User Administration -> TanOS -> tancopy -> Authorized Keys -> Add
<<<

Account: tancopy
Please paste the public key and press enter:
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA1ClmgkMrbbxB7jND/Y4/
Giupck35xAuGNKfZWqVLM5F0CNXuTScf6v2z
MDxW5TO5tm/U8P9sqh19RDEzTn2RayXzsoZmXyB8abCCpHG4+03Zv05RHiX4i5QomAMBnbZejdA9/
fGTxO1rPo1rdtTq
Z+KCgzbEhHLWUD44+If5RtG+U4kgyzlYsyjgwhfho+BrRY6e7QYBsXVbuBQ9ROGV6PCTB80jXZVAKrAbsTQ1D
VkpuBue
mftv7vOn3b8MKzJ/IY/
LLL1tIgpSGvgvjr2mOJJ+JoZF2XnPVUFmYiDSCkPAzhCyFHILHfOVAfws9n1G6p3fwILqNhvB
oPeaCFaApQ== rsa-key-20200123
 Validating input
 Adding key to authorized keys after validation
 Finished adding authorized keys for tancopy



 Press enter to continue
```

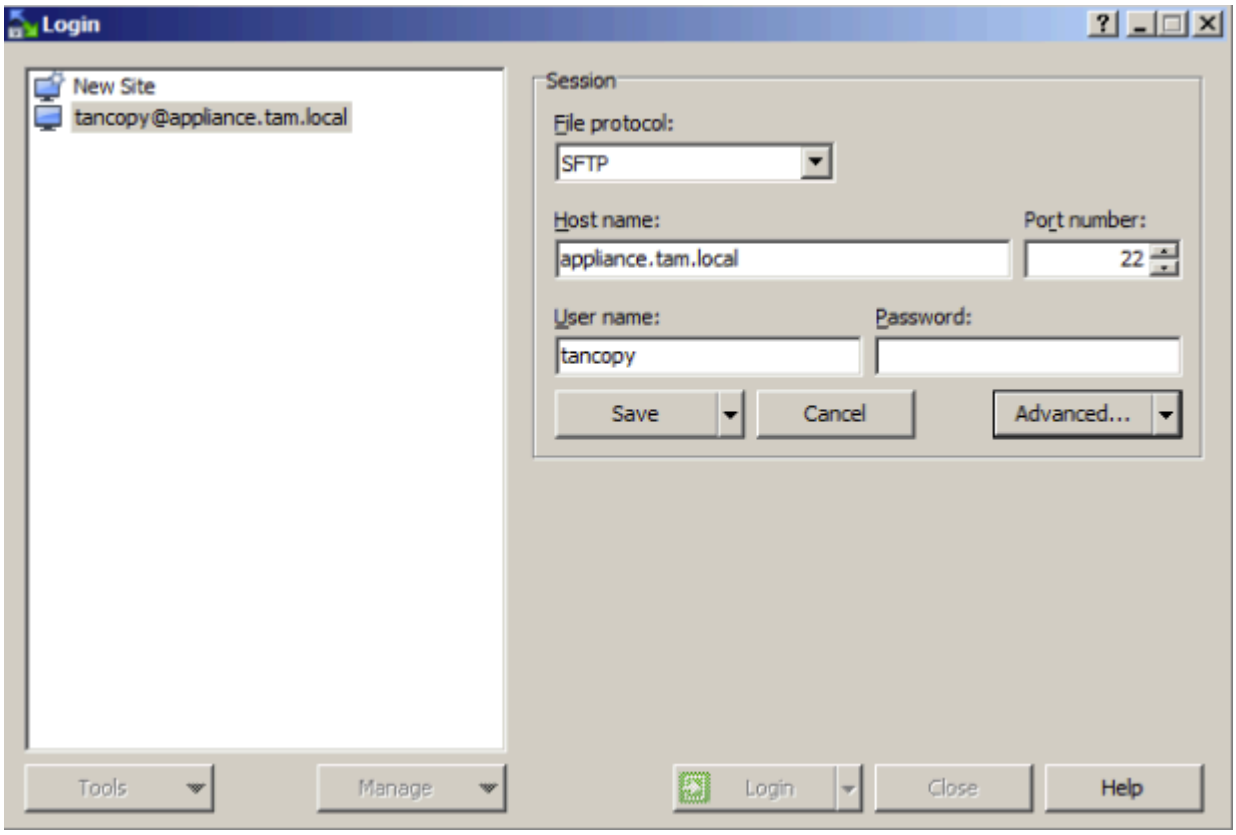
Connect using SFTP to transfer files

Use an SFTP client on your management computer, such as WinSCP in Windows or the sftp utility in macOS or Linux, to connect to the Tanium Server Appliance. The following steps demonstrate configuring the connection in WinSCP:

1. Specify `tancopy` for user name.

   Figure 54. WinSCP user name set to tancopy

©2026 Tanium Inc. All Rights Reserved

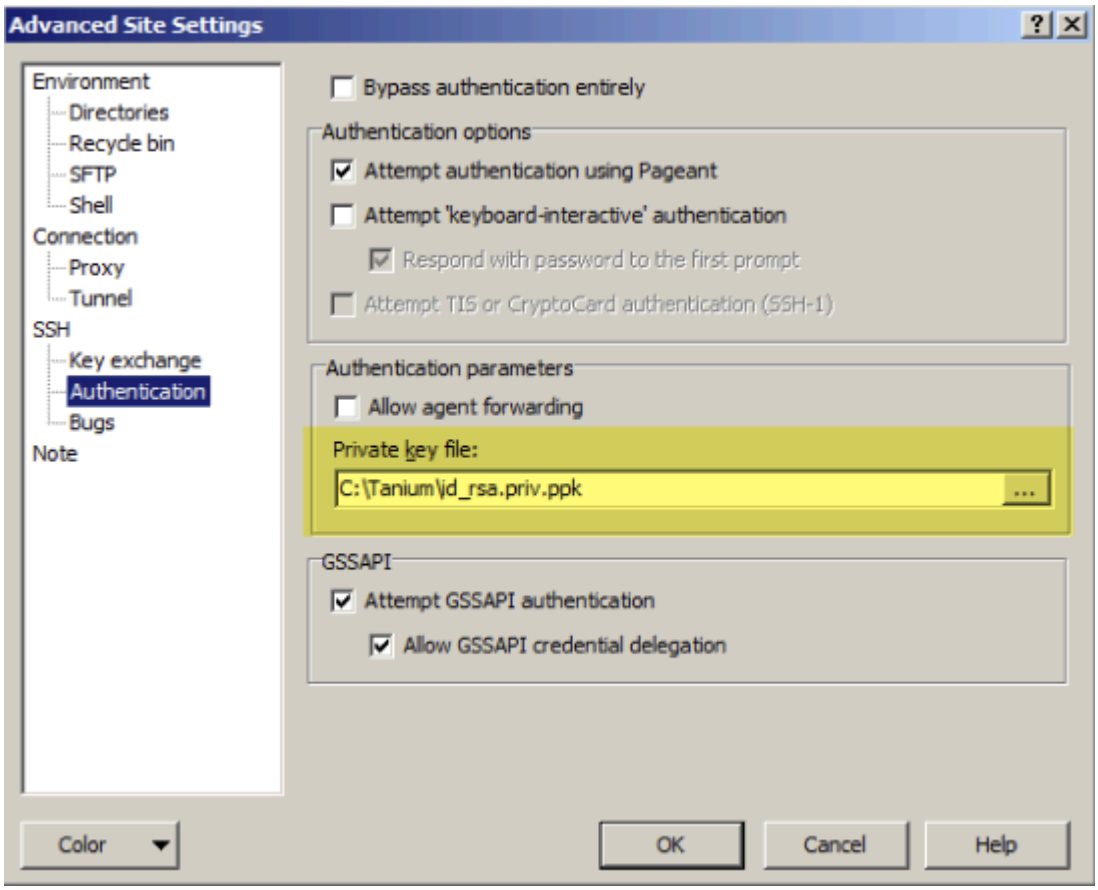


2. Click **Advanced**.

3. Under SSH, browse and select the private key that pairs with the public key uploaded to the Appliance.

   Figure 55. Selecting the private key in WinSCP

©2026 Tanium Inc. All Rights Reserved

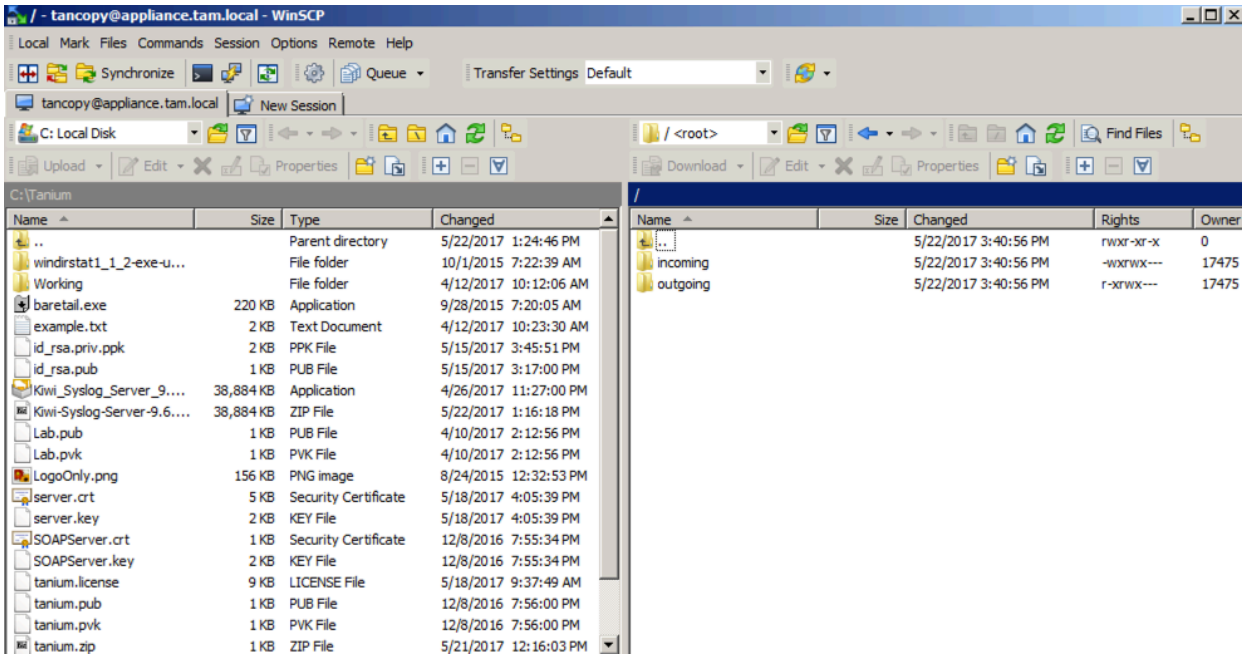


4. Save the configuration and click **Login** to initiate the connection.

   Connect to the Appliance and make sure you can access the /incoming and /outgoing directories.

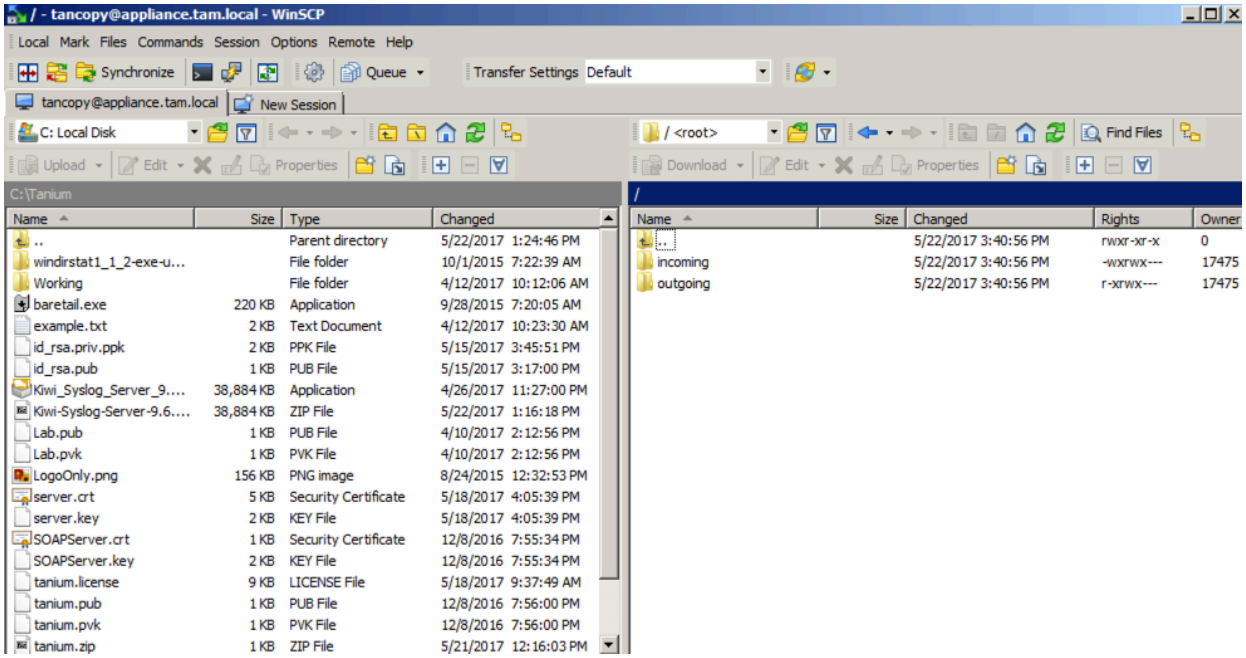
   Figure 56. Verifying the SFTP connection in WinSCP

©2026 Tanium Inc. All Rights Reserved



After you connect to the Appliance, upload files to the /incoming directory, and download files from the /outgoing directory.

Figure 57. Testing file transfer in WinSCP



©2026 Tanium Inc. All Rights Reserved

Reference: Tanium Core Platform command-line interface in an Appliance deployment

In special cases, such as troubleshooting specific issues with assistance from Tanium Support, you might use the command-line interface (CLI) on Tanium Core Platform Servers to configure platform settings.

Tip:

- Typically, you change platform settings through Tanium Console or the TanOS menu. For more information, see Managing Tanium Core Platform settings and Manage Tanium Core Platform settings on Tanium Appliances on page 314.
- For more information about the TanOS CLI, which is separate from the Tanium Core Platform CLI, see Reference: TanOS command line interface on page 587.

Important:

- Contact Tanium Support on page 510 for guidance before you create, edit, or delete platform settings.
- You must be granted read-write shell access before using this CLI. For more information, see Request read-write restricted shell or full shell access on page 507.

The following table lists the locations where the CLI programs reside. For descriptions of the settings that you can edit, see Reference: Deployment-related Tanium Core Platform settings in an Appliance deployment on page 632.

©2026 Tanium Inc. All Rights Reserved

CLI executables on Tanium Appliances

Component	CLI program location
Tanium Server	/opt/Tanium/TaniumServer/TaniumServer
Tanium Module Server	/opt/Tanium/TaniumModuleServer/TaniumModuleServer
Tanium Zone Server	/opt/Tanium/TaniumZoneServer/ZoneServer
TDownloader: Tanium Server	/opt/Tanium/TaniumServer/TaniumTDownloader
TDownloader: Module Server	/opt/Tanium/TaniumModuleServer/TaniumTDownloader

CLI examples

The following examples show how to use the CLI.

Display help

```
cmd-prompt>

 --help
Usage:

 [options] <command> [<args>]

General Options:
  -h [ --help ]         Print this help message
  -v [ --version ]      Print the version
  --verbose             Verbose output

Service Options:
  -i                    Install the service
  -u                    Uninstall the service
  -s                    Start the service
  -e                    Stop the service

Internal Tanium Options - DO NOT USE:
  -d                    Run without daemonizing

Commands:
  config                Manage configuration
  clean-downloads       Clean the downloads catalog
  database              Manages a database
  global-settings       Manages global settings
  license               Manages Deployment License
  pki                   Manages PKI
  registration-secret   Manages Client registration secrets
  server-registrations  Manages Server registration requests
  test-hsm              Test an HSM configuration
  trust-module-certs    Add trusted Module Server certificates
```

©2026 Tanium Inc. All Rights Reserved

```
For help on a specific command run `

 COMMAND -h`
```

Display config help

```
cmd-prompt>

 config --help
Usage:

 config <action> [<key>] [<value>]

Actions:
  config list                          List all keys and non-protected values
  config list-protected                List all keys and values
  config get <key>                     Print non-protected config value
  config get-protected <key>           Print config value
  config set <key> <value>             Set config value and try to guess type
  config set-string <key> <value>      Set string value
  config set-protected <key> <value>   Set protected string value
  config set-number <key> <value>      Set numeric value (in decimal or hex notation)
  config remove <key>                  Remove config value
```

Example: List configuration settings

When displaying the current settings, note that the CLI output displays `(protected)` instead of the actual value for settings that are designated as protected, which means they are sensitive in the security sense.

```
cmd-prompt>

 config list
Keys:
  - AddressMask: 16777215
  - ConsoleSettingsJSON: C:\Program Files\Tanium\Tanium Server\http\config\console.json
  - DBUserDomain: tam.local
  - DBUserName: taniumsvc
  - LogPath: C:\Program Files\Tanium\Tanium Server\Logs
  - LogVerbosityLevel: 1
  - Logs:
    - Logs.MiniDumpMessages:
      - Logs.MiniDumpMessages.FilterRegex: .*Begin MiniDumper.*
      - Logs.MiniDumpMessages.LogVerbosityLevel: 1
  - ModuleServer: tms1.tam.local,TMS1.tam.local:17477
  - ModuleServerPort: 17477
  - PGDLLPath: C:\Program Files\Tanium\Tanium Server\postgres\bin
  - PKIDatabasePassword: (protected)
  - PGRoot: C:\Program Files\Tanium\Tanium Server\postgres
  - Path: C:\Program Files\Tanium\Tanium Server
  - ProxyPassword: (protected)
  - ProxyPort:
  - ProxyServer:
  - ProxyType: NONE
  - ProxyUserid:
  - SQLConnectionString: postgres:localhost@dbname=postgres port=5432
```

©2026 Tanium Inc. All Rights Reserved

```
  - ServerName: 0.0.0.0
  - ServerPort: 17472
  - ServerSOAPPort: 443
  - TrustedCertPath: C:\Program Files\Tanium\Tanium Server\Certs\installedcacert.crt
  - TrustedModuleServerCertsPath: C:\Program Files\Tanium\Tanium Server\trusted-module-
servers.crt
  - Version: 7.9.3.1234
```

Example: Set configuration values

```
cmd-prompt>

 config set BypassProxyHostList host1.example.com,192.168.0.1
cmd-prompt>

 config get BypassProxyHostList
host1.example.com,192.168.0.1
```

Example: Set configuration values

```
cmd-prompt>

 config set ProxyServer 192.168.0.2
cmd-prompt>

 config get ProxyServer
192.168.0.2
```

Example: Configure global settings

```
cmd-prompt>

 global-settings -h
Usage:

 global-settings list|list-all|get|set|set-string|set-numbe
r|set-flags|unset-flags|remove

  -c [ --command ] arg  Command to run:
                            list
                            list-all
                            get <setting>
                            set <setting> <value>
                            set-string <setting> <value>
                            set-number <setting> <value>
                            set-flags <setting> [public|hidden|read-only|server...]
                            unset-flags <setting> [public|hidden|read-only|server ...]
                            remove <setting>

cmd-prompt>

 global-settings set ReportingTLSMode 0
```

Example: Add an administrator user

```
cmd-prompt>
```

©2026 Tanium Inc. All Rights Reserved

```
 -h
Usage:

 database create|upgrade|create-admin-user

  -c [ --command ] arg  Command to run:
                            create
                            upgrade
                            create-admin-user [username] [domain]
                             sqlserver2postgre outputfile

cmd-prompt>

 database create-admin-user admin-recover tam.local
```

©2026 Tanium Inc. All Rights Reserved

Reference: Deployment-related Tanium Core Platform settings in an Appliance deployment

While you configure the most critical Tanium Core Platform Server settings during initial installation, you can configure additional deployment-related settings afterward.

This section lists many of the deployment-related settings that you might need to change for your environment.

Tip:

You can change most Tanium Core Platform Server settings through Tanium Console. For more information, see Managing Tanium Core Platform settings.

For a reference of all Tanium Core Platform settings Reference: Tanium Core Platform settings.

To configure Tanium Client settings, see Tanium Client CLI and Client settings.

Contact Tanium Support on page 510 for help configuring settings for your deployment.

©2026 Tanium Inc. All Rights Reserved

Configure settings in TanOS

You can change most settings through Tanium Console (see Managing Tanium Core Platform settings), but if the Console is unavailable, you can use the following steps to configure these settings.

1. Sign in to the TanOS console as a user with the `tanadmin` role.
2. Enter `2`-`2` (Tanium Operations > Configuration Settings).
3. Enter the line number for the Tanium Core Platform Server on which to modify settings.
4. Use the menu to view and edit settings. Enter the line number for a setting to edit that setting, or enter `A` to add a new setting.

Deployment-related settings reference

Platform settings used during deployment

Settings	Platform components	Guidelines
AddressMask	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 510 for guidance before configuring this setting. For more information about the setting, see AddressMask .
AddressPrefixIPv6	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 510 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 AddressPrefixIPv6 .

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
AllowedHubs	Tanium Server (local) Zone Server	Configure this setting based on the server type. • 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.
BypassCRLCheckHostList	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 this setting in the TDownloader configuration on the Tanium Server and Module Server. If you configure the Tanium Server and Module Server to access Internet sites through a proxy server, you can configure BypassCRLCheckHostList through Tanium Appliance . For more information, see Configuring proxy server settings .
BypassProxyHostList	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 this setting in the TDownloader configuration on the Tanium Server and Module Server. For more information, see Configuring proxy server settings .
ConsoleSettingsJSON	Tanium Server	Path to the Tanium Console settings file.
content_base_url	Tanium Server	Do not edit this setting, which is automatically set to `https://fqdn/content` for air-gapped environments when you

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
		import air gap content (where `fqdn` is the fully qualified domain name of the Appliance on which you are installing the update).
DefaultHeaders	Tanium Server	The HTTP headers returned when a browser accesses Tanium Console. You can use this setting to enable HTTP Strict Transport Security (HSTS). For more information, see (Optional) Enable HTTP Strict Transport Security for Tanium Console access . Otherwise, do not change this setting unless Tanium Support instructs you to do so. **Important:** Do not enable HSTS if you have not installed a CA-issued certificate. Doing so disables access to Tanium Console.
EnforceAllowedHubs	Tanium Server (local) Zone Server	Configure this setting to enable (`1`) or disable (`0`) enforcement of the AllowedHubs setting. EnforceAllowedHubs is a Zone Server setting. The default value is `1` and you must not change it.
ForceIPV6	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 Appliance and Windows deployments. The setting is hidden by default and its default value is `0` . Contact Tanium Support for guidance before adding this setting (see Contact Tanium Support on page 510). For more information about proxy server settings, see Configuring proxy server settings on page 150 .
HubPriorityList	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

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
		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 Servers.
is_airgap	Tanium Server	Do not edit this setting, which indicates an air-gapped environment and is set automatically when you first import air gap content.
LogPath	Tanium Server Module Server Zone Server Tanium Client	The location for Tanium Server logs. The default is /opt/Tanium/TaniumServer/Logs .
LogVerbosityLevel	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 Logging levels on page 512 .  **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.

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
		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.
ModuleServer	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 before editing this setting (see Contact Tanium Support on page 510).
ModuleServerPort	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 before editing this setting (see Contact Tanium Support on page 510).
PKIDatabasePassword	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 .
ProxyPassword	Tanium Server Module Server TDownloader	For a proxy server that requires authentication, enter the password of the ProxyUserid user that establishes a connection with the proxy server. Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. For more information, see Configuring proxy server settings .
ProxyPort	Tanium Server Module Server TDownloader	Specify the proxy server listening port. Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. For more information, see Configuring proxy server settings .
ProxyServer	Tanium Server	Specify the IP address of the proxy server.

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
	Module Server TDownloader	Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. For more information, see Configuring proxy server settings . **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 to `1`.
ProxyType	Tanium Server Module Server TDownloader	Specify the type of proxy server authentication. Configure this setting in the TDownloader configuration on the Tanium Server and Module Server. The possible values are `Basic`, `NTLM`, or `None`. For more information, see Configuring proxy server settings .
ProxyUserid	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. ProxyUserid is a TDownloader setting on the Tanium Server and Module Server. For more information, see Configuring proxy server settings .
ReportingTLSCertPath	Tanium Server Zone Server	Setting for inbound connections. Path to the TLS certificate that was created upon installation. This certificate is used in TLS connections initiated by the Tanium Client, the Tanium Zone Server Hub, or the Tanium Zone Server.
ReportingTLSKeyPath	Tanium Server Zone Server	Setting for inbound connections. Path to the private key file used in TLS connections. This setting must be present to enable TLS.
ReportingTLSMode	Tanium Cloud	This setting applies only to Client 7.2, which Tanium release 2026H1 or later does not support. Upgrade any Client 7.2

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
	Tanium Client 7.2	installations to a new Client version as described in . 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 : • `0` (TLS not used): TLS is disabled. This is the default value. • `1` (TLS required): If a TLS handshake fails, the Tanium Client cannot register or communicate with the Tanium Server or Zone Server. • `2` (TLS optional): The Tanium Client tries to connect over TLS. If the TLS connection fails, the Tanium 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 Tanium Clients establish TLS connections reliably, setting the value to `1` will enforce the best security. For more information, see Securing Tanium Server, Zone Server, and Tanium Client access on page 288 .
RequireIncomingEncryption	Tanium Server Zone Server	Setting for inbound connections. Implicitly set to `0` by default. To set a different value, you must add the setting. • `0` (TLS not required) • `1` (TLS required) Important : When RequireIncomingEncryption is set to 1, only TLS connection requests are processed, so only Tanium Clients that have TLS enabled are able to register and be managed. Do not set this to `1` until you are sure all Tanium Clients that have been deployed are configured to use TLS (ReportingTLSMode=1 or ReportingTLSMode=2), and you are ready to deploy Tanium Client to new endpoints with TLS configured prior to initial registration.
ServerName	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 for guidance before changing this setting (see Contact Tanium Support).

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
		 **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 ServerName .  **Best Practice:** If you are manually configuring this setting, specify an FQDN. **Tip:** If you deploy an action to configure this setting on the Tanium Client, use the **Set Tanium Server Name** or **Set Tanium Server Name [Non-Windows]** package.
ServerNameIPv6	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 for guidance before adding this setting (see Contact Tanium Support on page 510).
ServerPort	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 and Server: For information about updating the port, see 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`.

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
		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 ServerPort. **Note:** If you configure the ListenPort or EnableRandomListeningPort setting, it overrides ServerPort for client-client communication. For more information, see Customize listening ports.
ServerSOAPPort	Tanium Server (local)	Specify the port for Tanium Appliance 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 Install the Tanium Server.
SQLConnectionString	Tanium Server (local)	Specify connection information for the Tanium database server, such as in the following examples: `postgres:<server IP address>@user=postgres dbname=tanium sslmode=require sslcert=/opt/Tanium/.postgresql/postgresql.crt sslkey=/opt/Tanium/.postgresql/postgresql.key sslcompression=1` For the supported PostgreSQL keywords, such as `dbname`, `port`, and `user`, see the PostgreSQL documentation. **Important:** If you change this setting, you must restart the Tanium Server: For more information, see Start, stop, and restart Tanium services.
SSLCipherSuite	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

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
		`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 Supported cipher suites on page 291 .
SSLHonorCipherOrder	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 633 setting. The Server applies an order of preference from left to right when selecting from the ciphers that SSLCipherSuite lists. For more information, see Supported cipher suites on page 291 .
TrustedCertPath	Tanium Server TDownloader	Path to the certificate file used for secure connections to the Tanium Console port.
TrustedHostList	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]`). TrustedHostList is a TDownloader setting on the Tanium Server and Module Server. For more information, see Configuring proxy server settings .
Version	Tanium Server (local) Module Server	Do not edit this setting, which indicates the Server or Client version.

©2026 Tanium Inc. All Rights Reserved

Settings	Platform components	Guidelines
	Zone Server Zone Server Hub Tanium Client	
ZoneHubFlag	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 the setting through the TanOS console. For more information, see Manage Tanium Core Platform settings .

©2026 Tanium Inc. All Rights Reserved

Reference: Tanium Appliance sizing and specifications

This page lists deployment sizing and specifications for the physical Tanium Appliance, cloud-based Tanium Appliance, and the virtual Tanium Appliance.

Note: Any modification to the Licensed Software by Customer or any third-party or failure by Customer to implement any Enhancements to the Licensed Software may void Tanium's obligation to provide Support Services and Tanium's warranties.

Tanium Appliance options and sizing

Tanium Appliance sizing options by endpoint count and role

Role	< 10,000 Endpoints	< 35,000 Endpoints	< 50,000 Endpoints	< 100,000 Endpoints	< 200,000 Endpoints	< 500,000 Endpoints	> 500,000 Endpoints
Tanium Server	Small physical Appliance on page 646 Virtual Appliance on page 651 Cloud-based Appliance on page 651	Small physical Appliance on page 646 Virtual Appliance on page 652 Cloud-based Appliance on page 652	Small physical Appliance on page 646 Virtual Appliance on page 652 Cloud-based Appliance on page 652	Medium physical Appliance on page 646 Virtual Appliance on page 652 Cloud-based Appliance on page 652	Medium physical Appliance on page 646 Cloud-based Appliance on page 652	Large physical Appliance on page 646 Cloud-based Appliance on page 653	Extra-large physical Appliance on page 646 Cloud-based Appliance on page 653
Module Server	Small physical Appliance	Small physical Appliance	Small physical Appliance	Small physical Appliance on	Small physical Appliance on	Medium physical Appliance on	Medium physical Appliance on

©2026 Tanium Inc. All Rights Reserved

Role	< 10,000 Endpoints	< 35,000 Endpoints	< 50,000 Endpoints	< 100,000 Endpoints	< 200,000 Endpoints	< 500,000 Endpoints	> 500,000 Endpoints
	on page 646 Virtual Appliance on page 651 Cloud-based Appliance on page 651	on page 646 Virtual Appliance on page 652 Cloud-based Appliance on page 652	on page 646 Virtual Appliance on page 652 Cloud-based Appliance on page 652	page 646 Virtual Appliance on page 652 Cloud-based Appliance on page 652	page 646 Cloud-based Appliance on page 652	page 646 Cloud-based Appliance on page 653	page 646 Cloud-based Appliance on page 653
Zone Server	Small physical Appliance on page 646 Virtual Appliance on page 651 Cloud-based Appliance on page 651	Small physical Appliance on page 646 Virtual Appliance on page 652 Cloud-based Appliance on page 652	Small physical Appliance on page 646 Virtual Appliance on page 652 Cloud-based Appliance on page 652	Medium physical Appliance on page 646 Virtual Appliance on page 652 Cloud-based Appliance on page 652	Medium physical Appliance on page 646 Cloud-based Appliance on page 652	Large physical Appliance on page 646 Cloud-based Appliance on page 653	Extra-large physical Appliance on page 646 Cloud-based Appliance on page 653
Development (any role)	Virtual Appliance on page 651 Cloud-based Appliance on page 651	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
Cloud Access Point	Virtual Appliance on page 651 Cloud-based	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported

©2026 Tanium Inc. All Rights Reserved

Role	< 10,000 Endpoints	< 35,000 Endpoints	< 50,000 Endpoints	< 100,000 Endpoints	< 200,000 Endpoints	< 500,000 Endpoints	> 500,000 Endpoints
	Appliance on page 651						

Physical Tanium Appliance specifications

The subsequent topics in this section provide the component, environmental, and dimensional specifications for physical Tanium Appliances.

Note: The specifications listed in this section apply to version 4 of each physical Tanium Appliance.

Physical Tanium Appliance component specifications

Physical Tanium Appliance component specifications

	Small	Medium	Large	Extra-Large
Operating System	TanOS	TanOS	TanOS	TanOS
Processor Count	2	2	4	4
Processor Core Count	24	48	72	96
RAM	128 GB	512 GB	1024 GB	1536 GB
Disk Space Available for Tanium Software and Data	1728 GB	3456 GB	3456 GB	5184 GB
Disk Type	SSD SAS 24Gbps FIPS 140-2	SSD SAS 24Gbps FIPS 140-2	SSD SAS 24Gbps FIPS 140-2	SSD SAS 24Gbps FIPS 140-2
Out-of-Band	iDRAC9 Enterprise	iDRAC9 Enterprise	iDRAC9 Enterprise with	iDRAC9 Enterprise with

©2026 Tanium Inc. All Rights Reserved

	Small	Medium	Large	Extra-Large
Management			dedicated NIC	dedicated NIC
NICs (Copper option)	2 x Dual Port 10GbE (RJ45)	2 x Dual Port 10GbE (RJ45)	2 x Quad Port 10GbE (RJ45)	2 x Quad Port 10GbE (RJ45)
NICs (Fiber option)	2 x Dual Port 10GbE (SFP+, short-range optics provided)	2 x Dual Port 10GbE (SFP+, short-range optics provided)	2 x Quad Port 10/25GbE (SFP28, short-range optics provided)	2 x Quad Port 10/25GbE (SFP28, short-range optics provided)
Power Supply	Dual, Fully Redundant Platinum 800W	Dual, Fully Redundant Platinum 800W	Dual, Fully Redundant Platinum 2400W	Dual, Fully Redundant Platinum 2400W

Physical Tanium Appliance environmental specifications

Physical Tanium Appliance environmental specifications

	Small / Medium	Large / Extra Large
Input Voltage / Current	100–240 VAC / 4.7–9.2 A	100–240 VAC / 13.5–16 A
Frequency	50/60 Hz	50/60 Hz
Power Cord	2 x C13 to C14 or 2 x C13 to NEMA 5-15P	2 x C19 to C20
PSU Heat Dissipation	3000 BTU/hr max	9000 BTU/hr max
Operating Temperature	50–95°F (10°C–35°C)	50–95°F (10–35°C)
Operating Altitude	< 10,000 ft (3048 m)	< 10,000 ft (3048 m)

Physical Tanium Appliance dimensions

Physical Tanium Appliance dimensions

	Small / Medium	Large / Extra-Large
Form Factor	1U (Std Rack)	2U (Std Rack)

©2026 Tanium Inc. All Rights Reserved

	Small / Medium	Large / Extra-Large
System Dimensions	19 in. (482 mm) W (with ears) 17.1 in. (434 mm) W (case only) 26.1 in. (662 mm) D (with PSU handle) 24.7 in. (627 mm) D (case only) 1.7 in. (43 mm) H	19 in. (482 mm) W (with ears) 17.5 in. (444 mm) W (case only) 33.4 in. (848 mm) D (with PSU handle) 32.2 in. (817 mm) D (case only) 3.4 in. (87 mm) H

Cloud-based Tanium Appliance and virtual Tanium Appliance specifications

Cloud-based Tanium Appliance deployment

Tanium provides cloud-based Tanium Appliance images for the following cloud providers:

Cloud Tanium Appliance supported deployment providers

Provider	Boot type
AWS (x86-64 processors)	UEFI
AWS GovCloud	UEFI
Google Cloud Platform (GCP)	BIOS
Microsoft Azure	UEFI
Microsoft Azure GovCloud	UEFI

Note: Any cloud-based Tanium Appliance deployed before TanOS 1.9.1 uses BIOS boot. The boot type is set when the VM is instantiated from the TanOS image, so existing Appliances cannot be converted to UEFI.

Virtual Tanium Appliance deployment

©2026 Tanium Inc. All Rights Reserved

Tanium provides virtual Tanium Appliance images for the following hypervisors:

Hypervisor	Virtual image format	Boot type
KVM	QCOW2	BIOS
VMware ESXi	OVA	UEFI
Microsoft Hyper-V	VHD	UEFI

Download the appropriate virtual image from the **Artifacts** section of your Tanium Account. For more information, see View Tanium artifacts.

Each virtual Tanium Appliance image contains the following default settings:

- 16GB RAM
- 4 CPU cores
- 1 NIC
- 500GB disk

Before you start the virtual Appliance for the first time, you might need to use the VM settings utility on the hypervisor to make changes to support the recommended specifications for your deployment size. For more information about sizing, see Cloud-based Tanium Appliance and virtual Tanium Appliance specifications on page 648.

©2026 Tanium Inc. All Rights Reserved

Note:

- **KVM:** The TanOS QCOW2 image includes the QEMU guest agent, which supports graceful shutdowns and snapshot quiescing. You must configure a VirtIO serial port in the virtual machine hardware settings to establish a dedicated communication channel between the KVM hypervisor and the QEMU guest agent. TanOS disables operations that allow the hypervisor to access or transfer files, execute commands, or change user passwords inside the guest.
- **VMware ESXi:** The TanOS OVA image includes Open VM Tools, which supports graceful shutdowns, snapshot quiescing, and time synchronization between host and guest. TanOS disables support for the VMware Guest Operations API to prevent the hypervisor from running programs, transferring files, or performing other credential-based actions inside the VM.

Recommended resources for cloud-based Tanium Appliances and virtual Tanium Appliances

The following specifications include a range for a given number of endpoints, depending on modules installed, usage, and other factors unique to each environment. It is reasonable to start at the low end of each range and increase resources as needed. Customers are responsible for ensuring adequate resource allocation for their Tanium instances.

©2026 Tanium Inc. All Rights Reserved

Important:

- Customers are entirely responsible for the performance of their virtual Tanium Appliances. You might need to adjust resource allocations based on performance indicators after your Tanium environment is running.
- Virtual Tanium Appliances support only up to 100,000 endpoints. Resource specification for greater numbers of endpoints apply only to cloud-based Tanium Appliances.
- To ensure that the response times of Tanium Core Platform Servers do not adversely affect the user experience, the Servers must be able to sustain I/O loads of at least 30 MBps at 2,500 IOPS and maintain disk utilization below 15 percent under such workloads. Sustaining 2,500 IOPS ensures that disk latency stays below 15 milliseconds (ms) on the drive where the Servers and modules are stored.

Note:

- Both Tanium Servers in a cluster must have the same amount of RAM, and both the active and standby Module Server must have the same amount of RAM.
- The disk space listed for the Tanium Server and Zone Server is the minimum space required for TanOS and the Tanium Core Platform Server software. If you use Tanium™ Patch, the Server needs an additional 500 GB of disk space to store and manage patches. If you use Tanium™ Deploy, the Server needs additional disk space greater than or equal to twice the Deploy software library storage.

Up to 10,000 endpoints

Recommended resources for up to 10,000 endpoints

	Tanium Server	Tanium Module Server	Tanium Zone Server	Tanium Cloud Access Point
CPU cores	8–16	8–16	8–16	8

©2026 Tanium Inc. All Rights Reserved

	Tanium Server	Tanium Module Server	Tanium Zone Server	Tanium Cloud Access Point
RAM	32–96 GB	32–96 GB	16–96 GB	16 GB
Disk Space	500 GB – 2 TB	500 GB – 2 TB	500 GB	500 GB

10,001 to 35,000 endpoints

Recommended resources for 10,001 to 35,000 endpoints

	Tanium Server	Tanium Module Server	Tanium Zone Server	Tanium Cloud Access Point
CPU cores	8–16	8–16	8–16	not supported
RAM	32–96 GB	32–96 GB	16–96 GB	
Disk Space	500 GB – 2 TB	500 GB – 2 TB	500 GB	

35,001 to 50,000 endpoints

Recommended resources for 35,001 to 50,000 endpoints

	Tanium Server	Tanium Module Server	Tanium Zone Server	Tanium Cloud Access Point
CPU cores	8–16	8–16	8–16	not supported
RAM	32–96 GB	32–96 GB	16–96 GB	
Disk Space	500 GB – 2 TB	500 GB – 2 TB	500 GB	

50,001 to 200,000 endpoints

Important: Virtual Tanium Appliances support only up to 100,000 endpoints. For 100,001–200,000 endpoints, the following resource specifications apply only to cloud-based Tanium Appliances.

©2026 Tanium Inc. All Rights Reserved

Recommended resources for 50,001 to 200,000 endpoints

	Tanium Server	Tanium Module Server	Tanium Zone Server	Tanium Cloud Access Point
CPU cores	16–32	8–16	16–32	not supported
RAM	128–384 GB	32–96 GB	128–384 GB	
Disk Space	500 GB – 2 TB	500 GB – 4 TB	500 GB	

200,001 to 500,000 endpoints (cloud-based Tanium Appliances only)

Recommended resources for 200,001 to 500,000 endpoints

	Tanium Server	Tanium Module Server	Tanium Zone Server	Tanium Cloud Access Point
CPU cores	16–42	16–32	16–42	not supported
RAM	256–640 GB	128–384 GB	256–640 GB	
Disk Space	500 GB – 2 TB	500 GB – 4 TB	500 GB	

Over 500,000 endpoints (cloud-based Tanium Appliances only)

Recommended resources for over 500,000 endpoints

	Tanium Server	Tanium Module Server	Tanium Zone Server	Tanium Cloud Access Point
CPU cores	32–64	16–32	32–64	not supported
RAM	512–1024 GB	128–384 GB	512–1024 GB	
Disk Space	500 GB – 2 TB	500 GB – 4 TB	500 GB	

©2026 Tanium Inc. All Rights Reserved

Reference: Default installation directory for the Tanium Client

The following table lists the default installation paths for the Tanium Client on each operating system (OS). If you troubleshoot issues for an installation that uses a non-default path, note this when you Contact Tanium Support on page 510.

OS	Installation Directory
Windows (64-bit OS versions)*	\Program Files (x86)\Tanium\Tanium Client\
Windows (32-bit OS versions)*	\Program Files\Tanium\Tanium Client\
macOS	/Library/Tanium/TaniumClient
Linux, UNIX	/opt/Tanium/TaniumClient
* On both 64-bit and 32-bit versions of Windows, Tanium Client is installed as a 32-bit application.	

©2026 Tanium Inc. All Rights Reserved

Tanium Core Platform and Tanium Client Export Commodity Classification (Appliance deployments)

The Export Commodity Classification Automated Tracking System (CCATS) number for Tanium is G172792. The Export Control Classification Numbers (ECCNs) for Tanium products are as follows:

Export Commodity Classification

Product	ECCN	License Exception	Authorized for Export (See Definitions List Below)
Tanium Client software	5D992.c	No License Required ("NLR")	All countries, except Embargoed Countries and the Crimea Region of Ukraine
Tanium Server software	5D002.c.1	ENC/(b)(1)	All countries, except Embargoed Countries and the Crimea Region of Ukraine
Tanium Module Server software	5D002.c.1	ENC/(b)(1)	All countries, except Embargoed Countries and the Crimea Region of Ukraine

Important: Tanium prohibits software and hardware (both physical and virtual) installations in certain countries. Contact Tanium Support on page 510 to determine whether a particular country is on the prohibited list.

©2026 Tanium Inc. All Rights Reserved