Comply User Guide

November 24, 2026



Table of contents

Comply home 10

Comply overview 13
- Operational Technology in Comply 13
- Interoperability with other Tanium products 13

Gaining organizational effectiveness with Comply 16

Requirements 26

Installing 48
- Before you begin 48
- Import Comply with default settings 48
  - Default settings for Comply 50
- Import Comply with custom settings 50
- Upgrade Comply 51
- Verify Comply version 51

Configuring 52
- Default settings for Comply 52
- Manage solution configurations with Tanium Endpoint Configuration 53
- Configure Comply 54
  - Configure the Comply action group 54
  - Set up Comply users 55
- Deploy scan engines and JREs 57
- Create deployments 58
  - Restrict assessment visibility 59
  - Create assessments 60
- Configure Comply for an air-gapped environment 60
  - Upload the Tanium Engines package 61
    - Upload the Tanium Vulnerability Library files 61

©2026 Tanium Inc. All Rights Reserved

Configure credentials lists for remote-authenticated scans 63
Prioritize credentials 66
Credentials list view 67

Get up and running 68
Import scan engines and set up endpoints 68
Import standards 68
Configure assessments 69
System generated assessments 69
View findings and create reports 72
Monitor the dashboard 73

Working with scan engines 74
Transitioning to Tanium Scan Engine 7.0 75
What is transitioning 75
How TSE 7.0 changes vulnerability scanning 76
Why is Comply moving to TSE 7.0 76
Scope: client-based vulnerability scans only 77
Before your endpoints transition 77
New Comply settings for TSE 7.0 78
How endpoints transition 79
Settings that do not apply to TSE 7.0 79
Tanium Index scan coverage best practices 80
Configure exclusions safely 81
Configure blockout windows safely 82
Configure the maximum Index database size 83
Deploying the legacy Tanium Scan Engine and JRE using ECM 85
Legacy Tanium Scan Engine (TSE) default targeting 87
Download and import the CIS-CAT engine 88
Download and import the SCC scan engine 91
Target Computer groups 92
Upload a Java Runtime Environment (JRE) package 93
Import JREs 94
Target Computer groups 95
Import custom settings 95
Prioritize endpoint configurations 98

©2026 Tanium Inc. All Rights Reserved

Upload the Tanium Engines package for air-gapped environments 99

Setting up endpoints 101
Configure engines 101
Custom settings 103

Working with standards and vulnerability sources 109
Configuration compliance standards 109
Importing individual standards and assigning categories 110
Filter standards 111
Change a Standards label 111
Create a standard 112
Delete a standard 112
Filtering standards 113
Viewing configuration compliance standard profiles and creating assessments 113
Vulnerability sources 114
Default vulnerability sources 114
View changes to the Tanium Vulnerability Library 117
Search for CVEs 117
Upload the vulnerability source file for air-gapped environments 117
Create a new vulnerability source 118
Edit or delete a vulnerability source 119
Perform a vulnerability scan and create an assessment 119

Creating compliance assessments 121
Configure a client-based scan assessment 122
Configure a remote authenticated scan assessment 125
Remote authenticated scan workflow 136
Create a configuration compliance assessment from the Standards page 136
Status definitions 137
Run an assessment again 137
Run an on-demand scan 138
Export an assessment 141
Edit an assessment 142
Clone an assessment 144
Delete an assessment 144
Download audit history 145

©2026 Tanium Inc. All Rights Reserved

Creating vulnerability assessments **146**
Configure a client-based scan assessment 146
Configure a remote authenticated scan assessment 152
Remote authenticated scan workflow 165
Create a vulnerability assessment from the Standards page 165
Configure a network unauthenticated scan assessment 165
Before you begin 166
View findings 170
Create a network unauthenticated report 170
Create an SBOM scan assessment 172
Before you begin 172
Configure a container registry scan assessment 175
Before you begin 176
Configure an operational technology scan assessment 180
Before you begin 180
Status definitions 181
Run an assessment again 182
Run an on-demand scan 183
Export an assessment 186
Update vulnerability assessments 188
Edit an assessment 188
Clone an assessment 189
Delete an assessment 190
Download audit history 190
Update CVE definitions type (One-time bulk action) 191

Viewing and filtering findings **194**
Filter compliance findings 194
Standard filter 195
Filter builder 195
Quick filter 198
Filter vulnerability findings 198
Standard filter 199
Quick filter 200
Filter builder 201

©2026 Tanium Inc. All Rights Reserved

Expand details ... 204
Integration with Patch ... 206
Integration with Reporting ... 208
Findings field descriptions ... 209
Using Tanium Ask ... 211
Custom Sensors ... 212
Download as CSV ... 212
Create reports from findings ... 215

Creating exceptions for findings ... 216
Before you begin ... 216
Configure exceptions ... 217
Configure exceptions from Findings ... 217
Configure exceptions from All Findings (multiple endpoints) ... 219
Configure exceptions from scratch ... 221
Export exceptions list ... 223
Exception examples ... 224
Compliance finding exception example ... 224
Vulnerability finding exception example ... 226

Investigating findings ... 229
Investigate compliance findings ... 230
Compliance investigations ... 231
Filter tests list ... 233
Expand Details ... 234
Investigate vulnerability findings ... 236
Vulnerability investigations ... 236
Filter tests list ... 238
Expand Details ... 239
Identify CVEs in error or unknown state ... 241
Export investigations ... 241

Remediating findings ... 245
Configure an OS patch remediation ... 245
View findings ... 246
Filter findings ... 247
Remediate actionable findings ... 248

©2026 Tanium Inc. All Rights Reserved

Export remediation findings 251
Investigate remediation findings 251
Configure a software update remediation 252
View findings 253
Filter findings 254
Remediate actionable findings 255
Export remediation findings 257
Investigate remediation findings 257

Exporting findings and assessments 259
Before you begin 259
Exporting findings 259
Exporting vulnerability assessments 263
Create a connection 263
Findings field descriptions 265
Test a connection and review data 266
Exported columns 267

Working with Comply reports 273
Viewing reports 273
Compliance report results 274
Vulnerability report results 275
Create a new Comply report 275
Exporting Comply network unauthenticated reports 276
Downloading exported Comply reports 278

Customizing compliance results 279
Custom profiles 279
Create a new custom profile 279
Import a new custom profile 283
Cloning custom profiles 283
Editing custom profiles 284
Custom checks 285
Reference: Troubleshoot custom script issues 288
Custom ID mappings 288
View ID Mappings and Score Mappings in Interact 289

©2026 Tanium Inc. All Rights Reserved

Export custom check or ID mapping 290

Customizing vulnerability results 292
Custom scores 292
Custom ID mappings 294
Upload IAVM mapping definitions 296
View ID Mappings and Score Mappings in Interact 297
Download custom ID mapping 299

Managing application settings 301

Maintaining Comply 304
Comply monthly maintenance 304
Comply quarterly maintenance 304
Monitor and troubleshoot Comply coverage 305
Monitor and troubleshoot endpoint compliance distribution 306
Monitor and troubleshoot endpoints with critical or high vulnerabilities 308
Monitor and troubleshoot mean time to identify vulnerability findings 308

Troubleshooting Comply 310
Collect logs 310
Collect troubleshooting information from endpoints 311
Locate log files 312
Endpoint log files 312
Tanium Module Server log files 312
Database corruption issue upgrading from Comply 2.19 or earlier to Comply 2.23 313
SBOM false positives 313
Delete stale assessments from endpoints 314
Manually remove Comply content from endpoints 317
Java tool options when executing java 317
Scans do not run as expected 317
Remote vulnerability source fails in proxied environment 318
Update the Tanium Vulnerability Library for CVSS v3 support 318
Restart Connect service after upgrade 318
RBAC synchronization with SUS adoption after upgrade 319
Remote authenticated scan timeout failure 319
Remote authenticated scans fail on ESXi and vCenter devices 319

©2026 Tanium Inc. All Rights Reserved

Results directory on endpoint after upgrade 321
Incomplete findings for endpoints after upgrade 321
Incorrect or missing findings for reports with custom profiles after upgrade 321
Missing vulnerability reports after upgrade 322
Deployments do not run as expected 322
License expiration impact 323
Identify and resolve issues with Client Extensions 323
Verify endpoint tools 326
Remove Comply tools from endpoints 327
Uninstall Comply 329
Remove Comply content from endpoints 329
Remove the Comply solution from the Tanium Module Server 331
Contact Tanium Support 332

Reference: Supported engines and JREs 333

Reference: Remote authenticated scanning 341

Reference: Common errors in Comply 347

Reference: Deprecated sensors 357

Reference: Repackage the IBM JRE for deployment to AIX endpoints 362

Reference: Gateway examples for Comply 365

©2026 Tanium Inc. All Rights Reserved

Tanium™ Comply

Use Comply to assess endpoint security posture, identify configuration exposures, and detect software vulnerabilities using industry standards and custom compliance checks.

Evaluate endpoints for security configuration exposures and software vulnerabilities using industry security standards, vulnerability definitions, and custom compliance checks.

- 2026H2
- 2026H1
- 2025H2

Learn about Comply



- Comply overview on page 13

  Understand terminology, scanning options, and how Comply integrates with other Tanium products

- Comply requirements on page 26

  Review the system requirements for clients and servers, required configurations, and user role configurations

Create and work with assessments



©2026 Tanium Inc. All Rights Reserved

- Creating compliance assessments on page 121

  Create configuration compliance assessments and vulnerability assessments

- Viewing and filtering findings on page 194

  Analyze findings to determine security exposures and software vulnerabilities on endpoints

Other resources



- Release notes

  Get a list of changes for each Comply release

- Video tutorials

  Watch tutorials about how to use Comply

- Product brief

  Learn about the high-level business and use cases for Comply

- Glossary

  Review Tanium terms

This documentation may provide access to or information about content, products (including hardware and software), and services provided by third parties (“Third Party Items”). With respect to such Third Party Items, Tanium Inc. and its affiliates (i) are not responsible for such items, and expressly disclaim all warranties and liability of any kind related to such Third Party Items and (ii) will not be responsible for any loss, costs, or damages incurred due to your access to or use of such Third Party Items unless expressly set forth otherwise in an applicable agreement between you and Tanium. Further, this documentation does not require or contemplate the use of or combination with Tanium products with any particular Third Party Items and neither Tanium nor its affiliates shall have any responsibility for any infringement of intellectual property rights caused by any such combination. You, and not Tanium, are responsible for determining that any combination of Third

Party Items with Tanium products is appropriate and will not cause infringement of any third party intellectual property rights.

Tanium is committed to the highest accessibility standards to make interaction with Tanium software more intuitive and to accelerate the time to success. For more information, see Tanium Product Accessibility.

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

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

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

©2026 Tanium Inc. All Rights Reserved

Comply overview

Tanium™ Comply evaluates endpoints for security configuration exposures and software vulnerabilities using industry standards and custom checks to help reduce risk and prepare for compliance audits.

Use Tanium™ Comply to evaluate endpoints for security configuration exposures and software vulnerabilities using industry security standards, vulnerability definitions, and custom compliance checks. With comprehensive, on-demand results across the entire enterprise, you can reduce your organization's overall risk, improve your security hygiene, and simplify preparation for industry compliance audits such as Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley Act (SOX).

Comply utilizes Security Content Automation Protocol (SCAP) compliant content, such as standards published by the Defense Information Systems Administration (DISA) or the Center for Internet Security (CIS), to evaluate operating systems and applications for configuration of password policies, file permissions, and other components. Comply supports Windows, macOS, Linux, AIX, and Solaris endpoints.

Operational Technology in Comply

Learn how Operational Technology in Comply integrates with OT scan assessments and Tanium Exposure Management.

Use Tanium™ Exposure Management for Operational Technology to configure Tanium™ Comply vulnerability assessments for OT endpoints and view vulnerability findings for those endpoints.

For more information, see Create an OT scan assessment on page 180 and Tanium Endpoint Management for Operational Technology User Guide: Using Tanium Exposure Management for Operational Technology.

Interoperability with other Tanium products

Comply integrates with other Tanium solutions to extend vulnerability reporting, remediation, and endpoint visibility.

©2026 Tanium Inc. All Rights Reserved

Comply works with other Tanium solutions, such as Tanium™ Connect and Tanium™ Patch for additional reporting of related data.

Tanium™ Connect

You can use Comply vulnerability reports as a connection source. For more information, see Exporting findings and assessments on page 259.

Tanium™ Direct Connect

Remote authenticated scanning uses Tanium Clients as satellites to scan endpoints that do not have the Tanium Client installed. Configure satellites for use in scanning with Direct Connect. For more information, see Tanium Direct Connect User Guide: Managing satellites and Configure a remote authenticated scan assessment on page 152.

Tanium™ Deploy

Remediation visibility provides a view of vulnerable findings and the unscheduled software updates that could remediate that finding. From the remediation view in Tanium Comply, you can take a Deploy action and pivot into Tanium Deploy to distribute that action to the endpoint. For more information, see Remediating findings on page 245.

Tanium™ Discover

When you configure remote authenticated scans, you can target Discovered Endpoints by running satellite scans in Tanium Discover before you configure the assessment. For more information, see Configure a remote authenticated scan assessment on page 152.

Tanium™ Patch

You can open Patch from a link in Comply vulnerability reports results to view details about the patch that resolves a reported vulnerability. You can also install the patch to endpoints directly from the patch details page. For more information, see Vulnerability report results on page 275.

Remediation visibility provides a view of vulnerable findings and the unscheduled patches that target those vulnerabilities. From the remediation view in Tanium Comply, you can take a patch remediation action and pivot into Tanium Patch to deploy that action to the endpoint. For more information, see Remediating findings on page 245.

©2026 Tanium Inc. All Rights Reserved

Tanium™ Reporting

When you filter Findings by endpoint, you can click the icon for an individual endpoint to view more details. From the details pop-up, you can click the View Details button to go to Tanium Reporting. For more information, see Working with Comply reports on page 273.

Tanium™SBOM

Use an SBOM scan to find vulnerabilities on endpoints based on the results of a Software Bill of Materials assessment. A Tanium SBOM license is required. For more information, see Create an SBOM scan assessment on page 172.

©2026 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Comply

UseComplyto strengthen organizational governance through structured change management, clear roles and responsibilities, cross-functional alignment, and operational maturity metrics for compliance and vulnerability management.

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

- Develop a dedicated change management process. For more information, see Change management on page 16[1].
- Define distinct roles and responsibilities. For more information, see RACI chart on page 17.
- Validate cross-functional alignment. For more information, see Organizational alignment on page 20.
- Track operational maturity. For more information, see Operational metrics on page 21.

[1]An organization's vulnerability management program intersects with change management governance to drive remediation activities. For example, when to run reports, implementation of remediation activities, such as patching activities, as well as functional work schedules, such as the follow the sun model, authorized maintenance windows, and change control activities.

Change management

Develop a tailored, dedicated change management process that aligns with the organizational vulnerability management program to enable patching and configuration changes for a streamlined process using Comply.

- Update SLAs and align activities to key resources for Comply, where applicable. For more information, see Comply maturity on page 21 and RACI chart on page 17.
- Designate change or maintenance windows for various scenarios, where applicable. For

©2026 Tanium Inc. All Rights Reserved

example, set up third-party reporting technologies and integration with ticket systems, such as SIEM, Database Power BI, and Tableau.

- Identify internal and external dependencies to the vulnerability management process. For example, achieve effective integrations with SIEM, Database Power BI, and Tableau with Comply.
- Create a Tanium steering group (TSG) for discovery activities to expedite reviews and approvals of processes that align with SLAs and vulnerability management processes, as applicable.

RACI chart

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

RACI chart for Tanium Comply

Task	Security Team	Risk / Compliance Team	Operations Team	CISO	Rationale
Establish a Vulnerability Management Program	R/A	R/A	C	I	Align to the organizational Vulnerability Management Program, which is used to make Comply implementation decisions such as report scheduling. For example, whether the schedules use the "follow the sun" model. The organizational Vulnerability Management Program is also used to make decisions about remediation needs that are driven by data provided by Comply, such as: 1. Implementation of remediation activities, such as patching

©2026 Tanium Inc. All Rights Reserved

Task	Security Team	Risk / Compliance Team	Operations Team	CISO	Rationale
					2. Authorized maintenance windows 3. Change control activities
Findings verification: define policy assessment frequency	I	I	I	R/A	Define policy assessment frequency in alignment with any regulatory requirements. Schedule assessments in Comply to meet the frequency requirements.
Findings verification: define assessment requirements (regulatory)	I	I	I	R/A	Define policy requirements in alignment with any regulatory requirements. Create assessments in Comply to meet the policy requirements.
Operationalize assessment policies	R/A	I	I	C	Publish and distribute the assessment policies aligned to any regulatory requirements.
Execute assessment policies	I	R/A	I	I	After policies are created and published, execute the policies using Comply to define targets for assessments, create compliance profiles, and identify a vulnerability baseline.
Implement configuration compliance assessments	I	R/A	I	I	Implement the policies for the configuration compliance workflow by creating configuration compliance assessments in Comply.
Implement vulnerability assessments	I	R/A	I	I	Implement the policies for the vulnerability management workflow by creating vulnerability reports in Comply.
Conduct report:	I	R/A	I	I	Run assessments against identified targets based

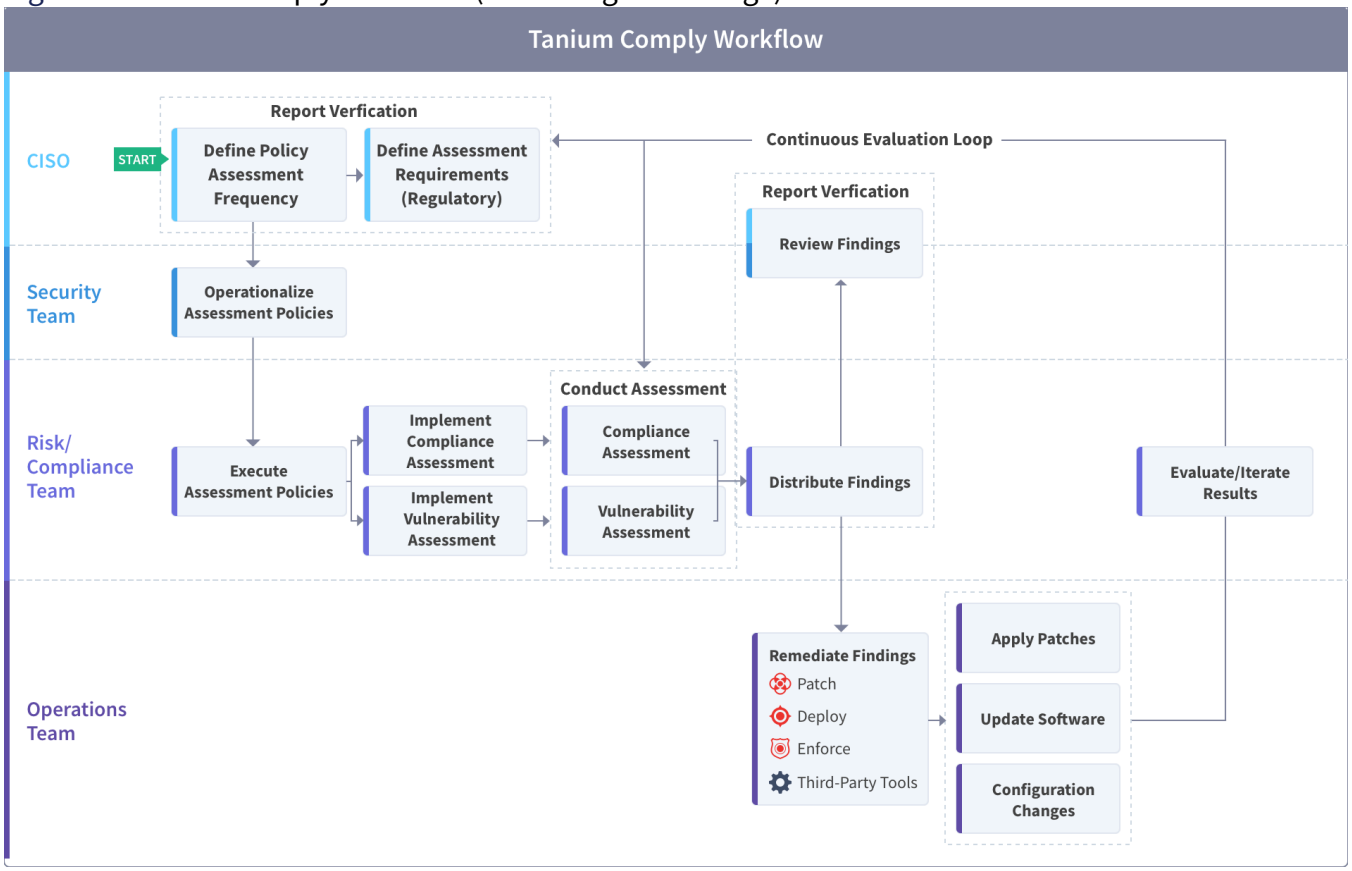
©2026 Tanium Inc. All Rights Reserved

Task	Security Team	Risk / Compliance Team	Operations Team	CISO	Rationale
vulnerability scan, network unauthenticated scan, and configuration compliance scan					on policies.
Assessments validation: distribute, review, and take action on findings	I	R/A	I	C/I	Take the results from the assessment activities and distribute, review, and take action on the findings. After the risk report is completed, the CISO team will validate the risk assessment results to identify criticality to implement controls, where applicable.
Remediate findings: apply patches	I	I	R/A	I	Changes to mitigate or take action on identified risks. For example, use Tanium Patch to install a patch on an endpoint to fix a vulnerability.
Remediate findings: update software	I	I	R/A	I	Changes to mitigate or take action on identified. For example, use Tanium Patch to update software on an endpoint to fix a vulnerability.
Remediate findings: configuration changes	I	I	R/A	I	Changes to mitigate or take action on identified risks that will implement a change in the configuration of a specific endpoint or device. This change may be a permanent change from the temporary controls implemented or a new change based on risk report, such as using Tanium to quarantine a device or shutting down a device.
Evaluate and iterate on results	I	R/A	I	I	Operations and Security teams inform the Risk / Compliance Team that controls are applied so they can verify the results. Then, the workflow starts

©2026 Tanium Inc. All Rights Reserved

Task	Security Team	Risk / Compliance Team	Operations Team	CISO	Rationale
					over to continually evaluate risk posture in security and vulnerability management.

Figure 1. Tanium Comply Workflow (click image to enlarge)



Organizational alignment

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

In the absence of cross-functional alignment, functional silos often spend time and effort in litigating data quality instead of making decisions on how to improve configuration compliance and reduce vulnerabilities.

©2026 Tanium Inc. All Rights Reserved

Operational metrics

Comply maturity

Managing compliance and vulnerability management programs successfully includes operationalization of the technology and measuring success through key standards metrics. The four key processes to measure and guide operational maturity of your Tanium Comply program are as follows:

Process metrics for Tanium Comply coverage

Process	Description
Usage	how and when Tanium Comply is used in your organization, and is Tanium the sole tool or is it supplemented by other tools, such as a remote assessment tool for network devices.
Automation	how automated Tanium Comply is, and how well is it used in automation of other systems
Functional Integration	how integrated Tanium Comply is across IT security, IT operations, patch and software deployment, and Asset Management teams
Reporting	how is data from Tanium Comply used by people and systems within the organization

Standards metrics

In addition to the key compliance and vulnerability management programs, the key standards metric that aligns to the operational maturity of the Tanium Comply program to achieve maximum value and success is as follows:

Executive metrics for Tanium Comply coverage

Executive Metrics	Comply Coverage	Endpoints with Critical or High Vulnerabilities
Description	The number of endpoints in each of these categories:	Percentage of endpoints that have executed vulnerability reports which found at least 1 critical or high severity vulnerability.

©2026 Tanium Inc. All Rights Reserved

Executive Metrics	Comply Coverage	Endpoints with Critical or High Vulnerabilities
	• **Optimal**: Endpoints where Comply is operational • **Needs attention**: Endpoints with an underlying issue that might impact Comply, such as low disk space, out of date scan engine, or out of date Comply tools • **Unsupported**: Endpoints with an operating system version that is not supported by Comply For steps to investigate endpoints that are categorized as **Needs Attention** or **Unsupported**, see Monitor and troubleshoot Comply Coverage on page 310. For operating system and Tanium Client versions supported by Comply, see Comply requirements on page 26.	
Instrumentation	Uses the `Comply - Coverage Status` sensor to return the number of endpoints where Comply is optimal, needs attention, and is unsupported.	Number of endpoints that have had a vulnerability report which resulted in 1 or more critical or high severity vulnerabilities divided by the number of endpoints that have run a vulnerability report.
Why this metric matters	If you are not scanning all endpoints, then you are at risk.	If you have a significant number of endpoints with outstanding high or critical vulnerabilities, you are at greater risk.

Vulnerability Findings

Use vulnerability findings to aid in determining levels of compliance and remediation needs.

©2026 Tanium Inc. All Rights Reserved

Vulnerability levels for Tanium Comply

Vulnerability Level	Definition
High	Endpoint has at least 1 high vulnerability found
Medium	Endpoint has no high vulnerabilities but has at least 1 medium vulnerability found
Low	Endpoint has no high or medium vulnerabilities but has at least 1 low vulnerability found
Not scored	Endpoint has no high, medium, or low vulnerabilities but has at least 1 unscored vulnerability found
No Vulnerabilities	Endpoint has been scanned in the last 30 days with no vulnerabilities found
Not scanned	Endpoint has not been scanned in the last 30 days

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

Maturity level for Tanium Comply usage

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Comply installed and configured. One or more users have access and are asking basic questions.	Third-party components uploaded and deployments created.	Configuration compliance and vulnerability assessments configured.	Customized configuration compliance and vulnerability assessments configured (client based, remote authenticated, and network unauthenticated).	Custom standards created and used for organizational reports. Custom vulnerability sources configured and in use. Ongoing maintenance of checks and standards.
	Automation	Only manual, ad hoc assessments in use.	Only manual, ad hoc reports in use.	Automated, recurring configuration	Customized configuration compliance and	Configuration compliance and vulnerability

©2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
				compliance and vulnerability assessments.	vulnerability assessments running. Documented compliance and vulnerability management life cycle with SLAs on mitigation time frames.	risk data used as input to threat hunting activities by correlating risk data with security alerts to determine risk scoring for environment.
	Functional integration	Comply installed, but not operationalization.	Using default Comply dashboards and reports within Tanium Reporting.	Creating custom Comply dashboards and reports within Tanium Reporting.	Integration with third-party reporting technologies, integration with IT ticket systems, automated workflow with Tanium Patch for approval and deployment of patches, automated export into data repository/ warehouse)	Integration with remediation process and capabilities. Integration with Tanium Benchmark for additional context around enterprise risk.
	Reporting	Manual; Reporting for Operators only through Comply	Manual; Export of recurring assessments	Automated; Export through Tanium Connect	Automated; Third-party technologies reporting from Comply	Automated; Third-party technologies reporting from Comply
Metrics	Compliance	0-49%	51-65%	66-85%	86-95%	>95%

©2026 Tanium Inc. All Rights Reserved

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
	Percentage (of scanned endpoints)					
	Comply Coverage (for managed endpoints)	0-49%	51-65%	66-85%	86-95%	>95%

©2026 Tanium Inc. All Rights Reserved

Comply requirements

Review the platform, solution, endpoint, security, and user role requirements before you use Comply.

Core platform dependencies

Make sure that your environment meets the following requirements:

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

Computer group dependencies

When you first sign in to the Tanium Console after a fresh installation of Tanium Server, the server automatically imports the computer groups that Comply requires.

For earlier versions of the Tanium Server, or after upgrading from an earlier version, you must manually create the computer groups. For more information, see Tanium Console User Guide: Create a computer group.

Solution dependencies

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

©2026 Tanium Inc. All Rights Reserved

Note: Some Comply dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 27 and Feature-specific dependencies on page 28. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Comply requires.

Tanium recommended installation

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

Required dependencies

Comply has the following required dependencies at the specified minimum versions:

- Tanium™ Connect
- Tanium™ Discover
- Tanium™ Endpoint Configuration
- Tanium™ Interact
- Tanium™ Data Service (TDS)
- Tanium™ Reporting service
    - Tanium™ API Gateway
    - Tanium™ Blob service
- Tanium™ RDB service
- Tanium™ Secrets service

©2026 Tanium Inc. All Rights Reserved

Feature-specific dependencies

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

Remote authenticated scanning requirements

- Tanium™ Direct Connect

  > **Note:** Tanium™ Discover, only required if targeting Discovered Endpoints

Remediation visibility requirements

- Tanium™ Patch
- Tanium™ Deploy
- Tanium™ Interact
- Tanium™ Connect

Reporting requirement for endpoint details

- Tanium™ Reporting

SBOM vulnerability assessment

- Tanium™ SBOM
- Tanium™ Client Index Extension

Container registry vulnerability assessment

- Tanium™ Cloud Workloads
- Tanium™ SBOM

Tanium Scan Engine 7.0

©2026 Tanium Inc. All Rights Reserved

- Tanium™ Client Index Extension

Client extensions and endpoint tools

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

Note: The change management feature of Endpoint Configuration might affect the version of each endpoint tool installed on endpoints. For more information, see Configure Tanium Endpoint Configuration on page 53.

Endpoints

Supported operating systems

Tanium Client operating system support for Comply is the same as Tanium Client support (see Tanium Client Management User Guide: Client version and host system requirements) with the following exceptions.

Comply supports Oracle Solaris endpoints as follows:

Solaris endpoint support

Operating System	Version
Solaris	Minimum version: • Oracle Solaris 10u11 SPARC or later • Oracle Solaris 10u11 x86 or later

Comply supports AIX endpoints for compliance and vulnerability scans as follows:

©2026 Tanium Inc. All Rights Reserved

AIX endpoint support

Operating System	Version
AIX	7.1.4 or later The IBM XL C++ runtime libraries file set (xlC.rte), version 16.1.0.0 or later, and the IBM LLVM runtime libraries file set (libc++.rte) must be installed. For installation instructions, see Tanium Client Management User Guide: Deploying the Tanium Client to AIX endpoints using a package file .

Note: Comply supports AIX endpoints for vulnerability assessments. For compliance assessments on AIX endpoints, only custom checks and automated AIX benchmarks up to version 1.1.0 are supported.

Disk space requirements

Endpoints must have at least 2 gigabytes (GB) available in free disk space.

If you are using SBOM scan assessments, you should have an additional 2 GB of free disk space.

Resource recommendations for satellites running remote authenticated scans

Satellite endpoints should have a minimum of 16 gigabytes (GB) RAM, 4 CPUs, and a 64-bit operating system.

Note: A minimum of 4 gigabytes (GB) allocation will be reserved by default for RAS scan heap size requirements. This can be increased in Comply Custom Settings.

Scan engines

A scan engine evaluates endpoints for security configuration exposures and software vulnerabilities using industry security standards, vulnerability definitions, and custom compliance checks.

©2026 Tanium Inc. All Rights Reserved

In Comply, the scan engine evaluates Open Vulnerability Assessment Language (OVAL) or Security Content Automation Protocol (SCAP) content to determine endpoint compliance and vulnerability status. Comply generates findings based on the results of this evaluation by the scan engine.

At least one scan engine is required to use Comply. Comply includes the Tanium Scan Engine and Amazon Corretto Java Runtime Environment (JRE) in the **Comply Engines** tool. For more information, see Deploying the legacy Tanium Scan Engine and JRE using ECM on page 85. JRE version 11.x is provided for use with supported Windows, Linux, and macOS endpoints. JRE version 11.0.15.9.1 and later also support Mac on Apple silicon (M1 and later) and Amazon Linux 2 EC2. Most organizations can use the Tanium Scan Engine and Amazon Corretto JRE and do not need to upload any scan engines or JREs.

Note: The Amazon Corretto JRE v11.x provided with the latest Tanium Scan Engine is not supported on Red Hat Enterprise Linux 5, Oracle Linux Server 5, CentOS 5, Solaris, AIX, Windows 7, and Server 2008 R2. For legacy operating systems, an earlier version of the Tanium Scan Engine is provided, but you will need to upload and target your own Java 8 JREs on the **Configuration** page.

Tanium Scan Engine and CIS-CAT also require PowerShell and do not work if PowerShell is in ConstrainedLanguage mode.

If needed, you can upload other scan engines to Comply. Comply supports the Tanium Scan Engine (which is included by default), SCC (used by the United States government), and CIS-CAT scan engines (for compliance scans). The supported versions of the scan engines are listed in the Import Engine window and on this page: Reference: Supported engines and JREs on page 333.

The following JRE requirements apply to the legacy Tanium Scan Engine. Client-based vulnerability scans that use Tanium Scan Engine 7.0 do not require a Java runtime on the endpoint.

Supported JRE distributions by operating system (legacy Tanium Scan Engine)

Operating system	Operating system version	Supported JRE distributions and versions	Can deploy using Comply?
Microsoft Windows Server	Microsoft Windows Server 2008 R2	Java version 8 distributions provided by Oracle	Yes [4]
	Microsoft Windows Server 2012 and 2012 R2	• JRE provided with Comply • Java version 8 distributions provided by	Yes

©2026 Tanium Inc. All Rights Reserved

Operating system	Operating system version	Supported JRE distributions and versions	Can deploy using Comply?
		either Oracle or Amazon	
	Microsoft Windows Server 2016 and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
Microsoft Windows Workstation	Microsoft Windows 7	Java version 8 distributions provided by Oracle	Yes [4]
	Microsoft Windows 10 and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
macOS	macOS 10.15 Catalina and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
Linux	Amazon Linux 2023	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	Amazon Linux 1 AMI (2016.09, 2018.03)	• JRE provided with Comply • Java version 8 distributions provided by Amazon	Yes
	Amazon Linux 2 LTS	• JRE provided with Comply • Java version 8 distributions provided by Amazon	Yes
	Debian 8.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	Red Hat Enterprise Linux (RHEL) 5.x	Upload your own version of Java 8	No [5]

©2026 Tanium Inc. All Rights Reserved

Operating system	Operating system version	Supported JRE distributions and versions	Can deploy using Comply?
	Red Hat Enterprise Linux (RHEL) 6.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	AlmaLinux 8.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	Rocky Linux 8.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	Oracle Linux 5.x and later	Java version 8 distributions provided by either Oracle or Amazon	Yes
	CentOS 6.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	SUSE Linux Enterprise Server (SLES) 12.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	openSUSE 12.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	Ubuntu 14.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
AIX	IBM AIX 7.1 TL1SP10 and later [1]	IBM JRE 8	Yes [2]
		OpenJDK JRE version 8 with the HotSpot JVM	Yes [3]

©2026 Tanium Inc. All Rights Reserved

Operating system	Operating system version	Supported JRE distributions and versions	Can deploy using Comply?
	IBM AIX 7.2	IBM JRE version 8	Yes [2]
		OpenJDK JRE version 8 with the HotSpot JVM	Yes [3]
Solaris [4]	Oracle Solaris 10u11 SPARC	Oracle JRE 8	Yes [4]
	Oracle Solaris 10u11 x86 [1]	Oracle JRE 8	Yes [4]
	Oracle Solaris 11 SPARC	Oracle JRE 8	Yes [4]
	Oracle Solaris 11 x86 [1]	Oracle JRE 8	Yes [4]

[1] 64-bit only.

[2] Only IBM JRE 8 64-bit is supported for deployment through Comply. You must repackage the JRE before it can be deployed through Comply. For more information, see Repackage the IBM JRE for deployment to AIX endpoints on page 362.

[3] Only version 8 is supported for deployment through Comply. Check the OpenJDK release site for supported service pack levels for a particular OpenJDK JRE release: AdoptOpenJDK: Latest release.

[4] Only version 8 is supported for deployment through Comply. Upload Java version 8 distributions provided by Oracle. See Import JREs on page 94. This footnote applies to the legacy Tanium Scan Engine. Tanium Scan Engine 7.0 vulnerability scans on Solaris do not require a JRE.

[5] The JRE provided with Comply may not work with older versions of Linux. Refer to the support information provided in Amazon Corretto FAQs. Upload your own version of Java 8 if you have older versions of Linux.

For more information, see Working with scan engines on page 74.

Unmanaged Endpoints

This section refers to remote authenticated scan support for unmanaged endpoints. Unmanaged endpoints are endpoints that do not have the Tanium Client installed. Comply provides standards for scanning the following unmanaged endpoints using a remote authenticated scan:

©2026 Tanium Inc. All Rights Reserved

Important: Listed operating systems may not be supported for both compliance and vulnerability scans. For the most complete, up to date support information, refer to the list of benchmarks and CVEs provided by the links in the table below.

Unmanaged endpoints, no Tanium client installed

Operating system	Operating system version
Cisco Systems	Compliance scan support: • Cisco ASA 9.x • Cisco ASA 8.x • Cisco IOS 15 • Cisco IOS 16 • Cisco NX OS • Cisco IOS-XE 12.2+ (There is no certified CIS benchmark, but Tanium has tested against the Cisco IOS-XE Router NDM STIG Benchmark and Cisco IOS-XE Router RTR STIG Benchmark)
	Vulnerability scan support: • Cisco IOS 12.2+ • Cisco IOS-XE 12.2+ • Cisco ASA 9.0+ • Cisco NX OS
Juniper Networks	Compliance and Vulnerability scan support: JunOS 8.5R1 and later
Palo Alto Networks	Compliance scan support only: • PanOS 10 • PanOS 11
VMware	• ESX • ESXi
All operating systems supported by	Remote authenticated scanning is useful for obtaining information from endpoints and subnets that do not support having the Tanium Client installed. Although you can use remote authenticated scanning for endpoints that do support the Tanium Client, you should use client-based scanning in that case for performance reasons and

©2026 Tanium Inc. All Rights Reserved

Operating system	Operating system version
the Tanium Client	to take advantage of the linear chain architecture. * Some standards are still provided for older OS types that do not support the Tanium Client and therefore could be scanned using remote authenticated scanning, such as Windows XP. The complete list of standards is viewable in the **Standards** dropdown field when you create an assessment. The complete list of benchmarks Comply provides can be viewed here: https://content.tanium.com/files/published/tvl/benchmarks.html The complete list of CVEs Comply provides can be viewed here: https://content.tanium.com/files/published/tvl/tvl.html (Both lists are updated daily and should display newly added benchmarks and CVEs as they appear in Comply.)

See Configure a remote authenticated scan assessment on page 125 for configuration details.

Host and network security requirements

Specific ports and processes are needed to run Comply.

Ports

The following ports are required for remote authenticated scanning.

Port requirements

Source	Destination	Port	Protocol	Purpose
Satellite	Scan target endpoint	22	TCP	Required for SSH endpoints
Satellite	Scan target endpoint	5985	TCP	Required for Windows remote management
Satellite	Scan target endpoint	443	TCP	Required for VMware API endpoints

©2026 Tanium Inc. All Rights Reserved

Important: Remote authenticated scanning results are received by the Tanium Server using Direct Connect. See Direct Connect: Host and network security requirements for DEC port requirements.

Note: All other Comply port requirements are the same as Tanium Client port requirements. See Tanium Client: Network connectivity, ports, and firewalls.

Security exclusions

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

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

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

Comply security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	*<Module Server>* \services\comply-service\node.exe
		Process	*<Module Server>* \services\comply-service\node_modules\ovalindex\build\bin\ovalindex.exe

©2026 Tanium Inc. All Rights Reserved

Target Device	Notes	Exclusion Type	Exclusion
		Process	*<Module Server>* \services\endpoint-configuration-service\ TaniumEndpointConfigService.exe
		Process	*<Module Server>* \services\comply-service__new__\src\lib\bzip\platform-*\win-x64\ TaniumExtractor.exe

Tanium Comply security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Exclusion
Windows		Process	*<Tanium Client>* \TaniumCX.exe
	Required if using the Tanium Scan Engine	File	*<Tanium Client>* \extensions\comply\engines\ joval\Joval-Utilities.jar
		File	*<Tanium Client>* \TaniumClientExtensions.dll
		File	*<Tanium Client>* \TaniumClientExtensions.dll.sig
		File	*<Tanium Client>* \extensions\TaniumComply.dll
		File	*<Tanium Client>* \extensions\ TaniumComply.dll.sig
		File	*<Tanium Client>* \extensions\comply\data\ comply.db
		File	*<Tanium Client>* \extensions\comply\data\ current-ciscat-config.json
		File	*<Tanium Client>* \extensions\comply\data\ current-intel-config.json
		File	*<Tanium Client>* \extensions\comply\data\ current-java-config.json
		File	*<Tanium Client>* \extensions\comply\data\ current-joval-config.json
		File	*<Tanium Client>* \extensions\comply\data\ current-scan-config.json
		File	*<Tanium Client>* \extensions\comply\ downloads\download.db

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
		Process	*<Tanium Client>* \extensions\comply\jre\bin\java.exe
		File	*<Tanium Client>* \Tools\Comply\run-assessment.vbs
		File	*<Tanium Client>* \Tools\Comply\delete-assessment.vbs
Linux/macOS/AIX		Process	*<Tanium Client>* /TaniumCX
	Required if using the Tanium Scan Engine	File	*<Tanium Client>* /extensions/comply/engines/joval/Joval-Utilities.jar
		File	*<Tanium Client>* /libTaniumClientExtensions.so
		File	*<Tanium Client>* /libTaniumClientExtensions.so.sig
		File	*<Tanium Client>* /extensions/libTaniumComply.so
		File	*<Tanium Client>* /extensions/libTaniumComply.so.sig
		File	*<Tanium Client>* /extensions/comply/data/comply.db
		File	*<Tanium Client>* /extensions/comply/data/current-ciscat-config.json
		File	*<Tanium Client>* /extensions/comply/data/current-intel-config.json
		File	*<Tanium Client>* /extensions/comply/data/current-java-config.json
		File	*<Tanium Client>* /extensions/comply/data/current-joval-config.json
		File	*<Tanium Client>* /extensions/comply/data/current-scan-config.json
		File	*<Tanium Client>* /extensions/comply/downloads/download.db
		Process	*<Tanium Client>* /extensions/comply/jre/bin/java
		File	*<Tanium Client>* /Tools/Comply/run-assessment.sh
		File	*<Tanium Client>* /Tools/Comply/delete-assessment.sh

©2026 Tanium Inc. All Rights Reserved

Endpoint OS	Notes	Exclusion Type	Exclusion
SCC engine - Windows		Process	*<Tanium Client>* \extensions\comply\engines\scc\cscc.exe
		Process	*<Tanium Client>* \extensions\comply\engines\scc\lib32\cscc32.exe
		Process	*<Tanium Client>* \extensions\comply\engines\scc\lib64\cscc64.exe
		Process	*<Tanium Client>* \extensions\comply\engines\scc\scc.exe
		Process	*<Tanium Client>* \extensions\comply\engines\scc\lib32\scc32.exe
		Process	*<Tanium Client>* \extensions\comply\engines\scc\lib64\scc64.exe
SCC engine - Linux/macOS		Process	*<Tanium Client>* /extensions/comply/engines/scc/cscc
		File	*<Tanium Client>* /extensions/comply/engines/scc/cscc.bin
		Process	*<Tanium Client>* /extensions/comply/engines/scc/scc
		File	*<Tanium Client>* /extensions/comply/engines/scc/scc.bin
CIS-CAT engine-all supported endpoints		File	*<Tanium Client>* /extensions/comply/engines/ciscat/CISCAT.jar
CIS-CAT engine-Linux		File	*<Tanium Client>* /extensions/comply/engines/ciscat/CIS-CAT.sh
CIS-CAT engine-Windows		File	*<Tanium Client>* \extensions\comply\engines\ciscat\CIS-CAT.BAT

Note: For remote vulnerability assessments, see Tanium Discover User Guide: Host and network security requirements for Nmap security exclusions.

For best results, add a recursive security exclusion for the Tanium Client directory:

- Windows endpoints: <Tanium Client>

  This path is usually C:\Program Files (x86)\Tanium\Tanium Client.

©2026 Tanium Inc. All Rights Reserved

- Linux endpoints: /opt/Tanium/TaniumClient

User role requirements

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

- Table 13. Comply solution permissions on page 41
- Table 15. Comply platform content user role permissions on page 46: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Comply users on page 55.

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

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



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

Comply solution permissions

Permission	Comply Administrator	Comply Operator	Comply Deployment Administrator	Comply Report Content Administrator	Comply Report Administrator
Comply View the Comply workbench	✓	✓	✓	✓	✓

©2026 Tanium Inc. All Rights Reserved

Permission	Comply Administrator	Comply Operator	Comply Deployment Administrator	Comply Report Content Administrator	Comply Report Administrator
	ADMIN OPERATOR SHOW	OPERATOR SHOW	SHOW	SHOW	SHOW
Comply Components Manage all back-end components in Comply such as actions	✗	✗	✗	✗	✗
Comply Custom Check View, create, and edit custom checks	✓ WRITE	✓ WRITE	✗	✗	✗
Comply Deployment View, create, and edit targets and update Comply engines	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✗	✗
Comply Exception View and create findings exceptions	✓ READ WRITE	✓ READ WRITE	✗	✗	✗
Comply Investigation View and create findings investigations	✓ EXECUTE	✓ EXECUTE	✗	✗	✗
Comply Report View, create, and edit Comply reports and assessments	✓ READ WRITE	✓ READ WRITE	✗	✗	✓ READ WRITE
Comply Report Content View and manage Comply standards	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ

©2026 Tanium Inc. All Rights Reserved

Permission	Comply Administrator	Comply Operator	Comply Deployment Administrator	Comply Report Content Administrator	Comply Report Administrator
	WRITE	WRITE	WRITE	WRITE	
Comply Reports View and create reports (minimum required privileges for viewing and creating reports and findings)	✗	✗	✗	✗	✓ READ WRITE
Comply Credential View, create, and edit credentials for RAS assessments	✓ READ WRITE	✓ READ WRITE	✗	✗	✓ READ
Comply RAS Assessment View, create, and edit RAS assessments	✓ READ WRITE	✓ READ WRITE	✗	✗	✓ READ WRITE
Comply Scan View assessments and run on demand scans	✓ EXECUTE	✓ EXECUTE	✗	✗	✓ EXECUTE
Comply Endpoint Configuration Enables approver privileges in Tanium Endpoint Configuration for Comply changes	✗	✗	✗	✗	✗
Interact Result Expansion Content View, create, and edit expansions (internal purposes only)	✓ READ WRITE	✓ READ WRITE	✗	✗	✗

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

©2026 Tanium Inc. All Rights Reserved

Permission	Comply Administrator	Comply Operator	Comply Deployment Administrator	Comply Report Content Administrator	Comply Report Administrator
effective role permissions .					

Comply solution permissions (continued)

Permission	Comply Report Reviewer	Comply Custom Check Writer	Comply RAS Assessment Creator	Comply Endpoint Configuration Approver
Comply View the Comply workbench	✓ SHOW	✓ SHOW	✓ SHOW	✗
Comply Components Manage all back-end components in Comply such as actions	✗	✗	✗	✗
Comply Custom Check View, create, and edit custom checks	✗	✓ WRITE	✗	✗
Comply Deployment View, create, and edit targets and update Comply engines	✗	✗	✗	✗
Comply Exception View and create findings exceptions	✗	✗	✗	✗
Comply Investigation View and create findings investigations	✗	✗	✗	✗
Comply Report View, create, and edit Comply reports and assessments	✓ READ	✗	✓ READ WRITE	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Comply Report Reviewer	Comply Custom Check Writer	Comply RAS Assessment Creator	Comply Endpoint Configuration Approver
Comply Report Content View and manage Comply standards	✓ READ	✓ READ	✓ READ	✗
Comply Reports View and create reports (minimum required privileges for viewing and creating reports and findings)	✓ READ	✗	✗	✗
Comply Credential View, create, and edit credentials for RAS assessments	✗	✗	✓ READ	✗
Comply RAS Assessment View, create, and edit RAS assessments	✗	✗	✓ READ WRITE	✗
Comply Scan View assessments and run on demand scans	✗	✗	✓ EXECUTE	✗
Comply Endpoint Configuration Enables approver privileges in Tanium Endpoint Configuration for Comply changes	✗	✗	✗	✓ APPROVE
Interact Result Expansion Content View, create, and edit expansions (internal purposes only)	✗	✗	✗	✗

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

©2026 Tanium Inc. All Rights Reserved

Comply platform content user role permissions

Permissions	Comply Administrator	Comply Operator	Comply Deployment Administrator	Comply Report Content Administrator
Action	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✗
Action For Saved Question	✓ WRITE	✓ WRITE	✗	✗
Own Action	✓ READ	✓ READ	✓ READ	✗
Package	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✗
Plugin	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE
Saved Question	✓ READ WRITE	✓ READ WRITE	✓ READ WRITE	✗
Sensor	✓ READ	✓ READ	✓ READ	✗

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

Comply platform content user role permissions (continued)

Permissions	Comply Report Administrator	Comply Report Reviewer	Comply Custom Check Writer	Comply RAS Assessment Creator
Action	✓	✓	✗	✓

©2026 Tanium Inc. All Rights Reserved

Permissions	Comply Report Administrator	Comply Report Reviewer	Comply Custom Check Writer	Comply RAS Assessment Creator
	READ WRITE	READ		READ WRITE
Action For Saved Question	✓ WRITE	✗	✗	✓ WRITE
Own Action	✓ READ	✓ READ	✗	✓ READ
Package	✓ READ WRITE	✗	✗	✓ READ WRITE
Plugin	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE
Saved Question	✓ READ WRITE	✓ READ	✗	✓ READ WRITE
Sensor	✓ READ	✓ READ	✗	✓ READ

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

©2026 Tanium Inc. All Rights Reserved

Installing Comply

Install Comply from the **Solutions** page and choose automatic configuration with recommended defaults or manual configuration with custom settings.

About this task

Use the **Solutions** page to install Comply and choose either automatic or manual configuration:

- Automatic configuration with default settings: Comply is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information, see Import Comply with default settings on page 48.
- Manual configuration with custom settings: After installing Comply, you must manually configure required settings. Select this option only if Comply requires settings that differ from the recommended default settings. For more information, see Import Comply with custom settings on page 50.

Before you begin

Before you begin, review the release notes, requirements, and upgrade information for Tanium Comply.

- Read the .
- Review the Comply requirements on page 26.
- If you are upgrading from a previous version, see Upgrade Comply on page 51.

Import Comply with default settings

Import Comply with Tanium-recommended default settings by applying all recommended configurations during module import, then verify that the correct version is installed.

About this task

©2026 Tanium Inc. All Rights Reserved

When you import Comply with automatic configuration, the following default settings are configured:

Default settings for Tanium Comply

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group
Comply tools	Comply tools and the Legacy Tanium Scan Engine are deployed to endpoints.
Default configuration	The default configuration does the following: • Sets up a scheduled TVL download (by default 3am every day) • Downloads and imports the certified benchmarks from content.tanium.com • Downloads and installs the engines • Downloads the latest TVL • Creates default compliance and vulnerability assessments for each operating system

Note: Scans begin to run after the installation completes.

Note: Deployments begin immediately after solution installation. The **Distribute over** setting for the deployments is set to three minutes. After the three minute distribution window completes, reports will run. The **Distribute over** setting for reports is also three minutes.

To import Comply and configure default settings, be sure to select the **Apply All Tanium recommended configurations** option while performing the steps in Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed: see Verify Comply version on page 51.

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

©2026 Tanium Inc. All Rights Reserved

deployment and restricted targeting.

Default settings for Comply

When you import Comply with automatic configuration, the following default settings are configured:

Default settings for Tanium Comply

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group
Comply tools	Comply tools and the Legacy Tanium Scan Engine are deployed to endpoints.
Default configuration	The default configuration does the following: • Sets up a scheduled TVL download (by default 3am every day) • Downloads and imports the certified benchmarks from content.tanium.com • Downloads and installs the engines • Downloads the latest TVL • Creates default compliance and vulnerability assessments for each operating system

Note: Scans begin to run after the installation completes.

Note: Deployments begin immediately after solution installation. The **Distribute over** setting for the deployments is set to three minutes. After the three minute distribution window completes, reports will run. The **Distribute over** setting for reports is also three minutes.

Import Comply with custom settings

Import Comply without applying default Tanium-recommended configurations, then verify the installed version and configure the Comply action group as needed.

About this task

To import Comply without automatically configuring default settings, be sure to clear the **Apply All**

©2026 Tanium Inc. All Rights Reserved

Tanium recommended configurations checkbox while performing the steps in Tanium Console User Guide: Import, re-import, or upgrade to the latest versions of specific modules. After the import, verify that the correct version is installed: see Verify Comply version on page 51.

Reports and statistics on the Comply **Home** page might not be updated immediately with current results since this data is updated every 10 minutes.

To configure the Comply action group, see Configure the Comply action group on page 54.

Other Tanium solutions are required for Comply to function (required dependencies) or for specific Comply features to work (feature-specific dependencies).

Upgrade Comply

Learn where to find the steps to upgrade Comply and how to verify the installed version, including guidance on troubleshooting upgrade issues.

For the steps to upgrade Comply, see Tanium Console User Guide: Manage Tanium modules. After the upgrade, verify that the correct version is installed: see Verify Comply version on page 51.



Note: For information on upgrade issues you may experience, see the Troubleshooting Comply on page 310 section.

Verify Comply version

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

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

©2026 Tanium Inc. All Rights Reserved

Configuring Comply

Configure Comply features and default settings when Tanium-recommended configurations are not applied during installation.

About this task

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

Default settings for Comply

When you import Comply with automatic configuration, the following default settings are configured:

Default settings for Tanium Comply

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group
Comply tools	Comply tools and the Legacy Tanium Scan Engine are deployed to endpoints.
Default configuration	The default configuration does the following: • Sets up a scheduled TVL download (by default 3am every day) • Downloads and imports the certified benchmarks from content.tanium.com • Downloads and installs the engines • Downloads the latest TVL • Creates default compliance and vulnerability assessments for each operating system



Note: Scans begin to run after the installation completes.

©2026 Tanium Inc. All Rights Reserved

Note: Deployments begin immediately after solution installation. The **Distribute over** setting for the deployments is set to three minutes. After the three minute distribution window completes, reports will run. The **Distribute over** setting for reports is also three minutes.

Manage solution configurations with Tanium Endpoint Configuration

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

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

Important:

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

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

©2026 Tanium Inc. All Rights Reserved

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

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

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

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

Configure Comply

Configure Comply to align with your policies, workflows, and organizational compliance requirements.

Configure the Comply action group

Configure the Tanium Comply action group to target the appropriate endpoints or update it when configuration changes are required.

About this task

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

If you used automatic configuration and restricted targeting was disabled when you imported

©2026 Tanium Inc. All Rights Reserved

Comply, configuring the Comply action group is optional.

Important: You must register sensors that are referenced by the action group. For more information, see Register or unregister sensors for collection.

You can update the action group if needed.

1. From the Main menu, go to **Administration** > **Actions** > **Action Groups**.
2. Select **Tanium Comply** and click **Edit** to update the action group.

Set up Comply users

Use predefined Comply user roles to configure access, manage deployments, and control how users create, review, and administer compliance content.

About this task

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

To review specific permissions for each role, see User role requirements on page 41.

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

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

Comply Administrator

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

- View and modify Comply configurations
- Create deployments to endpoints and update engines
- View and modify Comply standards

©2026 Tanium Inc. All Rights Reserved

Comply Operator

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

- View and modify Comply configurations
- Create deployments to endpoints and update engines
- View and modify Comply standards

Comply Deployment Administrator

Assign the **Comply Deployment Administrator** role to users who create and view Comply endpoint configurations. This role can perform the following tasks:

- Create deployments to endpoints and update engines
- View and modify Comply standards

Comply Report Content Administrator

Assign the **Comply Report Content Administrator** role to users who create and manage Comply compliance and vulnerability standards. This role can view and modify Comply standards.

Comply Report Administrator

Assign the **Comply Report Administrator** role to users who configure and manage Comply assessments. This role can perform the following tasks:

- View and modify Comply assessments and reports
- View Comply standards

Comply Report Reviewer

Assign the **Comply Report Reviewer** role to users who review Comply assessments and standards. This role can perform the following tasks:

- View Comply assessments and reports
- View Comply standards

©2026 Tanium Inc. All Rights Reserved

Comply Custom Check Writer

Assign the **Comply Custom Check Writer** role to users who create custom checks to review a condition on endpoints that might not be included in any standard. This role can perform the following tasks:

- View and modify custom checks
- View Comply standards

Comply RAS Assessment Creator

Assign the **Comply RAS Assessment Creator** role to a user to users who configure and manage remote authenticated scans. This role can perform the following tasks:

- View and modify credentials
- View and modify RAS assessments

Comply Endpoint Configuration Approver

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

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

Deploy scan engines and JREs

Deploy scan engines and Java Runtime Environments (JREs) for on-premises installations.

About this task

A scan engine evaluates endpoints for security configuration exposures and software vulnerabilities using industry security standards, vulnerability definitions, and custom compliance checks.

In Comply, the scan engine evaluates Open Vulnerability Assessment Language (OVAL) or Security Content Automation Protocol (SCAP) content to determine endpoint compliance and vulnerability

©2026 Tanium Inc. All Rights Reserved

status. Comply generates findings based on the results of this evaluation by the scan engine.

At least one scan engine is required to use Comply. Comply includes the Tanium Scan Engine and Amazon Corretto Java Runtime Environment (JRE) in the **Comply Engines** tool. For more information, see Deploying the legacy Tanium Scan Engine and JRE using ECM on page 85. JRE version 11.x is provided for use with supported Windows, Linux, and macOS endpoints. JRE version 11.0.15.9.1 and later also support Mac on Apple silicon (M1 and later) and Amazon Linux 2 EC2. Most organizations can use the Tanium Scan Engine and Amazon Corretto JRE and do not need to upload any scan engines or JREs.

Note: The Amazon Corretto JRE v11.x provided with the latest Tanium Scan Engine is not supported on Red Hat Enterprise Linux 5, Oracle Linux Server 5, CentOS 5, Solaris, AIX, Windows 7, and Server 2008 R2. For legacy operating systems, an earlier version of the Tanium Scan Engine is provided, but you will need to upload and target your own Java 8 JREs on the **Configuration** page.

Tanium Scan Engine and CIS-CAT also require PowerShell and do not work if PowerShell is in ConstrainedLanguage mode.

If needed, you can upload other scan engines to Comply. Comply supports the Tanium Scan Engine (which is included by default), SCC (used by the United States government), and CIS-CAT scan engines (for compliance scans). The supported versions of the scan engines are listed in the Import Engine window and on this page: Reference: Supported engines and JREs on page 333.

Create deployments

Create deployments to deliver engines and JREs to targeted endpoints based on their architecture and platform.

About this task

You must have the **Comply Deployment Administrator** role to create deployments. For more information, see User role requirements on page 41.

Create deployments based on the architecture and platform of the targeted endpoints to deploy engines and JREs to endpoints on a schedule. For example, you might want to create the following deployments:

- Windows 64-bit

©2026 Tanium Inc. All Rights Reserved

- Windows 32-bit
- macOS 64-bit
- Linux 64-bit

Best Practice:

- Ensure that the computer groups targeted by each deployment include all applicable endpoints. Review the deployments to confirm that no computer groups are missing.
- Ensure that deployment are created for all possible architectures (bitness) and platforms. For example, some environments still contain 32-bit Linux and Windows endpoints. These endpoints require specific deployments.

For steps to create a deployment, see Setting up endpoints on page 101.

Restrict assessment visibility

Limit assessment visibility so reviewers can only see assessments that target computer groups they are authorized to manage.

About this task

By default, users with the **Comply Assessment Reviewer** role can see all assessments, even assessments that target computer groups for which the user does not have management rights.

If you want users to only see assessments that target computer groups for which they have management rights, set the **Management Rights: Filtering** setting to **On**. When you enable this setting, users can only see assessments when they have management rights to all computer groups that the assessment targets. If an assessments targets multiple computer groups, but the user does not have management rights to one or more of the targeted computer groups, the user cannot see the assessment.

1. From the Main menu, go to **Modules** > **Comply > Overview** and click Settings .
2. Find the **Management Rights: Filtering** setting and click **Edit**.
3. In the **Edit Setting** window, turn the setting **On**.

©2026 Tanium Inc. All Rights Reserved

4. Click **Save**.

Result

The change takes effect immediately and does not require you to restart Comply.

Create assessments

Use the Assessments page to create and manage configuration compliance, vulnerability, and network unauthenticated assessments.

About this task

From the Main menu, go to **Modules** > **Comply > Assessments** to open the **Assessments** page. From this page, you can create configuration compliance assessments, vulnerability assessments, and network unauthenticated assessments. You can also view and update existing assessments.

For more information, see Creating compliance assessments on page 121 and Creating vulnerability assessments on page 146.

Configure Comply for an air-gapped environment

Configure Comply to operate in an air-gapped environment and manually upload Tanium Engines and Tanium Vulnerability Library files.

About this task

When your Tanium Server is in an air-gapped environment, the server cannot download the Tanium Engines or Tanium Vulnerability Library files from the internet. You must configure Comply for an air-gapped environment and upload these files to Comply.

Important: Starting with Comply 2.13, Tanium Vulnerability Library files on content.tanium.com support CVSS v3 and higher. If you are upgrading from a previous version and are in airgap mode, it is recommended that you upgrade to the latest TVL prior to upgrading to Comply 2.13. For more information, see Upload the Tanium Vulnerability Library files on page 61 for instructions.

1. From the Main menu, go to **Modules** > **Comply > Overview** and click Settings.
2. Find the **Is Airgapped** setting and turn it **On**.

©2026 Tanium Inc. All Rights Reserved

3. Click **Save**.

Result

Important: You must restart Comply each time you change the value of the **is_airgapped** setting for the Tanium Vulnerability Library (TVL) to update properly.

Upload the Tanium Engines package

Download the air-gap engine manifest and Joval license on an Internet-connected machine, transfer them to the air-gapped machine, and upload them in the Tanium Engines configuration.

About this task

1. From the Main menu, go to **Modules** > **Comply**, click **Setup** > **Configuration** and go to the **Engines** tab.
2. Click **Upload Airgap Engine Files**.
3. Download the air-gap engine files from the link indicated in the **Upload Airgap Engine Files** window, using a machine that can connect to the Internet, and save them on the air-gapped machine. You must download the both the engines manifest and the standalone Joval license.
    - Download the supported engines manifest from https://content.tanium.com/files/published/comply-engines/supported-engines.cson
    - Download the Joval license from https://content.tanium.com/files/published/comply-engines/joval.sig.cml
4. Click **Browse for Files** in the **Upload Airgap Engine Files** window, and upload the engine and Joval license files from the location where you saved them on the air-gapped machine.
5. After your upload is complete, click **Close**.

UPLOAD THE TANIUM VULNERABILITY LIBRARY FILES

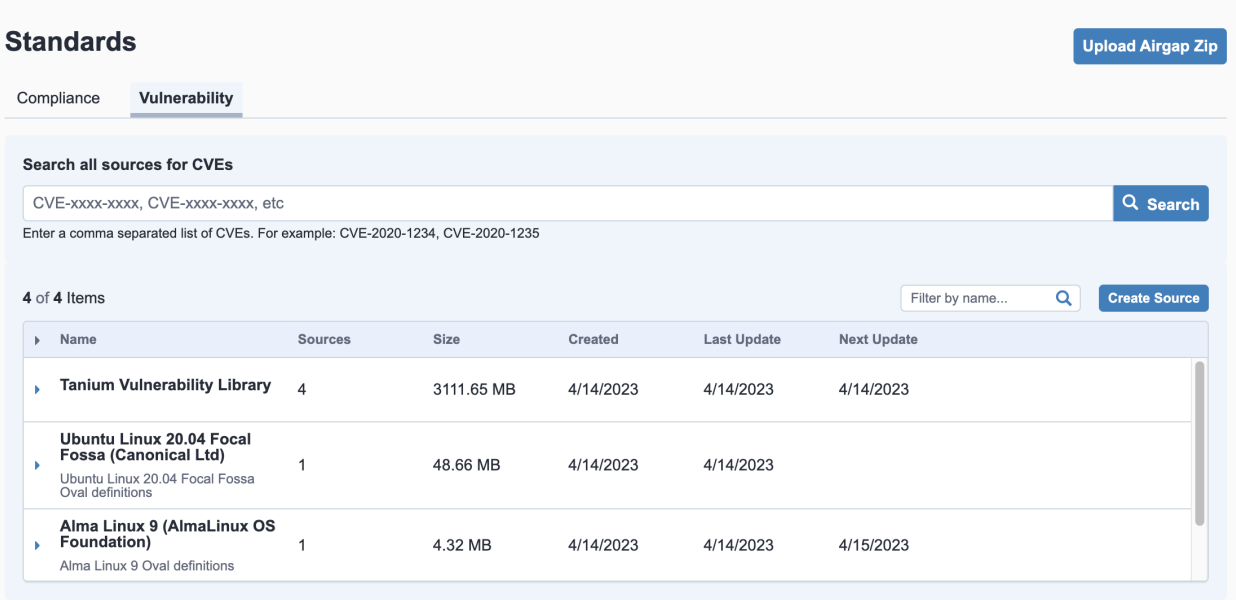
Upload the Tanium Vulnerability Library air gap ZIP file to update the Comply vulnerability standards on an air-gapped environment.

About this task

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Comply**, and click **Standards** > **Vulnerability** to open the **Vulnerability Standards** page.

2. Click **Upload Airgap Zip**.



3. Download the air gap ZIP file from the link indicated in the **Upload Tanium Standards Library Airgap Zip** window (https://content.tanium.com/files/published/tvl/Comply-Standards-Airgap-v2.zip) using a machine that can connect to the internet and save it on the air-gapped machine.

> **Note:** Starting with Comply 2.22 or later, you should use Comply-Standards-Airgap-v2.zip since that has a valid SBOM intel DB. (Comply-Standards-Airgap-v1.zip does not).

4. Click **Select File**, select the Comply-Standards-Airgap-v2.zip file from the location where you saved it on the air-gapped machine, and click **Open**.

5. Click **Upload**.

6. After your upload is complete, click **Close** on the **Upload Tanium Standards Library Airgap Zip** window. Allow approximately five minutes for Comply to update the vulnerability standards. If you expand a vulnerability source, you will see the **Type** indicated as **Local** as well as a completed count of **CVEs** after the standards are successfully updated from the uploaded air gap ZIP file.

©2026 Tanium Inc. All Rights Reserved

Note: File uploads have a default file size setting. If you edit this value, you must restart the Comply process for this change to take effect. See Managing application settings on page 301.

Configure credentials lists for remote-authenticated scans

Configure credentials lists so satellites can use remote-authenticated scans to securely access endpoints without the Tanium Client installed.

About this task

For satellites to perform secure scans of endpoints without the Tanium Client installed, the login credentials for those endpoints are required. Following the instructions detailed here, add endpoint credentials for use in remote-authenticated scans.

Note: The Comply **Credential** RBAC permission is required to configure credentials.

CAUTION: Use as few sets of credentials as possible for any credential lists used for satellite scans. Adding more credentials can increase the time necessary to complete a task as the task attempts each set of credentials. Additionally, the more credentials you use, the greater risk you run of credentials failing and possibly triggering security alerts or account lockouts.

1. From the Main menu, go to **Modules** > **Comply** and click **Setup** > **Credentials Lists**. Then click **Create**.
2. In the **Summary** section, configure the following:
   - Enter a **Name** and **Description** for the credentials list.
   - The **Content Set** is **Comply**. (This cannot be changed at this time.)
3. In the **Credentials** section, click **Add**.
   - **Best Practice:** Create separate credentials for each login service type.
4. In the **Login Service** section, select the connection method: **WinRM, SSH, VMware API** or **Palo Alto Networks**.

©2026 Tanium Inc. All Rights Reserved

- If you are using WinRM credentials, do the following
    - (Optionally) Enter a **Domain** name.
    - Enter a **Username**.
    - Enter the corresponding **Password**.
    - For **Port** number, enter a single port or comma-separated list of ports. The default is 5985.
    - Click **Add**.
- If you are using SSH credentials, do the following:
    - Select an **Authentication Type**: **SSH Key (recommended)** or **Password**.
        - For **SSH**, a **Username** and **SSH Private Key** are required. A **Keyphrase** is optional.
        - For **Password**, a **Username** and **Password** are required.
        - For **Port** number, enter a single port or comma-separated list of ports. The default is 22.
    - Expand **Advanced Settings** to optionally configure one or more of the following:
        -  **Note:** The fields provided here allow the Tanium Scan Engine to perform compliance and vulnerability checks that require elevated privileges. The engine knows when it needs to use these additional privileges to gain access to endpoints. For example, on a Cisco Systems endpoint, there are configuration settings that require elevated privileges to read the value so that the Tanium Scan Engine can evaluate a compliance rule. If the Tanium Scan Engine requires these privileges for an endpoint and they are not provided here, it will return an error status for those rules, instead of pass or fail.
        - For **Sudo Escalation**, select the **checkbox** to indicate that the sudo command should be used for privilege escalation. If you enable the

©2026 Tanium Inc. All Rights Reserved

checkbox, and the authentication type is SSH Key, you must also enter a **Password** here.

- For **Cisco IOS Enable Password**, enter the password for privilege elevation on Cisco IOS devices.
- Under **Substitute Credentials**, enter a **Substitute Name** and **Substitute Password**, for su-based privilege escalation.
- Click **Add**.

- If you are using VMware API credentials, do the following:
  - Enter a **Username**. Must be the same username you enter for the VMware vCenter UI. Any username syntax that is supported by the vCenter UI is supported here. For example, domain names and Windows domain syntax are supported.
  - Enter a **Password**. Must be the same password you enter for the VMware vCenter UI.
  - For **Port** number, enter a single port or comma-separated list of ports. The default is 443.
  - Click **Add**.

    Important: At this time, only connecting through a VMware vCenter application is supported. You cannot connect directly to an ESXi host.

- If you are using **Palo Alto Networks** credentials to run RAS scans on Palo Alto devices, the following needs to be done first:
  - On the satellite endpoint, enter:
    - `/TaniumClient config set Cx.comply.RasDisableSslValidation 1`
    - `/TaniumClient config set Cx.comply.RasDisableTlsAlgorithms "X25519"`

©2026 Tanium Inc. All Rights Reserved

- On Palo Alto devices:
    - Configure data-plane interfaces. Confirm the configuration is valid by running `show interface all` in the PAN-OS CLI and verify the output is non-empty.
- Enter a **Username**. Must be the same username you enter for the PAN-OS device.
- Enter a **Password**. Must be the same password you enter for the PAN-OS device.

  > **Note:** Username and Password here should be the firewall's management username and password on the PAN-OS device. They must be valid credentials for authenticating to that firewall for the scan, typically the same ones you would use to log into the management plane or API.

- For **Port** number, enter the HTTPS management port. The default is 443. The valid range is 1–65535. Use another value only if your device uses a custom management HTTPS port.
- Click **Add**.

  > **Note:** Only remote authenticated compliance scans are supported on PanOS devices.

5. Click **Save** on the Credentials page to preserve the endpoint credential criteria you added.

Prioritize credentials

Set the priority of credentials in a list to control the order in which they are attempted on endpoints.

About this task

Set the priority of credentials within a credentials list. This determines the order in which credentials are attempted on endpoints.

1. Click the **Prioritize** button.

©2026 Tanium Inc. All Rights Reserved

2. Drag and drop items in the list to set their priority.

Result

After you set the priority, select a credential list in the **Assessments** page when you choose **Remote Authenticated** as the **Scan Method**.



Note: You cannot delete credentials that are used in an assessment.

Credentials list view

View additional information about credentials, including creation and update dates and associated assessments, from the credentials list view.

After you create credentials, you can click the **Additional data** arrow from the list view to see information about the credentials such as date they were created or updated and the assessments in which the credentials are used.

©2026 Tanium Inc. All Rights Reserved

Get up and running

Perform the initial Comply tasks to collect, evaluate, and organize data into reports after installation or setup.

About this task

After you complete the installation (Installing Comply on page 48) and), perform the following tasks to collect, evaluate, and organize data into reports.

Import scan engines and set up endpoints

Import scan engines, verify JREs, and configure endpoint targeting to prepare Comply for evaluating security configuration exposures and software vulnerabilities.

About this task

A scan engine evaluates endpoints for security configuration exposures and software vulnerabilities using industry security standards, vulnerability definitions, and custom compliance checks. At least one scan engine is required to use Comply. Most organizations can use the included Tanium Scan Engine and Amazon Corretto JRE and do not need to upload any scan engines or JREs. After you determine scan engines and JREs are in place, you can use the default targeting (Tanium Comply Action Group) or configure custom targeting.

For more information, see

- Working with scan engines on page 74
- Setting up endpoints on page 101

Import standards

Import compliance and vulnerability standards and, optionally, create custom profiles that define which standards are deployed to endpoints.

About this task

A standard is a collection of checks that are run on endpoints. Standards are used in compliance and

©2026 Tanium Inc. All Rights Reserved

vulnerability assessments. Import compliance and vulnerability standards, and optionally create custom profiles to specify a subset of standards to be deployed to endpoints. For example, you may have a baseline of compliance and vulnerability standards you regularly check for.

For more information, see

- Working with standards and vulnerability sources on page 109
- Customizing compliance results on page 279

Configure assessments

Learn how to configure compliance and vulnerability assessments by selecting scan engines, standards or vulnerability libraries, and target endpoints.

About this task

An assessment is what you use to deploy a scan engine and a standard to endpoints for running checks. Configure a compliance assessment by selecting a scan engine, a standard, and endpoints to target. Configure a vulnerability assessment by selecting a scan engine, a vulnerability library, and one or more CVEs. An assessment can be changed or edited at any time. You can also create a regular schedule for running an assessment.

For more information, see

- Creating compliance assessments on page 121
- Creating vulnerability assessments on page 146

System generated assessments

Comply automatically creates and configures default compliance and vulnerability assessments for new operating systems added to the Comply action group.

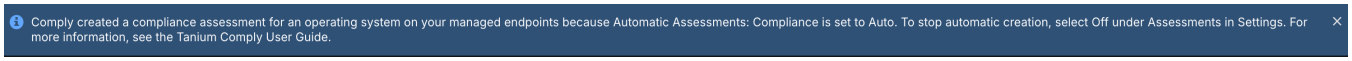
When the **Automatic Assessments: Compliance** and **Automatic Assessments: Vulnerability** settings are set to Auto, Comply automatically creates and deploys default assessments for operating systems represented by endpoints in the Comply action group. For each operating system that does not have a compliance assessment, Comply creates a default compliance assessment. For each operating system that does not have a vulnerability assessment, Comply creates a default vulnerability assessment. By default, these settings are set to Auto.

©2026 Tanium Inc. All Rights Reserved

Comply considers only endpoints that do not yet report results for an existing assessment. If an endpoint that already reports results updates to a new operating system, Comply does not create a default assessment for that operating system.

To stop Comply from creating compliance or vulnerability assessments automatically, select **Off** for the corresponding setting in Comply **Settings**. Assessments that Comply already created remain. For more information, see Managing application settings on page 301.

When Comply creates an assessment automatically, a banner appears on the Comply Main page. You can dismiss the banner.



Note: The Operating System Generation Sensor is used to return the generation of the operating system from endpoints.

Note: Existing installations keep their current settings for **Automatic Assessments: Compliance** and **Automatic Assessments: Vulnerability**. In earlier releases, these settings changed to Off after 14 days. To have Comply create default assessments, select **Auto** for each setting.

Tip: If an assessment for an operating system has ever existed in Comply, whether active, stale, or deleted, the system will not create a default assessment for that operating system.

Tip: System created assessments have **Comply** in the **Created By** column on the Assessments page, along with the date it was created.

A system generated compliance assessment has the following default configuration:

©2026 Tanium Inc. All Rights Reserved

Default compliance assessment settings

System created default compliance assessment settings	
Scan Method	Client-Based
Targeting	A computer group matching the operating system for which the system assessment was created (matches based on OS Generation)
Platform	Matches the platform for which the system assessment was created
Engine	Tanium Scan Engine
Comply Process Priority	Low
Network Drives	Unchecked
Standard	The latest available benchmark related to the operating system for which the system assessment was created
Profile	Level 1
Custom Checks	None selected
Custom ID Mapping	None selected
Start/End Times	None
Distribute Over Time	3 minutes
Schedule	Use assessment age set to 7 days

A system generated vulnerability assessment has the following default configuration:

Default vulnerability assessment settings

System created default vulnerability assessment settings	
Scan Method	Client-Based

©2026 Tanium Inc. All Rights Reserved

System created default vulnerability assessment settings	
Targeting	A computer group matching the operating system for which the system assessment was created (matches based on OS Generation)
Platform	Matches the platform for which the system assessment was created
Engine	Tanium Scan Engine
Comply Process Priority	Low
Network Drives	Unchecked
TVL Source	TVL source matching the operating system for which the system assessment was created
Operating System	Matches the operating system for which the system assessment was created
CVE Definitions Type	Both Standard and High
Years	All years
Start/End Times	None
Distribute Over Time	3 minutes
Schedule	Use assessment age set to 24 hours

View findings and create reports

View, filter, and sort compliance and vulnerability findings, then save customized reports that you can re-run using selected finding data.

About this task

A finding is the output or result of an assessment on an endpoint. Findings can be filtered and sorted using multiple criteria, including status (pass/fail), standard, and endpoint. Filtered compliance and vulnerability findings can be saved as reports, allowing you to customize and re-run reports using

©2026 Tanium Inc. All Rights Reserved

any combination of available finding data you choose.

For more information, see

- Viewing and filtering findings on page 194

Monitor the dashboard

Use the Comply dashboard to monitor key metrics, visualize findings, and quickly assess the overall health of your environment.

After you complete the tasks above and begin to receive results, you spend the majority of your time viewing the metrics displayed in the dashboard. The Comply dashboard, located on the **Overview** page, features charts that provide data visualizations of Comply findings. At a glance, you can view the overall health of your environment and if necessary, drill down to investigate any issues.

For more information, see

- Interoperability with other Tanium products on page 13
- Working with Comply reports on page 273

©2026 Tanium Inc. All Rights Reserved

Working with scan engines

Learn how to work with Comply scan engines, including importing engines and understanding the required Deployment Administrator role.

About this task

A scan engine evaluates endpoints for security configuration exposures and software vulnerabilities using industry security standards, vulnerability definitions, and custom compliance checks.

In Comply, the scan engine evaluates Open Vulnerability Assessment Language (OVAL) or Security Content Automation Protocol (SCAP) content to determine endpoint compliance and vulnerability status. Comply generates findings based on the results of this evaluation by the scan engine.

At least one scan engine is required to use Comply. Comply includes the Tanium Scan Engine and Amazon Corretto Java Runtime Environment (JRE) in the **Comply Engines** tool. For more information, see Deploying the legacy Tanium Scan Engine and JRE using ECM on page 85. JRE version 11.x is provided for use with supported Windows, Linux, and macOS endpoints. JRE version 11.0.15.9.1 and later also support Mac on Apple silicon (M1 and later) and Amazon Linux 2 EC2. Most organizations can use the Tanium Scan Engine and Amazon Corretto JRE and do not need to upload any scan engines or JREs.



Note: The Amazon Corretto JRE v11.x provided with the latest Tanium Scan Engine is not supported on Red Hat Enterprise Linux 5, Oracle Linux Server 5, CentOS 5, Solaris, AIX, Windows 7, and Server 2008 R2. For legacy operating systems, an earlier version of the Tanium Scan Engine is provided, but you will need to upload and target your own Java 8 JREs on the **Configuration** page.

Tanium Scan Engine and CIS-CAT also require PowerShell and do not work if PowerShell is in ConstrainedLanguage mode.

If needed, you can upload other scan engines to Comply. Comply supports the Tanium Scan Engine (which is included by default), SCC (used by the United States government), and CIS-CAT scan engines (for compliance scans). The supported versions of the scan engines are listed in the Import Engine window and on this page: Reference: Supported engines and JREs on page 333.

You must have the Comply Deployment Administrator role to import scan engines. For more

©2026 Tanium Inc. All Rights Reserved

information, see User role requirements on page 41.

Transitioning to Tanium Scan Engine 7.0

Learn how Comply transitions endpoints from the legacy Tanium Scan Engine to Tanium Scan Engine 7.0 (TSE 7.0) and how to monitor rollout readiness in the dashboard.

About this task

Comply is replacing its legacy Tanium Scan Engine with Tanium Scan Engine 7.0 (TSE 7.0). Both the legacy and new engine use the product name Tanium Scan Engine (TSE), but TSE 7.0 fundamentally changes the way endpoints are scanned.



Note: A **Tanium Scan Engine 7.0 Readiness** managed dashboard is provided in Tanium Reporting to help monitor the roll out of TSE 7.0 across endpoints. Dashboard values may appear unpopulated until TSE 7.0 has been released to your environment.

What is transitioning

Tanium Scan Engine 7.0 (TSE 7.0) replaces the legacy Tanium Scan Engine as the default vulnerability scan engine and uses Tanium Index inventory data to evaluate vulnerabilities without additional manual installation or configuration.

Tanium Scan Engine 7.0 replaces the legacy Tanium Scan Engine as the default engine for vulnerability scans on endpoints. New Comply environments are provisioned with the Tanium Scan Engine (TSE) by default for vulnerability scanning.

TSE 7.0 runs vulnerability scans against an inventory of endpoint files and registry keys created by Tanium™ Client Index Extension. Tanium Index continuously maintains that inventory in the background by detecting file and registry key changes and storing the results in a local SQLite database on the endpoint. When an assessment is run, TSE 7.0 evaluates vulnerability definitions against the existing inventory created by Tanium Index.

Tanium distributes TSE 7.0 to endpoints automatically through Tanium Endpoint Configuration. When an endpoint runs a Comply-CX version that meets the required threshold (see Minimum Comply-CX version for Tanium Scan Engine 7.0 support on page 76), Comply routes vulnerability scans to TSE 7.0. TSE 7.0 is built into the Comply-CX endpoint tool, which is different from the legacy Tanium Scan Engine that is provided through the Comply Engines tool. You do not need to install or

©2026 Tanium Inc. All Rights Reserved

configure TSE 7.0 manually; however, it is recommended that you review your Index configuration before endpoints transition.

Comply-CX version support for Tanium Scan Engine 7.0

Minimum Comply-CX version for Tanium Scan Engine 7.0 support		
Comply 2026H2	comply-cx 1.33.636	Tanium Scan Engine 7.0 for client-based vulnerability scans only
Comply 2026H1 MR11 and later	comply-cx 1.31.418	Tanium Scan Engine 7.0 for client-based vulnerability scans only
Upgrading to 2026H2 from 2026H1 MR11 and later will keep the minimum Comply-CX version needed for TSE 7.0 support at 1.31.418.		

How TSE 7.0 changes vulnerability scanning

Tanium Scan Engine 7.0 separates continuous background data collection from the scan evaluation step, changing how endpoint data is gathered.

With the legacy scan engine, endpoint data collection and vulnerability evaluation occur together during each scan. In TSE 7.0, Tanium Index collects endpoint data continuously in the background, and scans become a separate evaluation step.

Differences in vulnerability scanning

Considerations	Tanium Scan Engine 7.0	Legacy Tanium Scan Engine
What happens during a scan	TSE 7.0 evaluates vulnerability definitions in the assessment against the file system and registry items already collected by Tanium Index.	The legacy engine enumerates file system, and registry items live on the endpoint, scoped to the vulnerability definitions in the assessment.
How endpoint data is collected	By Tanium Index, continuously in the background	By the engine, live during the scan
Java runtime requirements	Not required for vulnerability scans only	Required

Why is Comply moving to TSE 7.0

TSE 7.0 improves endpoint vulnerability assessments by reusing Tanium Index data, shifting collection out of the scan window, removing the standalone Java runtime from client-based scans,

©2026 Tanium Inc. All Rights Reserved

and maintaining existing detection coverage.

TSE 7.0 is a significant upgrade to how vulnerabilities are assessed on endpoints.

- Scans reuse work Tanium Index has already done - Assessments no longer re-enumerate the file system and registry every time they run.
- Collection moves out of the scan window - Tanium Index gathers data continuously in the background, so the work is spread across normal operation instead of concentrated when an assessment starts.
- No standalone Java runtime for vulnerability scans - TSE 7.0 removes a component from the client-based vulnerability scan path. (Java runtime is still required for the legacy engine used for compliance and RAS scans)
- Detection coverage is unchanged - TSE 7.0 changes how scan data is gathered, not which vulnerabilities Comply detects.

Scope: client-based vulnerability scans only

TSE 7.0 supports only client-based vulnerability scans; Remote Authenticated Scans (RAS) and compliance scans continue to use the legacy Tanium Scan Engine and its JRE.

TSE 7.0 currently supports client-based vulnerability scans only. Remote Authenticated Scans (RAS) and compliance scans, including those based on benchmarks such as CIS or DISA STIGs, continue to use the legacy Tanium Scan Engine. Because these scan types still run on the legacy engine, the legacy Tanium Scan Engine and its JRE remain in place.

Before your endpoints transition

Review and adjust your global Tanium Index settings in Tanium Client Management to ensure the desired scan coverage before your endpoints transition to TSE 7.0.

TSE 7.0 evaluates vulnerability definitions against data Tanium Index has already collected. That makes your Tanium Index configuration now part of your vulnerability scanning setup.

Three Tanium Index settings configured in Tanium Client Management globally control how much of each endpoint Index collects:

- Exclusions — files and directories Index skips during its scan

©2026 Tanium Inc. All Rights Reserved

- Blockout windows — scheduled periods when Index scanning stops on a computer group
- Maximum database size — a cap on how large the Index database can grow on an endpoint

These settings are configured in Tanium Client Management and are global: they govern Tanium Index for every solution that uses it, not only Comply. If other Tanium solutions in your environment rely on Index, coordinate changes with the teams that own them.

Take time to confirm these three settings reflect the coverage you want before your endpoints transition. For specific values, exclusion patterns, and blockout window scheduling guidance, see Tanium Index scan coverage best practices on page 80.

New Comply settings for TSE 7.0

Learn about Comply index scan configuration settings that apply when endpoints transition to TSE 7.0, including scan frequency, initial scan distribution, and exclusions.

Review the following changes that apply when an endpoint transitions to TSE 7.0. These settings do not appear until endpoints in your environment have begun their transition to TSE 7.0.

New index scan configuration options are available. In **Setup** > **Configuration** > **Custom Settings**, a new TSE index scan configuration section controls how Comply builds that index. The defaults are appropriate for most environments.

- **Index Scan Frequency**: How often Tanium Index scans the files and registry keys in scope for TSE 7.0. Index reconciles this interval with scan requests from other solutions that use Index, and scans everything in scope at least once per interval. Default is 1 day.
- **Index First Scan Distribute Over Time**: Randomizes the start time of scans across a configured time range after the initial Index scan, so that endpoints do not all scan at once. The default is 1 day.
- **Exclusions**: Files and directories excluded from indexing for TSE 7.0. These only apply to the TSE 7.0 for vulnerability scanning and are separate from the Tanium Index exclusions configured in Tanium Client Management. Leave this empty unless you have a specific need. Whether an exclusion here takes effect depends on which other Tanium solutions use Tanium Index in your environment. Tanium Index collects whatever any subscribed solution asks for. If Comply is the only solution using Index, an exclusion configured in Comply keeps that path from being indexed. If another solution, such as Tanium Threat Response, also uses Index and its configuration covers that path, Index still collects it, and TSE 7.0 still evaluates it.

©2026 Tanium Inc. All Rights Reserved

Important:

Leave these settings at their defaults unless there is a specific reason to change them. Overly broad file or directory exclusions can create gaps in vulnerability coverage. Comply reports no findings even when Tanium Index never scanned the files that would have shown a vulnerability.

How endpoints transition

Endpoints transition to Tanium Scan Engine 7.0 based on configured Endpoint Configuration rings and the Comply-CX version.

Endpoints transition based on configured Endpoint Configuration rings. TSE 7.0 rolls out based on the Comply-CX version running on each endpoint. Endpoints that have not reached the required version continue to use the legacy Tanium Scan Engine for vulnerability scans. During the transition period, some endpoints report findings from TSE 7.0 while others report findings from the legacy TSE. Both sets of results appear in Comply. Once the first endpoints have downloaded the required Comply-CX version, a banner appears on the **Comply** > **Overview** page.



Finding counts may differ slightly from legacy TSE results. Because TSE 7.0 processes scan data differently from the legacy TSE, vulnerability finding counts may differ slightly when an endpoint transitions from one engine to the other.

Settings that do not apply to TSE 7.0

TSE 7.0 supports only vulnerability scans, and several legacy Comply settings and options no longer apply or affect scan behavior after endpoints transition to TSE 7.0.

- TSE 7.0 supports vulnerability scans only. Compliance benchmark scans (CIS, STIG, and so on) continue to use the legacy TSE or the engine configured for those assessments.
- The **Threshold: Scan Timeout** setting does not apply to TSE 7.0. Tanium controls the timeout for TSE 7.0 scans.
    - This setting applies only to scans run by legacy TSE versions and other engines such as CIS-CAT and SCC.

©2026 Tanium Inc. All Rights Reserved

    - TSE 7.0 uses a hard-coded default timeout of 24 hours that Tanium manages. This setting no longer affects vulnerability scan behavior after an endpoint transitions to TSE 7.0.

- The **Process Priority** setting in the **Create Assessment** form does not apply to TSE 7.0.
- The **Include network drives in scan** option in the **Create Assessment** form does not apply to TSE 7.0. TSE 7.0 does not scan network drives.
- Endpoints running operating systems that cannot support the required Comply-CX version continue to use the legacy TSE and do not transition to TSE 7.0. For more information, see Tanium™ Client Index Extension: Supported operating systems.

Tanium Index scan coverage best practices

Configure Tanium Index exclusions, blockout windows, and database size to maximize Comply vulnerability scan coverage while avoiding silent gaps in findings.

Vulnerability scanning in Comply depends on Tanium Index to see files and registry keys on an endpoint. Three Index settings control how completely that scan runs: exclusions, blockout windows, and maximum database size. All three are configured in Tanium Client Management:

Tanium Index Settings in Tanium Client Management

Setting	What it constrains	How to start	When to revisit
Exclusions	What Index collects	Leave the default (no exclusions)	Apply if an operational need arises, for example if database size becomes a concern, or when a directory holds high-volume content with little security value.
Blockout windows	When Index can run	Allow Index to scan as much as possible. Configure when there is an operational need or commitment to endpoint owners.	Revisit when endpoints fall behind on indexing, or if commitments change.
Maximum database size	How much Index can store	Leave the default (no size limit)	Disk space is constrained on specific endpoints

Leave these settings at their defaults unless there is a specific reason to change them. A setting that is

©2026 Tanium Inc. All Rights Reserved

too restrictive creates a gap in vulnerability coverage that produces no error and no warning; the endpoint simply reports no findings.

Important:

Comply uses Tanium Index to collect file and registry metadata and compare it to known-vulnerable software. If Index skips items because of exclusions, blockout windows, or database size limits, Comply cannot detect vulnerabilities there. No error or warning appears—the finding is simply missing, and the endpoint reports no findings.

Configure exclusions safely

Configure Tanium Index exclusions to reduce database size by skipping low-value content while ensuring that critical application and system directories remain scanned so Comply can detect vulnerabilities.

Index exclusions instruct Tanium Index to skip specific files or directories during its scan. Use exclusions to reduce the database size by skipping high-volume, low-value content such as logs, caches, and temporary files. Do not use exclusions for directories where software is installed, such as executables, libraries, scripts, JARs, or DLLs. Comply cannot detect a vulnerability in a file that Index has not scanned.

Exclusion guidelines for Tanium Index

Platform	Do not exclude
Windows	Common application or system directories, such as C:\Program Files , C:\ProgramData , C:\Windows\System32 , C:\Users.* , and so on.
Linux	Common application or system directories, such as /usr , /opt , /etc , /var/lib , /bin , /sbin , /lib , /home , and so on.
macOS	Common application or system directories, such as /Applications , /Library , /Users , /System/Library , /usr , /opt , and so on.

©2026 Tanium Inc. All Rights Reserved

Note:

The Tanium Index exclusions described here are configured in Tanium Client Management and apply to every solution that uses Index, including vulnerability scanning. Comply also has its own exclusion settings for TSE 7.0, configured in **Setup** > **Configuration** > **Custom Settings** under **TSE index scan config**. Whether an exclusion configured there takes effect depends on which other Tanium solutions use Tanium Index in your environment. For more information, see New Comply settings for TSE 7.0 on page 78.

Configure blockout windows safely

Configure Index blockout windows so that scanning pauses only when operationally necessary, ensuring endpoints have enough open time for complete and accurate vulnerability findings.

A blockout window is a scheduled period during which Tanium Index scanning stops completely on the endpoints in the assigned computer group via Tanium Client Management (TCM). Index does not crawl files, hash files, or update its database while a blockout window is active.

Give Index as much open time as you can

Index uses whatever time it has to keep its data current, and it throttles itself when an endpoint is busy. The more open time it has, the more complete and current your vulnerability findings are. Use a blockout window only for a confirmed operational need, such as a high-I/O backup or a maintenance freeze. A blockout window is not a substitute for resource tuning. Index already throttles its own CPU usage automatically when an endpoint is busy. If Index resource usage is a concern, adjust or add **Exclusions** instead of blocking Index entirely.

The initial crawl

When Index is first deployed to an endpoint, or after an Index database reset, Index must complete an initial full-disk crawl before it has a usable index. This crawl is the longest-running operation Index performs and can take several hours to several days, longer on large or slow disks. Index can pause a crawl when a window opens and resume afterward, though a reboot or unexpected interruption may restart it, so long, uninterrupted stretches matter most during this period. Avoid blockout windows until the initial crawl is confirmed complete on the targeted computer groups.

©2026 Tanium Inc. All Rights Reserved

Recurring scans

After the initial crawl, Index runs recurring scans, approximately every 1 day for standard scans, and every 7 days for low resource scans, to keep the index current. Comply reports findings from whatever Index last collected, so regular open time keeps findings accurate.

> **Important:**
>
> Comply's vulnerability assessments read directly from the Index database. If blockout windows leave insufficient open time, vulnerability scans return incomplete or zero results.

Minimum open time guidelines

Open time per week	Classification
Less than 8 hours	Too restrictive — remediate immediately
8 – 39 hours	Potentially restrictive — remediate
40 hours or more	Meets the minimum

Configure the maximum Index database size

Configure the maximum Tanium Index database size to balance disk usage with full coverage, using recommended starting values and avoiding low caps that suppress indexing.

Tanium Index maintains an on-disk database (index.db) that catalogs the files on each endpoint. The maximum database size setting caps how large that database can grow. When the database reaches the limit, Index pauses scanning and hashing. Because pruning runs during scans, the database stays at its current size while scanning is paused, so exclusions or file deletions take effect once scanning resumes rather than immediately. To resume scanning, raise the maximum database size above the current size, or unset the max database size setting. Pruning restarts along with scanning, and any exclusions you added apply from that point forward. Alternatively, if disk space prevents raising the limit, resetting the Index database clears it and starts a fresh index.

©2026 Tanium Inc. All Rights Reserved

Important:

In most typical environments, Tanium Index requires approximately 1 GB of database storage for every 2 million items indexed (files, directories, and registry keys/values combined). Actual usage may vary depending on configured settings and other modules that use Index.

Recommended guidelines for database size

Endpoint type	Recommended minimum
General-purpose workstation	2,048 MB
Server (application, database, file)	8,192 MB, scaled up based on installed software
Broad or catch-all computer group (for example, All Windows)	8,192 MB or higher
Purpose-built appliance or kiosk	2,048 MB
Environments where disk space is unconstrained	Leave the default (no limit)

These values are starting points based on typical deployments. Use these recommendations to estimate requirements for your own endpoints and adjust based on what you observe.

You may leave the default setting (unlimited) when disk space is not a constraint. There is no coverage downside to a larger or unlimited database size. Scale the cap up, not down, for computer groups that cover more endpoints or more varied hardware; broader groups have more variation in file system size to accommodate.

Important:

Do not use the max DB size as a performance tuning knob. Tanium Index is designed to run efficiently at much larger DB sizes. Using a low cap to limit Index's resource usage will suppress its coverage long before it affects run-time behavior.

©2026 Tanium Inc. All Rights Reserved

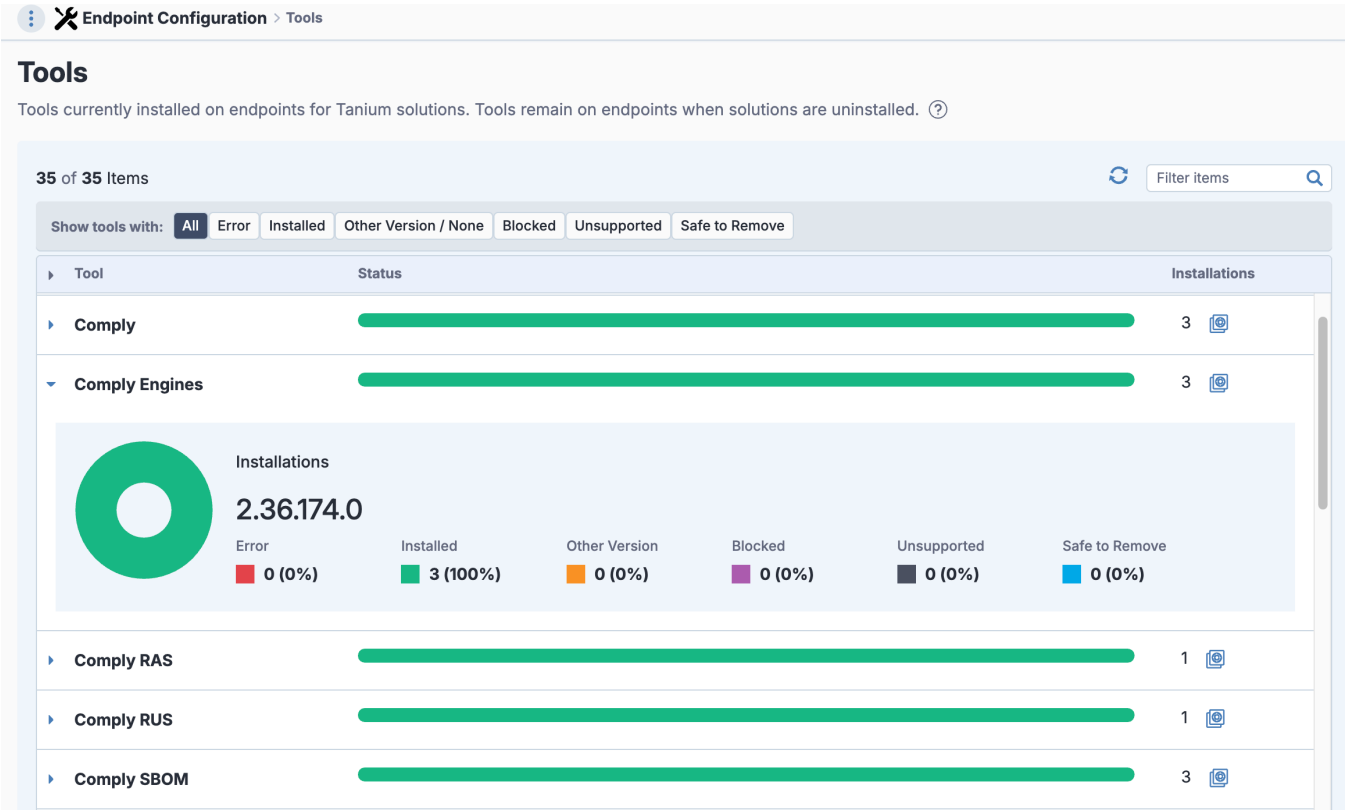
Deploying the legacy Tanium Scan Engine and JRE using ECM

Use Endpoint Change Management (ECM) to deploy the legacy Tanium Scan Engine and Amazon Corretto JRE with ring-based targeting, manage engine and JRE priorities, and retire legacy engines after migration to Comply Engines.

About this task

> **Note:** Tanium Scan Engine 7.0 currently supports client-based vulnerability scans only.
>
> Remote Authenticated Scans (RAS) and compliance scans, including those based on benchmarks such as CIS or DISA STIGs, continue to use the legacy Tanium Scan Engine and are deployed with JREs using ECM.

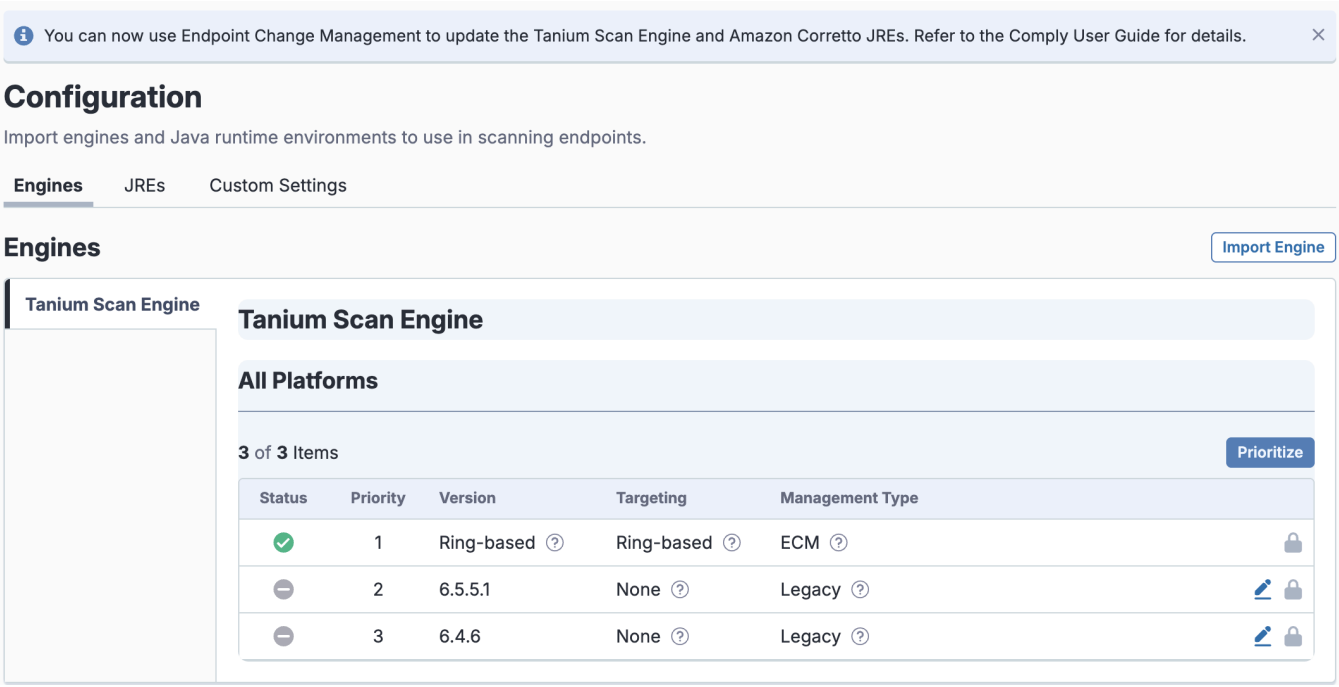
Deploy the legacy Tanium Scan Engine and Amazon Corretto Java Runtime Environment (JRE) using Endpoint Change Management. This lets you perform a staged rollout of the engine files just as you do the rest of the Tanium endpoint toolset, by configuring upgrade rings through which a new version of the Tanium Scan Engine and JRE will be promoted. You can assign computer groups to each ring to determine the endpoints that receive the engine after each promotion. For more information, see Manage solution configurations with Tanium Endpoint Configuration on page 53.



©2026 Tanium Inc. All Rights Reserved

When the **Comply Engines** tool is available in ECM, the **Engines** tab and **JREs** tab in the Comply **Configuration** page have a **Management Type** column that displays **ECM**. The **Version** and **Targeting** columns display **Ring-based.**

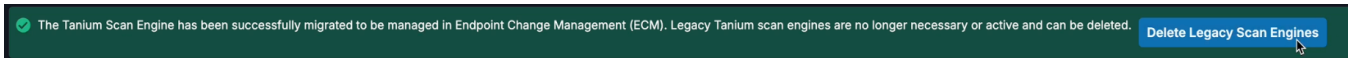
Important: For Comply toolset/engine/JRE version information, see Legacy Tanium Scan Engine (Joval) on page 335.



You cannot edit or target the Tanium Scan Engine in ECM through the **Configuration** > **Engines** page. You must do those tasks in Endpoint Change Management.

Note: Engines and JREs always have the following priority: User Provided is first, then ECM, and lastly Legacy. If there are more than two in a particular management type, then you can reprioritize within that type.

When the **Comply Engines** tool reaches the final ECM ring, and all endpoints have been targeted to receive the **Comply Engines** tool, you can delete all the legacy engines through a banner that informs you when the Tanium Scan Engine has been migrated to ECM. You can then click the **Delete Legacy Scan Engines** button in the banner.



©2026 Tanium Inc. All Rights Reserved

Note: When you delete a legacy engine, the modal may indicate that the engine has assessments associated with it. You can still proceed with the deletion, but you should reevaluate your targeting. Associated assessments will no longer scan with the deleted engine and may not scan at all.

Once a toolset with **Comply Engines** is available in ECM, the legacy method of updating engines is obsolete and you will only be able to update the Comply-provided engines via ECM.

Note: Other supported engines (CIS-CAT, SCC) and user-provided JREs will continue to be managed through the **Configuration** page. Custom settings for all engines, including the Tanium Scan Engine, are still set in the **Configuration** > **Custom Settings** page. For more information, see Custom settings on page 103.

Legacy Tanium Scan Engine (TSE) default targeting

Describes how legacy Tanium Scan Engines use default targeting and how this behavior differs from the static, non-configurable targeting in ECM engines.

Note: **Apply All Tanium recommended configurations** only applies to legacy engines. Engines in ECM have static default targeting that you cannot change.

Tanium provides multiple Tanium Scan Engines and automatically targets endpoints.

Comply includes the Tanium Scan Engine and JREs with the Comply toolset to be managed through ECM. For more information, see Deploying the legacy Tanium Scan Engine and JRE using ECM on page 85.

Note: You cannot change default targeting for the Comply Engines tool. You can only change what endpoints are targeted. For more information, see Managing Tanium Client and endpoint tool upgrade rollouts.

©2026 Tanium Inc. All Rights Reserved

Comply toolset version support for Tanium Scan Engines and JREs

Toolset	Tanium Scan Engines	JREs
2.39.125	TSE 6.6.5.1, TSE 6.4.6	Amazon Corretto JRE 11.0.30.7.1
2.39.19	TSE 6.5.5.1, TSE 6.4.6	Amazon Corretto JRE 11.0.30.7.1

Default targeting for Tanium Scan Engines in ECM

Tanium Scan Engine	Default Targeting
6.6.5.1	All Computers (in the Comply action group) except for CentOS 5, RHEL 5, Oracle Linux 5, AIX, and Solaris.
6.4.6	CentOS 5, RHEL 5, Oracle Linux 5, AIX, and Solaris computers (in the Comply action group).

Download and import the CIS-CAT engine

Upload the CIS-CAT engine and standards bundle to Comply so you can use CIS-CAT for compliance assessments.

About this task

Note: Comply includes Tanium Scan Engine. Most organizations can use the Tanium Scan Engine and do not need to upload the CIS-CAT engine.

Note: Only CIS-CAT 4.0 through 4.62.0 is supported with a valid license. CIS-CAT versions later than 4.62.0 require Java 21, but Comply supports only the bundled Amazon Corretto JRE 11 or an uploaded Java 8 JRE.

©2026 Tanium Inc. All Rights Reserved

Important:

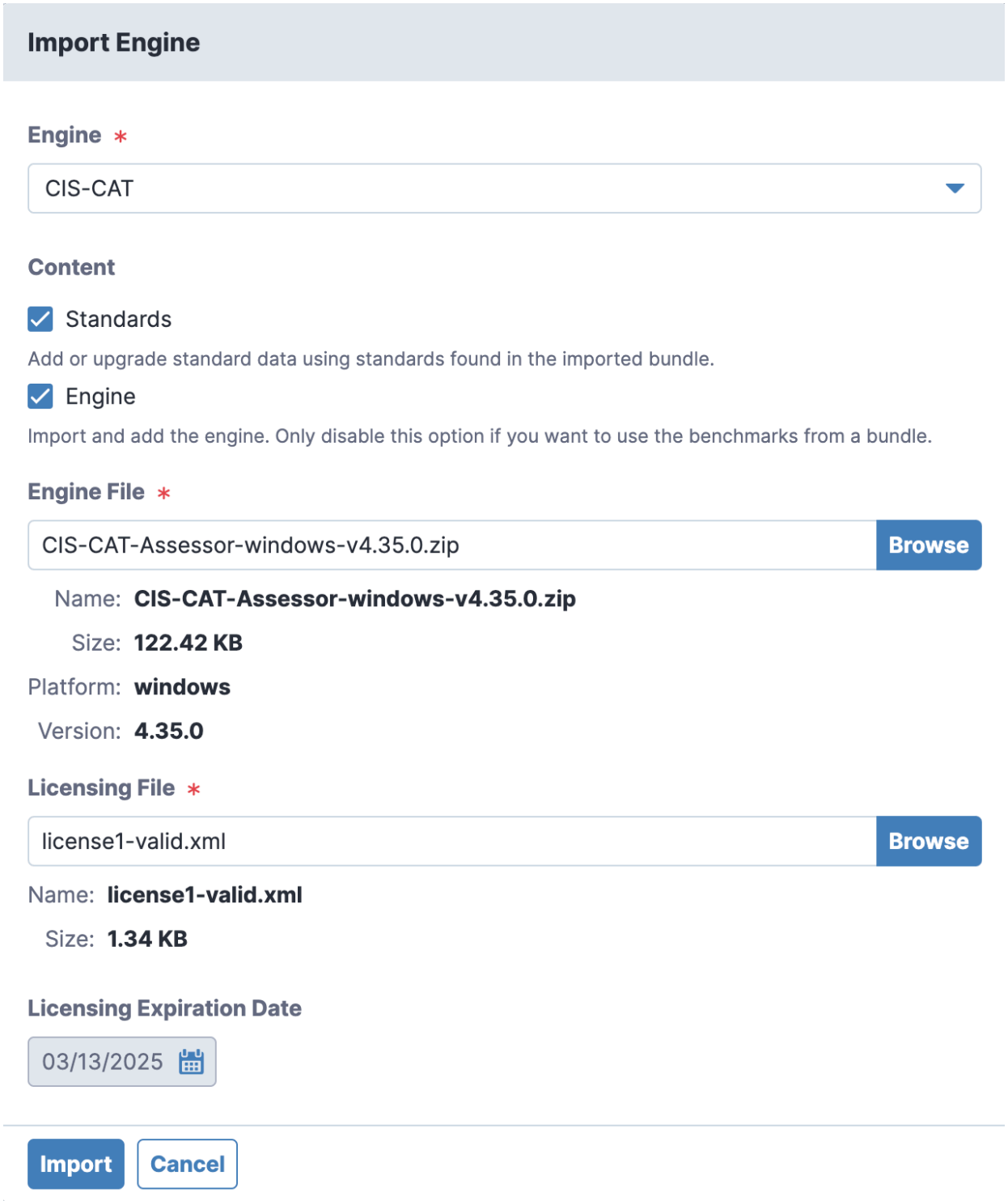
The CIS-CAT engine is no longer supported for vulnerability assessments. Existing vulnerability assessments that use the CIS-CAT engine must be recreated to use the Tanium Scan Engine.

Existing compliance assessments that use the CIS-CAT engine will automatically start using the CIS-CAT 4 engine when a valid CIS-CAT 4 engine and license are uploaded. Until a valid CIS-CAT 4 engine and license are uploaded, existing CIS-CAT engines will be untargeted and those compliance assessments will have a pending status.

1. From the Main menu, go to **Modules** > **Comply**, and select **Setup** > **Configuration**.
2. In the **Engines** tab, click **Import Engine**.
3. In the **Engine** dropdown list, select **CIS-CAT**.
4. To import the standards in the bundle into Comply, leave the **Standards** option selected.

   Best Practice: For best results, select this option. This option is enabled by default the first time you upload the CIS-CAT bundle.
5. If you already imported the required scan engine and you only want to import standards, clear the **Engine** option.
6. Click **Browse** to select the ZIP file you downloaded.
   A valid license is required for the CIS-CAT engine.

©2026 Tanium Inc. All Rights Reserved



7. Click **Import**.

Result

©2026 Tanium Inc. All Rights Reserved

Note:

For the CIS-CAT scan engine to work, you must also install the JRE package. For more information, see Upload a Java Runtime Environment (JRE) package on page 93.

Comply does not use the JRE that is included in a CIS-CAT download. When you import the CIS-CAT engine, Comply removes the embedded jre folder. A JRE that you upload must be Java 8, so uploading a JRE does not make CIS-CAT versions that require Java 21 work.

To upgrade your standards when CIS releases a new version of the bundle, select **Standards** only. This is how new, updated standards are imported into Comply in bulk. Existing reports and standards will not be affected by this process, and the standards used in these reports are not automatically upgraded to the new versions of the respective standards.

Download and import the SCC scan engine

Download and import the SCC scan engine bundle into Comply, including optional DISA STIG standards.

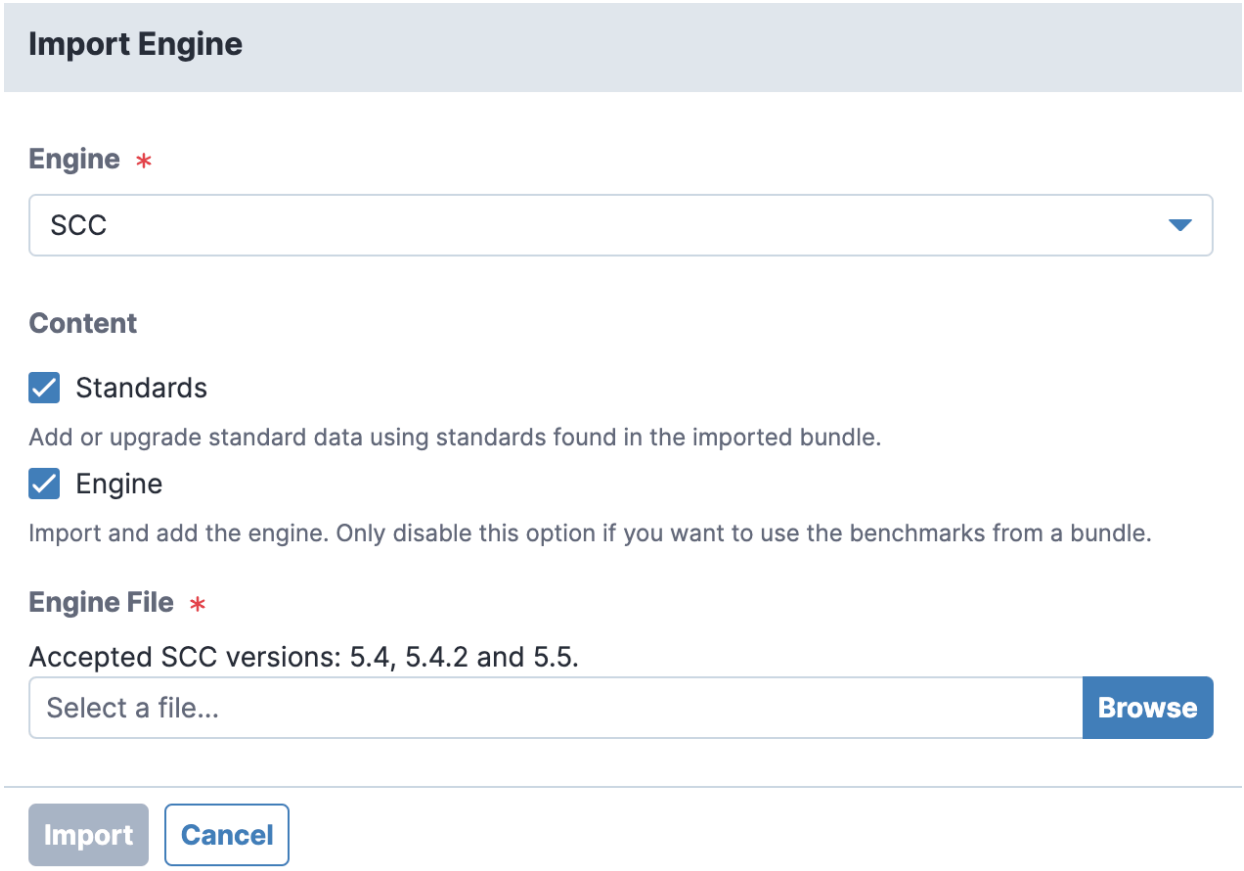
About this task

SCC is the scan engine generally used by the United States government.

Note: Within each SCC ZIP file, there is another ZIP file (on Windows) or a TGZ file (on Linux/macOS). Comply will accept these inner ZIP or TGZ files as well as the original ZIP archive. This reduces the amount of data in half that you must upload.

1. From the Main menu, go to **Modules** > **Comply** and select **Setup** > **Configuration**.
2. In the **Engines** tab, click **Import Engine**.
3. In the **Engine** dropdown list, select **SCC**.
4. Select content: **Standards** and/or **Engines**.
5. Click **Browse** to select the SCC bundle that you want to upload.

©2026 Tanium Inc. All Rights Reserved



6. Click **Import**.

Result

Note: Some SCC bundles come packaged with DISA STIG standards. To import these, be sure to select **Standards**. Not all SCC bundles include this content.

To remove a scan engine, hover over it and click Delete engine . You cannot remove the Legacy Tanium Scan Engine or any engine that is associated with an assessment.

Target Computer groups

Configure target computer groups to control how engines are distributed to endpoints, including default targeting, custom groupings, and options to prevent distribution.

1. In the **Engines** tab, hover over an engine and click Edit engine .

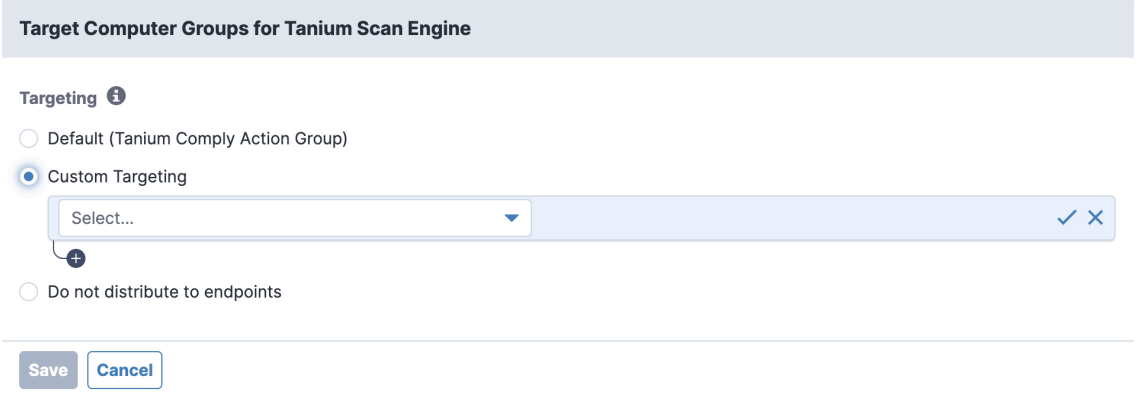
2. Select endpoints to receive this engine by choosing one of the following options:

   - Default: Default targeting uses the Comply action group.

©2026 Tanium Inc. All Rights Reserved

- Custom Targeting: Choose this option to build your own groupings. Use the **And**/**Or** buttons to build upon or narrow your selection. Use the **Add Row** option to add a new row to the group. Use the **Add Group** option to build another And/Or combination for targeting. When finished, click Apply ✓ for each selection and then click **Save**.

- **Do not distribute to endpoints**: Choose this option to prevent the engine from being distributed to endpoints systems.



Upload a Java Runtime Environment (JRE) package

Upload Java Runtime Environment (JRE) packages to Comply when the bundled Amazon Corretto JRE is not supported on your endpoints, ensuring the correct JRE is used to run scans.

About this task

Note: The Amazon Corretto Java Runtime Environment (JRE) is included with the Comply toolset. The zip file on the endpoint that contains the JRE is encrypted to prevent access to the JRE. This JRE is supported on Windows, macOS, and most distributions of Linux. If you use this JRE, you do not need to upload any JREs to Comply.

The Amazon Corretto JRE is not currently supported on some distributions of Windows, Linux, AIX, and Solaris. If you need to run a scan on an endpoint with one of these operating systems and do not want to use the existing JRE on the endpoint, you can upload a different JRE to Comply. For best results on these operating systems, upload a JRE and use Comply to install that JRE (rather than using the existing JRE on the endpoint) so that you know which JRE is used to run scans.

If you need to upload a JRE to Comply, download the appropriate JRE package for each platform and

©2026 Tanium Inc. All Rights Reserved

architecture required for the endpoints in your environment. For a list of the supported JRE distributions and versions, see Java Runtime Environment (JRE) on page 337.

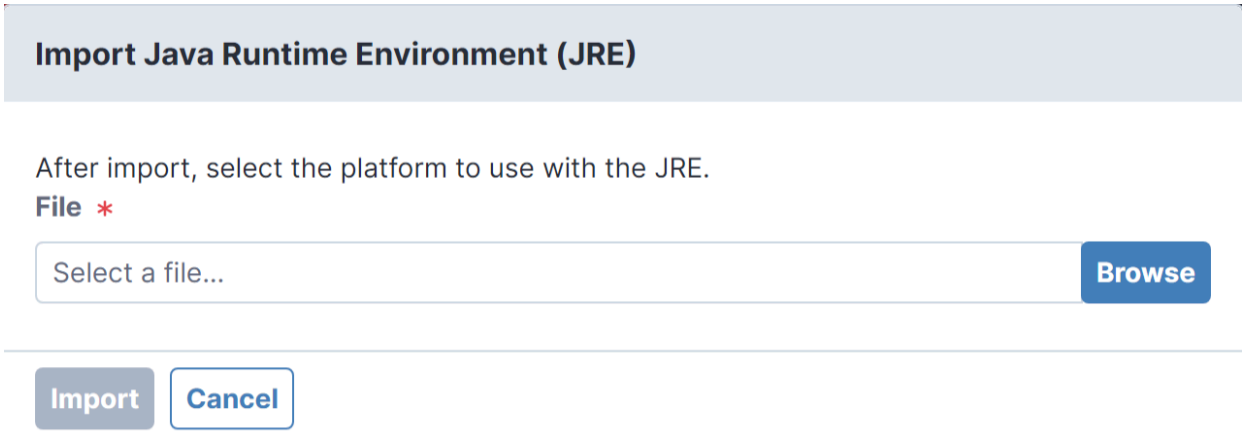
Comply accepts only Java 8 JRE packages for upload. Comply rejects other Java versions when you import them.

If you upload an Oracle JRE, both the standard JRE and server JRE packages are supported. Because the underlying binary files that Comply uses are the same for both packages, you can upload only one package (standard JRE or server JRE) for a particular platform/architecture. Either package can be used for scanning all endpoints (workstations and servers) on the associated platform. You can upload only the TGZ or ZIP packages to Comply. Be sure to download the TGZ or ZIP packages, not the EXE, RPM, or DMG files. Download the JRE packages from the following URL: http://www.oracle.com/technetwork/java/javase/downloads/index.

Import JREs

Import Java Runtime Environment (JRE) files into the system configuration.

1. From the Main menu, go to **Modules** > **Comply** and select **Setup** > **Configuration**.
2. On the **JREs** tab, click **Import JRE**.



3. Click **Browse** to select one of the TAR, GZ, or ZIP files that you downloaded earlier.
4. Click **Import**.

Result

To remove a scan engine or JRE, select it and click **Remove**.

©2026 Tanium Inc. All Rights Reserved

TARGET COMPUTER GROUPS

Configure target computer groups to control which endpoints receive a JRE engine, using default Comply groups, custom targeting rules, or excluding endpoints from distribution.

> **Note:** This does not apply to JREs in ECM.

1. On the **JREs** tab, select an operating system.
2. Hover over an engine and click the **Edit** icon that appears.
3. Select endpoints to receive this engine by choosing one of the following:
    - **Default**: Default targeting uses the Comply action group.
    - **Custom Targeting**: Choose this option to build your own groupings. Use the **And**/**Or** buttons to build upon or narrow your selection. Use the **Row** button to add a new row to the group. Use the **Grouping** button to build another And/Or combination for targeting. When finished, click **Apply** for each selection and then click **Save**.
    - **Do not distribute to endpoints**: Choose this option to prevent the engine from being distributed to endpoint systems.

Import custom settings

Configure custom settings for Tanium Scan Engine and SBOM assessments, including index scan behavior, resource optimization, and endpoint targeting.

1. From the Main menu, go to **Modules** > **Comply** and select **Setup** > **Configuration**.
2. In the **Custom Settings** tab, click **Add Custom Settings**.
3. In the **Create Custom Settings** window, set the following:
    - **TSE index scan config**: These index scan settings apply to Tanium Scan Engine 7.0. TSE 7.0 uses an index of endpoint files to evaluate vulnerability definitions efficiently. In the **TSE index scan config** section, configure the following:
        - **Index Scan Frequency**: Enter a value in Days, Hours, or Minutes for how often the index scan runs. The default is 1 day. For any endpoint running low

©2026 Tanium Inc. All Rights Reserved

resource assessments, the default is 7 days.

- **Index First Scan Distribute Over Time**: Enter a value in Days, Hours, or Minutes over which to randomize the distribution of initial index scans to endpoints. The default is 1 day.

- **File Exclusions by Regular Expression**: Enter file names, using regular expressions, to exclude from the index scan. Each exclusion must appear on a separate line.

- **Directory Exclusions by Regular Expression**: Enter directory paths, using regular expressions, to exclude from the index scan. Each exclusion must appear on a separate line.

-  **Note:** If SBOM or another Tanium product has indexed a file or file system that you exclude from the Tanium Scan Engine 7.0 index scan, an entry for that exclusion can still appear in Findings. This can happen because OVAL scans perform a complete scan of the index database, and other scans, such as SBOM, can detect modifications to the index file during scanning.

- Optimization: These settings apply to the legacy Tanium Scan Engine and all user-imported engines, all compliance assessments, and vulnerability assessments running Tanium Scan Engines prior to version 7.0. These settings determine how scans affect endpoint resources.

    - **Resource Mode**: The default setting is **Normal**. Change this setting to **Low**, and the Tanium Scan Engine will utilize fewer resources on the endpoint.

        - **CPU Utilization** (Windows OS types only) can be set as low as 10%. If other resources are using CPU, the scan will pause until the set amount of CPU is available.

        Note the following about Low Resource Mode:

        - The CPU Count automatically defaults to 1 and the Max Java Heap size is set to 128 MB.

        - Scans take more time to complete.

        - Scans produce simplified JSON result files instead of XML.

©2026 Tanium Inc. All Rights Reserved

- Running a low resource mode scan with debug enabled does not produce any additional scan debug output files. The debug JSON configuration state files are captured in the support subdirectory: <Tanium Client>\extensions\comply\data\results\<scan name>\support

- **CPU Count**: Set a maximum number of CPUs for scanning. The default recommendation is 1 CPU.

- **Java Heap Size**: Set the maximum amount of Java heap memory used for scanning. The default recommendation is 768 MB.

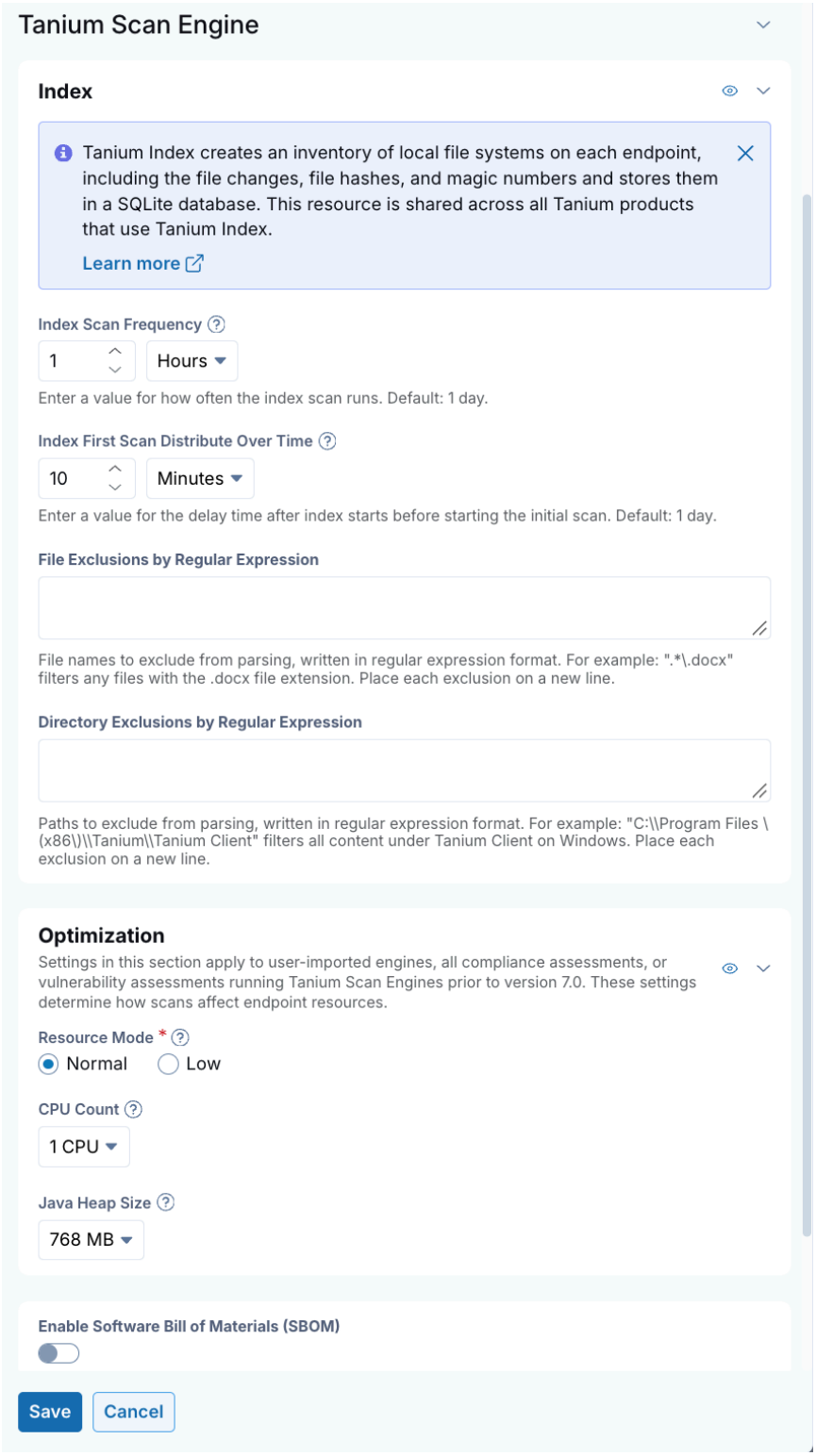
- **SBOM**: (SBOM requires a Tanium SBOM license) If you are creating an SBOM assessment, you must select the **Enable SBOM** checkbox and choose at least one file ecosystem. For more information, see Custom settings on page 103.

- **Targeting Type**: Select endpoints to receive these customized settings. Select **Default (Tanium Comply Action Group)** or **Custom Targeting**.

  - **Custom Targeting**: Choose this option to build your own groupings. Use the **And**/**Or** buttons to build upon or narrow your selection. Use the **Row** button to add a new row to the group. Use the **Grouping** button to build another And/Or combination for targeting. When finished, click the check for each selection.

4. Click **Save**.

©2026 Tanium Inc. All Rights Reserved



Prioritize endpoint configurations

Set priority values for endpoint configurations so that the correct engine, JRE, or custom setting is applied when targeting overlaps.

©2026 Tanium Inc. All Rights Reserved

About this task

Endpoint configurations can contain overlapping targeting settings. For example, you can have one configuration that targets all computer groups and a second configuration that targets of subset of computers within all computer groups. Without setting a prioritization for the configuration, you cannot be sure which settings are applied to that subset of computers. Designating a prioritization determines which setting is applied if a conflict exists.

The setting with the highest priority has the lowest priority number. For example, an engine with a priority of **1** takes precedence over an engine with a priority of **10**.

> **Note:** For engines, prioritization occurs only for engines of the same name. Prioritization does not block different engines from being installed on an endpoint.

1. From the Main menu, go to **Modules** > **Comply** and click **Setup** > **Configuration**. Changing the priority is available for Engines, JREs, and Custom Settings.
2. Click the **Prioritize** button to make configurations moveable.
3. Select the configuration you want to change the priority of and drag it up or down.
4. Click **Save** to keep the new priorities or **Cancel** to undo them and revert back to the original priorities. When you click **Save**, the priority for all items is reordered based on your change.

Result

Upload the Tanium Engines package for air-gapped environments

Upload the Tanium Scan Engine and Amazon Corretto JRE package to Comply in an air-gapped environment after configuring air-gap settings.

About this task

If you are working in an air-gapped environment and you want to use the Tanium Scan Engine and Amazon Corretto Java Runtime Environment (JRE), you must configure that setting in Comply and then upload the Tanium engine files. For the steps to configure Comply for an air-gapped environment, see Configure Comply for an air-gapped environment on page 60.

©2026 Tanium Inc. All Rights Reserved

1. After you specify that you are working in an air-gapped environment (in Setttings ⚙, set **is_airgapped** to **True**), click **Setup** > **Configuration** to open the **Engines** page.
2. Click **Upload Engines Package**.
3. Download the air gap ZIP file from the link indicated in the **Upload Tanium Engines Airgap Archive** window (https://content.tanium.com/files/published/comply-engines/engines3.cgz) using a machine that can connect to the internet and save it on the air-gapped machine.
4. Click **Browse**, select the engines3.cgz file from the location where you saved it on the air-gapped machine, and click **Open**.
5. Click **Upload**.
6. After your upload is complete, click **Close**.

©2026 Tanium Inc. All Rights Reserved

Setting up endpoints

Scan endpoints by configuring engines for targeted computer groups and by configuring custom settings.

About this task

Scan endpoints by configuring engines for targeted computer groups and by configuring custom settings.

Configure engines

Configure scan engines and JRE deployments by targeting computer groups based on endpoint architecture and platform.

About this task

Target deployments to computer groups based on the architecture and platform of the targeted endpoints to deploy engines and JREs to endpoints on a schedule. For example, you might want to create the following deployments:

- Windows 64-bit
- Windows 32-bit
- macOS 64-bit
- Linux 64-bit

©2026 Tanium Inc. All Rights Reserved

Best Practice:

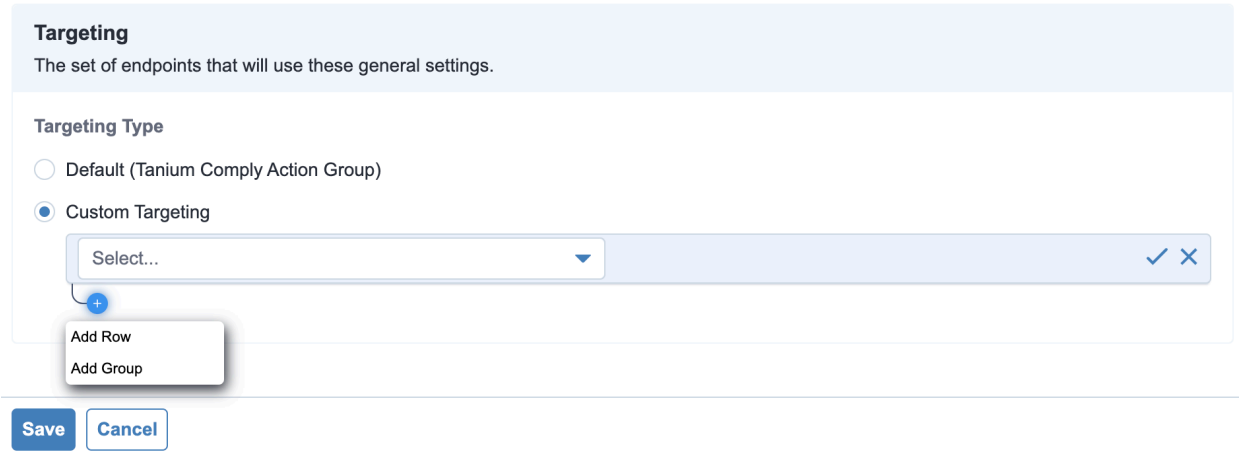
- Ensure that the computer groups targeted by each deployment include all applicable endpoints. Review the deployments to confirm that no computer groups are missing.
- Ensure that deployments are created for all possible architectures (bitness) and platforms. For example, some environments still contain 32-bit Linux and Windows endpoints. These endpoints require specific deployments.

By default, Tanium provides the Tanium Scan Engine, but if you uploaded another supported engine, target that engine as follows. For more information on targeting the Tanium Scan Engine, see Transitioning to Tanium Scan Engine 7.0 on page 75 or Deploying the legacy Tanium Scan Engine and JRE using ECM on page 85.

1. From the Main menu, go to **Modules** > **Comply** and click **Setup** > **Configuration**.
2. In the **Engines** tab, do the following:
3. Click  for an engine in the list to open the targeting window.
4. Select **Computer Groups** you want to target.
   - **Default**: Default targeting uses the Comply action group.
   - **Custom Targeting**: Choose this option to build your own groupings. Use the **And**/**Or** buttons to build upon or narrow your selection. Use the **Row** button to add a new row to the group. Use the **Grouping** button to build another And/Or combination for targeting. When finished, click the check mark for each selection and then click **Save**.

     Important: You must register sensors that are referenced by the action group. For more information, see Register or unregister sensors for collection
5. Click **Save**.

©2026 Tanium Inc. All Rights Reserved



Custom settings

Configure custom settings profiles to control scan behavior, resource usage, SBOM indexing, and targeting for Comply engines on endpoints.

Set limits for engines on endpoints using targeting.

From the Main menu, go to **Modules** > **Comply** and click **Setup** > **Configuration**. Then select the **Custom Settings** tab.

Note: Comply includes a default custom settings profile. The default profile has the lowest priority in the list. You can edit its settings and targeting, but you cannot delete it — clicking **Delete** resets it to the default values. A warning appears if the default profile is not targeted to any endpoints. The default profile uses the following settings:

- **Index Scan Frequency**: 1 day
- **Index First Scan Distribute Over Time**: 1 day
- **CPU Count**: 1 CPU
- **Java Heap Size**: 768 MB
- **Targeting**: **Default** (all endpoints in the Comply action group)

1. To create a custom configuration, click the **Add Custom Settings** button.

©2026 Tanium Inc. All Rights Reserved

2. In the **Create Custom Settings** window, set the following:

    - **TSE index scan config**: These index scan settings apply to Tanium Scan Engine 7.0. TSE 7.0 uses an index of endpoint files to evaluate vulnerability definitions efficiently. These settings are separate from and independent of any SBOM index scan settings. In the **TSE index scan config** section, configure the following:

        - **Index Scan Frequency**: Enter a value in Days, Hours, or Minutes for how often the index scan runs. The default is 1 day. For any endpoint running low resource assessments, the default is 7 days.

        - **Index First Scan Distribute Over Time**: Enter a value in Days, Hours, or Minutes over which to randomize the distribution of initial index scans to endpoints. The default is 1 day.

        - **File Exclusions by Regular Expression**: Enter file names, using regular expressions, to exclude from the index scan. Each exclusion must appear on a separate line.

            Note: Exclude only high-volume, low-security-value content, such as logs, caches, and temp files. Do not exclude directories where applications are installed, such as C:\Program Files, C:\ProgramData, C:\Windows\System32, or /opt/. Tanium Comply cannot detect a vulnerability in a file that Tanium Index never scanned, and the endpoint reports as compliant even though coverage is incomplete. Anchor each regular expression to the start of the path with ^ to avoid unintentionally broad matches.

            Note: Tanium Client Management and Tanium Threat Response can also define Index exclusions for the same endpoints, independently of the exclusions you configure here. Review exclusions on every surface that targets an endpoint to understand its full exclusion scope.

        - **Directory Exclusions by Regular Expression**: Enter directory paths, using regular expressions, to exclude from the index scan. Each exclusion must appear on a separate line.

©2026 Tanium Inc. All Rights Reserved

- **Note:** If SBOM or another Tanium product has indexed a file or file system that you exclude from the Tanium Scan Engine 7.0 index scan, an entry for that exclusion can still appear in Findings. This can happen because OVAL scans perform a complete scan of the index database, and other scans, such as SBOM, can detect modifications to the index file during scanning.

- Optimization: These settings apply to the legacy Tanium Scan Engine and all user-imported engines, all compliance assessments, and vulnerability assessments running Tanium Scan Engines prior to version 7.0. These settings determine how scans affect endpoint resources.

    - **Resource Mode**: The default setting is **Normal**. Change this setting to **Low**, and the Tanium scan engine will utilize fewer resources on the endpoint.

      Note the following about Low Resource Mode:

        - Tanium scan engine version 6.3.7 or higher is required.
        - Scans take more time to complete.
        - The CPU Count automatically defaults to 1 and the Max Java Heap size is set to 128 MB with a hard limit of 256 MB.
        - CPU Utilization (Windows OS types only) can be set as low as 10%. If other resources are using CPU, the scan will pause until the set amount of CPU is available.
        - The Investigate feature does not work in Low Resource Mode. For more information, see Investigating findings on page 229.

    - **CPU Count**: Set a maximum number of CPUs for scanning. The default recommendation is 1 CPU.
    - **Java Heap Size**: Set the maximum amount of Java heap memory used for scanning. The default recommendation is 768 MB.

- **SBOM**: (Requires a Tanium SBOM license. For more information, see Tanium Solutions & Bundles.) SBOM scanning is useful for determining vulnerabilities on endpoints based on the results of a Software Bill of Materials assessment. If you are

©2026 Tanium Inc. All Rights Reserved

configuring an SBOM scan assessment, you must select the **Enable SBOM** checkbox and choose at least one file ecosystem. For more information, see Create an SBOM scan assessment on page 172. In the **Candidate Ecosystems** section, select at least one ecosystem:

- **File Types**: Select the file types to be scanned by the SBOM scan assessment. The following are supported: Java (JAR, PAR, SAR, WAR, EAR, JHI, JPI LPKG), JavaScript (Node/NPM), Python, Ruby (Gem), PHP (Composer), Go binary files, Native binary files.

  > **Important:** Scanning binary files can impact performance on endpoints. If you choose to scan binary files, it is recommended you use file and directory exclusions to minimize the impact.

  > **Important:** The scanning of native binary files is not supported on Windows endpoints.

- In the **Settings** section, configure the following:

  - **Index Scan Frequency**: Enter a value, in Days, Minutes, or Hours for how often the Index scan will run. The default is 7 days. It is recommended that you do not change this default. A week is approximately how long it may take to index files systems for endpoints when first deploying SBOM.

  - **First Scan Distribute Over Time**: Enter a value, in Days, Minutes, or Hours, over which to randomize the distribution of scans to endpoints after the initial scan begins. The default is 1 day.

  - **File Exclusions by Regular Expression**: Enter file names, using regular expressions, to be excluded from scans. For example, ".*\.csv" filters all .csv files. Each exclusion should appear on a separate line.

  - **Directory Exclusions** : By default, Tanium Client directories are included in this exclusion list and will not be scanned. To take an unnecessary load off of index and not scan files that don't require scanning, enter any additional directories that can be excluded. Each exclusion should appear on a separate line.

©2026 Tanium Inc. All Rights Reserved

Excluded Tanium Client directories are as follows:

/opt/Tanium/TaniumClient

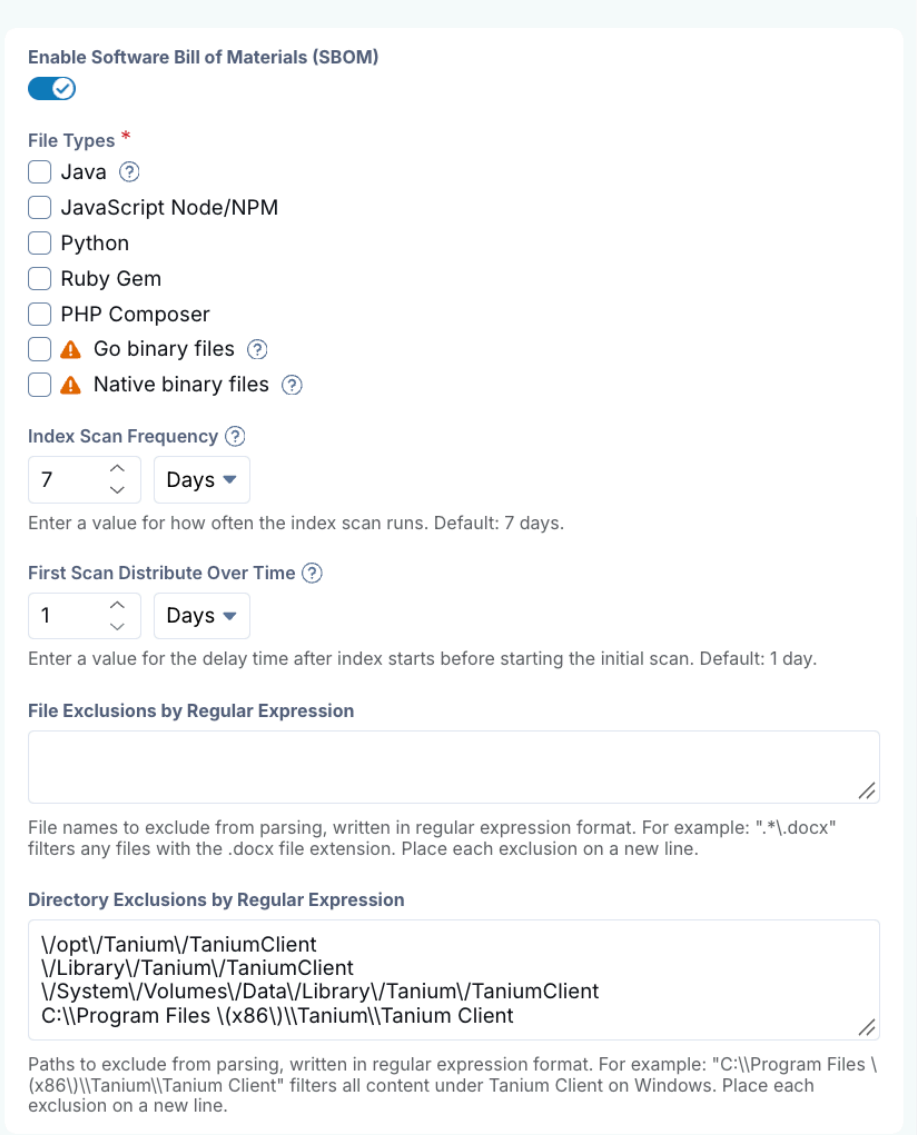
/Library/Tanium/TaniumClient

/System/Volumes/Data/Library/Tanium/TaniumClient

C:\\Program Files\(x86\)\\Tanium\\Tanium Client

Note: Index exclusions that you define in Client Management apply globally to all Tanium solutions that use Index. Exclusions that you add directly in other solutions (Comply in this case) are not visible in Client Management and apply only to those solutions; make sure to view the exclusions in each solution to understand the full list of exclusions. For more information, see Client Index Extension overview.

©2026 Tanium Inc. All Rights Reserved



Note: After SBOM custom settings are configured and saved, you can Create an SBOM scan assessment on page 172.

- **Targeting Type**: Select endpoints to receive these customized settings. Select **Default (Tanium Comply Action Group)** or **Custom Targeting**.
    - **Custom Targeting**: Choose this option to build your own groupings. Use the **Add** buttons to build upon or narrow your selection. When finished, click the check mark for each selection.

3. Click **Save**.

©2026 Tanium Inc. All Rights Reserved

Working with standards and vulnerability sources

Learn how to manage configuration compliance standards and vulnerability sources in Comply, including required roles and available benchmark lists.

About this task

You must have the Comply Report Content Administrator role to read and write configuration compliance standards and vulnerability sources. For more information, see User role requirements on page 41.

> **Note:**
>
> Comply 2.4 and later includes several Tanium Certified standards. These standards have a Tanium certified label. You can use these standards only with the Legacy Tanium Scan Engine.
>
> If you want to use other standards or scan engines, you must import them. See Download and import the CIS-CAT engine on page 88 and Download and import the SCC scan engine on page 91 for instructions on how to import or upgrade standards in bulk.

> **Note:** The complete list of standards Comply provides can be viewed here: https://content.tanium.com/files/published/comply/benchmarks/refs/onprem/benchmarks.html. This list is updated daily.

Configuration compliance standards

Learn how to define and manage configuration compliance standards to ensure that systems remain aligned with organizational and regulatory requirements.

©2026 Tanium Inc. All Rights Reserved

Importing individual standards and assigning categories

Import configuration compliance standards into Comply and organize them with categories and labels so you can filter and manage standards more efficiently.

About this task

You can import standards in Comply that have the following file formats:

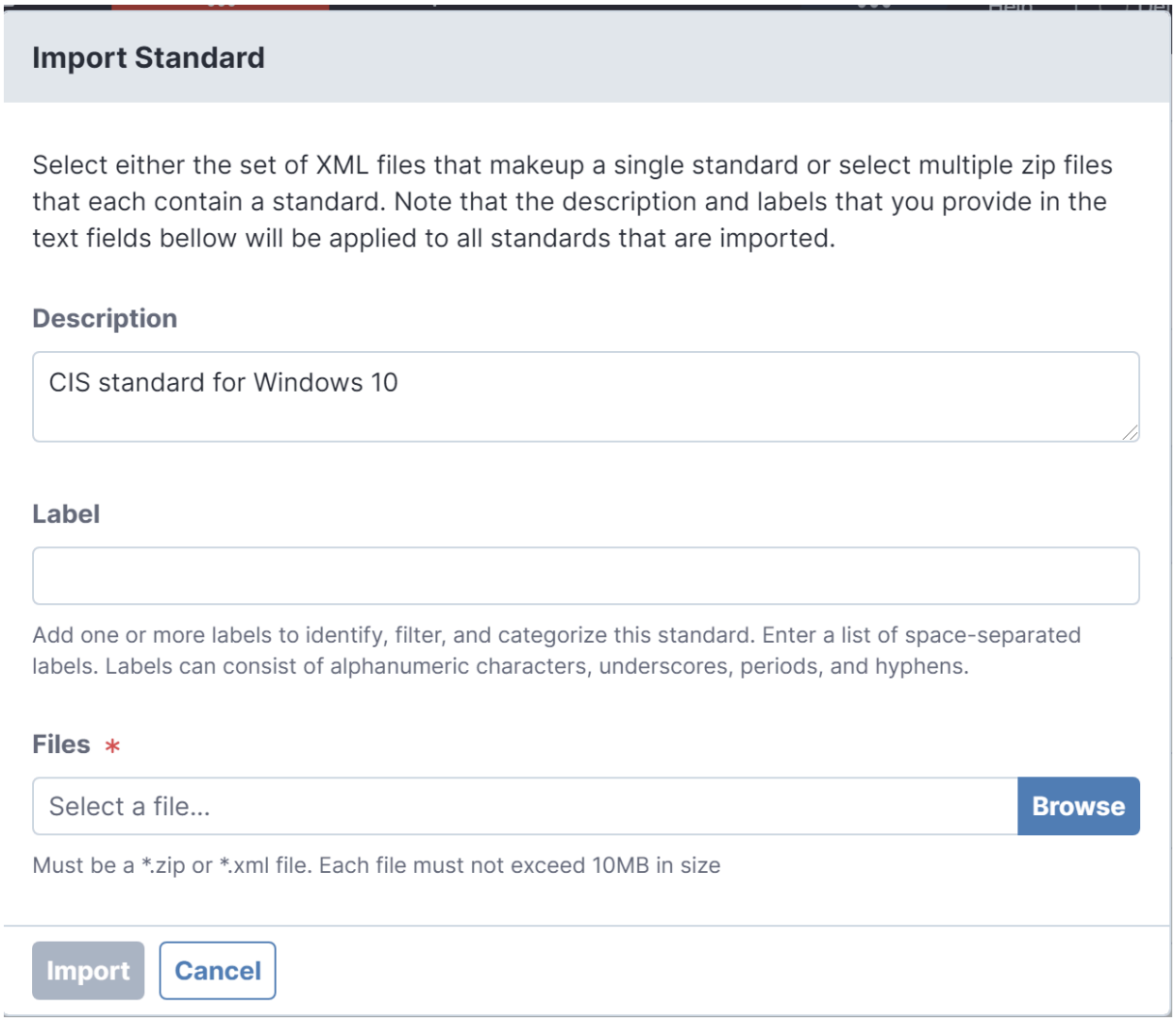
- Split XCCDF format: XCCDF file, OVAL file, CPE, and CPE-dictionary
- Single SCAP 1.2 datastream single file
- Multiple ZIP files containing split XCCDF files (Make sure that all referenced files are included in the zip.)

> **Note:** Benchmarks can refer to scripts that reside in other files. Make sure all referenced files are included in the import.

Use categories and labels to group the standards. You can filter the list of standards on the **Standards > Compliance** page by category and label.

1. From the Main menu, go to **Modules > Comply > Standards.**
2. In the **Compliance** tab, click the **Import** button to import configuration compliance standards.
3. Provide a **Description** for the standard.
4. (Optional) Enter custom labels in the **Labels** field to describe the standard.
5. Click **Select Files** and select the standard files.
6. Click **Import**.

©2026 Tanium Inc. All Rights Reserved



FILTER STANDARDS

Filter standards by category on the **Standards** page in the **Compliance** tab using the **Filter** arrow and **Label** list.

About this task

You can filter standards by category on the **Standards** page, in the **Compliance** tab by selecting a category from the **Filter** arrow and choosing from the **Label** list.

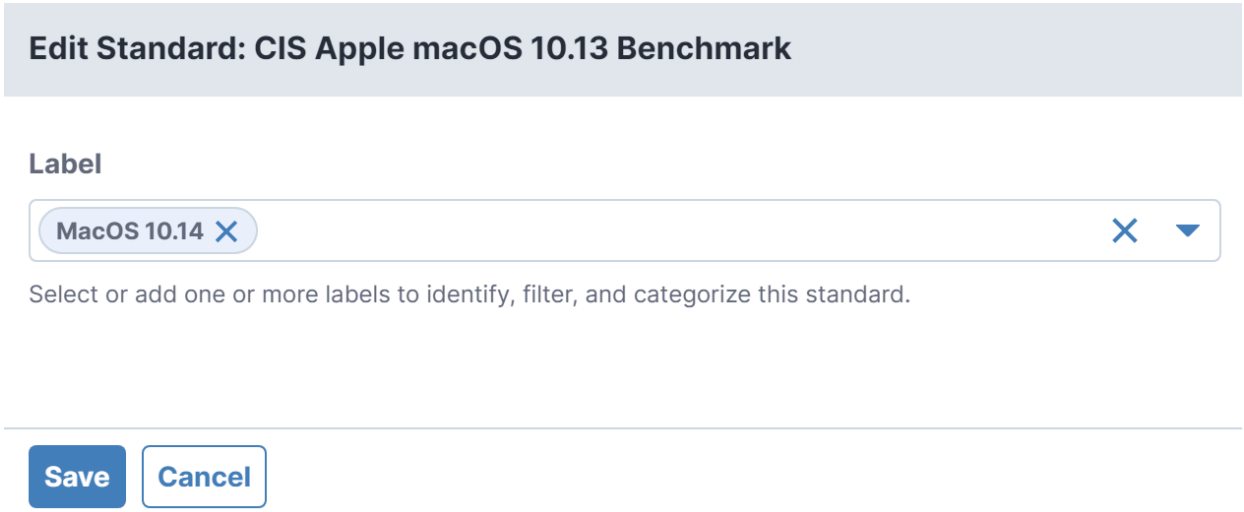
CHANGE A STANDARDS LABEL

Change the label for a standard on the **Compliance** tab of the **Standards** page.

1. On the **Standards** page **Compliance** tab, hover over a standard to show the **Edit** icon.

©2026 Tanium Inc. All Rights Reserved

Click this icon.



2. In the **Standard Metadata** window, edit the **Labels** for the standard.
3. Click **Save**.

CREATE A STANDARD

Create a custom compliance standard by navigating to Compliance setup, entering a title and description, and selecting a standard to create.

1. From the Main menu, go to **Modules** > **Comply > Setup** > **Compliance**.
2. Click **Create** .
3. In the **Custom Profile**, enter a title and a description.
4. Select a standard and click **Create**.

DELETE A STANDARD

Delete a custom compliance standard from the Custom Profiles tab. You cannot delete a standard that is used in an assessment.

1. From the Main menu, go to **Modules** > **Comply > Setup** > **Compliance**.
2. On the **Custom Profiles** tab, click Delete next to the standard you want to delete.
3. Click **OK**.

©2026 Tanium Inc. All Rights Reserved

Result

Note: You cannot delete a compliance standard that is used in an assessment. You must delete the assessment first, and then you can delete the compliance standard.

Filtering standards

Filter standards by label to control which verified, unverified, or unsupported standards display in the Comply Standards page.

About this task

Use the **Label Filter** field at the top right of the **Standards** page, in the **Compliance** tab to filter the standards. Begin entering text to see a list of available labels or click the **X** next to an existing label to remove it from the list of filters.

Comply includes several Tanium Certified standards. These standards have a Tanium Certified icon. You can use these standards only with the Legacy Tanium Scan Engine.

Note: Tanium Certified standards are not supported by Tanium Scan Engine 7.0.

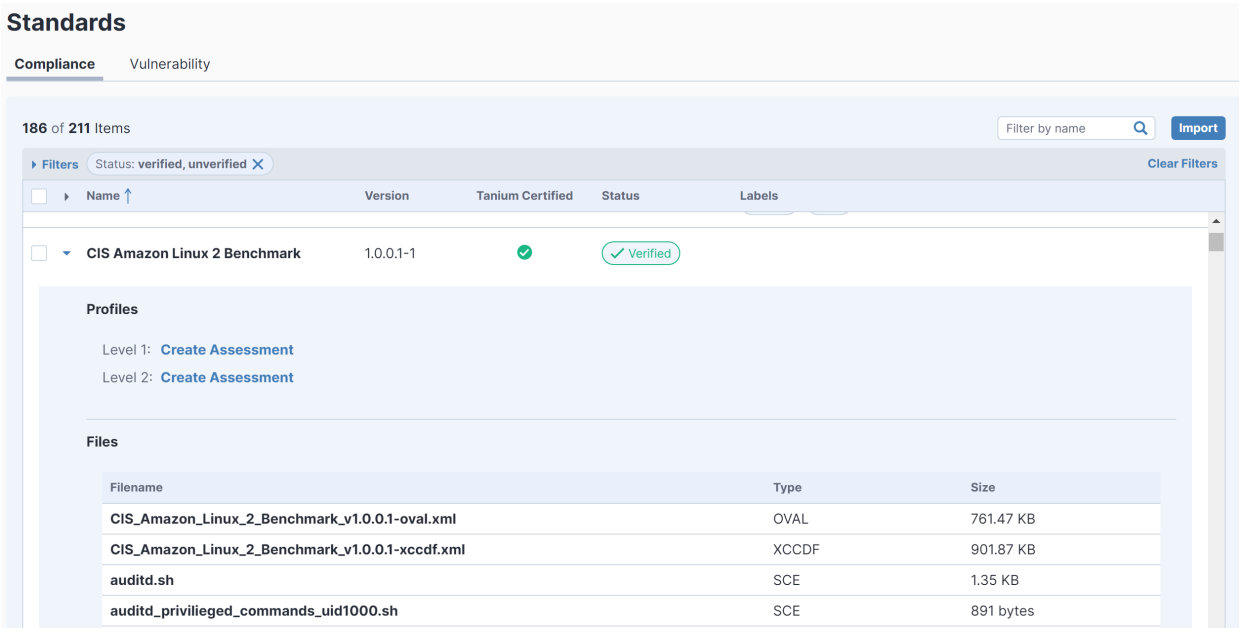
Standards with a **Verified** label were tested and confirmed to work with Comply. Only verified standards display by default. Standards with an **Unverified** label were not tested with Comply. This label does not mean that the standard does not work with Comply. Standards with an **Unsupported** label do not work with Comply.

Viewing configuration compliance standard profiles and creating assessments

View configuration compliance standard profiles and create assessments for selected profiles from the **Standards** page.

1. On the **Standards** page, in the **Compliance** tab , click Expand to see the details of a configuration compliance standard.

©2026 Tanium Inc. All Rights Reserved



2. In the **Profiles** section, hover over a profile and click the **Create Assessment** button next to a standard profile to create an assessment for that profile.

   > **Note:** Click the **Create Assessment** button at the top to create an assessment for the first profile listed.

   The **Create Configuration Compliance Assessment** page opens. For more information, see Creating compliance assessments on page 121.

Vulnerability sources

Use the **Standards** menu and the **Vulnerability** tab to access the **Vulnerability Standards** page.

In the Comply menu, click **Standards** and select the **Vulnerability** tab to open the **Vulnerability Standards** page.

Default vulnerability sources

View the default Tanium Vulnerability Library sources that Comply uses, see the CVEs they include, and understand how their update schedule works.

Expand **Tanium Vulnerability Library** to see the vulnerability sources provided by Comply:

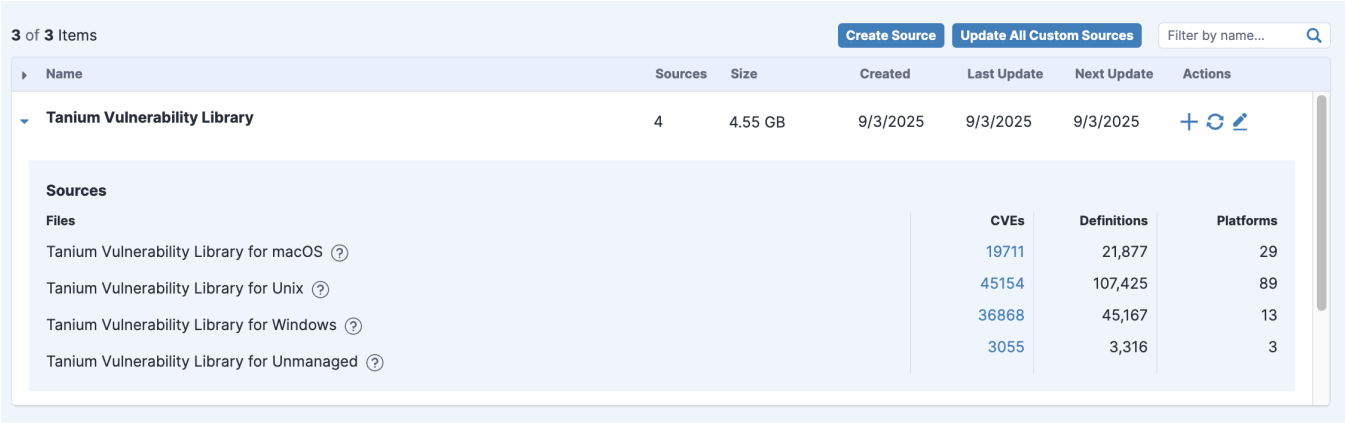
- Tanium Vulnerability Library for Unix

©2026 Tanium Inc. All Rights Reserved

- Tanium Vulnerability Library for macOS
- Tanium Vulnerability Library for Windows
- Tanium Vulnerability Library for Unmanaged

Note: The complete list of CVEs Comply provides can be viewed here: https://content.tanium.com/files/published/tvl/tvl.html. This list is updated daily.

Note: Not all CVEs listed in the Tanium Vulnerability Library can be detected using Comply assessments.



The dates displayed for the Tanium Vulnerability Library indicate the following:

- **Created**: The date the vulnerability database was created before being put on content.tanium.com.
- **Last Update**: The last date that data was added to the vulnerability database. This could be from creation time or from custom sources being added on the Tanium Module Server.
- **Next Update**: The next time Comply will check if there is a new vulnerability database available. This is the next occurrence of the schedule on the TVL.

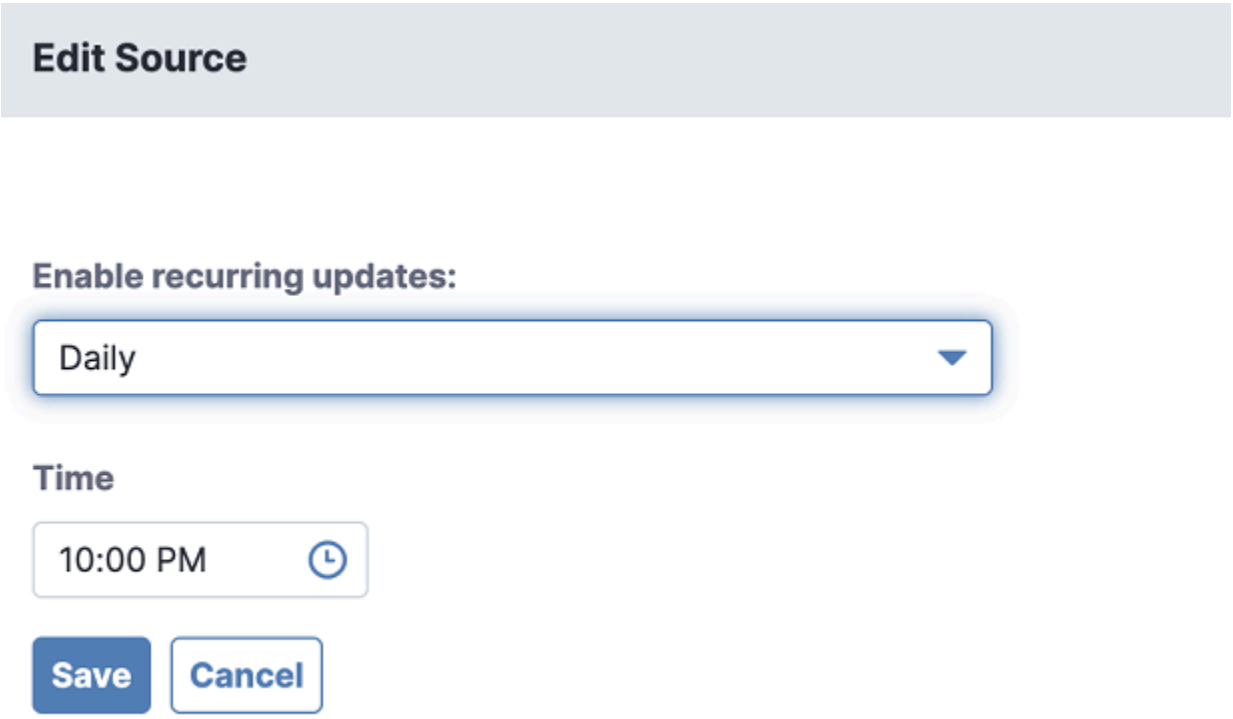
Expand default vulnerability sources to view details. Click on the number of CVEs to see the full list of CVEs included in a standard. You can search the CVE list by using **Filter by Name** field. When CVEs are found, you can further filter that list by clicking **Filters** and using the available filter categories.

©2026 Tanium Inc. All Rights Reserved

Tanium maintains the Tanium Vulnerability Library daily. The new version of the Tanium Vulnerability Library is available for download by clicking **Update Source** in the **Tanium Vulnerability Library** section on the **Vulnerability Standards** page.

Note: The Tanium Vulnerability Library is downloaded from https://content.tanium.com/files/published/tvl/vuln.db.cgz

By default, the Tanium Vulnerability Library is automatically updated daily. To change this schedule, hover over the Tanium Vulnerability Library and click **Edit Source**. Under **Enable recurring updates**, you can select **Check every 30 minutes**, or schedule updates for **Daily**, **Weekly**, **Monthly**, or **Never** and set a specific time. When you select **Check every 30 minutes**, Comply checks for a new Tanium Vulnerability Library every 30 minutes and downloads it if a newer version is available.



Best Practice: Keep the default schedule that updates the Tanium Vulnerability Library daily.

©2026 Tanium Inc. All Rights Reserved

View changes to the Tanium Vulnerability Library

View and download the Tanium Vulnerability Library content change log to see updates to CVE definitions between releases.

About this task

Every time an updated TVL is released, a content change log is created. The change log is a ZIP file that contains JSON files listed by date. The JSON files include the changes made to CVE definitions since the last release. Click here to view the TVL change log information (requires a Tanium Resource Center login).

Best Practice: Because the change log download links are subject to change, you should always access the link from the **Tanium Vulnerability Library Content Change Log Information** page in the Tanium Resource Portal to ensure you are downloading the most recent file.

Note: In some cases, depending on your Comply settings and the Tanium vulnerability update process, there may be a delay in when content updates appear in the change log and when those updates are available in Comply.

Search for CVEs

Search for CVEs across all vulnerability sources to identify which sources contain specified CVE IDs.

Enter one or more CVEs in the **Search all sources for CVEs** field at the top of the **Vulnerability** page and click Search for CVEs. You can use a search to scan all vulnerability sources to identify which sources contain the specified CVEs.

Upload the vulnerability source file for air-gapped environments

Configure Comply for an air-gapped environment and upload the vulnerability standards air gap ZIP file to update local CVE vulnerability sources.

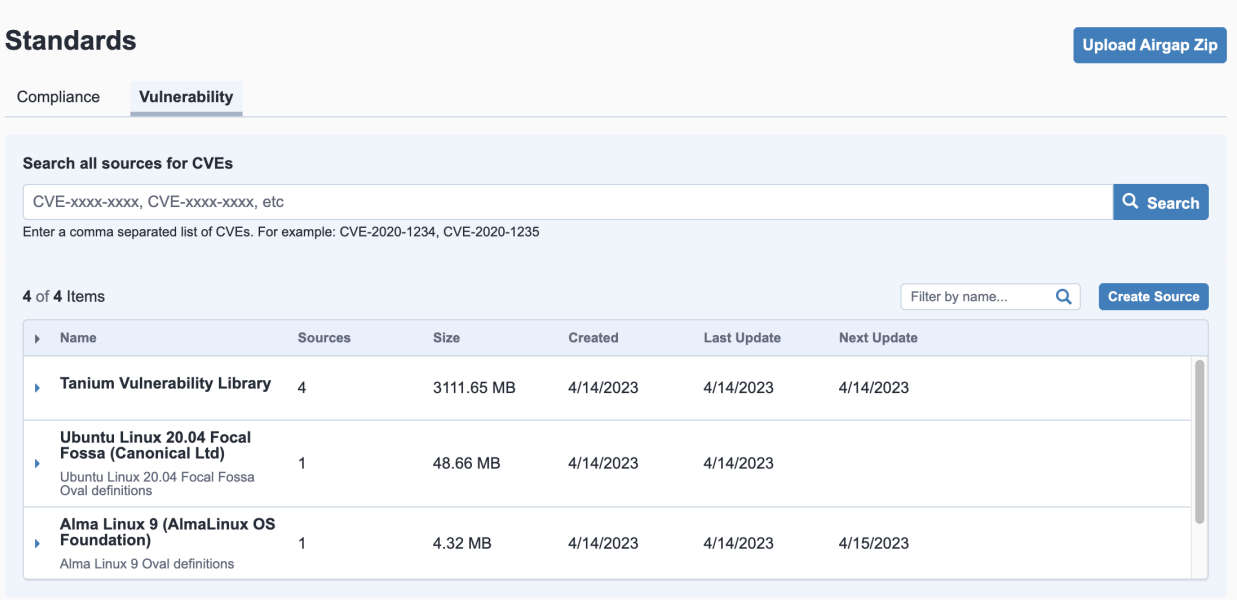
About this task

If you are working in an air-gapped environment, you must configure that setting in Comply and then upload the air gap ZIP file. For the steps to configure Comply for an air-gapped environment, see

©2026 Tanium Inc. All Rights Reserved

Configure Comply for an air-gapped environment on page 60.

1. After you specify that you are working in an air-gapped environment (set **is_airgapped** to **True** on the Settings page) click the **Vulnerability** tab on the **Standards** page to open the **Vulnerability Standards** page.
2. Click **Upload Airgap Zip**.



3. Download the air gap ZIP file from the link indicated in the **Upload Tanium Standards Library Airgap Zip** window (https://content.tanium.com/files/published/tvl/Comply-Standards-Airgap-v2.zip) using a machine that can connect to the internet and save it on the air-gapped machine.
4. Click **Select File**, select the air gap ZIP file from the location where you saved it on the air-gapped machine, and click **Open**.
5. Click **Upload**.
6. After your upload is complete, click **Close** on the upload window. Allow approximately five minutes for Comply to update the vulnerability standards. If you expand a vulnerability source, you will see the **Type** indicated as **Local** as well as a completed count of **CVEs** after the standards are successfully updated from the uploaded air gap ZIP file.

Create a new vulnerability source

Create a vulnerability source that defines how Comply retrieves and updates OVAL vulnerability definitions from remote or imported feeds.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Comply > Standards**.
2. On the **Vulnerability** tab click the **Create Source** button.
3. In the **Details** section, provide a **Name**, **Vendor**, and **Description**.
4. In the **OVAL Definitions** section, for **Definition Type**, select **Remote** or **Import**.
   A remote source is a URL that points to an OVAL definition XML file. Comply updates the source when you click **Update** next to the standard on the **Vulnerability Standards** page.

   > **Note:** Remote sources are best suited when OVAL content is updated periodically. Uploaded sources are best suited to air-gapped environments or when you would like to manually download and provide the source feed. In proxied environments, an entry to the hosts file on the Tanium Module Server may be needed to ensure proper resolution of the remote source URL. For more information, see Remote vulnerability source fails in proxied environment on page 318. You can follow the instructions found here: https://github.com/CISecurity/OVALRepo to generate an OVAL definition file from CIS that provides access to all vulnerability definitions.
5. Enter the path for the **Remote** or **Select file** for **Import** as appropriate.
6. To schedule automatic updates, select **Recurring**.
7. Click **Create**.

Edit or delete a vulnerability source

Edit or delete a vulnerability source from the Vulnerability Standards page.

About this task

On the **Vulnerability Standards** page, click Edit to edit a vulnerability source or Delete to delete a vulnerability source.

Perform a vulnerability scan and create an assessment

Run a vulnerability scan and create an assessment based on a selected vulnerability standard.

1. Click Expand to see the details of a vulnerability standard and view information about the associated XML file and operating systems. Click **Create Assessment** to create a new vulnerability assessment.

©2026 Tanium Inc. All Rights Reserved

2. Click **Create and Deploy** to run the vulnerability scan.

©2026 Tanium Inc. All Rights Reserved

Creating compliance assessments

Create and run configuration compliance and vulnerability assessments in Comply, understand required roles, and review assessment findings.

About this task

> **Note:** When you first set up Comply, the system automatically creates assessments, with default values, for operating systems that are represented by endpoints in the Comply action group. For more information, see Comply overview on page 13 for details.

You can create a new assessment on the **Assessments** page or create one using an existing standard on the **Standards** page. You must have the **Comply Report Administrator** role to create assessments that use client-based scanning. You must have the **Comply RAS Assessment Create** role to create assessments that use remote authenticated scanning. For more information, see User role requirements on page 41.

Run a configuration compliance assessment to check the security configuration compliance state of a group of machines on a set schedule. This will execute data collection using Security Content Automation Protocol (SCAP) Extensible Configuration Checklist Description Format (XCCDF) standards. Run a vulnerability assessment to execute Open Vulnerability and Assessment Language (OVAL) checks against your endpoints to check for the presence of identified vulnerabilities.

The results of assessments are listed in the Findings page. From the Main menu, go to **Modules** > **Comply > Findings**.

> **Best Practice:** Run general assessments that address all known configuration compliance issues and vulnerabilities once a month or bi-monthly. In addition to that large, general assessment, configure a small lightweight assessment that uses only targeted compliance standards or high and critical severity vulnerability definitions from the current year so that you can run it frequently without negative performance impact. For example, you might run the lighter assessment weekly or every 3 days.

Configuration compliance assessments are supported for endpoint operating systems that are

©2026 Tanium Inc. All Rights Reserved

supported by Comply: Windows, macOS, Linux, AIX, and Solaris, with the following exception: For AIX endpoints, only custom checks and automated AIX benchmarks up to version 1.1.0 are supported for compliance scans.

Configure a client-based scan assessment

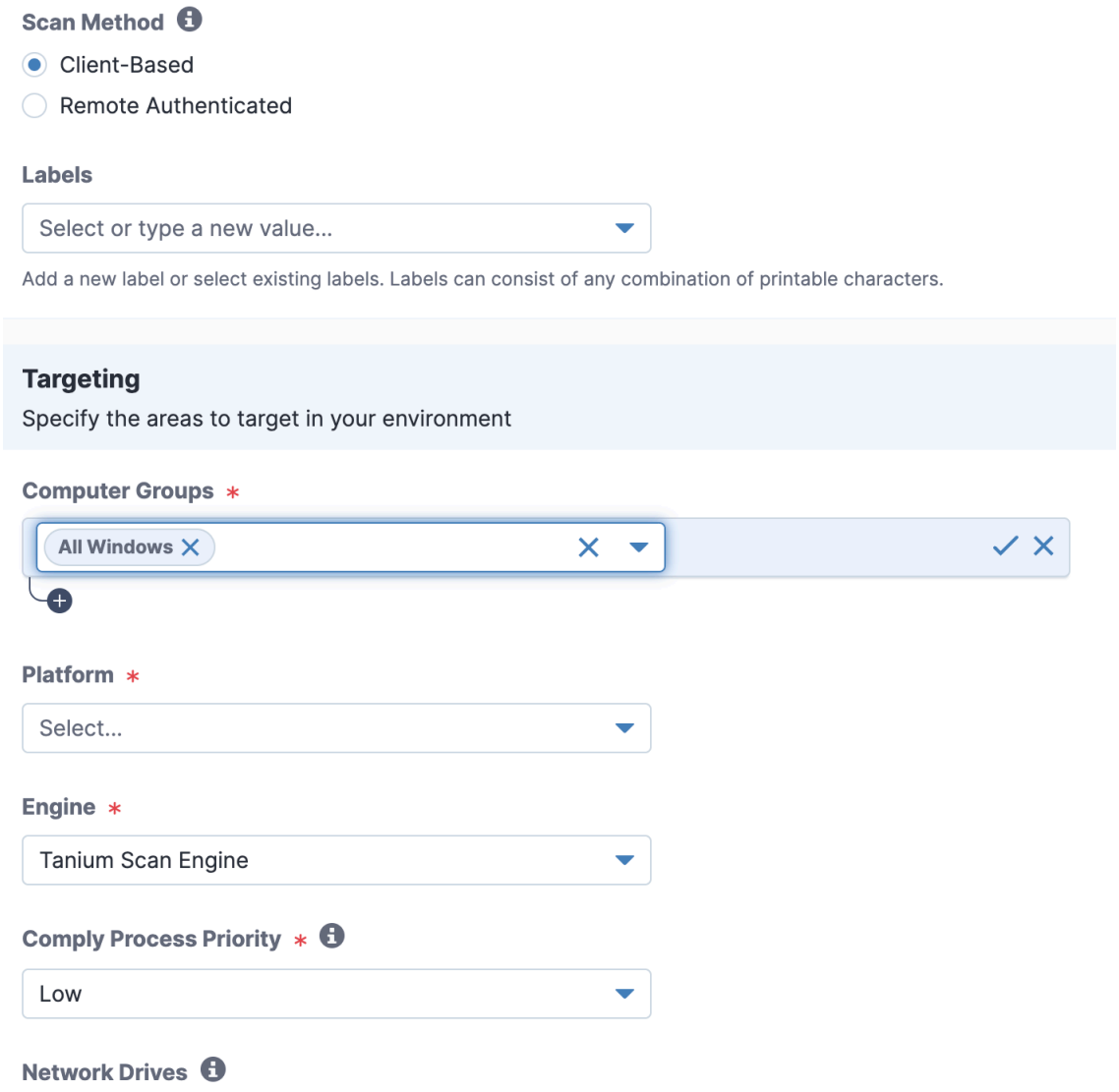
Configure a client-based compliance assessment, including targeting, standards, advanced settings, and optional scheduling, to scan endpoints with Tanium Clients and review results on the Findings page.

1. From the Main menu, go to **Modules** > **Comply > Assessments**.
2. Select **Compliance** from the **Create Assessment** button.
3. In the **Summary** section:
   - Enter a **Name**.
   - Provide a **Label**.
4. Select a **Scan Method** (This field is only visible to users with the Comply RAS Assessment permission. All assessments are client-based scans unless otherwise specified.):
   - **Client-Based**: Client-based scanning uses Tanium Clients installed on endpoints. This is the recommended method of scanning. (The following instructions are for this scan method.)
   - **Remote Authenticated**: Remote authenticated scanning uses Tanium Clients as satellites to scan endpoints that do not have the Tanium Client installed. This scan type is useful for obtaining information from endpoints that do not support having the Tanium Client installed. For more information, see Configure a remote authenticated scan assessment on page 125.
5. In the Targeting section:
   - Select **Computer Groups**. Use the dropdown list to select a group. Add additional groups using the same dropdown list and use the **And**/**Or** buttons to build upon or narrow your selection. Use the **Row** button to add a new row to the group. Click the check mark to save each selection.

     Important: Be sure to select the appropriate platform (**AIX**, **Linux**, **Mac**, or **Windows**) and **Computer Groups** containing endpoints that align with the **Platform** for Comply to work correctly.
   - Select a **Platform**.

©2026 Tanium Inc. All Rights Reserved

- Select the **Engine**. The **Engine** field displays only when more than one engine is installed.



- Select either **Low** or **Normal** from the **Comply Process Priority** list.

  If you select **Low**, the Comply scan process yields processor utilization to other processes running on the endpoint. If you select **Normal**, the scan process runs with the same priority as other processes on the endpoint.

  > **Note:** Selecting **Low** might increase the duration of the scan processes on endpoints with high processor utilization.

©2026 Tanium Inc. All Rights Reserved

> **Note:** This setting applies to the legacy Tanium Scan Engine, CIS-CAT, and SCC only. It does not apply to Tanium Scan Engine 7.0.

- Optionally, when the **Tanium Scan Engine** is selected, you can enable the **Include network drives in scan** checkbox. Network drives are not included in scans by default. Scanning them can be time-consuming and resource intensive.

6. In the **Standards** section:
   - Select the **Standard** from the list. Click **Add Standard** to include more than one.
   - In the **Profile** list, select an existing profile for the selected standard.

     > **Note:** When standards are imported with an engine, such as CIS-CAT or SCC, they are automatically assigned the applicable category. By default, new standards are assigned the **Imported** category.

   - In the **Advanced Settings** section, optionally select a **Custom ID**. Custom ID mappings allow you to create a custom column on results that associates a specific tag with a CVE. Create Custom IDs from the **Setup** > **Compliance** page in the **Custom ID** tab. For more information, see Customizing compliance results on page 279.

     > **Note:** Custom checks should take less than a minute to run – they can output anything to standard output as long as the last line is a valid rule result string such as `pass`, `fail`, or `error`.

7. (Optional) In the **Schedule** section:
   - Select **Start on** and **End on** and complete the date and time values to limit the assessment to run only during a specific time period.

     The date and time displayed by default is the local browser time.

   - (Optional) Select the **Distribute Over** option and enter values to run the assessment over minutes, hours or days. For more information, see Tanium Console User Guide: Deploying actions.
   - In the **Repeat** field, select **Interval**, **Using assessment age**, or **Never**.
     - If you choose **Interval**, the **Reissue every** field displays, and you can specify

©2026 Tanium Inc. All Rights Reserved

how often the assessment runs.

- If you choose **Using assessments age**, then the **Run when results are older than** field displays, and you can specify how old you want the results to be before the assessment runs again. If a targeted endpoint comes online that has never run the assessment, the assessment runs as soon as the next age-check occurs. The age of results is checked every hour.

  Best Practice: Use the **Using assessments age** option and set it to `7 days`.

- Under **Scan Timeout**, you can change the default of 6 hours to allow for scans that may take more time. The minimum you can set the timeout value to is 30 minutes and the maximum is 7 days. It is recommended that you do not change this default without a specific reason.

  Note: This setting applies to the legacy Tanium Scan Engine, CIS-CAT, and SCC only. Tanium Scan Engine 7.0 uses a timeout managed by Tanium and is not affected by this setting.

8. Click **Create & Deploy** and enter your credentials. Results will display on the **Findings** page.

Configure a remote authenticated scan assessment

Configure a remote authenticated scan assessment to use Tanium satellites for scanning unmanaged endpoints, define targeting and credentials, and apply compliance standards and scheduling options.

About this task

Remote authenticated scanning is useful for obtaining information from endpoints and subnets that do not support having the Tanium Client installed. For all other endpoints, you should use client-based scanning for performance reasons and to take advantage of the linear chain architecture.

Important: Remote Authenticated Assessment (RAS) support for Windows, Linux, MacOS, AIX, and Solaris devices will be removed in a future release. If you are currently using RAS to scan endpoints running these operating systems, you should move to client-based assessments.

©2026 Tanium Inc. All Rights Reserved

Before you begin

- Review Reference: Remote authenticated scanning security best practices on page 341 before configuring this feature.
- Remote authenticated scanning requires specific versions of other Tanium solutions. For more information, see Tanium solutions for remote authenticated scanning on page 28.
- Tanium Client operating system support for executing remote authenticated scans is the same as Tanium Client support (see Tanium Client Management User Guide: Client version and host system requirements) with the following exceptions.
    - See CPU and memory requirements for satellites running remote authenticated scans on page 30.
    - Running remote authenticated scans from AIX or Solaris satellites is not supported at this time.
    - Using a zone server as a satellite is not supported at this time.
- Comply provides standards for scanning unmanaged endpoints using a remote authenticated scan. See Unmanaged Endpoints on page 34 for support information.
- See Host and network security requirements on page 36 for remote authenticated scanning port requirements.
- The following RBAC role is required: Comply RAS Assessment Creator. For more information, see User role requirements on page 41.
- Create satellites in Tanium Direct Connect. For more information, see Tanium Direct Connect User Guide: Managing satellites.
- Plan your targeting. When you configure remote authenticated scans, you can manually enter IP addresses (ranges, CIDR, etc.) to be scanned by the selected satellite or you can choose to scan endpoints found by Tanium Discover (Discovered Endpoints). If you are targeting Discovered Endpoints, you must run satellite scans in Tanium Discover before you configure the assessment. For more information, see Tanium Discover User Guide: Running satellite scans.

  More information about targeting:

©2026 Tanium Inc. All Rights Reserved

- Targeting IP addresses: When using IP address targeting (the default), the addresses you enter do not have to be on the same subnet as the satellite to be scanned. They only have to be reachable by the satellite.

- Targeting Discovered Endpoints: When targeting Discovered Endpoints, if an endpoint does not match Tanium Discover's **Promote Unmanaged Interface** label, that endpoint is not promoted to Tanium Data Service (TDS). If an endpoint is not promoted to TDS, it cannot be scanned by Comply. Therefore you must promote interfaces to TDS in Tanium Discover. For more information, see Tanium Discover User Guide: Managing interfaces. Note that because Tanium Discover cannot get the MAC address from endpoints that are not in the same subnet as the satellite, only endpoints in the same subnet as the satellite will be scanned.

- WinRM 2.0 or higher must be installed on targeted Windows operating systems.

- Remote authenticated scans are supported on Arm-based Windows 11 clients. Scans run using an emulated x64 JVM.

- For ESXi endpoints, when you configure the assessment, you target the IP address of VMware vCenter managing the ESXi hosts. You cannot connect directly to an ESXi host. After the scan completes, Endpoint Statistics displays the ESXi endpoints. Comply does not know about those ESXi endpoints until the scan is run.

  Note: If you try to target ESXi endpoints directly, you may see results, but those results should not be considered reliable.

  Note: Because ESXi endpoints are not targeted directly, their status will not change or get updated in the UI until the scan is complete and all results are received.

  Note: Endpoint Statistics will include the VMWare vCenter in the number of scanned endpoints, but the vCenter endpoint is not scanned. Joval does not support scanning a vCenter instance (VCSA) at this time.

- Configure credentials in Tanium Comply. For more information, see Configure credentials for remote authenticated scans on page 63.

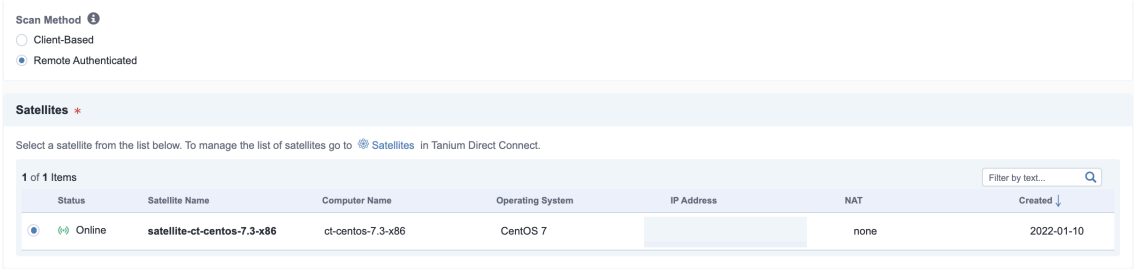
©2026 Tanium Inc. All Rights Reserved

- Do not target the same unmanaged assets with multiple remote authenticated scan assessments.
- Target a maximum of 256 unmanaged assets per remote authenticated scan assessment or the equivalent of a /24 network.

To configure a remote authenticated scan assessment, do the following:

1. From the Main menu, go to **Modules** > **Comply > Assessments**.
2. Select **Compliance** from the **Create Assessment** button.
3. In the **Summary** section:
   - Enter a **Name**.
   - Provide a **Label**.
4. Select a **Scan Method** (This field is only visible to users with the Comply RAS Assessment permission. All assessments are client-based scans unless otherwise specified.):
   - **Client-Based**: Client-based scanning uses Tanium Clients installed on endpoints. This is the recommended method of scanning.
   - **Remote Authenticated**: Remote authenticated scanning uses Tanium Clients as satellites to scan endpoints that do not have the Tanium Client installed. This scan type is useful for obtaining information from endpoints that do not support having the Tanium Client installed. Note that remote authenticated scanning only supports using the Tanium Scan Engine. (The following instructions are for this scan method.)

     Note: The Discover scan cannot get the MAC address from endpoints that are not in the same subnet as the satellite. Therefore only endpoints in the same subnet as the satellite will be scanned.



5. In the **Satellites** section, select a satellite from the list to perform the scan.
6. In the **Targeting** section, select a **Targeting Type**.

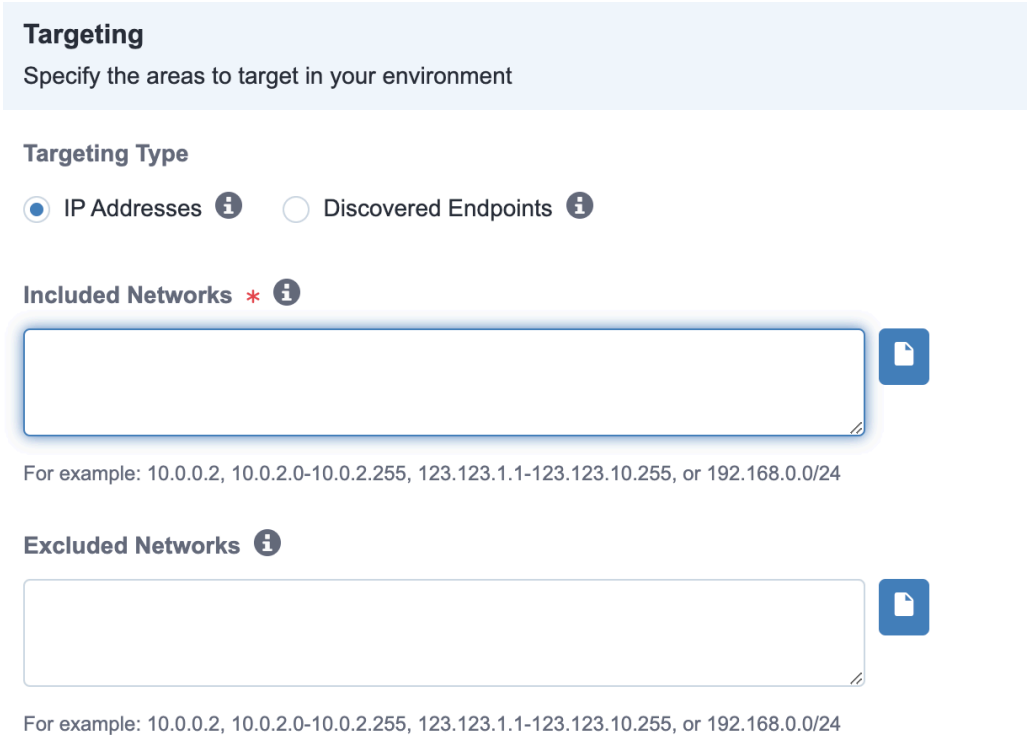
©2026 Tanium Inc. All Rights Reserved

- **Important:** If you use IP addresses (the default), the addresses you enter do not have to be on the same subnet as the satellite to be scanned. If you use discovered endpoints, because Tanium Discover cannot get the MAC address from endpoints that are not in the same subnet as the satellite, only endpoints in the same subnet as the satellite will be scanned.

- **IP Addresses**:

  - In the **Included Networks** field, enter a comma separated list of IP addresses, IP address ranges, or CIDR addresses. You can also click the **Copy** button to upload a text file containing IP addresses, IP ranges, or CIDRs separated either by commas or carriage returns.

  - In the **Excluded Networks** field, enter IP addresses, IP address ranges, or CIDR addresses to be excluded from the scan. You can enter them manually or upload a file of addresses.



Note: Be sure to enter IP addresses that the selected satellite can reach.

- **Discovered Endpoints**: Click the **+ROW** or **+Grouping** button to view the **Select**

©2026 Tanium Inc. All Rights Reserved

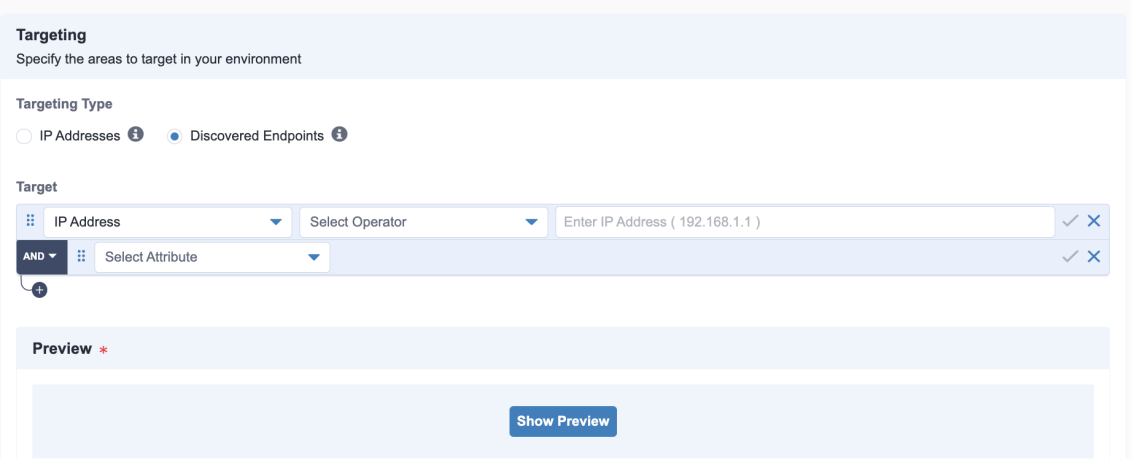
Attribute field. Select from the following Attribute combinations to filter the list of discovered endpoints:

Discovered endpoints attributes

Attribute	Available Operators	Value
IP Address	is equal to, is not equal to, contains, does not contain	Enter a single IP address or multiple addresses, each separated by a comma. For example, 192.168.1.1, 192.168.1.3
Discover Labels	include one of, include all of	Select one or more labels configured in Tanium Discover. For more information, see Tanium Discover User Guide: Labels .
IP Range	equals	Enter an IP address range. For example, 192.168.1.1 - 192.168.1.150
CIDR	equals	Enter an IP address range in CIDR format. For example, 192.168.1.0/24
OS Platform	contains, does not contain	Enter text for targeting a specific OS.

Tip: To select multiple items in the **Value** field, click within the field after adding an item, and you can select additional items.

Use the **And**/**Or** buttons to build upon or narrow your selection. Use the **Add Row** or **Add Group** button to add a new target to the group. Click the check mark to save each selection.

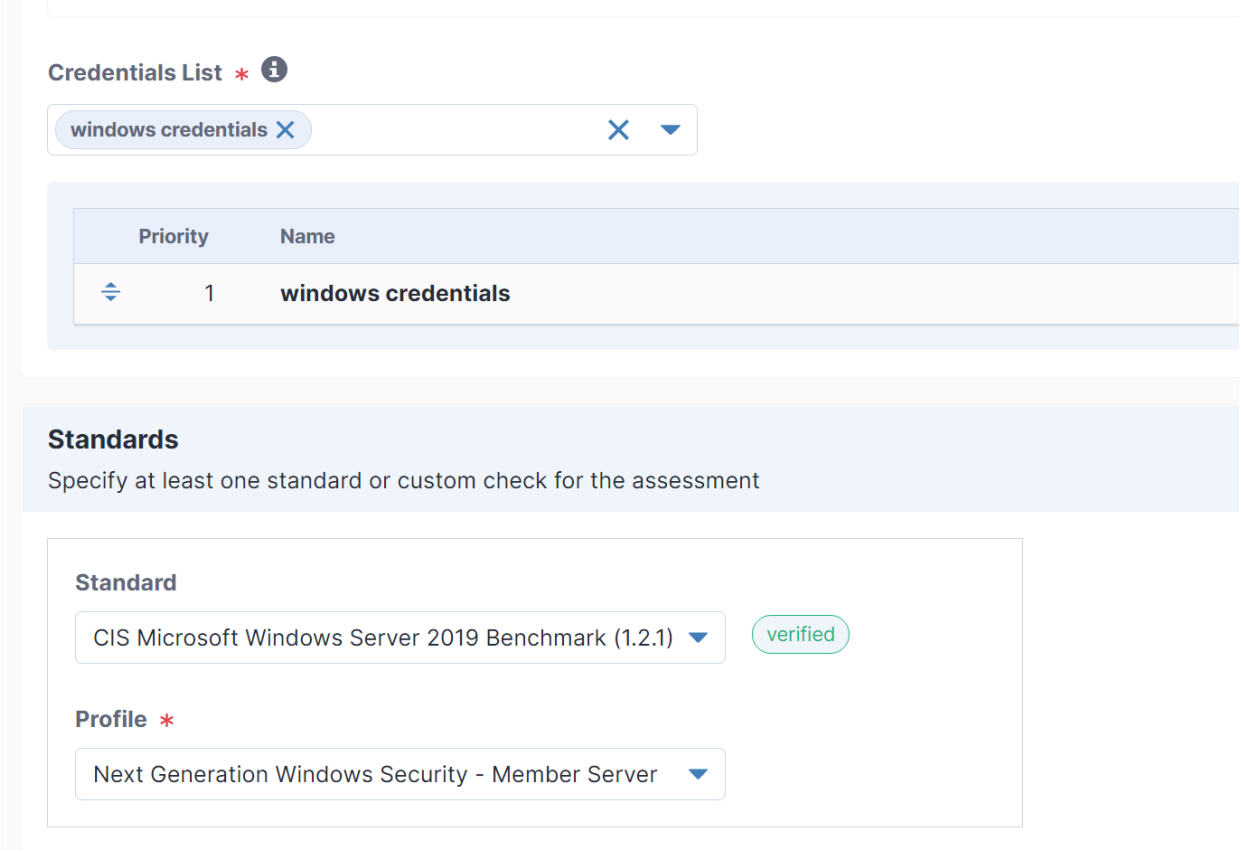


- In the **Preview** section for Discovered Endpoints, click the **Show Preview** button to

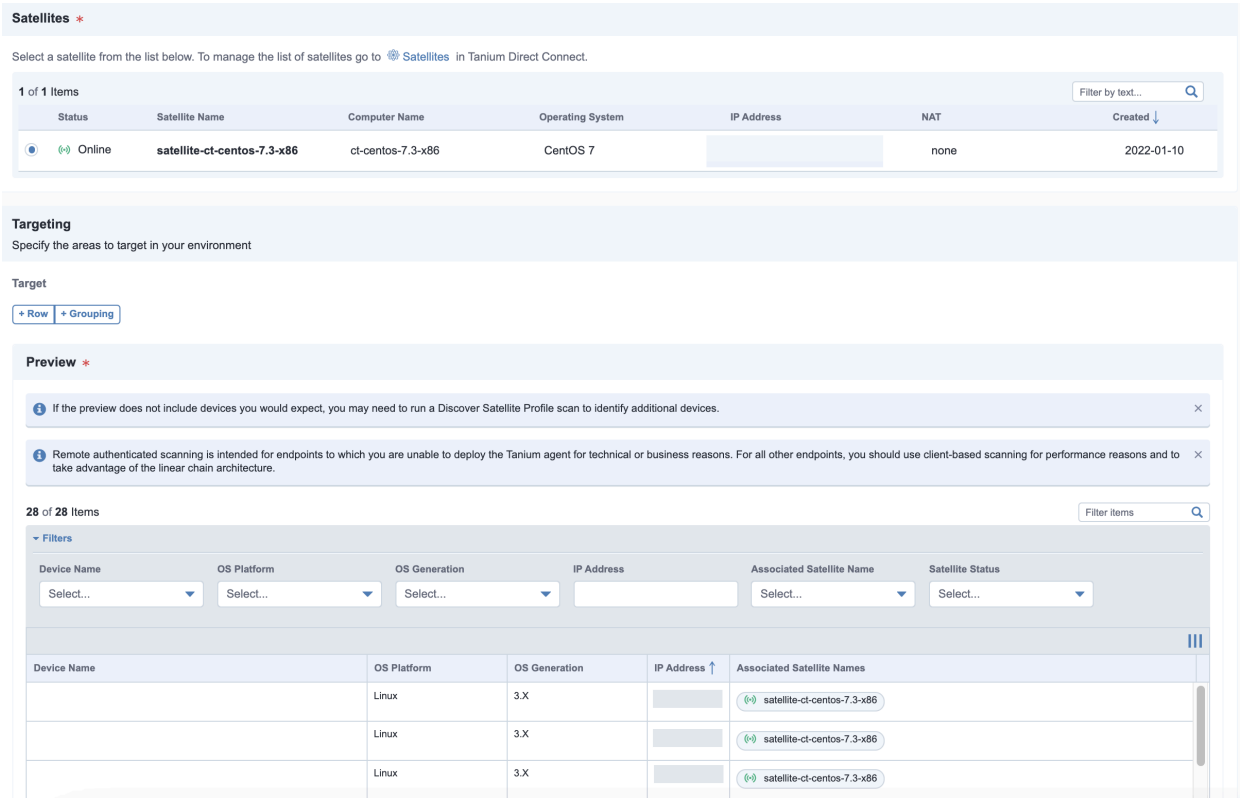
©2026 Tanium Inc. All Rights Reserved

view the list of unmanaged endpoints you selected for targeting. You can use the information in the preview grid to expand or narrow your targeting. For example, you can target a satellite initially and then add an IP range to further filter your targets based on what you observed in the preview.

7. Select the **Credential List** for this assessment.
   You can only use one list per assessment. In order for satellites to perform secure scans of non-Tanium endpoints, the login credentials for those endpoints are required. For more information, see Configure credentials lists for remote-authenticated scans on page 63.



©2026 Tanium Inc. All Rights Reserved



CAUTION: Make sure the credential list you select matches the targeting in the assessment. If too many incorrect credentials are attempted and fail, this could trigger security alerts and cause account lockouts.

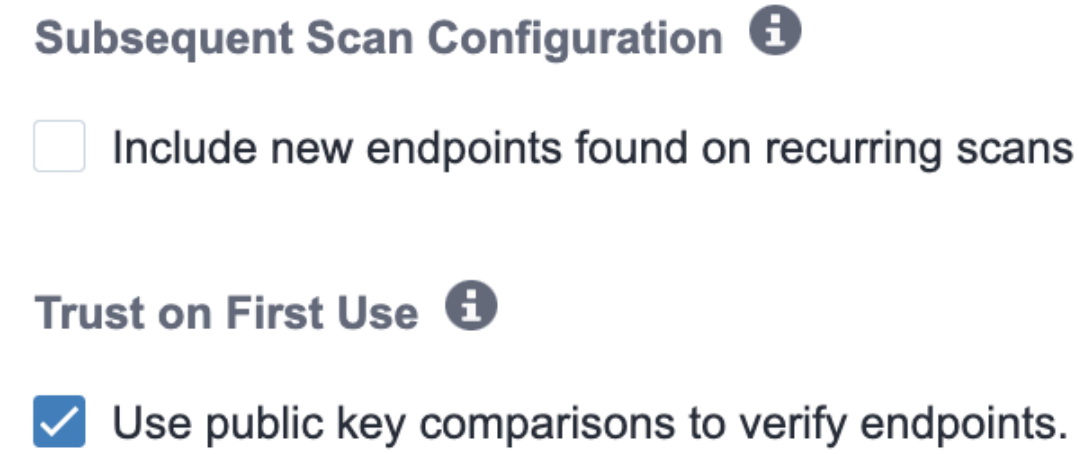
8. Optionally but not recommended, in the **Subsequent Scan Configuration** section, enable the **Include new endpoints found on recurring scans** checkbox. By default, if scans are recurring, Comply only scans endpoints that were reachable during the initial scan. If new endpoints come online, they are not scanned unless you change the assessment's targeting or select this checkbox.

   CAUTION: If you enable the **Include new endpoints found on recurring scans** checkbox and your network is compromised at any point after the initial scan, a honeypot could be installed in your environment that matches the scan configuration requirements. If that occurs, an unmanaged endpoint could capture the credentials being passed to it and use them with malicious intent.

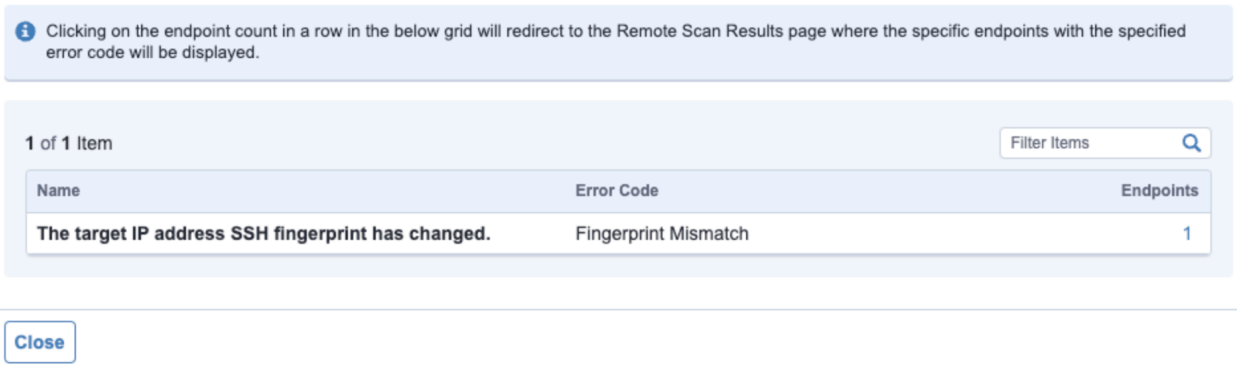
9. Enabled by default and recommended when you use SSH key and SSH password credentials, use **Trust on First Use** for fingerprint comparison.
   With this feature enabled, Comply will collect the SSH fingerprint the first time an endpoint connects. For every future connection, Comply will check to make sure the endpoint

©2026 Tanium Inc. All Rights Reserved

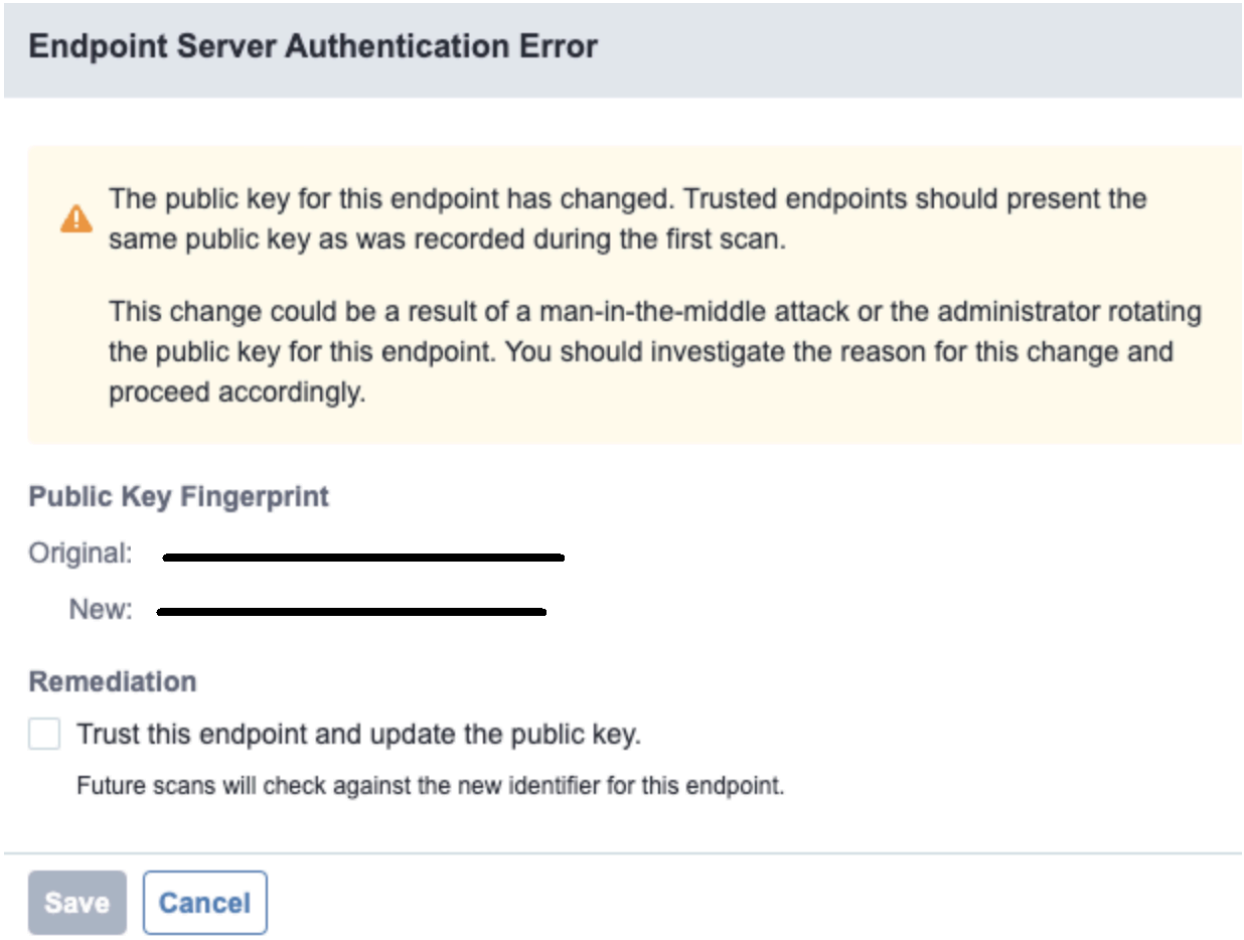
presents the same SSH fingerprint. If it does not, Comply will log a **Fingerprint Mismatch Error**. An endpoint that fails the fingerprint check will not be logged into or scanned.



If you receive a fingerprint mismatch error, you can click on the assessment error message and then click through to the endpoint to accept the new key to resolve the error.



©2026 Tanium Inc. All Rights Reserved



10. In the **Standards** section:
    - Select the **Standard** from the list. Click **Add Standard** to include more than one.
    - In the **Profile** list, select an existing profile for the selected standard.

      Note: When standards are imported with an engine, such as CIS-CAT or SCC, they are automatically assigned the applicable category. By default, new standards are assigned the **Imported** category.
    - In the **Advanced Settings** section, optionally select a **Custom ID**. Custom ID mappings allow you to create a custom column on results that associates a specific tag with a CVE. Create Custom IDs from the **Setup** > **Vulnerability** page in the **Custom ID** tab. For more information, see Customizing compliance results on page 279.

©2026 Tanium Inc. All Rights Reserved

> **Note:** Custom checks should take less than a minute to run – they can output anything to standard output as long as the last line is a valid rule result string such as `pass`, `fail`, or `error`.

11. (Optional) In the **Schedule** section:
    - Select **Start on** and **End on** and complete the date and time values to limit the assessment to run only during a specific time period.

      The date and time displayed by default is the local browser time.

    - (Optional) Select the **Distribute Over** option and enter values to run the assessment over minutes, hours, or days. For more information, see Tanium Console User Guide: Deploying actions.

    - In the **Repeat** field, select **Interval**, **Using assessment age**, or **Never**.

      - If you choose **Interval**, the **Reissue every** field displays, and you can specify how often the assessment runs.

      - If you choose **Using assessments age**, then the **Run when results are older than** field displays, and you can specify how old you want the results to be before the assessment runs again. If a targeted endpoint comes online that has never run the assessment, the assessment runs as soon as the next age-check occurs. The age of results is checked every hour.

        > **Best Practice:** Use the **Using assessments age** option and set it to `7 days`.

      - Under **Scan Timeout**, you can change the default of 6 hours to allow for scans that may take more time. The minimum you can set the timeout value to is 30 minutes and the maximum is 7 days. It is recommended that you do not change this default without a specific reason.

        > **Note:** This setting applies to the legacy Tanium Scan Engine, CIS-CAT, and SCC only. Tanium Scan Engine 7.0 uses a timeout managed by Tanium and is not affected by this setting.

©2026 Tanium Inc. All Rights Reserved

12. Click **Create & Deploy** and enter your credentials. Results will display on the **Findings** page.

Remote authenticated scan workflow

Learn how Comply determines scan targets and credentials for remote authenticated scans and how recurring assessments handle newly discovered endpoints.

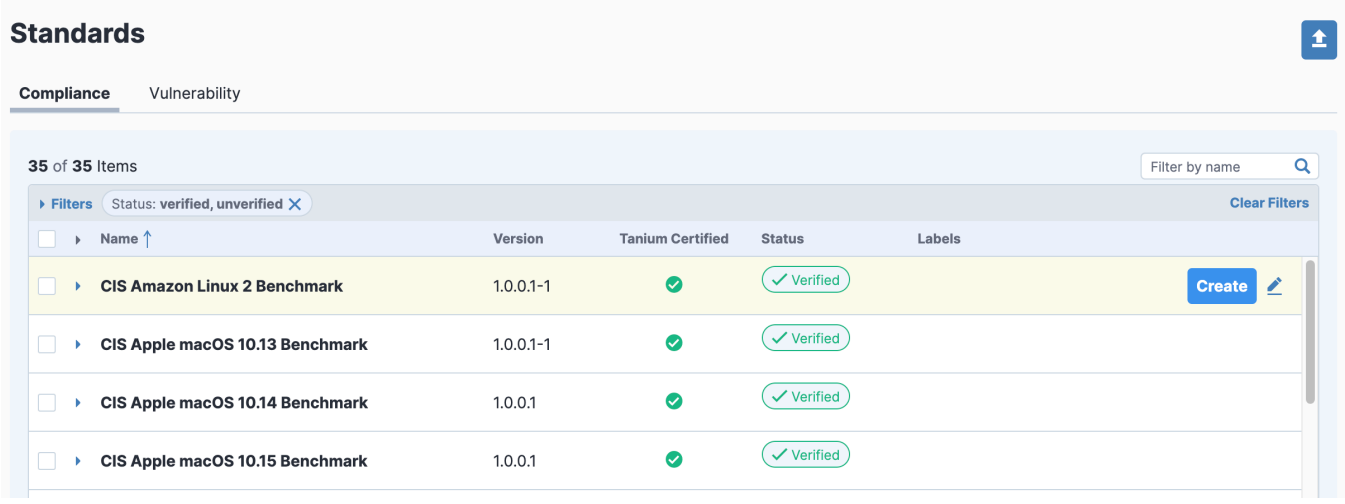
When a remote authenticated scan begins, it asks the Comply service for its targets and credentials. The service uses the scan's criteria for IP inclusion to query for currently reachable targets for that satellite and sends that list to the client to execute the scan. Scheduled periodic RAS scans do not automatically include new targets as they are identified by the associated Tanium Discover scan. Reoccurring assessments will only include the unmanaged assets that were reachable at the time of the initial scan, unless you select the **Include newly discovered endpoints on reoccurring scans** checkbox, which is not recommended.

Create a configuration compliance assessment from the Standards page

Create a configuration compliance assessment for a standards profile from the Standards Compliance tab.

About this task

On the **Standards Compliance** tab, click **Create** next to a profile to create an assessment for that profile.



©2026 Tanium Inc. All Rights Reserved

Status definitions

View and interpret assessment scan statuses in the **Status** column on the assessment list page.

View the status of a scan in the **Status** column on the assessment list page. Hover over the icon to see one of the following statuses:

In Progress

The assessment is being published.

Loading

No statistics have been received from the Comply service for the assessment.

Pending

At least one endpoint in the assessment has not yet run the scan, but there are no scan errors.

Success

The assessment has at least one successful run with no errors and no scans not run.

Error

The assessment has at least one endpoint that produced an error during the scan.

Warning

Any issue that does not fall into the other status categories.



Note: You must reload the page to update the status column.

Run an assessment again

Run an existing assessment again from the **Assessments** page to apply updated compliance configuration standards.

About this task

©2026 Tanium Inc. All Rights Reserved

On the **Assessments** page, select an assessment and click **Deploy** to run it again.

> **Note:** Updates to compliance assessments require a new assessment to use updated configuration compliance standards.

Run an on-demand scan

Run an on-demand scan for client-based assessments using existing targeting or additional filters, with optional debug logging for legacy Tanium Scan Engine.

About this task

> **Note:** On-demand scans are only supported for client-based assessments.

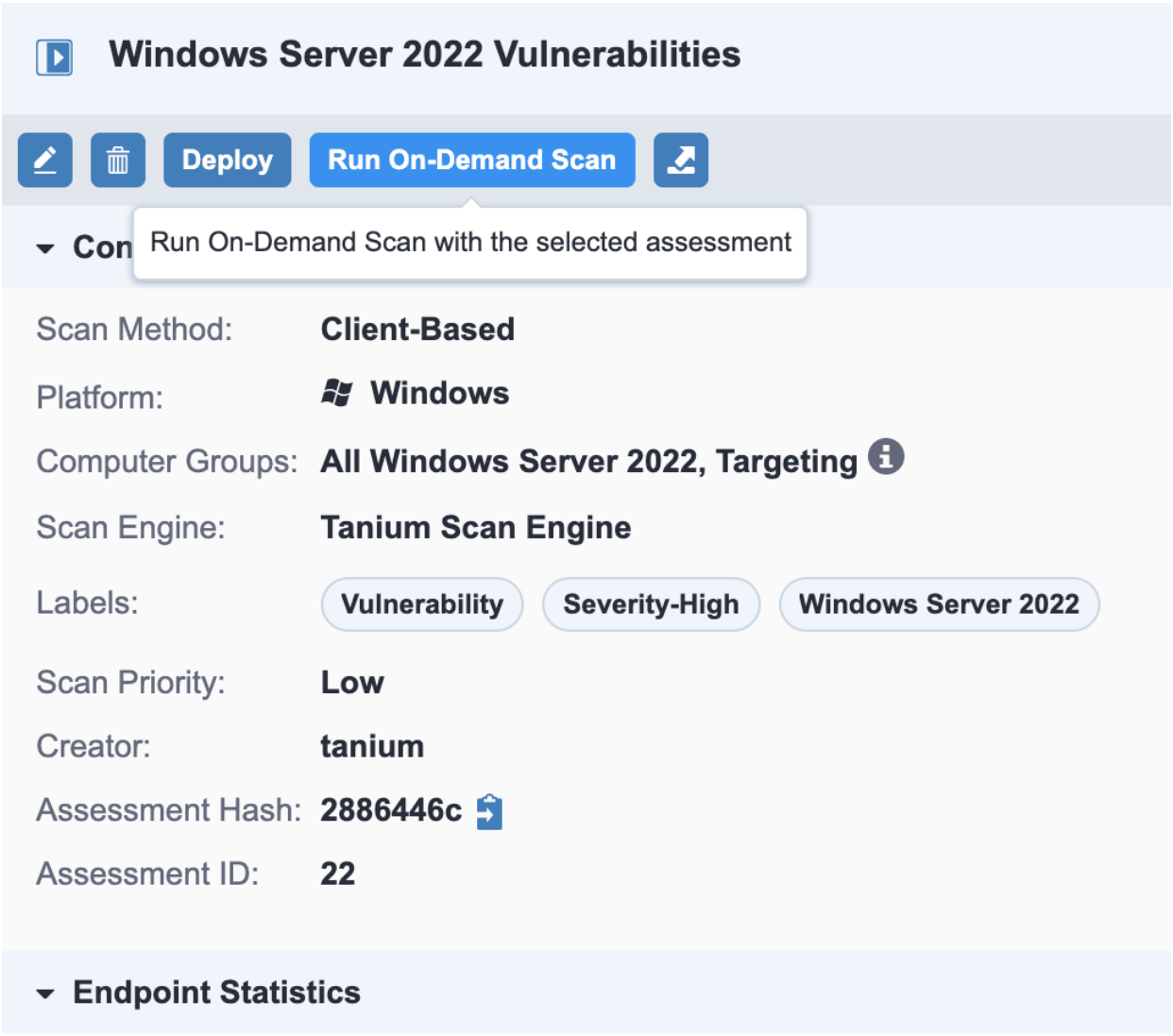
> **Note:** For vulnerability assessments that use Tanium Scan Engine 7.0 or later, a re-index of the endpoint occurs before the on-demand scan begins.

An on-demand scan lets you run an assessment at the push of a button using existing targeting or with additional filters. Optionally, you can run the assessment with or without debug enabled.

To run an on-demand scan:

1. Select the checkbox for an assessment or click the arrow for the Side Panel window to access the **Run on-demand Scan** button.

©2026 Tanium Inc. All Rights Reserved



2. Click the **Run on-demand scan** button and optionally configure the following:
   - Select the **Run with Debug** checkbox - Debug is only available for the legacy Tanium Scan Engine. With debug enabled, scans are run with more detailed logging and additional output that the CX stores is available to view (see Client extensions on page 29). A debug zip as well as an xml file are produced in /opt/Tanium/TaniumClient/extensions/comply/data/results/joval-<assessment ID>

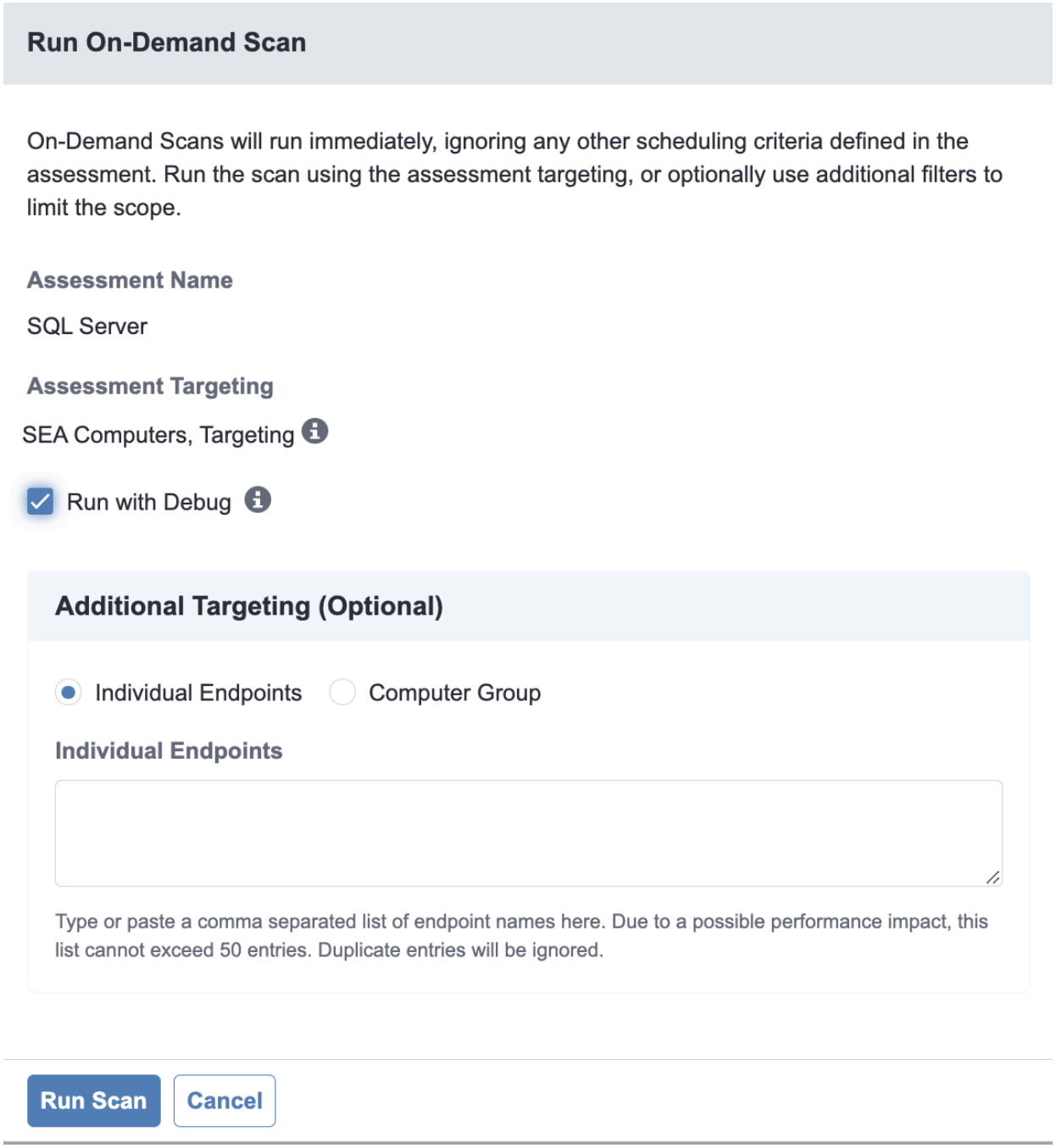
     Note: This file path applies to the Legacy Tanium Scan Engine.

   - Configure additional filtering - Select **Individual Endpoints** and enter those endpoints into the edit field or select **Computer Group** and choose a group to filter by.

©2026 Tanium Inc. All Rights Reserved

> **Important:** If you select **Individual Endpoints** and enter computer names, you must enter the computer name exactly as it is returned by the **Computer Name** sensor.

3. Click the **Run Scan** button.



©2026 Tanium Inc. All Rights Reserved

Export an assessment

Export a single compliance assessment and configure the file name, format, and details to include in the exported results.

About this task

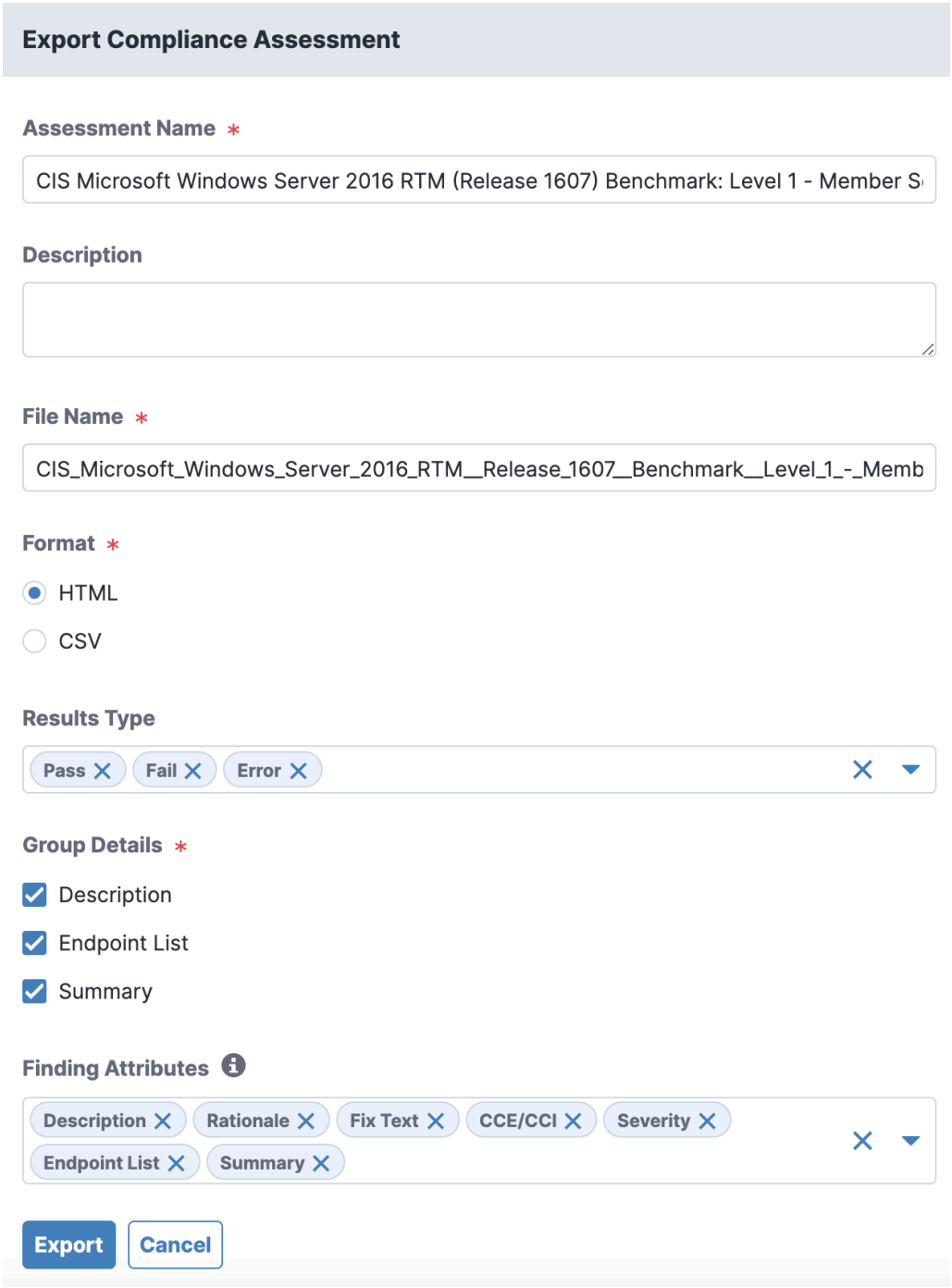
The following instructions are for exporting one assessment at a time. To export findings using Tanium Connect, see Exporting findings and assessments on page 259 for instructions.

1. From the Main menu, go to **Modules** > **Comply > Assessments**. Select an assessment and click the **Export** icon . You can only export one assessment at a time. If you have more than one assessment selected, the Export icon is not displayed.

   > **Note:** You can also access **Clone**, **Edit**, **Delete**, **Deploy**, **Run On-demand Scan**, and **Export** < **Actions** from the **Side Panel** for each assessment on the Assessments list page.

2. In the **Export Assessment** window, provide the following for each assessment type:
   - **Compliance**
     a. Enter an **Assessment Name**.
     b. Optionally, enter a **Description**.
     c. Enter a **File Name**.
     d. Select a **Format**: **HTML** or **CSV**. If you select CSV, no further information is required.
     e. Select one or more **Results Types** for the export.
     f. Select which **Group Details** to export: **Description**, **Endpoint list**, **Summary**.
     g. Select one or more **Finding Attributes** to export.

©2026 Tanium Inc. All Rights Reserved



h. **Click Export**.

Edit an assessment

Edit an existing assessment, including its name, labels, schedule, and custom checks, and then save your changes.

1. From the Main menu, go to **Modules** > **Comply > Assessments**. Select the assessment you

©2026 Tanium Inc. All Rights Reserved

want to edit and click the Edit icon .

> **Note:** You can also access **Clone**, **Edit**, **Delete**, **Deploy**, **Run On-demand Scan**, and **Export** < **Actions** from the **Side Panel** for each assessment on the Assessments list page.

2. Edit the **Name** if needed.
3. Add labels in the **Labels** field. Click the **X** next to a label to remove it.
4. Change the **Comply Process Priority** if needed.

> **Note:** This setting applies to the legacy Tanium Scan Engine, CIS-CAT, and SCC only. It does not apply to Tanium Scan Engine 7.0.

5. For compliance assessments, edit the **Custom Checks** selection if needed. Using the same field that is available when you create a new assessment, add or remove custom checks. You can also add custom checks even if the original assessment did not include any.

> **Note:** You must have the **Comply Custom Check Writer** role to view and select custom checks. For more information, see User role requirements on page 41.

6. Select **Start at** and **End at** and complete the date and time values to limit the assessment to run only during a specific time period. The date and time displayed by default is the local browser time. For more information, see Tanium Console User Guide: Deploying actions.
7. Select the **Distribute over** and enter values to run the assessment over minutes or hours.
8. Select **None**, **Interval**, or **Use assessment age** for the **Repeat** field.
    - If you choose **None**, the assessment will run once if the **Start At** field is specified for a date and time in the future. Otherwise, the assessment will not run again.
    - If you choose **Interval**, the **Reissue every** field will appear, and you can specify how often the assessment is run. The default value for this field is **1 Days** and, if you do not specify a value for **Start at**, the assessment will run immediately. If you choose **Interval** and do not enter a value for **End At**, the assessment will run at the specified interval forever.
    - If you choose **Use assessment age**, then the **Run when results are older than** field will appear, and you can specify how old you want the results to be before the assessment is run. The default value for this field is **1 Days** and, if you do not specify a value for **Start at**, the assessment will run immediately. If a targeted endpoint comes online that has never run the assessment, the assessment will be run as soon

©2026 Tanium Inc. All Rights Reserved

as the next age-check occurs. The age of results is checked either every hour or every 3 hours. If you specify an age less than 3 hours, the age of results will be checked every hour. If do not enter a value for **End At**, the assessment will continue to run forever.

9. Click **Save**.

Clone an assessment

Clone an existing assessment to quickly create a new one with the same settings, then edit and deploy it as needed.

You can quickly create a new assessment based on an existing assessment by using the clone feature.

1. From the Main menu, go to **Modules** > **Comply > Assessments**. Select the assessment you want to clone and click Clone . You can also clone an assessment from the assessment's side panel.

   Note: You can also access **Clone**, **Edit**, **Delete**, **Deploy**, **Run On-demand Scan**, and **Export** < **Actions** from the **Side Panel** for each assessment on the Assessments list page.

2. A new assessment page opens with all fields prepopulated with settings from the original assessment. In the name field, the name of the original assessment is prepended with the text Clone -.

3. Make necessary edits and click **Create and Deploy**.

Delete an assessment

Delete a configuration compliance assessment that uses an outdated standard so you can create a new assessment with the updated standard.

About this task

When an updated version of a new configuration compliance standard is released, you must delete the configuration compliance assessment that uses the old standard and create a new assessment with the updated standard.

©2026 Tanium Inc. All Rights Reserved

Note: You can also access **Clone**, **Edit**, **Delete**, **Deploy**, **Run On-demand Scan**, and **Export** < **Actions** from the **Side Panel** for each assessment on the Assessments list page.

Note: You cannot delete a standard, custom check, or custom ID mapping if they are associated with an assessment.

From the Main menu, go to **Modules** > **Comply > Assessments**. Select an assessment and click the **Delete** icon to delete it.

Download audit history

Download a CSV file of assessment audit history, including edits and deletions, for all assessments or a single assessment.

About this task

You can view the audit history of assessments, including edits and deletions, by time, date, and user.

1. From the Main menu, go to **Modules** > **Comply > Assessments**.
   Click the **Download Audit History** button to download a CSV file with the audit history of all assessments.



2. To download the audit history of a single assessment, go to the side panel for that assessment, scroll down to the **Audit History** section and click the download button.

©2026 Tanium Inc. All Rights Reserved

Creating vulnerability assessments

Learn how to create and manage vulnerability assessments in Comply, including required roles and available assessment options.

About this task

> **Note:** When you first set up Comply, the system automatically creates assessments, with default values, for operating systems that are represented by endpoints in the Comply action group. For more information, see Comply overview on page 13.

You can create a new assessment on the **Assessments** page or create one using an existing standard on the **Standards** page. You must have the **Comply Report Administrator** role to create assessments that used client-based scanning. You must have the **Comply RAS Assessment Create** role to create assessments that use remote authenticated scanning. For more information, see User role requirements on page 41.

Configure a client-based scan assessment

Configure a client-based vulnerability assessment, including targeting, platform and engine selection, CVE content and definitions, scheduling, and deployment options.

1. From the Main menu, go to **Modules** > **Comply > Assessments**.
2. Click **Create Assessment** > **Vulnerability**.
3. On the **Create Vulnerability Assessment** page, in the **Summary** section, enter a **Name** for the assessment. You can also provide **Labels**.
4. Select a **Scan Method**:
   - **Client-Based**: Client-based scanning uses Tanium Clients installed on endpoints. This is the recommended method of scanning. (The following instructions are for this scan method.)
   - **Remote Authenticated**: Remote authenticated scanning uses Tanium Clients as satellites to scan endpoints that do not have the Tanium Client installed. This scan type is useful for obtaining information from endpoints that do not support having

©2026 Tanium Inc. All Rights Reserved

the Tanium Client installed. For more information, see Configure a remote authenticated scan assessment on page 152.

- **Network unauthenticated**: Find vulnerabilities on unmanaged endpoints in your environment using Tanium Clients as satellites to scan endpoints that do not have the Tanium Client installed and cannot be authenticated to. You can also do distributed scans using the Discover module. For more information, see Configure a network unauthenticated scan assessment on page 165.
- **SBOM (Software Bill of Materials)**: (requires a Tanium SBOM license) An SBOM vulnerability scan has visibility into libraries and all files that are known to Software Manager. The results of an SBOM assessment analysis are mapped to CVEs on the endpoint. For more information, see Create an SBOM scan assessment on page 172.
- **Container Registries**: Container registry scanning is useful for determining vulnerabilities in images within the registry based on the results of a Software Bill of Materials assessment. Tanium SBOM and Tanium Cloud Workloads are required. For more information, see Configure a container registry scan assessment on page 175.

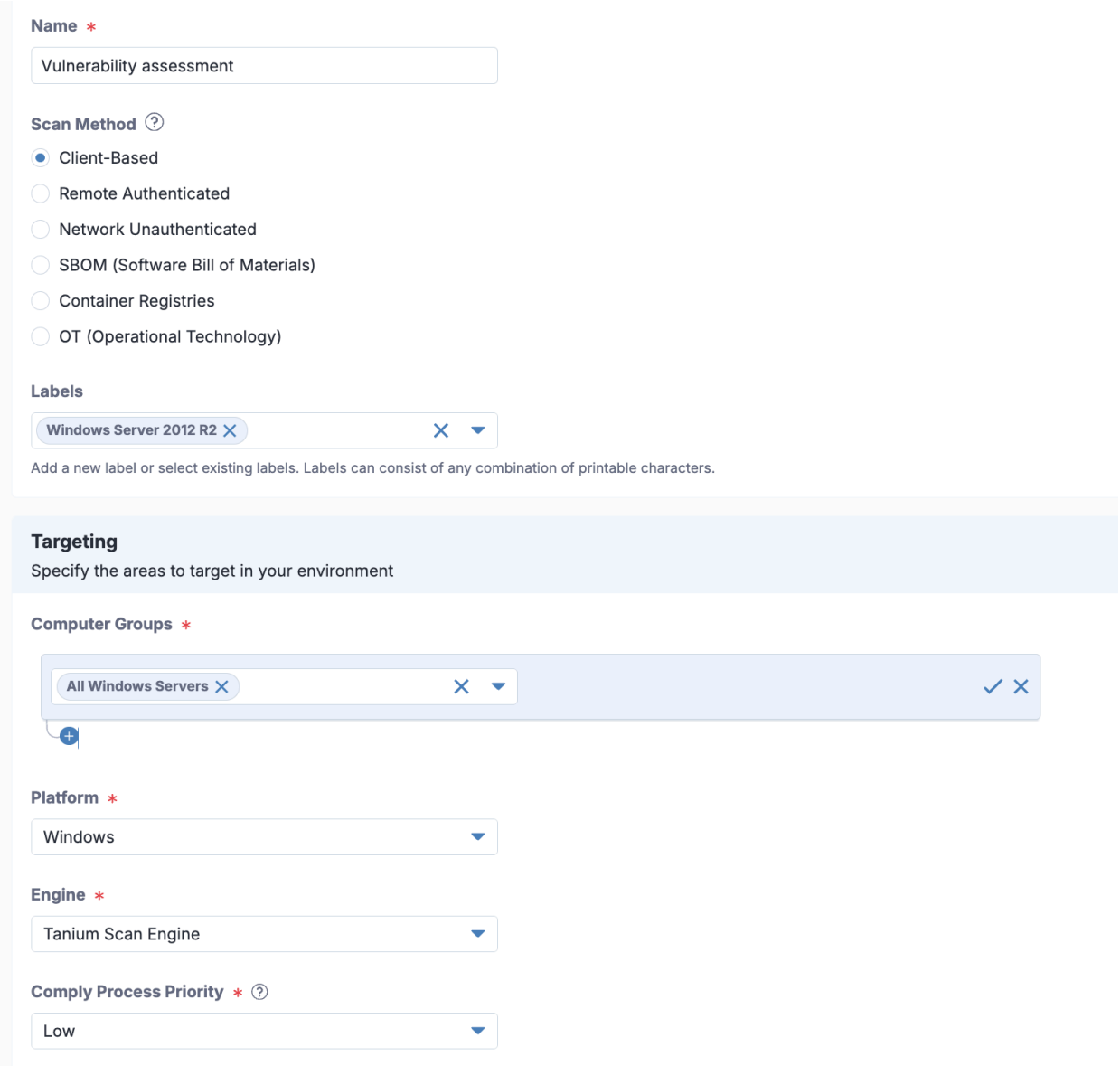
5. In the Targeting section:
   - Select **Computer Groups**. Use the dropdown list to select a group. Add additional groups by using the Add button to build upon or narrow your selection. When finished, click the check mark for each selection.



Best Practice: Be sure to select the appropriate platform and **Computer Groups** containing endpoints that align with the **Platform**.

6. Select a **Platform**.
7. Select the **Engine**. The **Engine** field displays only when more than one engine is installed.
8. Select either **Low** or **Normal** from the **Comply Process Priority** list.

©2026 Tanium Inc. All Rights Reserved



If you select **Low**, the Comply scan process yields processor utilization to other processes running on the machine. If you select **Normal**, the scan process runs with the same priority as other processes on the machine.

> **Note:** Selecting **Low** might increase the duration of the scan processes on endpoints with high processor utilization.

> **Note:** This setting applies to the legacy Tanium Scan Engine, CIS-CAT, and SCC only. It does not apply to Tanium Scan Engine 7.0.

9. Optionally, when the **Tanium Scan Engine** is selected, you can enable the **Include network drives in scan** checkbox. Network drives are not included in scans by default. Scanning them

©2026 Tanium Inc. All Rights Reserved

can be time-consuming and resource intensive.

10. Select the **Source** from the list in the **Vulnerability Content** section.
11. Select an **Operating System**.
12. Choose a **CVE Definitions Type**. Options are as follows:
    - **Standard Resource CVEs** – Select this option to include only standard resource CVEs in the assessment. This would exclude from scans CVEs that use OVAL definitions known to impact endpoint performance and reduce overall vulnerability scan coverage.

      Click **View excluded high resource CVEs** in the informational notice to go to the **CVE List** page where you can filter to view high resource CVEs.

    - **High Resource CVEs** – Select this option to include only CVEs that use OVAL definitions known to impact endpoint performance. Scanning for these CVEs can result in higher levels of resource consumption, which may have a negative impact on the endpoint. In most cases, you would select this option for an assessment to run on a controlled schedule based on endpoint resource availability. Click **View high resource CVEs** in the informational notice to go to the **CVE List** page where you can filter to view high resource CVEs.

    - **Both Standard and High Resource CVEs** - Select this option to scan for all CVE definitions types regardless of resource consumption. Click **View high resource CVEs** in the informational notice to go to the **CVE List** page where you can filter to view high resource CVEs.

      
      Note: Custom sources are also evaluated for resource impacting CVE definitions type settings.

      
      Important: The definitions type selection takes precedence over other CVE filtering settings you configure. For example, if you select to use only Standard Resource CVE definition types, but the Range of CVEs you enter includes High Resource CVEs, those High Resource CVEs are not included in the assessment. Similarly, if you select to use only Standard Resource CVE definitions types and enter a High Resource CVE in the List of Individual CVEs to Include field, that High Resource CVE is not included in the assessment. Check the **Preview** window to see what CVEs are included in the assessment.

©2026 Tanium Inc. All Rights Reserved

> **Note:** When CVE definitions type selections are available for assessments (after an upgrade), a notification appears in the Tanium Console. Click the **Set CVE Definition Type** button to change the definition type for multiple assessments at once. For more information, see Update CVE definitions type (One-time bulk action) on page 191.

> **Tip:** When you select a CVE definitions type, it is the OVAL definition that is excluded or included in the assessment, and that OVAL definition may not directly map to a CVE due to its applicability to the targeted platform. Therefore, if you select to use only standard resource CVEs, a specific CVE may be excluded as high resource for a Windows assessment, but that same CVE may not be excluded for a Linux assessment. This is because OVAL definitions apply for both platform and CVE. As a result, you might notice inconsistencies in CVE count previews during the creation or editing of assessments, or reviewing high resource CVEs without platform context.

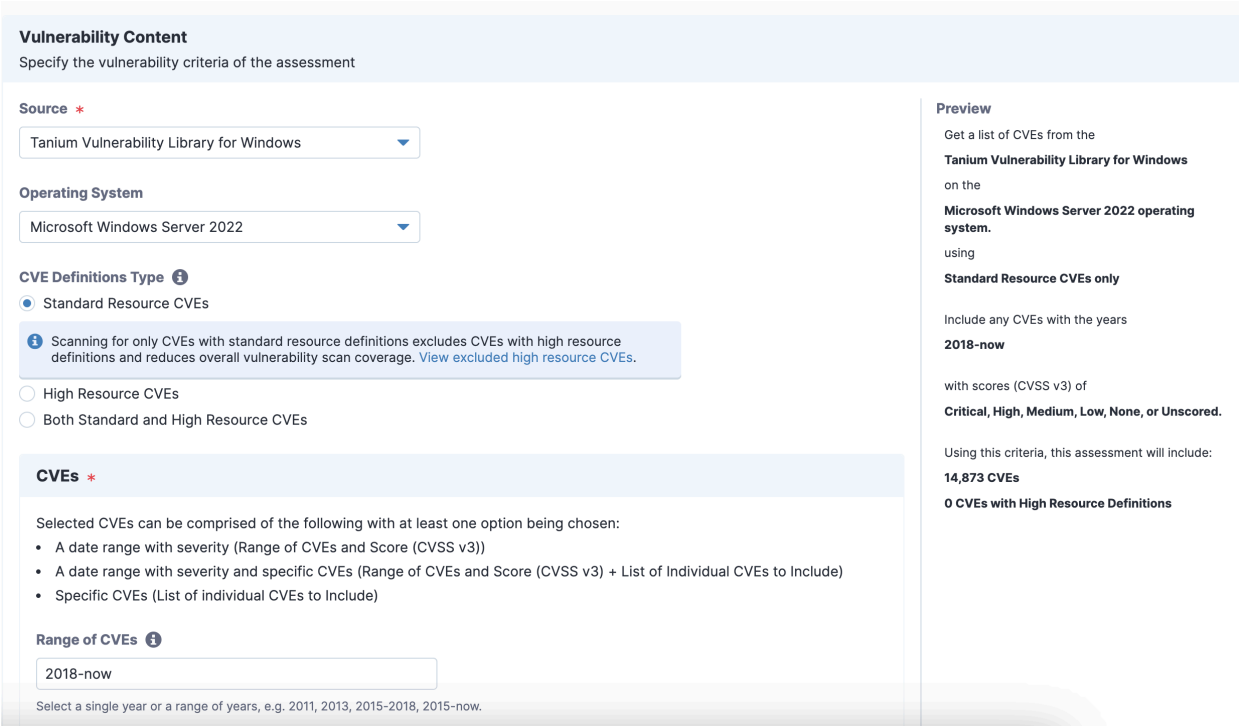
13. Specify the **Range of CVEs**. The **Preview** section on the right will show the number of **CVEs** and **Definitions** that will be included in the assessment.

    > **Note:**
    > You can specify `now` in the **Range of CVEs** field as the end of a range. For example, entering `2016-now` will run the assessment against all Common Vulnerabilities and Exposures (CVEs) from 2016 to the current date. By using this format, you can easily define a range that always is current.
    >
    > As a best practice, scan more frequently for recently released high and critical vulnerabilities (for example, 2018-now high and critical on a weekly basis), and conduct scans against all vulnerabilities less frequently (for example, monthly or quarterly).

14. Check the scores you want to see in **CVSS Score**.

15. List specific CVEs in the **List of Individual CVEs** field.

©2026 Tanium Inc. All Rights Reserved



> **Note:** If you specify a **List of Individual CVEs**, and there is no **CVE Definitions Type** setting that takes precedence, they will be included in the assessment regardless of the values specified for **Range of CVEs** or **CVSS Score**. To search by year and score, you must provide values for both fields for the search to be valid. If you specify **Range of CVEs**, you must select at least one score in **CVSS Score**. If you select a score in **CVSS Score**, you must specify **Range of CVEs**. If you list specific CVEs, you can choose to leave the **Range of CVEs** field blank and select no **CVSS Score**.

16. Optionally, enter a comma separated list of CVEs to include.
17. Optionally, enter a comma separated list of CVEs to exclude.
18. Optionally, select the checkbox to **Only include CVEs with CISA KEV**.
19. Specify the **Batch Size**.

> **Note:** **Batch Size** defines the number of checks that will run at a time. To run a manageable number of checks on your endpoints, the default value for this field is 500 for CIS-CAT and SCC, and the default is 2000 for Legacy Tanium Scan Engine. This setting does not typically need to be adjusted from the default value. However, in some cases, increasing the batch size can speed up scans and may avert scan timeouts. This increase may also require increasing the endpoint maximum heap size to avoid out-of-memory errors.

©2026 Tanium Inc. All Rights Reserved

20. Select **Start on** and **End on** and complete the date and time values to limit the assessment to run only during a specific time period.
    The date and time displayed by default is the local browser time.

21. Select the **Distribute Over** option and enter values to run the assessment over minutes, hours, or days. For more information, see Tanium Core Platform User Guide: Deploying actions.

22. Select **Interval**, **Using assessment age**, or **Never** for the **Repeat** field.
    - If you choose **Interval**, the **Reissue every** field displays, and you can specify how often the assessment is run.

    - If you choose **Using assessment age**, then the **Run when results are older than** field displays, and you can specify how old you want the results to be before the assessment is run. If a targeted endpoint comes online that has never run the assessment, the assessment will be run as soon as the next age-check occurs. The age of results is checked every hour.

      
      Best Practice: Use the **Using assessment age** option and set it to `7 days`.

    - Under **Scan Timeout**, you can change the default of 6 hours to allow for scans that may take more time. The minimum you can set the timeout value to is 30 minutes and the maximum is 7 days. It is recommended that you do not change this default without a specific reason.

      
      Note: This setting applies to the legacy Tanium Scan Engine, CIS-CAT, and SCC only. Tanium Scan Engine 7.0 uses a timeout managed by Tanium and is not affected by this setting.

23. Click **Create & Deploy** and enter your credentials. Results will display on the **Findings** page.

Configure a remote authenticated scan assessment

Configure a remote authenticated vulnerability assessment to scan unmanaged endpoints that do not have the Tanium Client installed, using satellites, targeted IP ranges or discovered endpoints, and CVE-based vulnerability content.

About this task

©2026 Tanium Inc. All Rights Reserved

Remote authenticated scanning is useful for obtaining information from endpoints and subnets that do not support having the Tanium Client installed. For all other endpoints, you should use client-based scanning for performance reasons and to take advantage of the linear chain architecture.

Important: Remote Authenticated Assessment (RAS) support for Windows, Linux, MacOS, AIX, and Solaris devices will be removed in a future release. If you are currently using RAS to scan endpoints running these operating systems, you should move to client-based assessments.

- Review Reference: Remote authenticated scanning security best practices on page 341 before configuring this feature.
- Remote authenticated scanning requires specific versions of other Tanium solutions. For more information, see Tanium solutions for remote authenticated scanning on page 28.
- Tanium Client operating system support for executing remote authenticated scans is the same as Tanium Client support (see Tanium Client Management User Guide: Client version and host system requirements) with the following exceptions.
    - See CPU and memory requirements for satellites running remote authenticated scans on page 30.
    - Running remote authenticated scans from AIX or Solaris satellites is not supported at this time.
    - Using a zone server as a satellite is not supported at this time.
- Comply provides standards for scanning unmanaged endpoints using a remote authenticated scan. See Unmanaged Endpoints on page 34 for support information.
- See Host and network security requirements on page 36 for remote authenticated scanning port requirements.
- The following RBAC role is required: Comply RAS Assessment Creator. For more information, see User role requirements on page 41.
- Create satellites in Tanium Direct Connect. For more information, see Tanium Direct Connect User Guide: Managing satellites.
- Plan your targeting. When you configure remote authenticated scans, you can manually

©2026 Tanium Inc. All Rights Reserved

enter IP addresses (ranges, CIDR, etc.) to be scanned by the selected satellite or you can choose to scan endpoints found by Tanium Discover (Discovered Endpoints). If you are targeting Discovered Endpoints, you must run satellite scans in Tanium Discover before you configure the assessment. For more information, see Tanium Discover User Guide: Running satellite scans.

More information about targeting:

- Targeting IP addresses: When using IP address targeting (the default), the addresses you enter do not have to be on the same subnet as the satellite to be scanned. They only have to be reachable by the satellite.
- Targeting Discovered Endpoints: When targeting Discovered Endpoints, if an endpoint does not match Tanium Discover's **Promote Unmanaged Interface** label, that endpoint is not promoted to Tanium Data Service (TDS). If an endpoint is not promoted to TDS, it cannot be scanned by Comply. Therefore you must promote interfaces to TDS in Tanium Discover. For more information, see Tanium Discover User Guide: Managing interfaces. Note that because Tanium Discover cannot get the MAC address from endpoints that are not in the same subnet as the satellite, only endpoints in the same subnet as the satellite will be scanned.
- WinRM 2.0 or higher must be installed on targeted Windows operating systems.
- Remote authenticated scans are supported on Arm-based Windows 11 clients. Scans run using an emulated x64 JVM.
- For ESXi endpoints, when you configure the assessment, you target the IP address of VMware vCenter managing the ESXi hosts. You cannot connect directly to an ESXi host. After the scan completes, Endpoint Statistics displays the ESXi endpoints. Comply does not know about those ESXi endpoints until the scan is run.

  Note: If you try to target ESXi endpoints directly, you may see results, but those results should not be considered reliable.

  Note: Because ESXi endpoints are not targeted directly, their status will not change or get updated in the UI until the scan is complete and all results are received.

©2026 Tanium Inc. All Rights Reserved

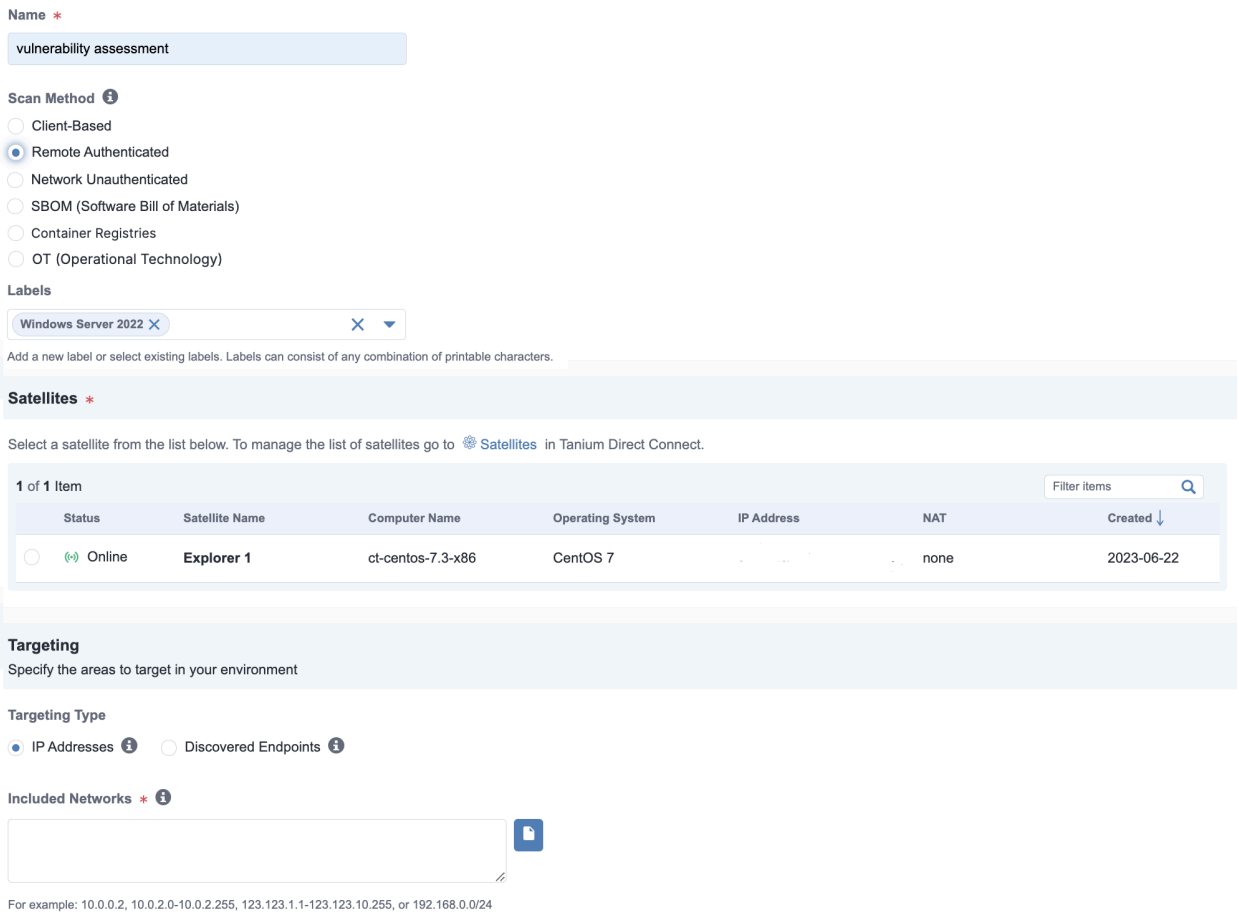
> **Note:** Endpoint Statistics will include the VMWare vCenter in the number of scanned endpoints, but the vCenter endpoint is not scanned. Joval does not support scanning a vCenter instance (VCSA) at this time.

- Configure credentials in Tanium Comply. For more information, see Configure credentials for remote authenticated scans on page 63.
    - Do not target the same unmanaged assets with multiple remote authenticated scan assessments.
    - Target a maximum of 256 unmanaged assets per remote authenticated scan assessment or the equivalent of a /24 network.

To configure a remote authenticated scan assessment, do the following:

1. From the Main menu, go to **Modules** > **Comply > Assessments**.
2. Click **Create Assessment** > **Vulnerability**.
3. On the **Create Vulnerability Assessment** page, in the **Summary** section, enter a **Name** for the assessment. You can also provide **Labels**.
4. Select a **Scan Method**:

©2026 Tanium Inc. All Rights Reserved



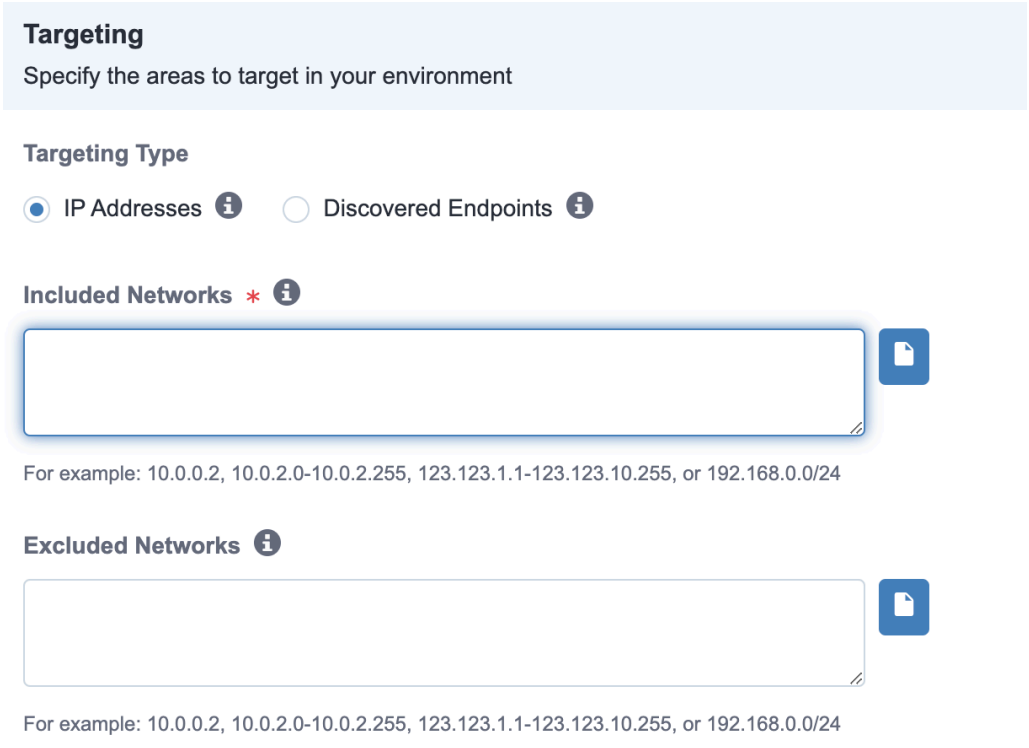
- **Client-Based**: Client-based scanning uses Tanium Clients installed on endpoints. This is the recommended method of scanning.
- **Remote Authenticated**: Remote authenticated scanning uses Tanium Clients as satellites to scan endpoints that do not have the Tanium Client installed. This scan type is useful for obtaining information from endpoints that do not support having the Tanium Client installed. Note that remote authenticated scanning only supports using the Tanium Scan Engine. (The following instructions are for this scan method.)
- **Network unauthenticated**: Find vulnerabilities on unmanaged endpoints in your environment using Tanium Clients as satellites to scan endpoints that do not have the Tanium Client installed and cannot be authenticated to. You can also do distributed scans using the Discover module. For more information, see Configure a network unauthenticated scan assessment on page 165.

5. In the **Satellite** section, select a satellite to perform the scan.
6. In the **Targeting** section, select a **Targeting Type**.

©2026 Tanium Inc. All Rights Reserved

Important: If you use IP addresses (the default), the addresses you enter do not have to be on the same subnet as the satellite to be scanned. If you use discovered endpoints, because Tanium Discover cannot get the MAC address from endpoints that are not in the same subnet as the satellite, only endpoints in the same subnet as the satellite will be scanned.

- **IP Addresses**:
    - In the **Included Networks** field, enter a comma separated list of IP addresses, IP address ranges, or CIDR addresses. You can also click the **Copy** button to upload a text file containing IP addresses, IP ranges, or CIDRs separated either by commas or carriage returns.
    - In the **Excluded Networks** field, enter IP addresses, IP address ranges, or CIDR addresses to be excluded from the scan. You can enter them manually or upload a file of addresses.



Note: Be sure to enter IP addresses that the selected satellite can reach.

©2026 Tanium Inc. All Rights Reserved

> **Note:** 256 is the maximum number of addresses that can be included in a scan. When you click the Create button, a calculation takes place to determine the number of included addresses less the number of excluded addresses to determine the final amount.

- **Discovered Endpoints**: Click the **+ROW** or **+Grouping** button to view the **Select Attribute** field. Select from the following Attribute combinations to filter the list of discovered endpoints:

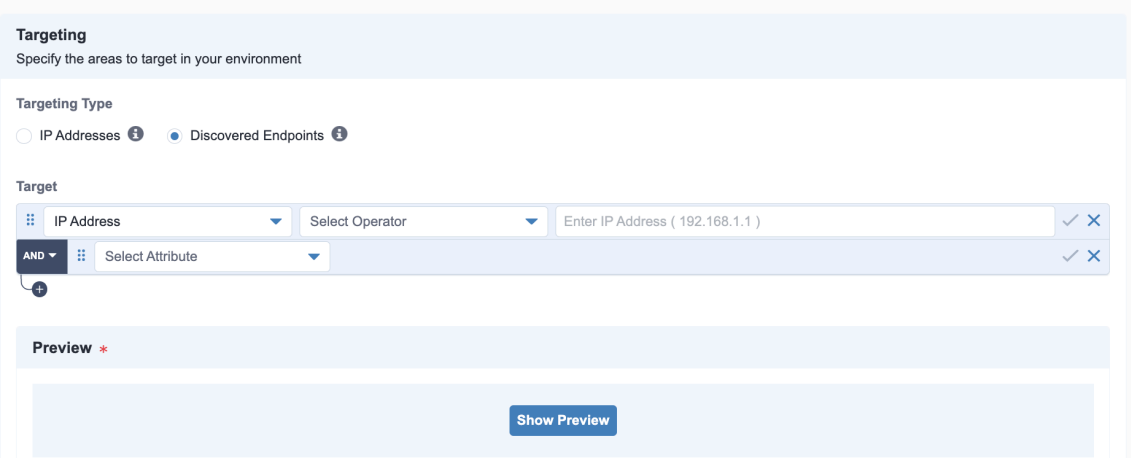
Discovered endpoints attributes

Attribute	Available Operators	Value
IP Address	is equal to, is not equal to, contains, does not contain	Enter a single IP address or multiple addresses, each separated by a comma. For example, 192.168.1.1, 192.168.1.3
Discover Labels	include one of, include all of	Select one or more labels configured in Tanium Discover. For more information, see Tanium Discover User Guide: Labels .
IP Range	equals	Enter an IP address range. For example, 192.168.1.1 - 192.168.1.150
CIDR	equals	Enter an IP address range in CIDR format. For example, 192.168.1.0/24
OS Platform	contains, does not contain	Enter text for targeting a specific OS.

> **Tip:** To select multiple items in the **Value** field, click within the field after adding an item, and you can select additional items.

Use the **And**/**Or** buttons to build upon or narrow your selection. Use the **Row** button to add a new target to the group. Use the **Grouping** button to build another And/Or combination for targeting. Click the check mark to save each selection.

©2026 Tanium Inc. All Rights Reserved



In the **Preview** section for Discovered Endpoints, click the **Show Preview** button to view the list of unmanaged endpoints you selected for targeting. You can use the information in the preview grid to expand or narrow your targeting. For example, you can target a satellite initially and then add an IP range to further filter your targets based on what you observed in the preview.

7. Select the **Credential List** for this assessment. You can only use one list per assessment. In order for satellites to perform secure scans of non-Tanium endpoints, the login credentials for those endpoints are required. For more information, see Configure credentials lists for remote-authenticated scans on page 63.

   CAUTION: Make sure the credential list you select matches the targeting in the assessment. If too many incorrect credentials are attempted and fail, this could trigger security alerts and cause account lockouts.

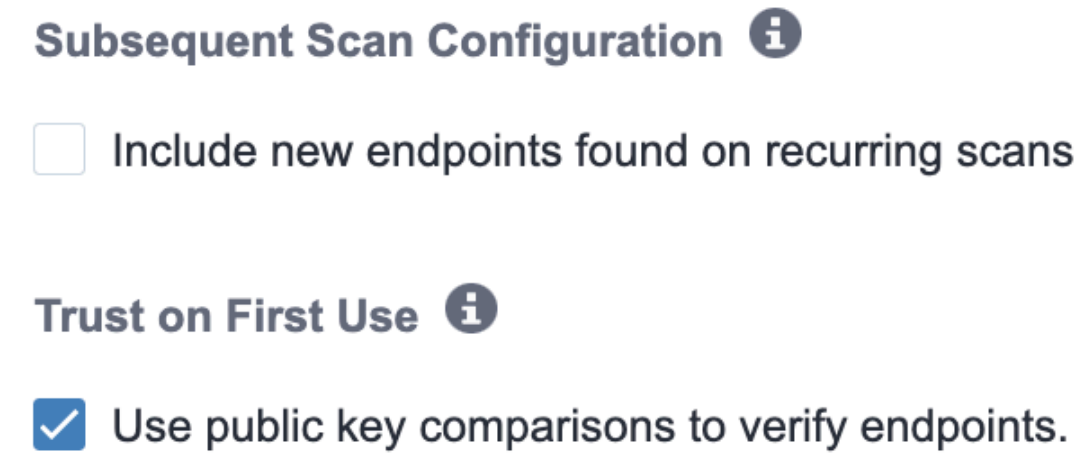
8. Optionally but not recommended, in the **Subsequent Scan Configuration** section, enable the **Include new endpoints found on recurring scans** checkbox. By default, if scans are recurring, Comply only scans endpoints that were reachable during the initial scan. If new endpoints come online, they are not scanned unless you change the assessment's targeting or select this checkbox.

   CAUTION: If you enable the **Include new endpoints found on recurring scans** checkbox and your network is compromised at any point after the initial scan, a honeypot could be installed in your environment that matches the scan configuration requirements. If that occurs, an unmanaged endpoint could capture the credentials being passed to it and use them with malicious intent.

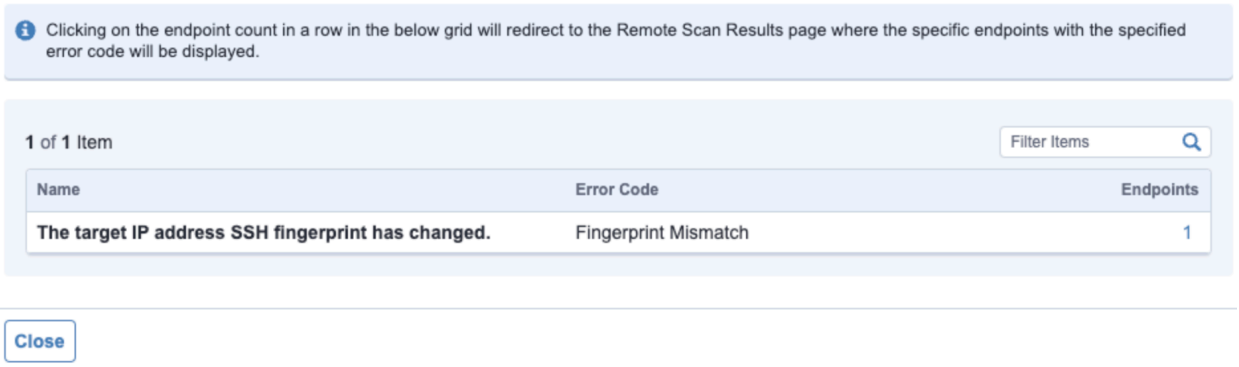
9. Enabled by default and recommended when you use SSH key and SSH password credentials, use **Trust on First Use** for fingerprint comparison.

©2026 Tanium Inc. All Rights Reserved

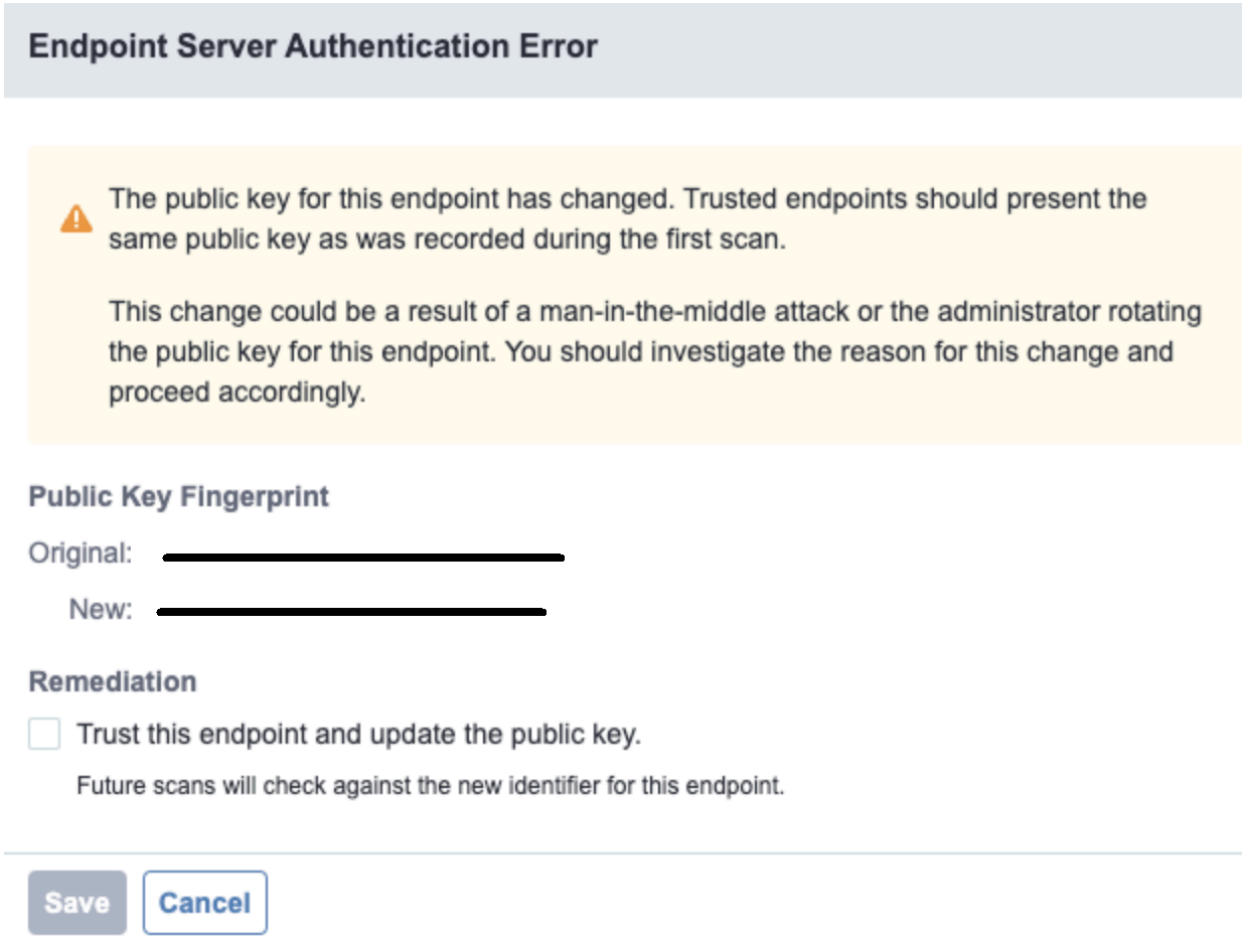
With this feature enabled, Comply will collect the SSH fingerprint the first time an endpoint connects. For every future connection, Comply will check to make sure the endpoint presents the same SSH fingerprint. If it does not, Comply will log a **Fingerprint Mismatch Error**. An endpoint that fails the fingerprint check will not be logged into or scanned.



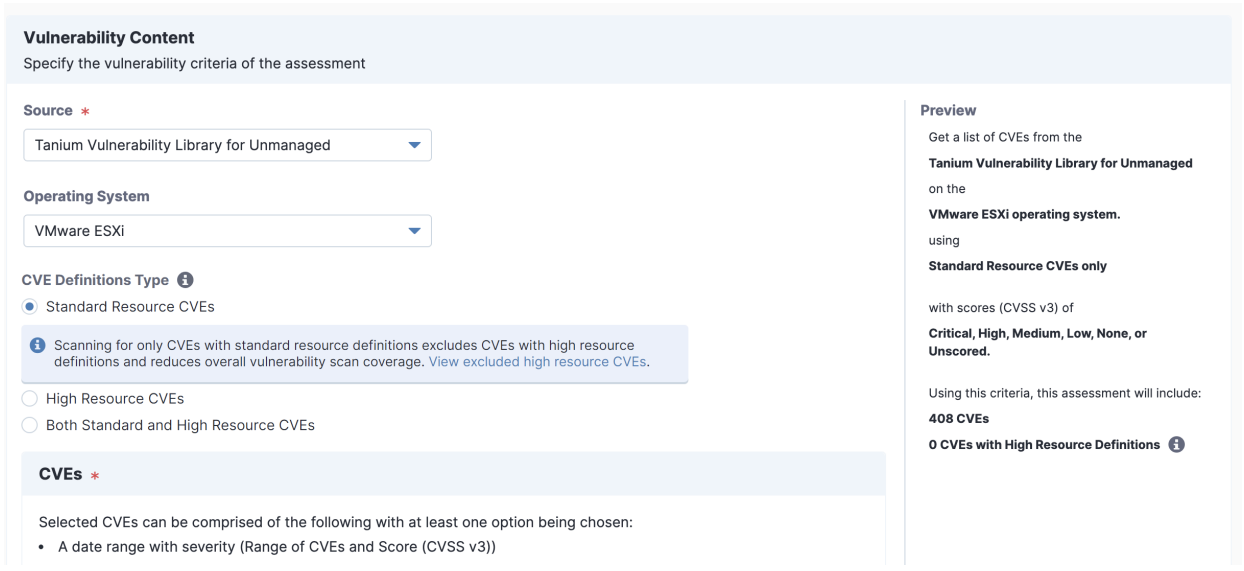
If you receive a fingerprint mismatch error, you can click on the assessment error message and then click through to the endpoint to accept the new key to resolve the error.



©2026 Tanium Inc. All Rights Reserved



10. Select the **Source** from the list in the **Vulnerability Content** section.



11. Select an **Operating System**.

12. Choose a **CVE Definitions Type**. Options are as follows:
    - **Standard Resource CVEs** – Select this option to include only standard resource CVEs

©2026 Tanium Inc. All Rights Reserved

in the assessment. This would exclude from scans CVEs that use OVAL definitions known to impact endpoint performance and reduce overall vulnerability scan coverage. Click **View excluded high resource CVEs** in the informational notice to go to the **CVE List** page where you can filter to view high resource CVEs.

- **High Resource CVEs** – Select this option to include only CVEs that use OVAL definitions known to impact endpoint performance. Scanning for these CVEs can result in higher levels of resource consumption, which may have a negative impact on the endpoint. In most cases, you would select this option for an assessment to run on a controlled schedule based on endpoint resource availability. Click **View high resource CVEs** in the informational notice to go to the **CVE List** page where you can filter to view high resource CVEs.

- **Both Standard and High Resource CVEs** - Select this option to scan for all CVE definition types regardless of resource consumption. Click **View high resource CVEs** in the informational notice to go to the **CVE List** page where you can filter to view high resource CVEs.

> **Note:** Custom sources are also evaluated for resource impacting CVE definitions type settings.

> **Important:** The definitions type selection takes precedence over other CVE filtering settings you configure. For example, if you select to use only Standard Resource CVE definition types, but the Range of CVEs you enter includes High Resource CVEs, those High Resource CVEs are not included in the assessment. Similarly, if you select to use only Standard Resource CVE definitions types and enter a High Resource CVE in the List of Individual CVEs to Include field, that High Resource CVE is not included in the assessment. Check the **Preview** window to see what CVEs are included in the assessment.

> **Note:** When CVE definitions type selections are available for assessments (after an upgrade), a notification appears in the Tanium Console. Click the **Set CVE Definition Type** button to change the definition type for multiple assessments at once. For more information, see Update CVE definitions type (One-time bulk action) on page 191.

©2026 Tanium Inc. All Rights Reserved

> **Tip:** When you select a CVE definitions type, it is the OVAL definition that is excluded or included in the assessment, and that OVAL definition may not directly map to a CVE due to its applicability to the targeted platform. Therefore, if you select to use only standard resource CVEs, a specific CVE may be excluded as high resource for a Windows assessment, but that same CVE may not be excluded for a Linux assessment. This is because OVAL definitions apply for both platform and CVE. As a result, you might notice inconsistencies in CVE count previews during the creation or editing of assessments, or reviewing high resource CVEs without platform context.

13. Specify the **Range of CVEs**. The **Preview** section on the right will show the number of **CVEs** and **Definitions** that will be included in the assessment.

    > **Note:**
    > You can specify `now` in the **Range of CVEs** field as the end of a range. For example, entering `2016-now` will run the assessment against all Common Vulnerabilities and Exposures (CVEs) from 2016 to the current date. By using this format, you can easily define a range that always is current.
    >
    > As a best practice, scan more frequently for recently released high and critical vulnerabilities (for example, 2019-now high and critical on a weekly basis), and conduct scans against all vulnerabilities less frequently (for example, monthly or quarterly).

14. Check the scores you want to see in **CVSS Score**.

15. List specific CVEs in the **List of Individual CVEs** field.

    > **Note:** If you specify a **List of Individual CVEs**, and there is no **CVE Definitions Type** setting that takes precedence, they will be included in the assessment regardless of the values specified for **Range of CVEs** or **CVSS Score**. To search by year and score, you must provide values for both fields for the search to be valid. If you specify **Range of CVEs**, you must select at least one score in **CVSS Score**. If you select a score in **CVSS Score**, you must specify **Range of CVEs**. If you list specific CVEs, you can choose to leave the **Range of CVEs** field blank and select no **CVSS Score**.

16. Optionally, enter a comma separated list of CVEs to include.

17. Optionally, enter a comma separated list of CVEs to exclude.

©2026 Tanium Inc. All Rights Reserved

18. Optionally, select the checkbox to **Only include CVEs with CISA KEV**.

19. Specify the **Batch Size**.

> **Note:** **Batch Size** defines the number of checks that will run at a time. To run a manageable number of checks on your endpoints, the default value for this field is 500 for CIS-CAT and SCC, and the default is 2000 for Legacy Tanium Scan Engine. This setting does not typically need to be adjusted from the default value. However, in some cases, increasing the batch size can speed up scans and may avert scan timeouts. This increase may also require increasing the endpoint maximum heap size to avoid out-of-memory errors.

20. Select **Start on** and **End on** and complete the date and time values to limit the assessment to run only during a specific time period.
    The date and time displayed by default is the local browser time.

21. Select the **Distribute Over** option and enter values to run the assessment over minutes, hours, or days. For more information, see Tanium Core Platform User Guide: Deploying actions.

22. Select **Interval**, **Using assessment age**, or **Never** for the **Repeat** field.
    - If you choose **Interval**, the **Reissue every** field displays, and you can specify how often the assessment is run.
    - If you choose **Using assessment age**, then the **Run when results are older than** field displays, and you can specify how old you want the results to be before the assessment is run. If a targeted endpoint comes online that has never run the assessment, the assessment will be run as soon as the next age-check occurs. The age of results is checked every hour.

      > **Best Practice:** Use the **Using assessment age** option and set it to `7 days`.

    - Under **Scan Timeout**, you can change the default of 6 hours to allow for scans that may take more time. The minimum you can set the timeout value to is 30 minutes and the maximum is 7 days. It is recommended that you do not change this default without a specific reason.

©2026 Tanium Inc. All Rights Reserved

> **Note:** This setting applies to the legacy Tanium Scan Engine, CIS-CAT, and SCC only. Tanium Scan Engine 7.0 uses a timeout managed by Tanium and is not affected by this setting.

23. Click **Create & Deploy** and enter your credentials. Results will display on the **Findings** page.

Remote authenticated scan workflow

Learn how remote authenticated scans obtain targets and credentials, handle IP inclusion criteria, and manage newly discovered endpoints in reoccurring assessments.

When a remote authenticated scan begins, it asks the Comply service for its targets and credentials. The service uses the scan's criteria for IP inclusion to query for currently reachable targets for that satellite and sends that list to the client to execute the scan. Scheduled periodic RAS scans do not automatically include new targets as they are identified by the associated Tanium Discover scan. Reoccurring assessments will only include the unmanaged assets that were reachable at the time of the initial scan, unless you select the **Include newly discovered endpoints on reoccurring scans** checkbox, which is not recommended.

Create a vulnerability assessment from the Standards page

Create a vulnerability assessment from the Standards page for a selected vulnerability standard.

About this task

From the Main menu, go to **Modules** > **Comply >Standards.** Select the **Vulnerability** tab, and click **Create Vulnerability Assessment** (plus sign) next to the vulnerability standard for which you want to create an assessment.

Configure a network unauthenticated scan assessment

Configure a network unauthenticated scan assessment to remotely identify vulnerabilities on target systems without requiring user credentials.

About this task

You can find vulnerabilities on managed and unmanaged endpoints in your environment by creating a network unauthenticated vulnerability assessment. Unlike remote authenticated scanning, which requires credentials for all endpoints, network unauthenticated scanning allows you to use satellite

©2026 Tanium Inc. All Rights Reserved

targeting to scan unmanaged devices without having to authenticate to them. You can also configure distributed targeting in Comply using the Discover module.

Before you begin

Review prerequisites and configuration options before you create a network unauthenticated vulnerability assessment, including required Discover module versions, targeting methods, port specifications, and scan frequency.

- If you are using satellite targeting, you must have the Discover module installed. You must create satellites in Tanium Direct Connect. For more information, see Tanium Direct Connect User Guide: Managing satellites. You must also have the following privileges: **Discover Profile Read** to view a network unauthenticated vulnerability assessment and **Discover Profile Write**.

- If you're using distributed targeting, you must have the Discover module installed and configured. You must also have the following privileges: **Discover Profile Read** to view a network unauthenticated vulnerability assessment and **Discover Profile Write**. There is background information and detailed instructions for this section in the Tanium Discover User Guide.

    - You must use Discover 4.0 or later.

    - Network unauthenticated scans are currently not supported on Windows 11 ARM clients.

To configure a network unauthenticated scan assessment, do the following:

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

2. Click the **Create Assessment** button and select **Vulnerability**.

3. In the **Summary** section, enter a **Name** for the assessment.

4. Select a **Scan Method**:

    - For this assessment type, select **Network Unauthenticated**.

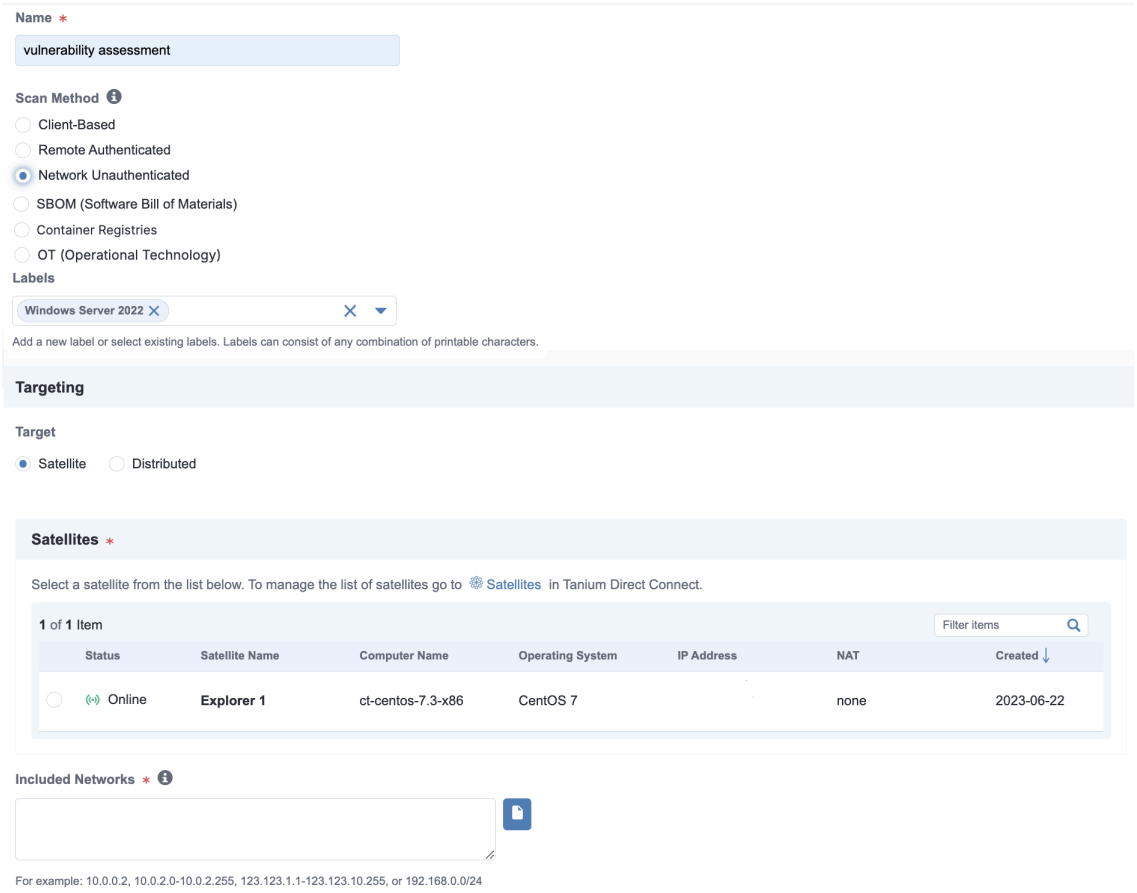
      With this scan type, you can do a distributed scan or you can use satellite targeting to scan unmanaged devices without having to authenticate to them.

©2026 Tanium Inc. All Rights Reserved

5. You can provide **Labels** to further identify the assessment.

6. In the **Targeting** section, select a **Targeting Type**.

    - **Satellite** - With a satellite scan, you manually enter IP addresses (ranges, CIDR, etc.) to be scanned by the selected satellite. The addresses you enter do not have to be on the same subnet as the satellite. They only have to be reachable by the satellite. The Discover module is required in satellite targeting for creating the "unmanaged_network_scan" namespace in TDS that results are uploaded to. You can view these results using remote reports. For more information, see Create a network unauthenticated report on page 170.



        - In the **Included Networks** field, enter a comma separated list of IP addresses, IP address ranges, or CIDR addresses. You can also click the Copy button to upload a text file containing IP addresses, IP ranges, or CIDRs separated either by commas or carriage returns.

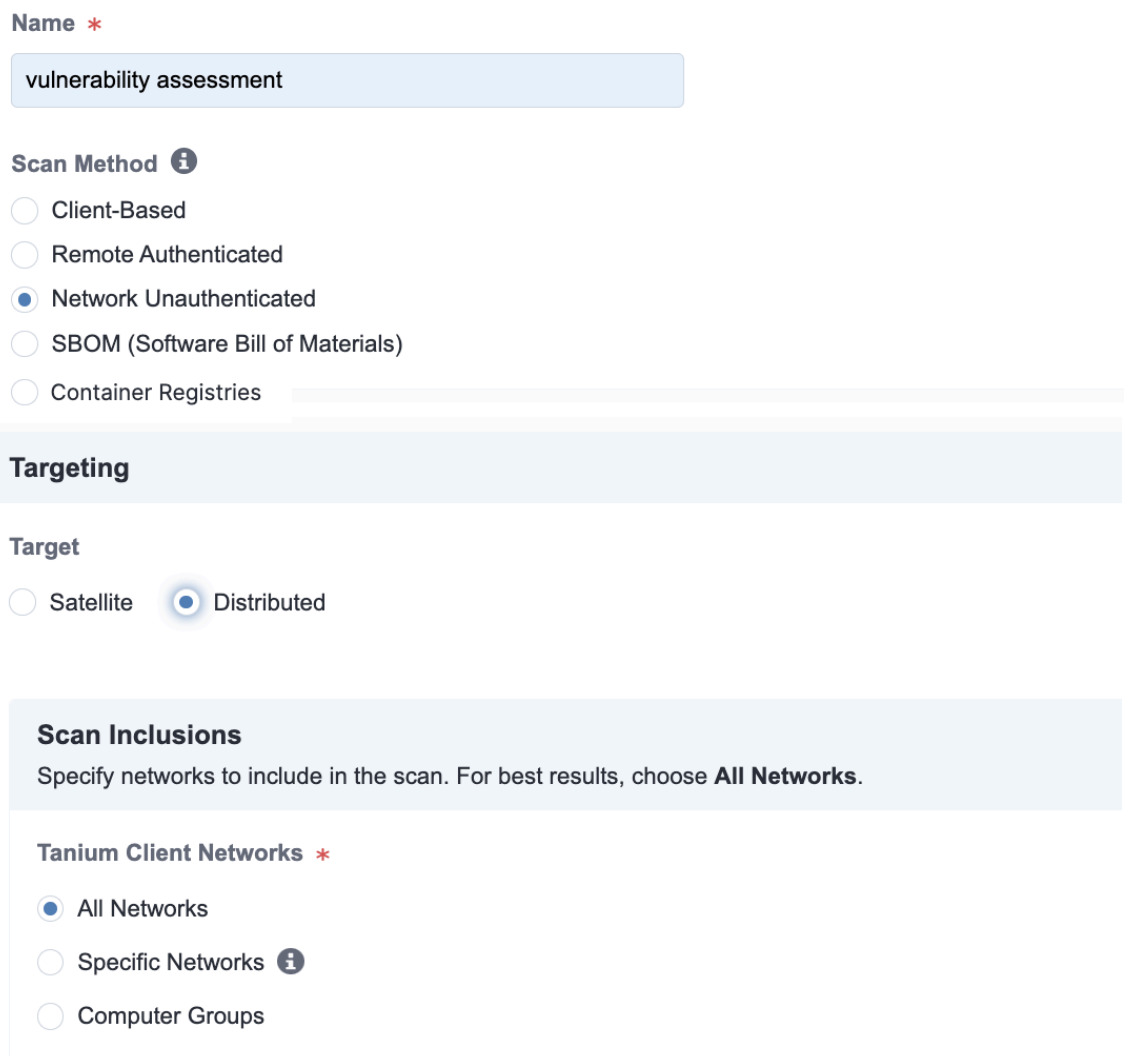
        - In the **Excluded Networks** field, enter IP addresses, IP address ranges, or

©2026 Tanium Inc. All Rights Reserved

CIDR addresses to be excluded from the scan. You can enter them manually or upload a file of addresses.

> **Note:** 4,096 is the maximum number of addresses, or a /20, that can be included in a scan. When you click the **Create** button, a calculation takes place to determine the number of included addresses less the number of excluded addresses to determine the final amount.

- **Distributed** - Scan endpoints in the same subnets as existing Tanium Clients. This uses the Discover module to run Nmap scans. Results from distributed scans are not viewable in Comply Findings. You can view these results using remote reports. For more information, see Create a network unauthenticated report on page 170.



©2026 Tanium Inc. All Rights Reserved

- Under **Scan Inclusions**, specify Tanium Client networks to scan as part of this assessment.
    - **All Networks**: It is recommended you include all networks in the scan.
    - **Specific Networks**: Enter the IP addresses for specific networks to include in the scan. Tanium clients within those networks will perform the scan.
    - **Computer groups**: Select specific computer groups to include in the scan.

      These are the computers from which the results will be pulled.
- Under **Scan Exclusions**, specify networks to exclude from the assessment. You can select multiple options.
    - **Isolated Subnets/Systems**: Select this checkbox to prevent devices that have no peers from performing scans.
    - **Specific Networks**: Enter IP addresses to be excluded from scans. These can be single addresses, address ranges, or comma-separated CIDRs.
    - **VPN Networks**: Enter VPN networks to be excluded from scans. This prevents computers that are not on the network from being scanned. These can be single addresses, address ranges, or comma-separated CIDRs.
    - **Zone Servers**: Enter zone servers to be excluded from scans. This prevents computers that are not on the network from being scanned by using IP addresses or host names of DMZ facing servers. These can be IP addresses or host names separated by commas.

7. In the **Port Specification** section, select one of the following:

©2026 Tanium Inc. All Rights Reserved

- **Note:** By default, the Network Mapper utility (Nmap) scans the top 1000 most commonly used TCP ports. If needed, you can customize the ports that are scanned during the discovery process and the source ports from which clients run scans.

  - **Target Ports**: Specify the TCP ports that you want to scan: **Top 1000 Ports**, **Top 1000 Ports plus specified ports**, or **Only Specified Ports**.
  - **Excluded Ports**: Specify a list of TCP ports to exclude from the ports scanned. These ports are excluded from all types of scans.
  - **Source Port**: Specify a source port from which Nmap on clients attempts to run scans.

8. In the **Scan Frequency** section, specify how often you want the scan to run.
9. Click **Create** or **Create & Deploy** and enter your credentials.

View findings

View findings from satellite and distributed scans by creating reports, exporting results with Tanium Connect, or using the Comply NMAP Scan results sensor.

About this task

To view findings for satellite and distributed scans:

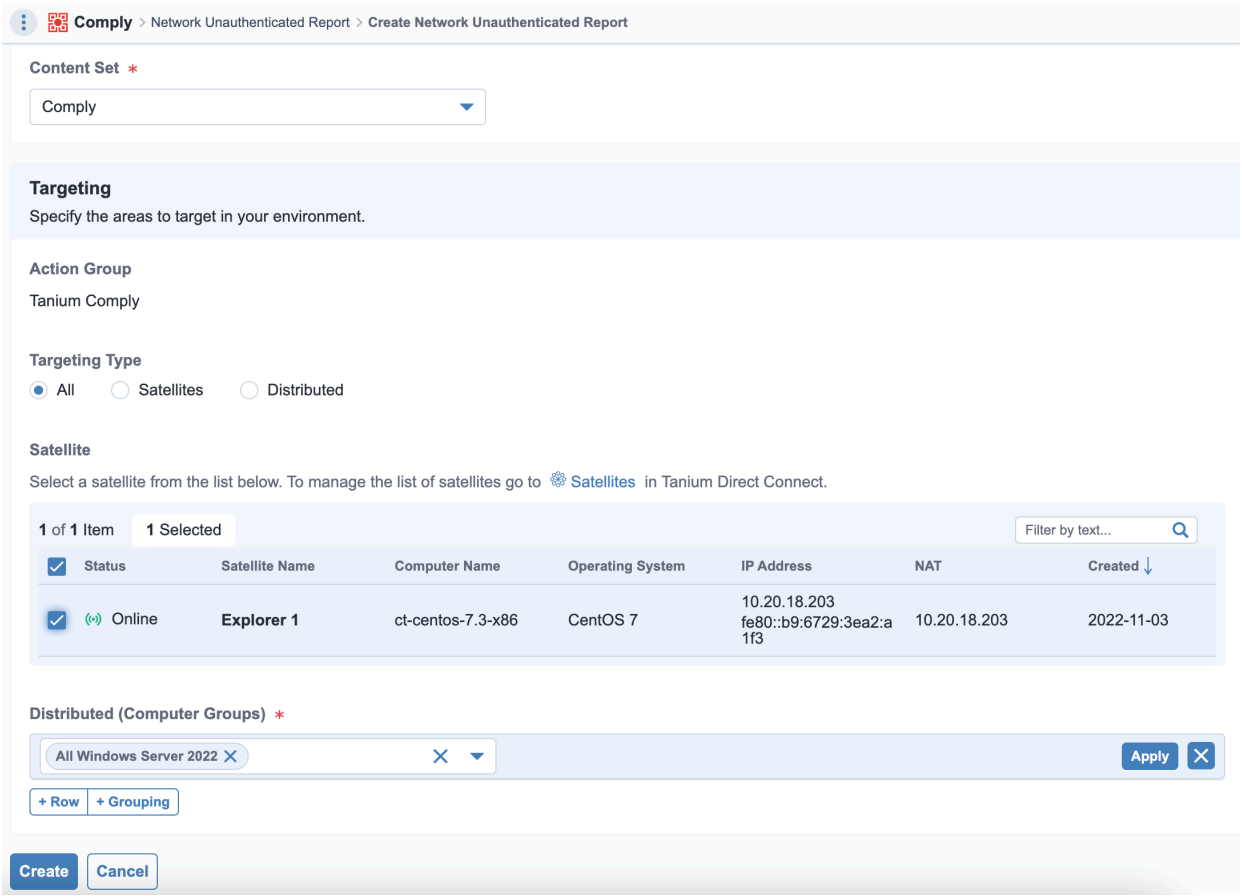
- Create a report. For more information, see Create a network unauthenticated report on page 170.
- Export the results using Tanium Connect. For more information, see Exporting vulnerability assessments on page 263.
- Use the Comply NMAP Scan results sensor ("Get Comply - NMap Scan Results from all machines").

Create a network unauthenticated report

Create a network unauthenticated report that defines the report name and content set, configures targeting options, and generates findings from network unauthenticated scans.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Comply > Reports**.
2. Select the **Network Unauthenticated** tab.
3. Click the **Create Report** button and select **Network Unauthenticated**.



4. Enter a **Name**.
5. Select a **Content Set**. For more information, see Tanium Core Platform User Guide: Managing RBAC.
6. Under **Targeting**, select a **Targeting Type**:

> **Note:** The Tanium Comply action group is created automatically by Comply and will be automatically populated in the Action Group field. All saved actions created by Comply will be created under this action group.

- **All** - The report will include findings from all network unauthenticated scan target types. Select a satellite and one or more computer groups to configure the report.
- **Satellite** - The report will include findings from network unauthenticated scans with satellite targeting.

©2026 Tanium Inc. All Rights Reserved

- Select a **Satellite** for the report.

- **Distributed** - The report will include findings from network unauthenticated scans with distributed targeting.

  - Select **Computer Groups**. Select a group from the list. Add additional groups from the same list using the **And**/**Or** buttons to build upon or narrow your selection. Click the check mark to save each selection.

7. Click **Create**.

Create an SBOM scan assessment

Use SBOM scanning to continuously identify vulnerabilities on endpoints based on Tanium Client Index Extension data mapped to CVEs.

About this task

SBOM scanning is useful for determining vulnerabilities on endpoints based on the results of a Software Bill of Materials assessment. An SBOM scan uses data obtained by the Tanium Client Index Extension, which indexes local file systems on Tanium Client endpoints and makes that list available to Software Manager. The results of the SBOM scan analysis are mapped to CVEs on the endpoint.

Unlike other scan types, SBOM scans are continuous, always running in the background. An SBOM scan is considered complete when one loop of the system is finished.

Before you begin

Review SBOM licensing, required extensions, custom settings, and scan behavior before configuring a Comply SBOM vulnerability scan assessment.

- A valid Tanium SBOM license is required.

  Note that when the SBOM license expires, after a 30 day grace period, SBOM assessments and findings are deleted.

- Tanium Client Index Extension is required.

- A Custom Setting with at least one ecosystem selected is required. SBOM scans use custom settings to configure index settings such as ecosystems to be scanned and file/directory

©2026 Tanium Inc. All Rights Reserved

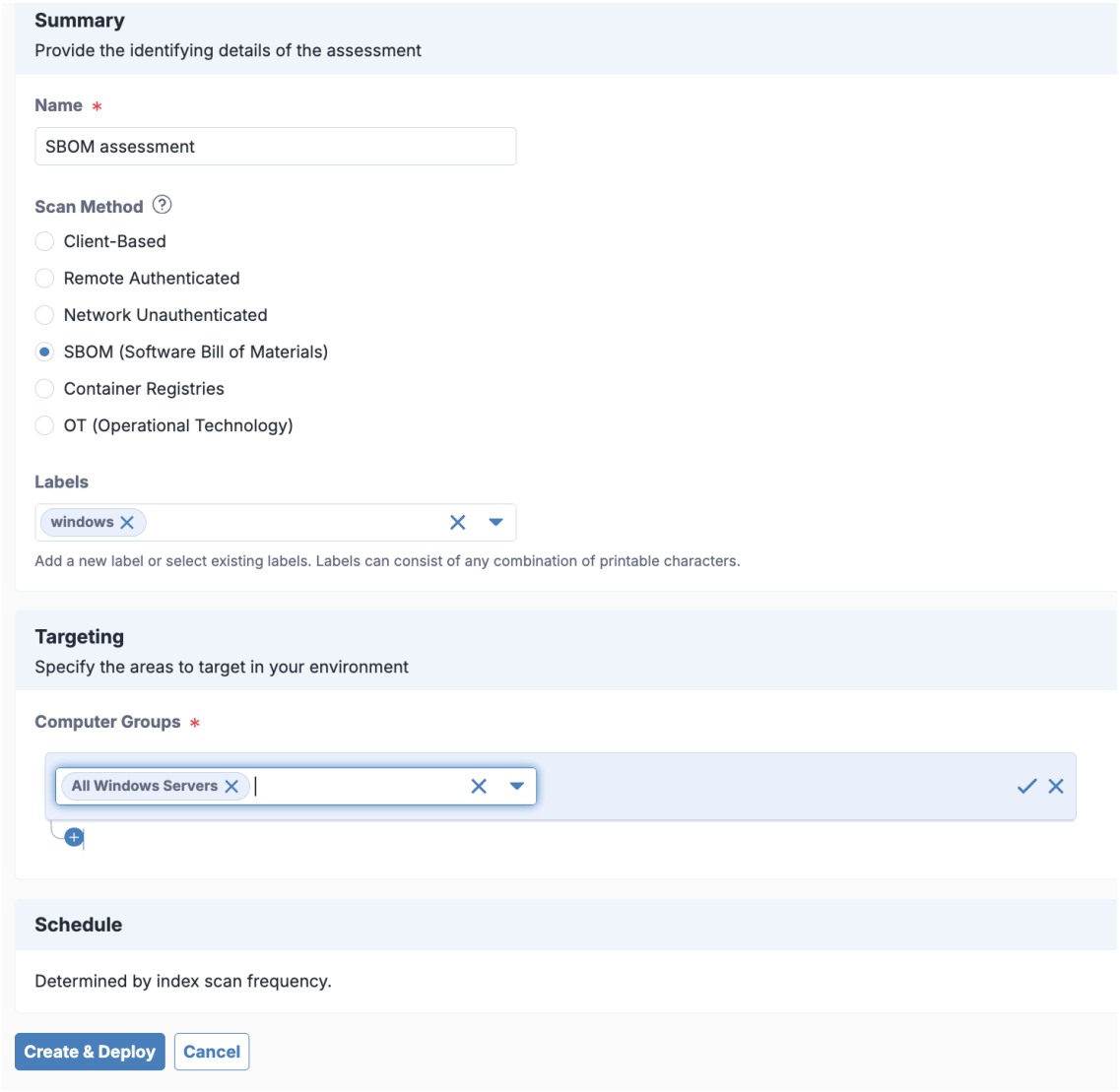
exclusions. You must configure Custom Settings and select at least one ecosystem for an SBOM assessment to begin scanning. From the Main menu, go to **Modules** > **ComplySetup** > **Configuration** and select the **Custom Settings** tab. For more information, see Custom settings on page 103.

- Refer to Comply requirements on page 26.
- You typically only need one Comply SBOM scan assessment for an environment. SBOM scans are continuous scans and use the Tanium Client Index Extension to index file systems.
- If both a client-based OVAL scan and an SBOM scan find a particular CVE, the OVAL finding takes precedence and is reported.
- An SBOM scan does not make an association between a library file and the application it belongs to.
- An SBOM scan does not include a defined set of CVEs to be evaluated. All CVEs are included and the list is updated periodically.

To configure an SBOM scan assessment, do the following:

1. From the Main menu, go to **Modules** > **Comply > Assessments**.
2. Click **Create Assessment** > **Vulnerability**.
3. On the **Create Vulnerability Assessment** page, in the **Summary** section, enter a **Name** for the assessment. You can also provide **Labels**.
4. Select a **Scan Method**:
    - **SBOM (Software Bill of Materials)**: (requires a Tanium SBOM license) An SBOM vulnerability scan has visibility into libraries and all files that are known to Software Manager. The results of an SBOM assessment analysis are mapped to CVEs on the endpoint.

©2026 Tanium Inc. All Rights Reserved



5. In the Targeting section:

    - Select **Computer Groups**. Use the dropdown list to select a group. Add additional groups by using the Add button to build upon or narrow your selection. When finished, click the check mark for each selection.

6. In the **Schedule** section, there are no configuration options. An SBOM scan runs according to the **Index Scan Frequency** set in Custom Settings.

    Note: To stop an SBOM scan, delete the SBOM scan assessment. You can also remove SBOM Custom Settings and the SBOM scan assessment will stop running.

7. Click **Create & Deploy** and enter your credentials. Results will display on the **Findings** page.

©2026 Tanium Inc. All Rights Reserved

Important: A Custom Setting with at least one ecosystem selected is required for the SBOM scan assessment to run.

Note: Because an SBOM scan runs continuously, results should be interpreted a bit differently for Comply - CVE Findings - Last Scan. In this case, the returned time indicates when the scan most recently resumed. Typically, this occurs on a client reset.

Note: You cannot export SBOM assessments using Tanium Connect. Only SBOM findings can be exported using Tanium Connect.

Tip: If you are experiencing false positives or false negatives, refer to SBOM false positives on page 313 in the Troubleshooting chapter.

Configure a container registry scan assessment

Configure Comply to scan container registries through Tanium Cloud Workloads, analyze SBOM results for CVE-mapped vulnerabilities in images, and add those findings to Comply.

About this task

Container registry scanning is useful for determining vulnerabilities in images within the registry based on the results of a Software Bill of Materials assessment. The results of the SBOM scan analysis are mapped to CVEs. If vulnerabilities are found in images, you can then create new images with the CVEs remediated.

To perform vulnerability scans of container registries, Comply works with the Tanium Cloud Workloads service. Container registries, with provider information, are configured in Cloud Workloads. The Cloud Workloads service then scans and inventories the images in the selected container registries. A Comply container registry vulnerability scan retrieves SBOM scan results associated with each image and maps those results to CVEs. That data is then added to Comply Findings.

©2026 Tanium Inc. All Rights Reserved

Important: Container registry scanning detects vulnerabilities in the following languages and libraries: Java, JavaScript, Go, Python, Node.js, PHP, and Ruby. It also detects vulnerabilities in the following package managers: dpkg and rpm, and in the Alpine Linux distribution.

Before you begin

Review licensing, configure Cloud Workloads and satellites, and set up container registries before creating a container registry vulnerability assessment in Comply.

- SBOM: A valid Tanium SBOM license is required.
- Cloud Workloads: Select satellites and configure registries through Cloud Workloads. You must have the Cloud Workloads RBAC Operator role.
- Satellites: Create satellites in Tanium Direct Connect. For more information, see Tanium Direct Connect User Guide: Managing satellites.

  Important: Container registry scanning detects vulnerabilities in the following languages and libraries: Java, JavaScript, Go, Python, Node.js, PHP, and Ruby. It also detects vulnerabilities in the following package managers: dpkg and rpm, and the Alpine Linux distribution.

To add container registries in Cloud Workloads, refer to the **Tanium Cloud Workloads** documentation. See Tanium Cloud Workloads: Requirements for supported container registry providers, and see Tanium Cloud Workloads: Add registries for configuration information.

Note: After container registries are configured in Cloud Workloads, the Cloud Workloads service begins scanning and inventorying images in the container registries.

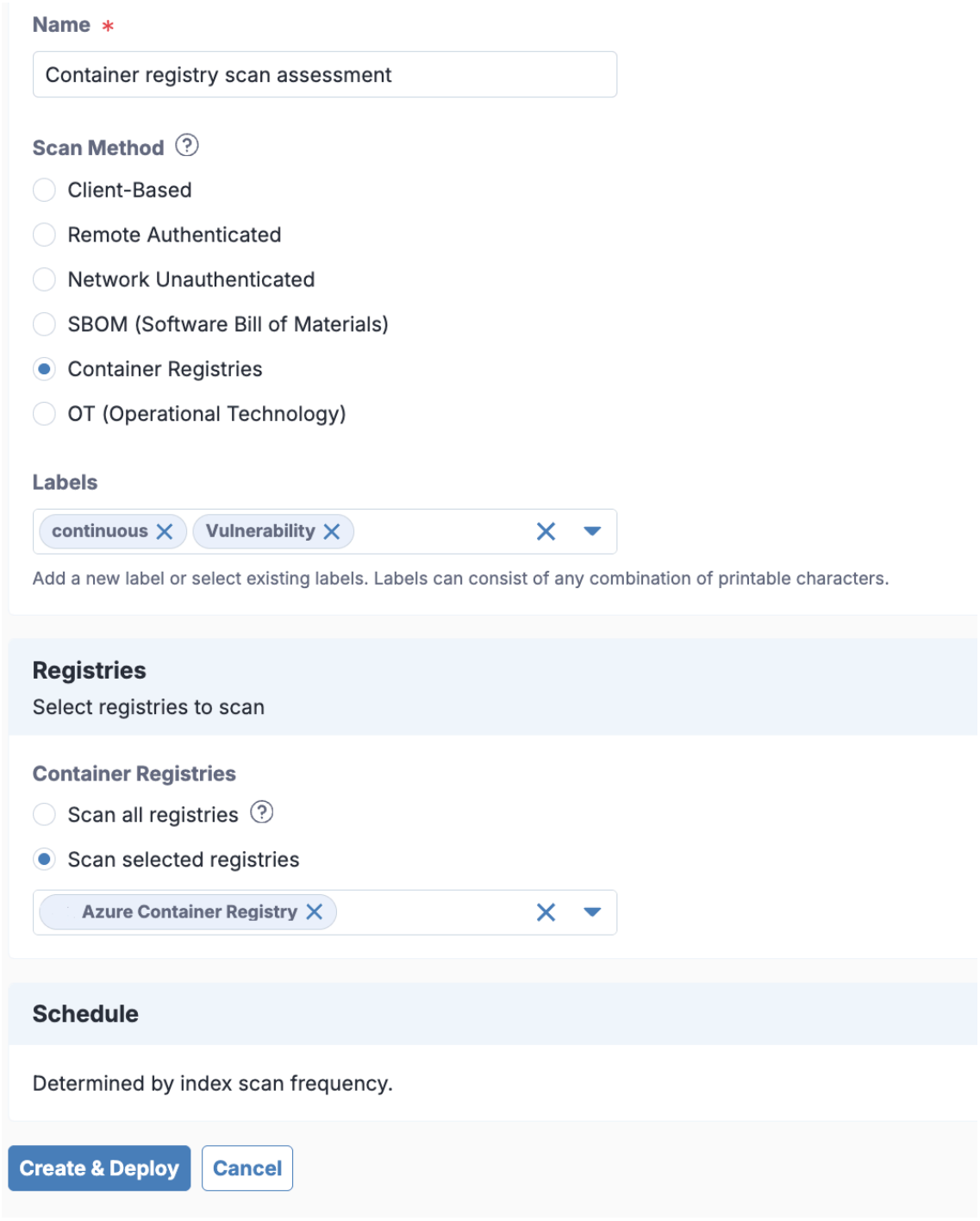
Note: In the list of **Providers** in Cloud Workloads, there is an **Other** option. You can use Other to create an “allow list” for image registries that Tanium may not know about, either because they are not supported or for any other reason. Therefore, **Other** indicates that the base address of an image is not an address of a registry Tanium knows about, but it should not be considered rogue.

To configure a container registry scan assessment in Comply, do the following:

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Comply > Assessments**.
2. Click **Create Assessment** > **Vulnerability**.
3. On the **Create Vulnerability Assessment** page, in the **Summary** section, enter a **Name** for the assessment. You can also provide **Labels**.
4. Select a **Scan Method**:
    - For this assessment type, select **Container Registries**.

©2026 Tanium Inc. All Rights Reserved



5. In the **Registries** section, select one of the following:

    - **Scan all registries**: All current registries configured in Cloud Workloads and any future registries added through Cloud Workloads will be scanned.

    - **Scan selected registries**: Select specific registries configured in Cloud Workloads for scanning, either from the list or from a searchable checkbox items list. In this case, any new registries added through Cloud Workloads will only be scanned by creating

©2026 Tanium Inc. All Rights Reserved

a new container registry scan assessment that includes them.

> **Note:** There may be up to a 30 minute delay between the time a registry is added in Cloud Workloads and it appears in Comply.

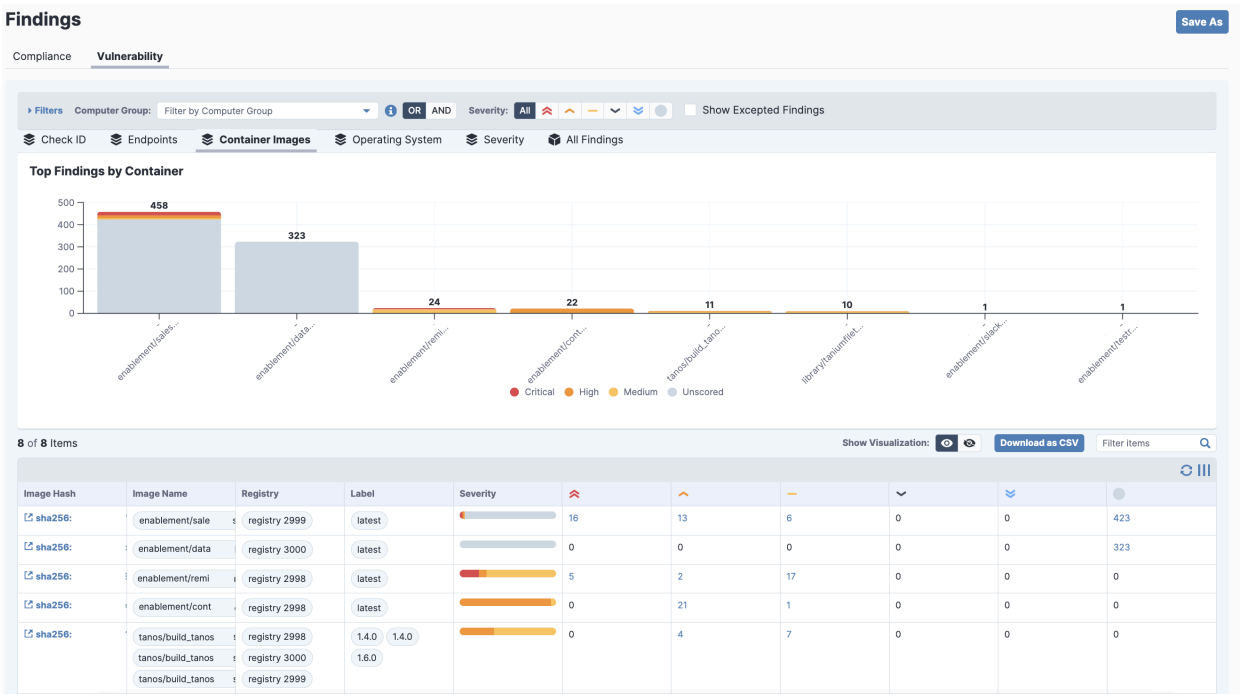
6. In the Schedule section, there are no configuration options. A Container Registry scan runs until the scan is complete.

> **Note:** Comply scans a disk once and does not continually scan a disk that has already been scanned.

7. Click **Create & Deploy** and enter your credentials. Results will display on the **Findings** page, in the **Vulnerability** > **Container Images** tab.

   Findings (Image Hash, Image Name, Registry, and Label) can also be exported using Tanium Connect. For more information, see Exporting findings on page 259.

> **Best Practice:** If a vulnerability is found in an image, a best practice would be to remove the vulnerable image.



> **Note:** Container registry scan findings are only available in Tanium Comply and Tanium Connect.

Configure an operational technology scan assessment

Configure an operational technology scan assessment to use the OT shared service satellite to gather details from OT devices.

About this task

> **Note: OT (Operational Technology)**: (requires a Tanium Endpoint Management for Operational Technology license and a Tanium Exposure Management for Operational Technology license): An Operational Technology scan uses the satellite configured for the Operational Technology shared service to gather details from OT devices.

For more information, see Viewing and filtering findings on page 194.

Before you begin

- Configuring an OT scan assessment requires a valid Tanium Endpoint Management for Operational Technology license and a Tanium Exposure Management for Operational Technology license.
- Configure Tanium Endpoint Management for Operational Technology to ingest OT device data.
- An OT scan assessment can target only certain communication protocols. For more information, see Endpoints.
- An OT scan assessment returns CVEs for both version-agnostic CPEs and firmware-version-specific CPEs. For Detected CPEs, there are two listed for each cell, one with an "o" (operating system) and one with an "h" (hardware).
- You typically need only one Comply OT scan assessment for an environment. The assessment runs on a predefined schedule and targets all devices managed using Tanium Endpoint Management for Operational Technology.

©2026 Tanium Inc. All Rights Reserved

- Air-gapped environments do not support OT scan assessments.

To configure an OT scan assessment in Tanium Comply to identify vulnerabilities on OT devices managed using Tanium Endpoint Management for Operational Technology, complete the following procedure:

1. From the Main menu, go to **Modules** > **Comply** > **Assessments**.
2. Click **Create Assessment** > **Vulnerability**.
3. On the **Create Vulnerability Assessment** page, in the **Summary** section, enter a **Name** for the assessment. You can also provide **Labels**.
4. Select a **Scan Method**:
    - **OT (Operational Technology)**: (requires a Tanium Endpoint Management for Operational Technology license and a Tanium Exposure Management for Operational Technology license) Use an endpoint managed using Tanium Client configured as a satellite to find vulnerabilities on endpoints managed using Tanium Endpoint Management for Operational Technology, based on communication protocol and firmware version.
5. Click **Create & Deploy** and enter your credentials. Results appear on the **Findings** page.

Result



Note: It might take up to 30 minutes for results to appear in the **Findings** page.

Status definitions

View and interpret assessment scan statuses in the **Status** column on the assessment list page.

View the status of a scan in the **Status** column on the assessment list page. Hover over the icon to see one of the following statuses:

In Progress

The assessment is being published.

Loading

No statistics have been received from the Comply service for the assessment.

©2026 Tanium Inc. All Rights Reserved

Pending

At least one endpoint in the assessment has not yet run the scan, but there are no scan errors.

Success

The assessment has at least one successful run with no errors and no scans not run.

Error

The assessment has at least one endpoint that produced an error during the scan.

Warning

Any issue that does not fall into the other status categories.

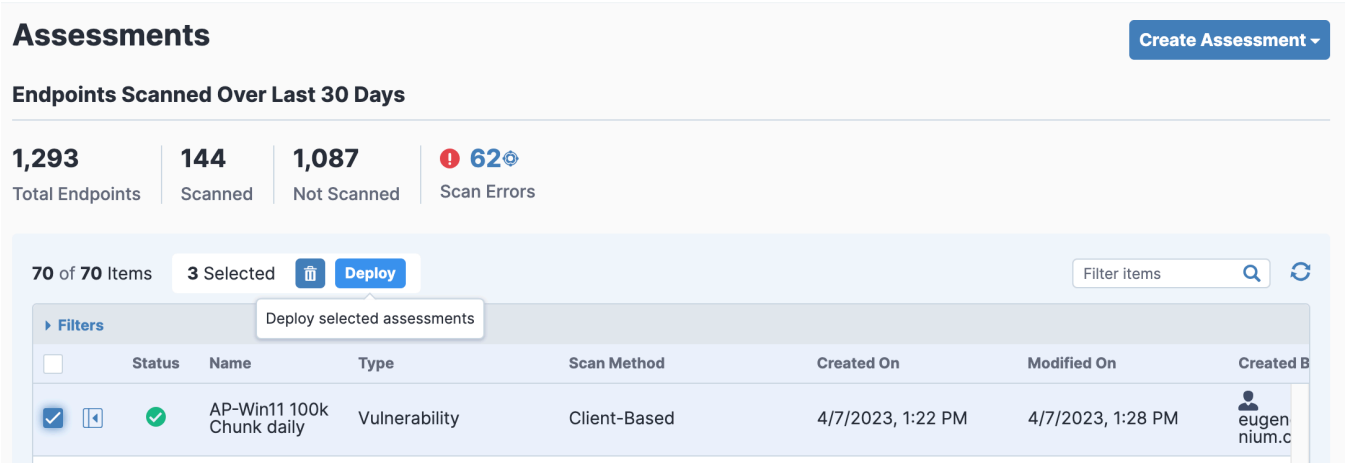
Note: You must reload the page to update the status column.

Run an assessment again

Run an existing assessment again from the **Assessments** page by selecting it and clicking **Deploy**.

About this task

On the **Assessments** page, select an assessment and click **Deploy** to run it again.



©2026 Tanium Inc. All Rights Reserved

Run an on-demand scan

Run an on-demand scan for client-based assessments using existing targeting or additional filters, with optional debug logging for legacy Tanium Scan Engine.

About this task

Note: On-demand scans are only supported for client-based assessments.

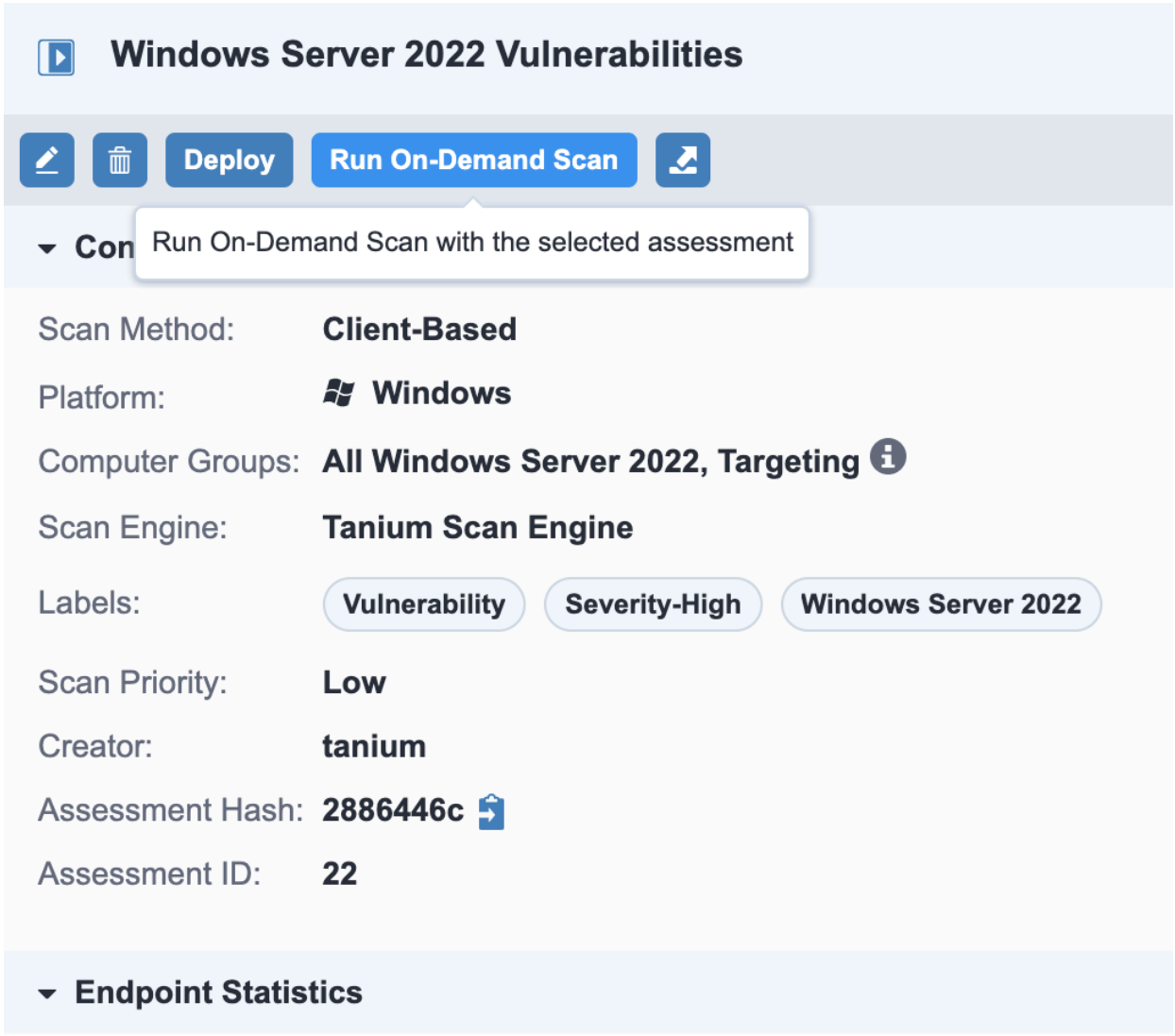
Note: For vulnerability assessments that use Tanium Scan Engine 7.0 or later, a re-index of the endpoint occurs before the on-demand scan begins.

An on-demand scan lets you run an assessment at the push of a button using existing targeting or with additional filters. Optionally, you can run the assessment with or without debug enabled.

To run an on-demand scan:

1. Select the checkbox for an assessment or click the arrow for the Side Panel window to access the **Run on-demand Scan** button.

©2026 Tanium Inc. All Rights Reserved



2. Click the **Run on-demand scan** button and optionally configure the following:
   - Select the **Run with Debug** checkbox - Debug is only available for the legacy Tanium Scan Engine. With debug enabled, scans are run with more detailed logging and additional output that the CX stores is available to view (see Client extensions on page 29). A debug zip as well as an xml file are produced in /opt/Tanium/TaniumClient/extensions/comply/data/results/joval-<assessment ID>

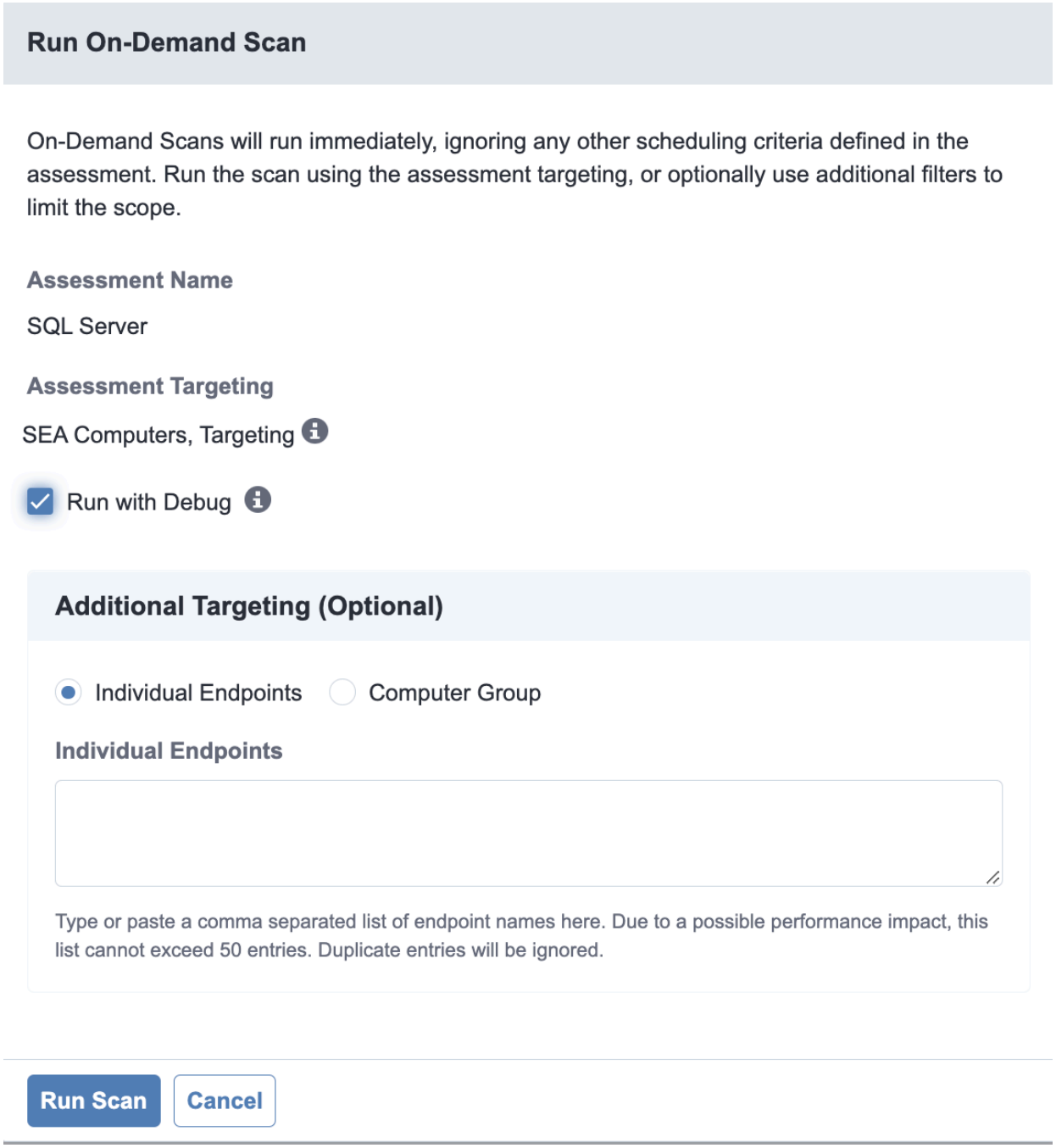
     Note: This file path applies to the Legacy Tanium Scan Engine.

   - Configure additional filtering - Select **Individual Endpoints** and enter those endpoints into the edit field or select **Computer Group** and choose a group to filter by.

©2026 Tanium Inc. All Rights Reserved

> **Important:** If you select **Individual Endpoints** and enter computer names, you must enter the computer name exactly as it is returned by the **Computer Name** sensor.

3. Click the **Run Scan** button.



©2026 Tanium Inc. All Rights Reserved

Export an assessment

Export a single vulnerability assessment report, choose the export format and results to include, and download the completed report.

About this task

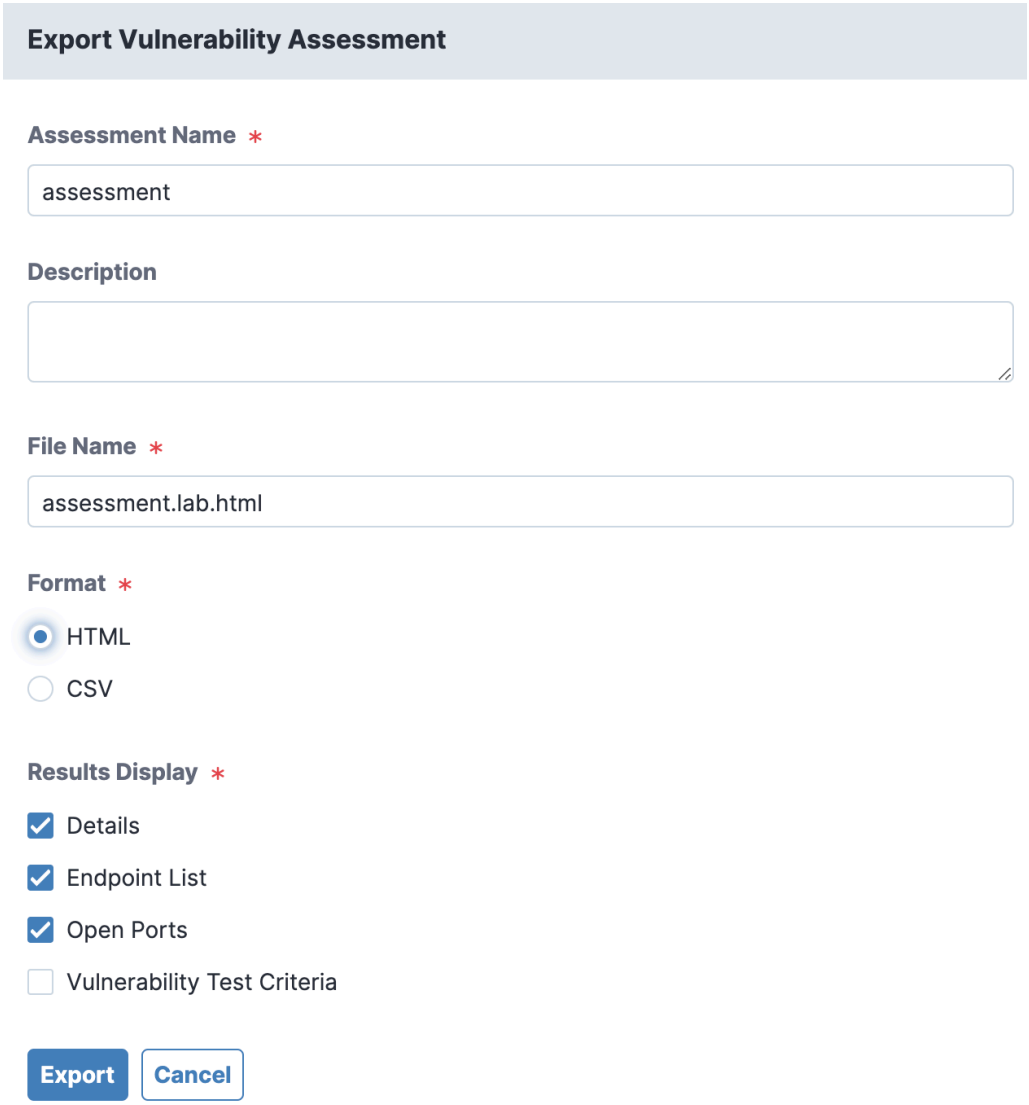
The following instructions are for exporting one assessment at a time. To export findings using Tanium Connect, see Exporting findings and assessments on page 259 for instructions.

1. From the Main menu, go to **Modules** > **Comply > Assessments**.
   On the **Assessments** page, select an assessment and click the **Export** icon . You can only export one assessment at a time. If you have more than one assessment selected, the Export icon is not displayed.

   > **Note:** You can also access **Clone**, **Edit**, **Delete**, **Deploy**, **Run On-demand Scan**, and **Export** < **Actions** from the **Side Panel** for each assessment on the Assessments list page.

2. In the **Export Assessment** window, provide the following:
   - **Vulnerability**
     a. Enter an **Assessment Name**.
     b. Optionally, enter a **Description**.
     c. Enter a **File Name**.
     d. Select a **Format**: **HTML** or **CSV**. If you select CSV, no further information is required.
     e. Select one or more **Results Display** types for the export: **Details**, **Endpoint List**, **Open Ports** (if applicable), and **Vulnerability Test Criteria**.

©2026 Tanium Inc. All Rights Reserved

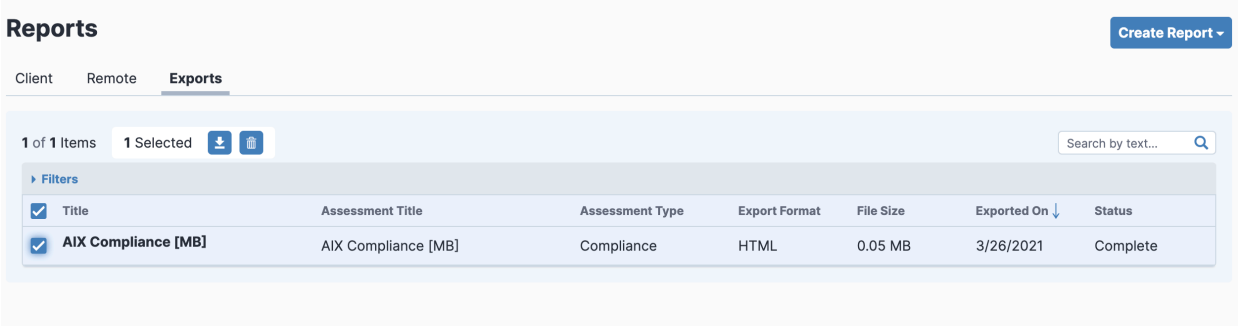


f. Click **Export**.

Note: Go to the **Reports** > **Exports** page to view the progress of any report export jobs currently running. The last column in the results table on indicates the status of the report export job.

3. When the export report is complete, select the export and click the **Download** icon to download the report in the format you selected.

©2026 Tanium Inc. All Rights Reserved



Update vulnerability assessments

Learn how vulnerability assessments receive updated vulnerability definitions and when you must manually deploy an assessment to get the latest feed.

About this task

When vulnerability sources are updated and contain new definitions that match an assessment's vulnerability content, the assessment will get the updated feed the next time it is deployed. That process occurs automatically if it is deployed by a set schedule. For more information, see View changes to the Tanium Vulnerability Library on page 117 If the vulnerability assessment does not have a recurring schedule, you must manually deploy it to receive the new vulnerability feed.

Note: This does not apply to configuration compliance assessments, which require a new assessment to use updated configuration compliance standards.

Edit an assessment

Edit an existing assessment, including its schedule, labels, and priority settings.

1. From the Main menu, go to **Modules** > **Comply > Assessments**.
2. On the **Assessments** page, select the assessment you want to edit and click Edit selected assessment .

   Note: You can also access **Clone**, **Edit**, **Delete**, **Deploy**, **Run On-demand Scan**, and **Export** < **Actions** from the **Side Panel** for each assessment on the Assessments list page.
3. Edit the **Name** if needed.

©2026 Tanium Inc. All Rights Reserved

4. Add labels in the **Labels** field. Click the **X** next to a label to remove it.
5. Change the **Comply Process Priority** if needed.

   Note: This setting applies to the legacy Tanium Scan Engine, CIS-CAT, and SCC only. It does not apply to Tanium Scan Engine 7.0.

6. Select **Start at** and **End at** and complete the date and time values to limit the assessment to run only during a specific time period. The date and time displayed by default is the local browser time.
7. Select the **Distribute over** and enter values to run the assessment over minutes or hours.
8. Select **None**, **Interval**, or **Use assessment age** for the **Repeat** field.
   - If you choose **None**, the assessment will run once if the **Start At** field is specified for a date and time in the future. Otherwise, the assessment will not run again.
   - If you choose **Interval**, the **Reissue every** field will appear, and you can specify how often the assessment is run. The default value for this field is **1 Days** and, if you do not specify a value for **Start at**, the assessment will run immediately. If you choose **Interval** and do not enter a value for **End At**, the assessment will run at the specified interval forever.
   - If you choose **Use assessment age**, then the **Run when results are older than** field will appear, and you can specify how old you want the results to be before the assessment is run. The default value for this field is **1 Days** and, if you do not specify a value for **Start at**, the assessment will run immediately. If a targeted endpoint comes online that has never run the assessment, the assessment will be run as soon as the next age-check occurs. The age of results is checked either every hour or every 3 hours. If you specify an age less than 3 hours, the age of results will be checked every hour. If do not enter a value for **End At**, the assessment will continue to run forever.
9. Click **Save**.

Clone an assessment

Learn how to quickly create a new assessment by cloning an existing one and updating its settings before deployment.

You can quickly create a new assessment based on an existing assessment by using the clone feature.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Comply > Assessments**.
2. On the **Assessments** page, select the assessment you want to clone and click Clone . You can also clone an assessment from the assessment's side panel.
3. A new assessment page opens with all fields prepopulated with settings from the original assessment. In the name field, the name of the original assessment is prepended with the text Clone -.
4. Make necessary edits and click **Create and Deploy**.

Delete an assessment

Learn when you can delete a vulnerability assessment and which associated items prevent deletion.

About this task

Vulnerability assessments are updated automatically.

You cannot delete a standard, custom check, or custom ID mapping if they are associated with an assessment.

Download audit history

Download a CSV file of assessment audit history, including edits and deletions, filtered by time, date, and user.

About this task

You can view the audit history of assessments, including edits and deletions, by time, date, and user.

1. From the Main menu, go to **Modules** > **Comply > Assessments**.
   Click the **Download Audit History** button to download a CSV file with the audit history of all assessments.



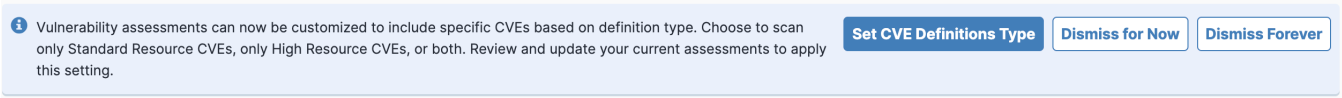
2. To download the audit history of a single assessment, go to the side panel for that assessment, scroll down to the **Audit History** section and click the download button.

©2026 Tanium Inc. All Rights Reserved

Update CVE definitions type (One-time bulk action)

Use the one-time bulk edit notification in Comply to update CVE definition types for multiple assessments at once, choosing standard, high resource, or both definition types.

About this task



When CVE definitions type selections are available for assessments, a notification appears in the Tanium Console. Through this notification, you can access a windows that lets you change the definitions type for multiple assessments at once. This is a bulk action that is available for a one-time edit, after which the banner stops appearing. By default, each assessment uses both Standard and High Resource definition types. If you do not use the bulk edit option in this notification to change the definitions type, you must edit each assessment individually to change this field.

Note: The **Dismiss Forever** button on the banner is only available to Administrator and Operator roles. If any user clicks the **Dismiss Forever** button, all users in that environment will no longer see the banner. To bring the banner back, edit the value to **On** in the **CVE Definitions Banner** setting from Comply **Overview** > Settings , so you can access the **Update CVE definitions type** bulk edit window from the banner again. For more information, see Managing application settings on page 301.

To perform a one-time bulk edit on CVE definitions types from the available notification:

1. Click the **Set CVE Definitions Type** button in the notification.
2. In the **Update CVE Definitions Type** window, select the checkbox for one or more assessments. To select all assessments, select the checkbox at the top of the column.
3. Click the **Set Definition Type** button and select an option:
   - **Standard Resource CVEs** – Select this option to only include standard resource CVEs in the assessment. This would exclude from scans CVEs that use OVAL definitions known to impact endpoint performance.
   - **High Resource CVEs** – Select this option to only include CVEs that use OVAL definitions known to impact endpoint performance. Scanning for these CVEs can

©2026 Tanium Inc. All Rights Reserved

result in higher levels of resource consumption, which may have a negative impact on the endpoint. In most cases, you would select this option for an assessment to run on a controlled schedule based on endpoint resource availability.

- **Leave as Standard and High Resource CVEs** - Select this option to scan for all CVE definition types regardless of resource consumption.

> **Note:** Custom sources are also evaluated for resource impacting CVE definitions type settings.

4. Click **Update**.

> **Note:** It can take several minutes for CVE definitions edits to take effect in scans.

Result

After you make changes in this window and click **Update**, the banner notification will not appear again. To edit definitions type, make changes in the individual assessment.

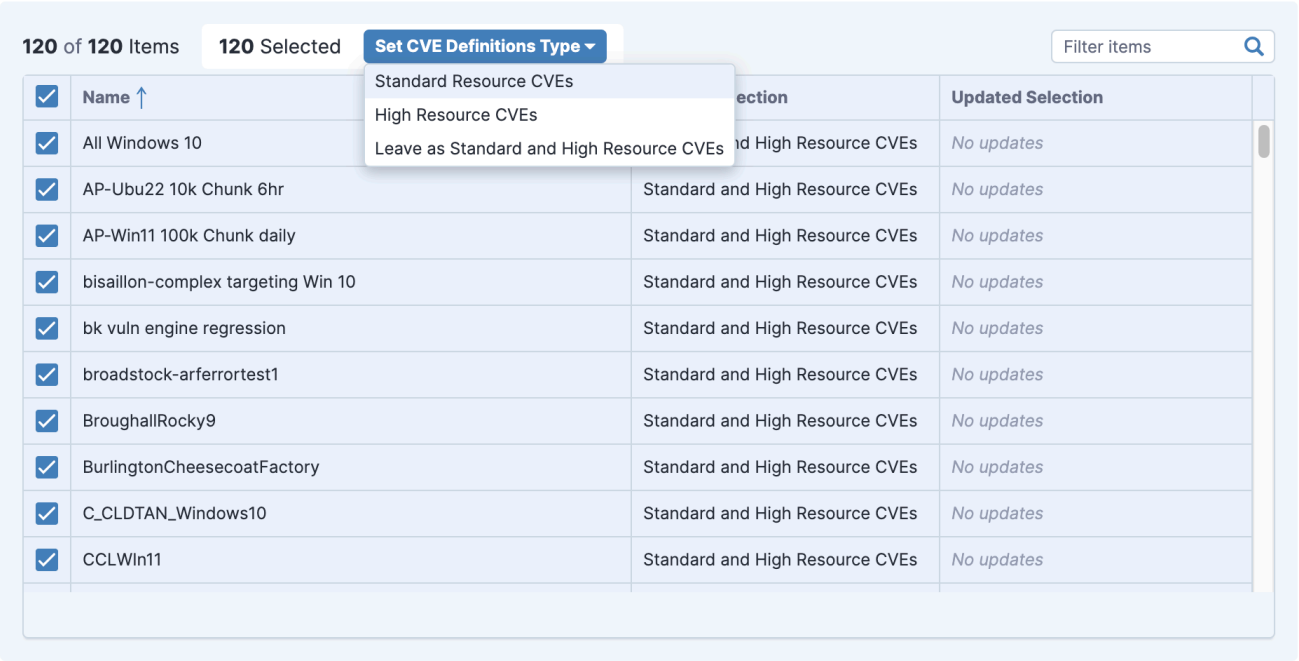
> **Note:** Click **View high resource CVEs** in the **Updated CVE Definitions Type** bulk edit page to go to the **CVE List** page where you can filter to view high resource CVEs.

©2026 Tanium Inc. All Rights Reserved

Update CVE Definitions Type

Review the CVE definition types in this list of assessments. The definition type controls what CVEs are included in this assessment: Standard Resource CVEs, High Resource CVEs, or both. The current setting is both. You can change the definition type to exclude either type of CVE definition or keep it as it is currently set.

This is a one-time action to change many assessments at once. You can change this value in the future for individual assessments using the Edit Assessment form. Changing this setting may result in fewer CVEs included in updated assessments. View high resource CVEs



Update Cancel

©2026 Tanium Inc. All Rights Reserved

Viewing and filtering findings

View and filter assessment findings on the **Findings** page to customize, save, and re-run reports based on available compliance and vulnerability data.

About this task

A finding is the result of a check on an endpoint at a specific point in time. When you run an assessment, the results appear on the **Findings** page in the **Compliance** tab or in the **Vulnerability** tab. Use the provided categories on the **Findings** page to filter results and save those filtered results as reports. Using findings, reports can be customized and re-run using any combination of available data.

> **Note:** Remediated and resolved vulnerability findings are removed from the findings list after the next scan if no further issues are found.

Filter compliance findings

Use filters in the **Compliance** tab to narrow compliance findings by computer group, exceptions, columns, and advanced filter categories.

About this task

From the Main menu, go to **Modules** > **Comply > Findings**. The findings for compliance assessments are displayed in the **Compliance** tab. At the top level, you can filter by **Computer Group**(s). Click within the edit field to add multiple groups to the filter. You can also apply the **OR** and **AND** buttons to the selected computer groups.

You can also select to hide or **Show Excepted Findings** if you have configured exceptions. For more information, see Creating exceptions for findings on page 216.

> **Note:** Only groups that include sensors that are collected by Tanium Data Service (TDS) are available for filtering.

©2026 Tanium Inc. All Rights Reserved

Tip: Click **Customize Columns** to add or remove categories from the findings grid.

To use filters with more categories, click the **Filters** link to access **Standard** filter categories and the **Filter Builder**.

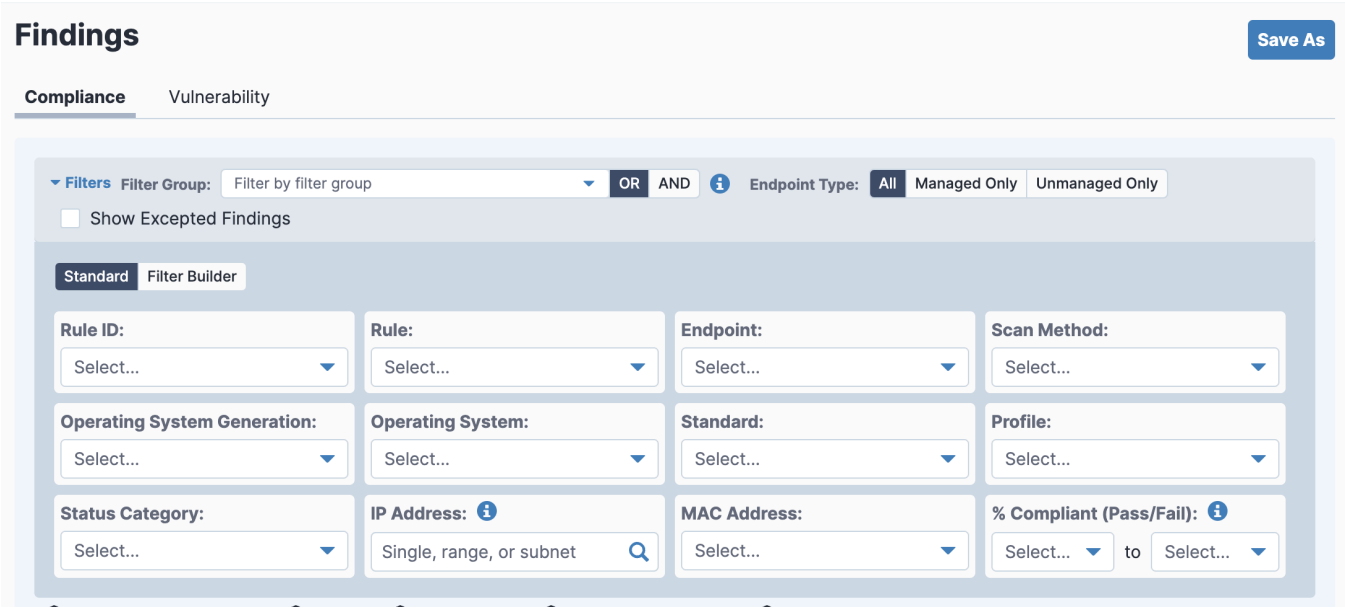
Standard filter

Use the standard filter to narrow compliance findings by computer group, rule details, endpoint, scan method, operating system, standard and profile, status, IP address, and percent compliant.

Using the provided fields, you can filter findings by **Computer Group**, **Rule ID**, **Rule**, **Endpoint**, **Scan Method** (Any, Client-Based, Remote Authenticated), **Operating System Generation**, **Operating System**, **Standard**, **Profile**, **Status Category**, **IP Address** and **% Compliant (Pass/Fail)**.

Note: **% Compliant (Pass/Fail)** is the percentage of the Pass column in relation to the Findings column. Note that this filter does not apply to Findings on the Standard and Profile and Rule tabs.

Compliance findings



Filter builder

Use the **Filter Builder** to create custom filters for compliance and vulnerability findings using Comply

©2026 Tanium Inc. All Rights Reserved

Tanium Data Service (TDS) and related sensors.

About this task

Click the **Filter Builder** button in the **Filters** section to create your own filter. With the filter builder, you can filter compliance and vulnerability findings using Comply Tanium Data Service (TDS) and additional TDS harvested sensors.

From the filter builder, you can filter on the following (This is a sample of some of the available sources):

Computer Groups - Filter compliance or vulnerability findings based on Tanium computer groups.

You can also filter on the following sensors:

Comply - Compliance Status - Create a complex filter using the metadata from the expansion columns that Comply supplies. The available columns for Compliance Status are as follows:

- **Check ID** - The unique identifier for a Compliance rule. It is made up of the benchmark name, benchmark version, profile name, profile version, and rule id.
- **Status (State)** - The result of the scan engine evaluation of the rule. (Many, but not all, of these are the same as Status Category).
    - fail - The endpoint did not satisfy all the conditions of the rule.
    - pass - The endpoint satisfied all the conditions of the rule.
    - fixed - The endpoint failed, but was then fixed (either by a tool or manually).
    - error - The engine could not complete the evaluation, therefore the endpoint's compliance status is uncertain. This might occur, for example, if a scan was run with insufficient privileges and could not gather all necessary data.
    - unknown - A problem was encountered and the results are unknown. This might occur, for example, if the output of the engine could not be interpreted.
    - notapplicable - The rule was not applicable to the targeted endpoint. For example, the rule may be specific to an OS that is not installed on the endpoint.
    - notchecked - The rule was not evaluated by the engine. This may occur if the rule contains elements that are not supported by the engine.

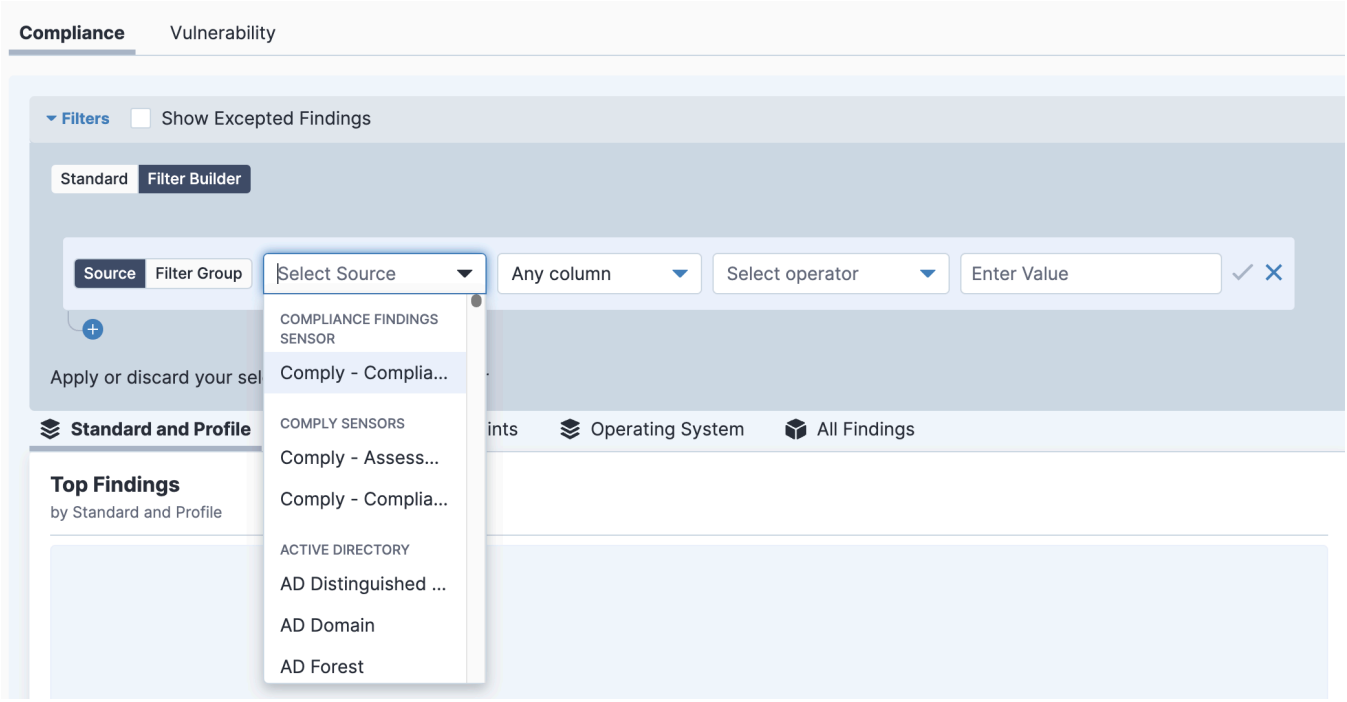
©2026 Tanium Inc. All Rights Reserved

        - notselected - The rule was not selected in the benchmark.
        - informational - The rule was checked, but the output from the engine is only informational for auditors or administrators and is not a compliance category. This status is intended for a rule whose main purpose is to extract information from the endpoint rather than to test the endpoint.
- **Status Category** - A computed value based on the state. The possible values for category are: fail, pass, error, informational. These are all mapped to the same state values. All other state values are ignored.
    - Fail - The endpoint did not satisfy all the conditions of the rule.
    - Pass - The endpoint satisfied all the conditions of the rule.
    - Error- The engine could not complete the evaluation, therefore the endpoint's compliance status is uncertain. This might occur, for example, if a scan was run with insufficient privileges and could not gather all necessary data.
    - Informational - The rule was checked, but the output from the engine is only informational for auditors or administrators and is not a compliance category. This status is intended for a rule whose main purpose is to extract information from the endpoint rather than to test the endpoint.
- **Rule ID** - The rule identifier for the benchmark rule.
- **Profile** - The name of the benchmark profile.
- **Rule** - The name of the benchmark rule.
- **Severity** - The severity value of the rule.
- **Standard** - The combination of the benchmark name and profile name.
- **Version** - The benchmark version.

Comply - Compliance Percentage - This sensor returns the aggregate compliance percentage from an endpoint.

Filter builder

©2026 Tanium Inc. All Rights Reserved



QUICK FILTER

Use quick filters in the Findings view to narrow results by standard and profile, rule, endpoints, operating system, or all findings.

You can also quick filter the Findings view by toggling the following tabs:

- **Standard and Profile**: A collection of checks and rules along with logic for how to combine those checks to determine a final status for an endpoint
- **Rule**: A standard and any filters applied to that standard in a custom profile
- **Endpoints**: The targets that are being evaluated
- **Operating system**: The operating system installed on the targets
- **All Findings**: Lists all results found by assessments. Click the **Get more details** icon for an individual finding to view pop-up with information for that finding.

Filter vulnerability findings

Filter vulnerability assessment findings by computer group, severity, and additional categories using the Vulnerability tab filters and column customization options.

©2026 Tanium Inc. All Rights Reserved

About this task

From the Main menu, go to **Modules** > **Comply > Findings**. The findings for vulnerability assessments are displayed in the **Vulnerability** tab. At the top level, you can filter by **Computer Group**(s). Click within the edit field to add multiple groups to the filter. You can also apply the **OR** and **AND** buttons to the selected computer groups.

You can also select to hide or **Show Excepted Findings** if you have configured exceptions. For more information, see Creating exceptions for findings on page 216.

Note: Only groups that include sensors that are collected by the Tanium Data Service (TDS) are available for filtering.

To use filters with more categories, click the **Filters** link to access **Standard** filter categories and the **Filter Builder**.

To add categories to the filter, click **Customize Columns** to include additional fields, for example, filter by CVSS v3 or CVSS v2.



You can filter findings by **Computer Group**, **Severity**, and expand the **Filters** link to use the following additional filters:.

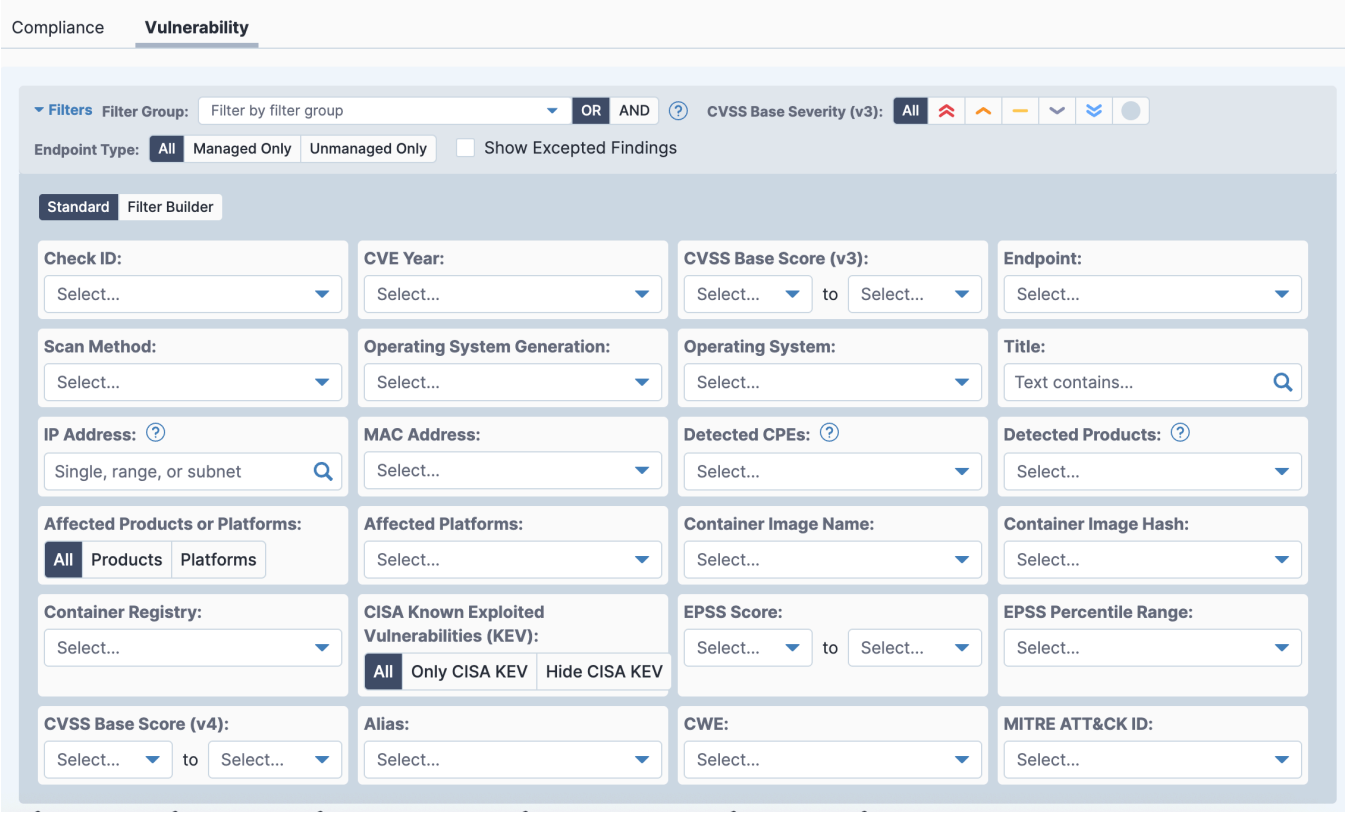
Standard filter

Use the standard filter to narrow vulnerability findings by categories such as check ID, CVE year, scores, assets, container details, and known exploited vulnerabilities.

Filter findings using any of the following categories: **Check ID**, **CVE Year**, **Score (CVSS 3)**, **Endpoint**,

©2026 Tanium Inc. All Rights Reserved

Scan Method, **Operating System Generation**, **Operating System**, **Title**, **IP Address**, **CPEs**, **Affected Products**, **Affected Platforms**, **Container Image Name**, **Container Image Hash**, **Container Registry**, and **CISA Known Exploited Vulnerabilities (KEV)**, EPSS Score, EPSS Percentile Range, CVSS Base Score (v4), Alias, CWE, MITRE ATT&CK ID (See the Filter builder on page 201 section for details on each category.)



QUICK FILTER

Use quick filters and focused tabs to narrow vulnerability findings by severity, check ID, endpoints, container images, operating system, and other categories.

You can also quick filter the findings by **Severity** by clicking the **Critical**, **High**, **Medium**, **Low**, **None**, **Unscored** buttons.

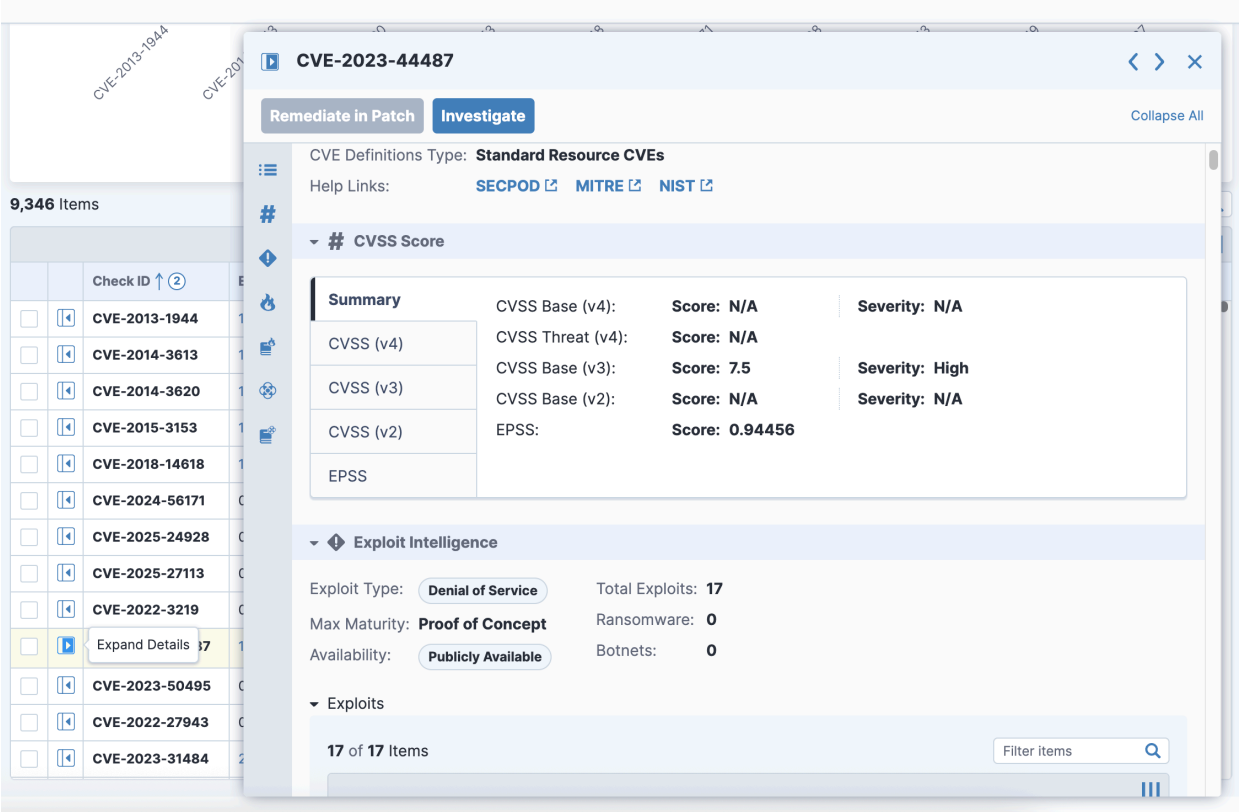
Additionally, focused tabs with following categories:

- **Check ID**: The CVE ID. For example, CVE-2020-0810
- **Endpoints**: The targets that are being evaluated
- **Container Images**: The image hash, the registry, label, severity, and endpoints by severity.

©2026 Tanium Inc. All Rights Reserved

> **Note:** Each image has a unique hash. If you remediate a CVE in an image, it's considered a new image, and it receives a new unique hash.

- **Operating system**: The operating system installed on the targets
- **Severity**: Critical, High, Medium, Low, None, Unscored
- **All Findings**: Lists all results found by assessments. Click the **Expand Details** icon for an individual finding to view.



Filter builder

Use the **Filter Builder** in the **Filters** section to create custom vulnerability filters based on available sensors, CVSS and EPSS scores, CISA KEV data, and related vulnerability attributes.

About this task

Click the **Filter Builder** button in the **Filters** section to create your own vulnerability filter. In the **Source** column for vulnerability filters, the following sensors are available:

©2026 Tanium Inc. All Rights Reserved

Vulnerability Findings Sensor - These findings are derived from the **Comply – Vulnerability Findings Details** sensor. Vulnerability findings may include the following columns:

> **Note:** The **Check ID** and **All Findings** tab in Vulnerability Findings have additional exploit columns, some of which are hidden by default.

- **Affected Platforms** - The list of platform names associated with the CVE.
- **Affected Products** - The list of product names associated with the CVE .
- **Affected Products or Platforms** - Filter results by one or the other, products or platforms.
- **Detected CPEs** - The list of vulnerable CPEs associated with a finding on an endpoint.
- **Detected Products** - The list of vulnerable products associated with a finding on an endpoint.
- **Check ID** - The CVE (Common Vulnerabilities and Exposure) ID.
- **CISA Date Added** - The date CISA added the vulnerability to the CISA KEV list.
- **CISA Due Date** - The date federal agencies must remediate by.
- **CISA KEV** - Is the vulnerability on the CISA KEV list.
- **CPEs** - The list of CPEs (Common Platform Enumeration) associated with the CVE.
- **CVE Modified Date** - The date when the CVE definition was last modified.
- **CVE Created Date** - The date when the CVE definition was created.
- **CVE Year** - The year the CVE was created.
- **Scan Type** - The scan method.
- **CVSS(v2) Base Score** - The Common Vulnerability Scoring System score assigned to the CVE from CVSS v2.
- **CVSS(v2) Base Severity** - The Common Vulnerability Scoring System severity assigned to the CVE from CVSS v2.

©2026 Tanium Inc. All Rights Reserved

- **CVSS(v3) Base Severity** -The Common Vulnerability Scoring System severity assigned to the CVE from CVSS v3.
- **CVSS(v3) Base Score** - The Common Vulnerability Scoring System score assigned to the CVE from CVSS v3.
- **CVSS(v3) Temporal Score** - The Common Vulnerability Scoring System score adjusted from the CVSS v3 score and based on exploitability and remediation. This score may change as the availability of remediation changes.
- **CVSS(v4) Base Score** - The Common Vulnerability Scoring System score assigned to the CVE from CVSS v4.
- **CVSS(v4) Base Severity** - The Common Vulnerability Scoring System severity assigned to the CVE from CVSS v4.
- **CVSS(v4) Threat Score** - The Common Vulnerability Scoring System adjusted from the CVSS v4 score and based on exploitability and remediation.
- **CVSS scoring system**:
    - Critical - CVSS score greater than or equal to 9.0
    - High - CVSS Score greater than or equal to 7.0 and less than 9.0.
    - Medium - CVSS Score greater than or equal to 4.0 and less than 7.0.
    - Low - CVSS Score greater than 0.0 and less than 4.0.
    - None - CVSS Score equal to 0.0.
    - Unscored - No CVSS Score has been assigned.
- **EPSS Score** - (Exploit Prediction Scoring System) – This value is between 0.00000 and 1.0000, and predicts the likelihood of a vulnerability being exploited within a specific time frame (the next 30 days). The higher the score the higher the odds of the vulnerability being exploited.
- **EPSS Percentile** - This value is a percentile between 0-100 (i.e. 85th) and represents the relative probability rank (high to low) of the EPSS score.
- **EPSS Percentile Range** - The EPSS percentile lets you group findings in quartile ranges as

©2026 Tanium Inc. All Rights Reserved

follows:

  - Unscored: No EPSS Score or Percentile assigned
  - 0-25th Percentile: EPSS Percentile = 0.00000-0.24999
  - 25-50th Percentile: EPSS Percentile = 0.25000-0.49999
  - 50-75th Percentile: EPSS Percentile = 0.50000-0.74999
  - 75-100th Percentile: EPSS Percentile = 0.75000-1.00000

- **Alias** -Alternative names (nicknames) for known vulnerabilities.
- **Max Maturity** - The highest observed exploit maturity (Proof of concept, weaponized, or "--" for no maturity,).
- **MITRE ATT&CK ID** - This corresponds with a known attack technique in the MITRE database and can be mapped to a CVE, for example, T1210.
- **MITRE ATT&CK ID Name** - The name of the attack or attack type, for example, Exploitation of remote services.
- **CWE** - CWE (Common Weakness Enumeration) A list of common vulnerabilities in hardware or software with categories that correspond to known vulnerability types, for example, CWE-200.
- **CWE Name** - CWE (Common Weakness Enumeration) A description of the underlying weakness. For example, Exposure of sensitive information.

Comply - Oval Findings - This sensor returns the list of OVAL (Open Vulnerability Assessment Language) definitions that the scan engine has determined apply to the endpoint. The OVAL definitions are associated with CVEs and are what is used by the scan engine to determine if an endpoint is vulnerable to a particular CVE.

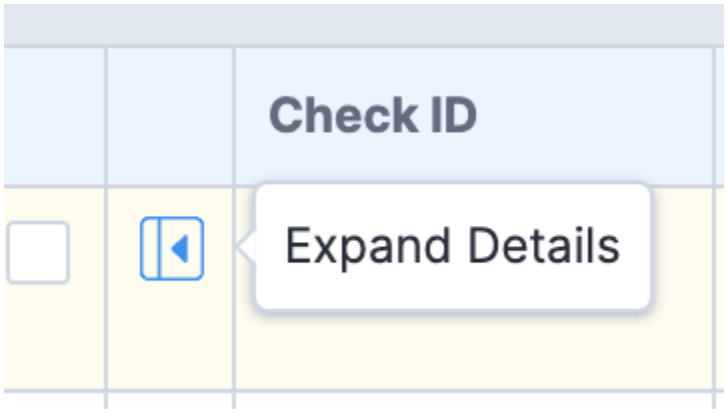
Expand details

View detailed vulnerability information for a finding, including CVE details, exploit intelligence, scores, and related patches and definitions.

About this task

©2026 Tanium Inc. All Rights Reserved

Click the Expand Details arrow on a finding to view more information for that finding. You can also investigate further and remediate the finding in Tanium Patch, if available.



The **Details** window includes the following sections:

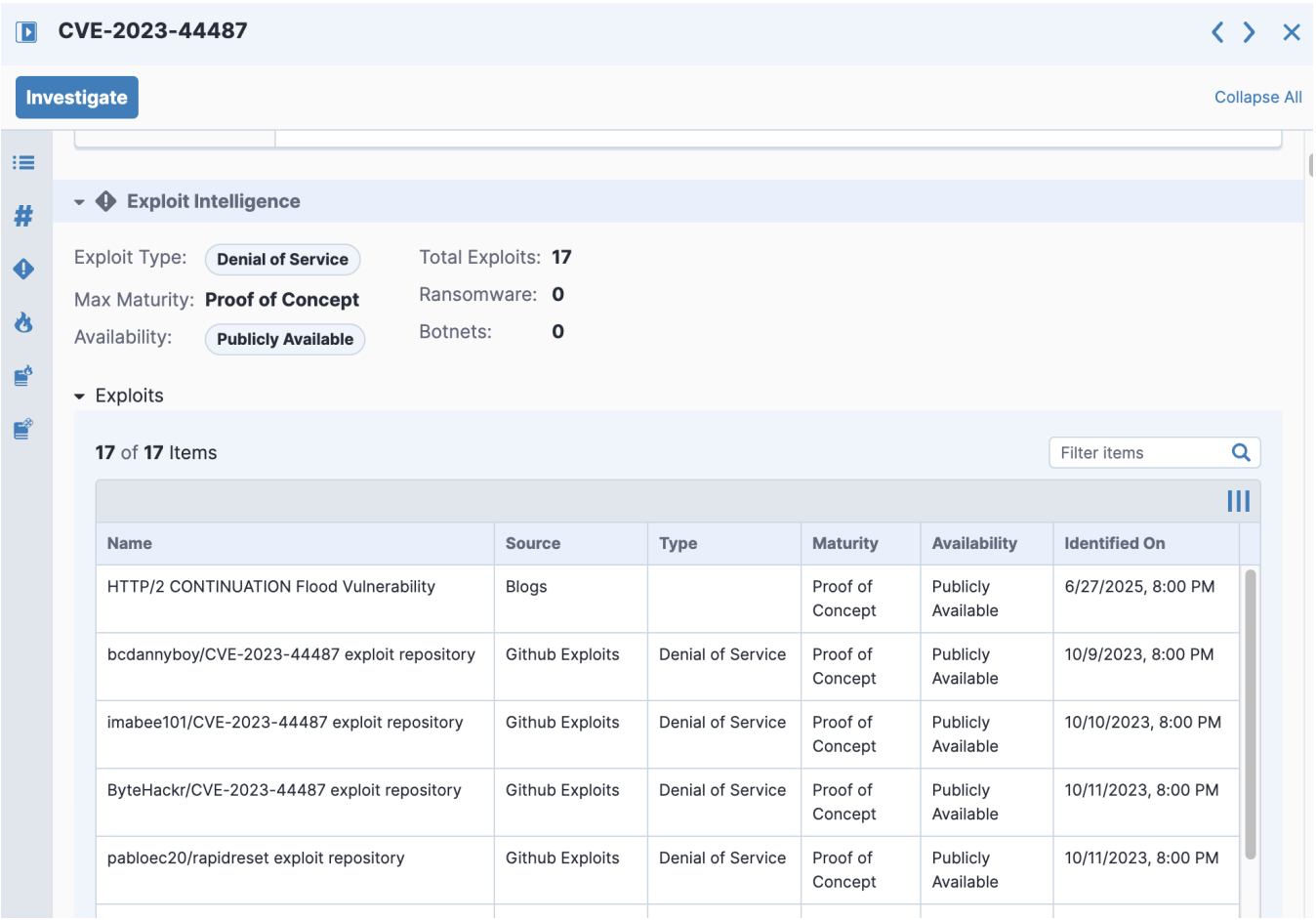
CVE Details - Provides the ID and description of the CVE, along with the endpoint name and corresponding OS it was detected on. It also includes the CVSS version score and severity.

CVSS Score - Lists the Common Vulnerability Scoring System score (per version) assigned to the CVE. It also lists the Exploit Prediction Scoring System.

Exploit Intelligence - Indicates the likelihood that a vulnerability could be exploited and therefore should take priority for remediation. Exploit intelligence provides the following information:

- **Exploit Type** - The type of exploit that is associated with the detected CVE vulnerability. For example, Denial of service.
- **Max Maturity** - The highest level of exploit code development for a given vulnerability. For example, Weaponized or Proof of Concept.
- **Availability** - The source or context in which the vulnerability was discovered.
    - Publicly Available: The vulnerability was discovered and disclosed by independent researchers, academics, open-source contributors, or security hobbyists.
    - Commercially Available: The vulnerability was discovered by a commercial security company, penetration testing firm, or bug bounty platform.
    - Privately Available: The exploit is not available publicly or commercially.

©2026 Tanium Inc. All Rights Reserved



Total Exploits - The number of exploits detected in a particular category.

Ransomware - The number of this exploit type that is associated with ransomware.

Botnets - The number of this exploit type that is associated with botnets.

CISA Known Exploited Vulnerabilities - If the vulnerability is on the CISA KEV list, this section provides details, including a name and description, of the vulnerability and when it was added to the CISA KEV catalog.

Vulnerability Definitions - List of the vulnerability definitions associated with the CVE.

Applicable Patches - List of patches (if any) that can remediate the vulnerability.

Patch Definitions - List of the patch definitions associated with the CVE.

Integration with Patch

Use Comply with Tanium Patch to identify CVEs with available patches and remediate applicable

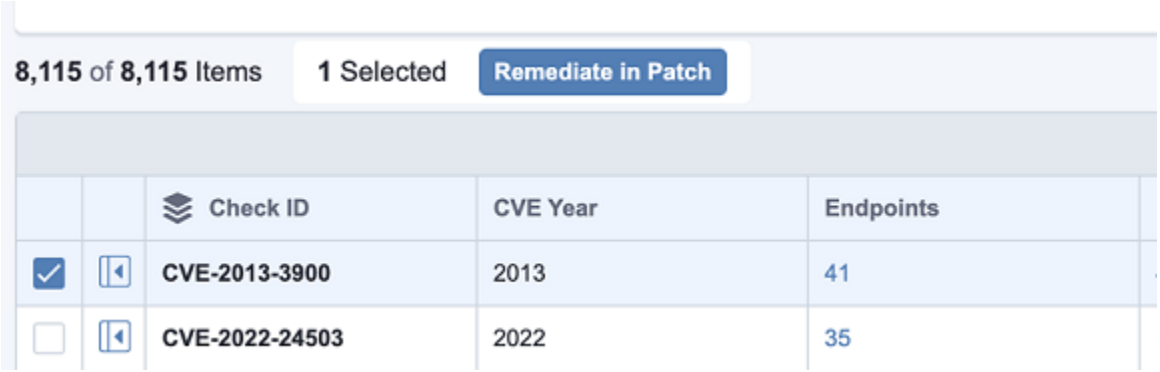
©2026 Tanium Inc. All Rights Reserved

findings directly from Patch.

The scan engine in Comply scans for both vulnerability and operating system patch definitions. If you have Tanium Patch installed and the scan engine finds a vulnerability definition and a patch definition that are associated with the same CVE, Comply checks Patch for the necessary patch. If the patch is available, when you select the checkbox for a CVE a **Remediate in Patch** button appears. This button is also available when you click the arrow to **Get more details**. Click the **Remediate in Patch** button to open the corresponding page in Patch.

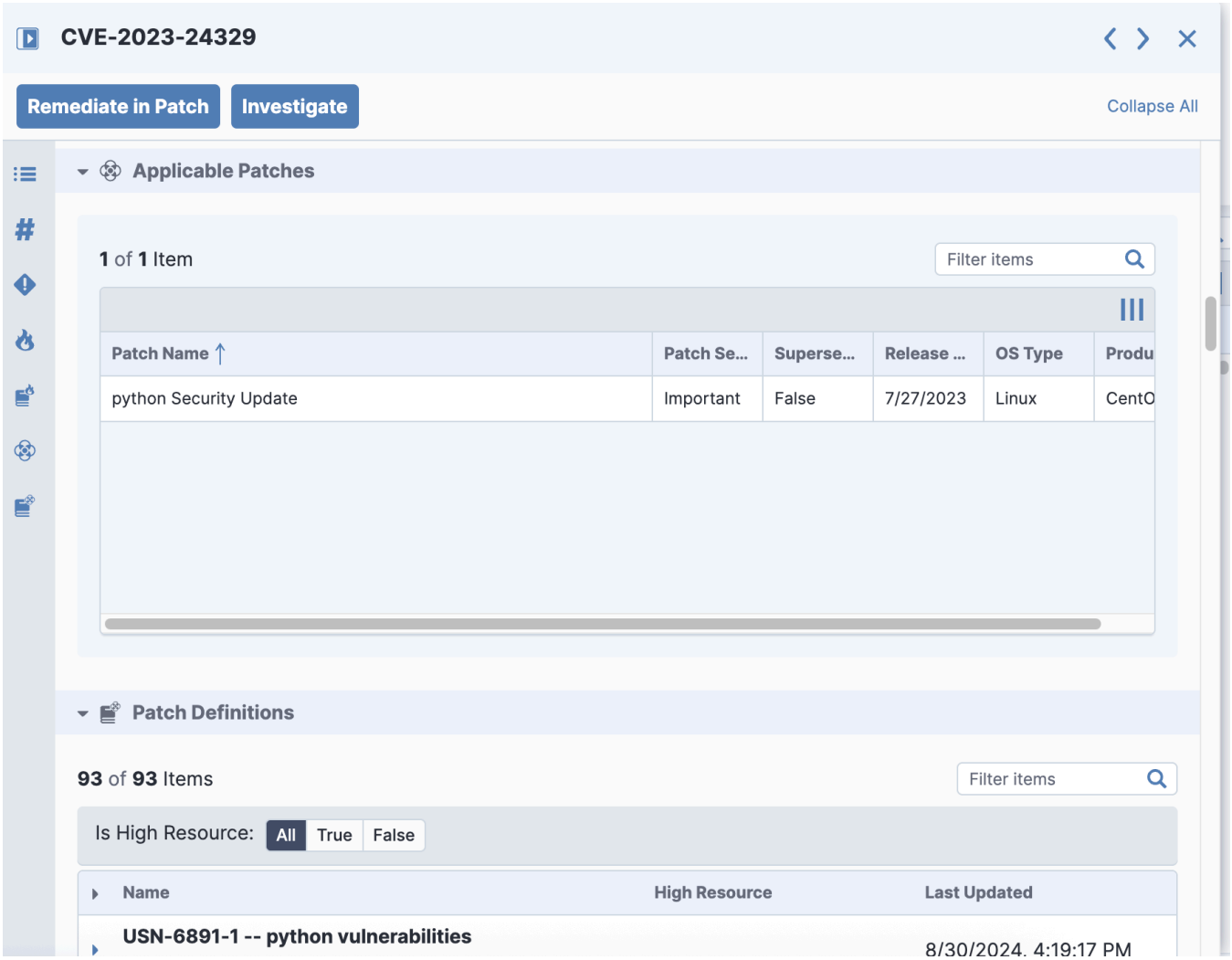
> **Note:** The **Remediate in Patch** button is only available to users with the **Show Patch** privilege.

> **Note:** All vulnerability findings that can be remediated with an unscheduled patch are listed on the Remediations page. For more information, see Remediating findings on page 245.



The **Expand Details** windows also provides more information on the applicable patches for the selected CVE.

©2026 Tanium Inc. All Rights Reserved



For more information, see Patch User Guide: Deploying patches.

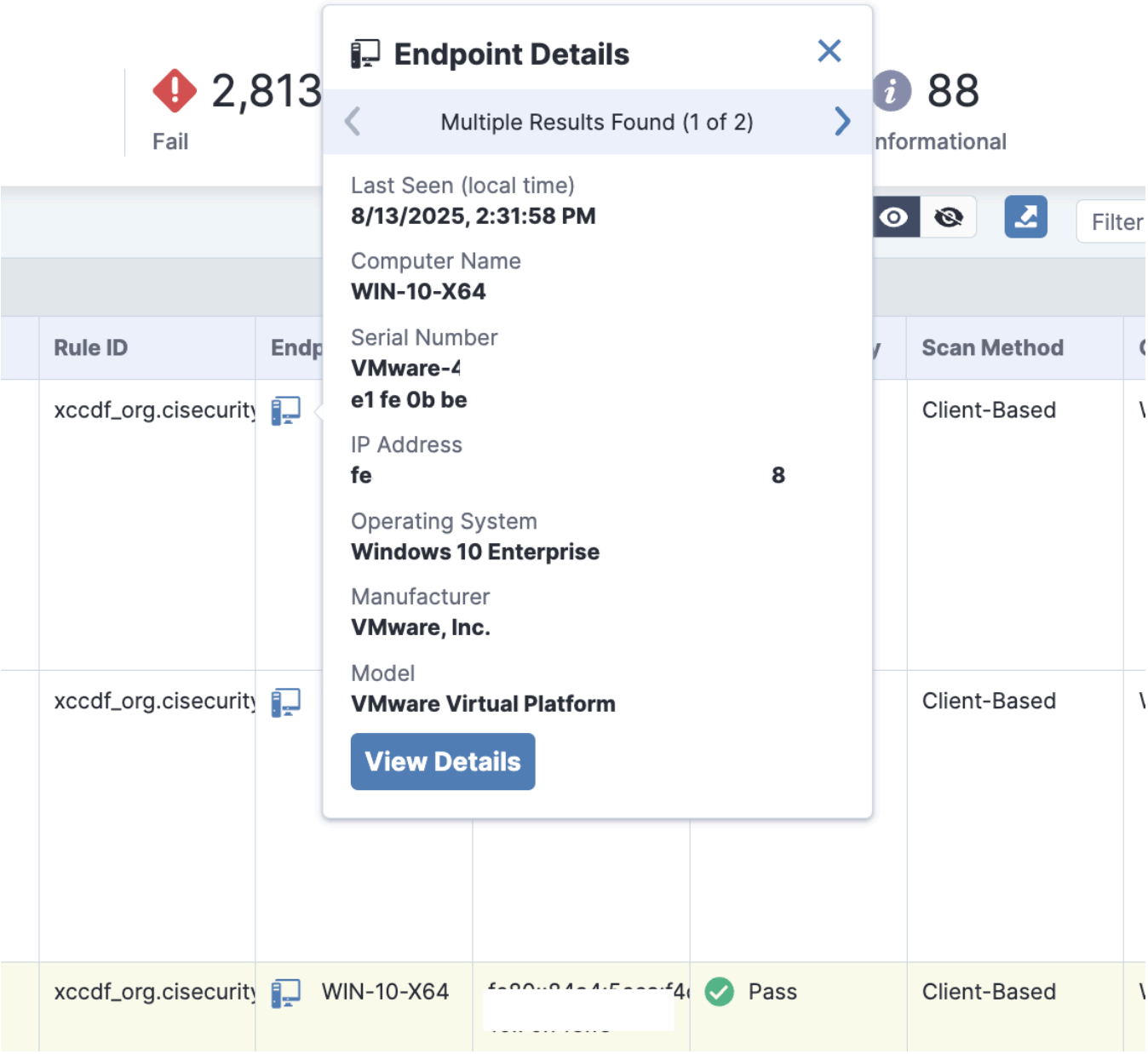
Integration with Reporting

Use the endpoint details pop-up to open Tanium Reporting and view compliance and vulnerability findings, including associated Comply assessments, for a single endpoint.

When you filter findings by endpoint, you can click the icon for an individual endpoint to view more details. From the details pop-up, click the **View Details** button to go to Tanium Reporting. To view compliance and vulnerability findings for a single endpoint, as well as associated Comply assessments, select the **Risk & Compliance** tab in Tanium Reporting. For more information, see Tanium Reporting Guide: View and manage a single endpoint.

©2026 Tanium Inc. All Rights Reserved

Note: Tanium Reporting 1.12 or later is required. Otherwise, Tanium Asset is used for endpoint details.



Findings field descriptions

Use these field descriptions to understand how Comply sensors report compliance and vulnerability findings, including dates, states, and other attributes in exports.

The following fields have distinct differences. If you select to include **First Found Date, Last Found Date**, **Absolute First Found Date**, and **Last Scan Date** columns in exports, you should understand

©2026 Tanium Inc. All Rights Reserved

the distinctions with each sensor.

Sensor descriptions

Sensor	Description
Comply – Compliance Status	You should use this sensor to return the following data: • **Check ID** -The unique identifier for a Compliance rule. It is made up of the benchmark name, benchmark version, profile name, profile version, and rule id. • **State** - The result of the scan engine evaluation of the rule. (Many, but not all, of these are the same as Status Category). • **Category** - A computed value based on the state. The possible values for category are: fail, pass, error, informational. • **Rule ID** - The rule identifier for the benchmark rule. • **First Found Date** - This returns the first found date for all the unique compliance findings present on an endpoint. If the compliance finding state changes (from Pass to Fail, for example), this date is reset to the new discovery date. • **Last Scan Date** - This returns the last scan date for all the unique compliance findings present on an endpoint. • **Excepted** - This returns true or false indicating whether it is an excepted finding. • **Scan Type** - Scan Method (Client-Based, Remote Authenticated) • **Max Cache Age** - The maximum age of the index cache, in seconds, that was acceptable when the scan ran. A value of 0 means the scan required a fresh index.
Comply – Vulnerability Status	You should use this sensor to return the following data: • **Check ID** - The CVE ID. For example, CVE-2020-0810. • **First Found Date** - This returns the first time a vulnerability is identified in an environment. Note that if a vulnerability is found and remediated and then found again, the first found date is set to the date of the most recent first finding. • **Last Found Date** - This returns the last found date for all observed vulnerabilities that the endpoint is currently vulnerable to. • **Absolute First Found Date** -This returns the very first time a vulnerability is found on an endpoint, and this date is not reset if the vulnerability is remediated. • **Last Scan** - This returns the last scan date for all observed vulnerabilities that the endpoint is currently vulnerable to. • **Scan Type** - Scan method, for example Client-Based, Remote Authenticated, Network Unauthenticated, SBOM (Software Bill of Materials), or Container Registries.

©2026 Tanium Inc. All Rights Reserved

Sensor	Description
	• **Excepted** - This returns true or false indicating whether it is an excepted finding. • **Detected Products** - The list of vulnerable products associated with a finding on an endpoint. • **Detected CPEs** - The list of vulnerable CPEs associated with a finding on an endpoint. • **Max Cache Age** - The maximum age of the index cache, in seconds, that was acceptable when the scan ran. A value of 0 means the scan required a fresh index.

Using Tanium Ask

Tanium Ask helps you perform Comply workflows, retrieve compliance findings from endpoints, and ask guided questions about Comply configurations and vulnerability issues.

Tanium Ask can help you perform Comply workflows, retrieve Comply-related information from endpoints, and ask questions about Comply configurations. For example:

Identify compliance issues: Returns a summary of compliance issues across your environment, including which endpoints are affected. Use this tool to get a broad view of your compliance posture or to identify endpoints that are failing specific benchmark checks.

Example questions:

- "What compliance issues are affecting the most endpoints?"
- "Which endpoints are failing CIS benchmark checks?"
- "Show me the top compliance findings across my environment."

Identify highest critical vulnerable systems: Returns a list of endpoints with the highest-severity vulnerability findings. Focuses on critical vulnerabilities (CVSS score 9.0 or higher) and can surface findings that have existed for an extended period.

Example questions:

- "What are the highest critical vulnerable systems?"
- "Which endpoints have critical CVEs that have been open for more than 7 days?"
- "Show me endpoints with long-standing critical vulnerabilities."

©2026 Tanium Inc. All Rights Reserved

Custom Sensors

Learn how custom sensors appear in the **Source** list and how to use them in the filter builder to find vulnerabilities, including limitations on column display.

If you have created a custom sensor and registered it in TDS, it appears at the end of the **Source** list for the filter, allowing you to filter by these custom sensors. For example, if you've tagged your endpoints by location, and you have a custom sensor for all the endpoints in your Dallas data center, you can select the sensor for the Dallas data center in the filter builder and use it to find all the vulnerabilities in the Dallas data center. Note that for custom sensors, no columns will appear in the filter builder.

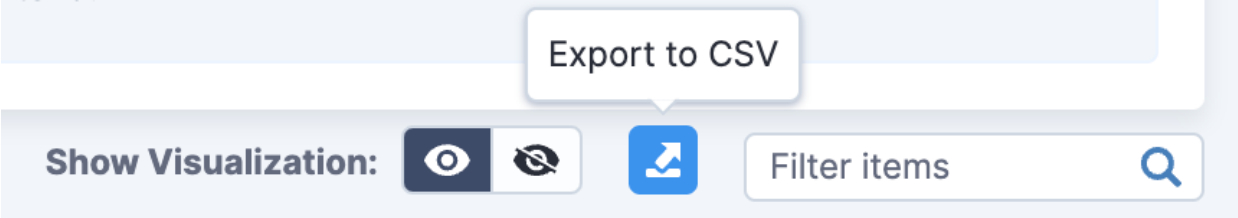
Download as CSV

Export Findings to a CSV file, configure the file options, and download the report to your local system.

About this task

You can export Findings to a CSV file and download the file by doing the following:

1. From the Main menu, go to **Modules** > **Comply > Findings**. Click the **Download as CSV**.



2. In the export window, enter **Name** for the CSV file. This file name cannot include spaces or relative paths.
3. Optionally, select the checkbox to **Include Header**s in the file.
4. Choose a **Compression Type** or select **None**.
5. **Filename**-
   Use the default filename or enter your own name.
6. **Include Headers**-This is selected by default.
7. Select what to use as a **Delimiter**: Comma, Semicolon, Single space, Tab

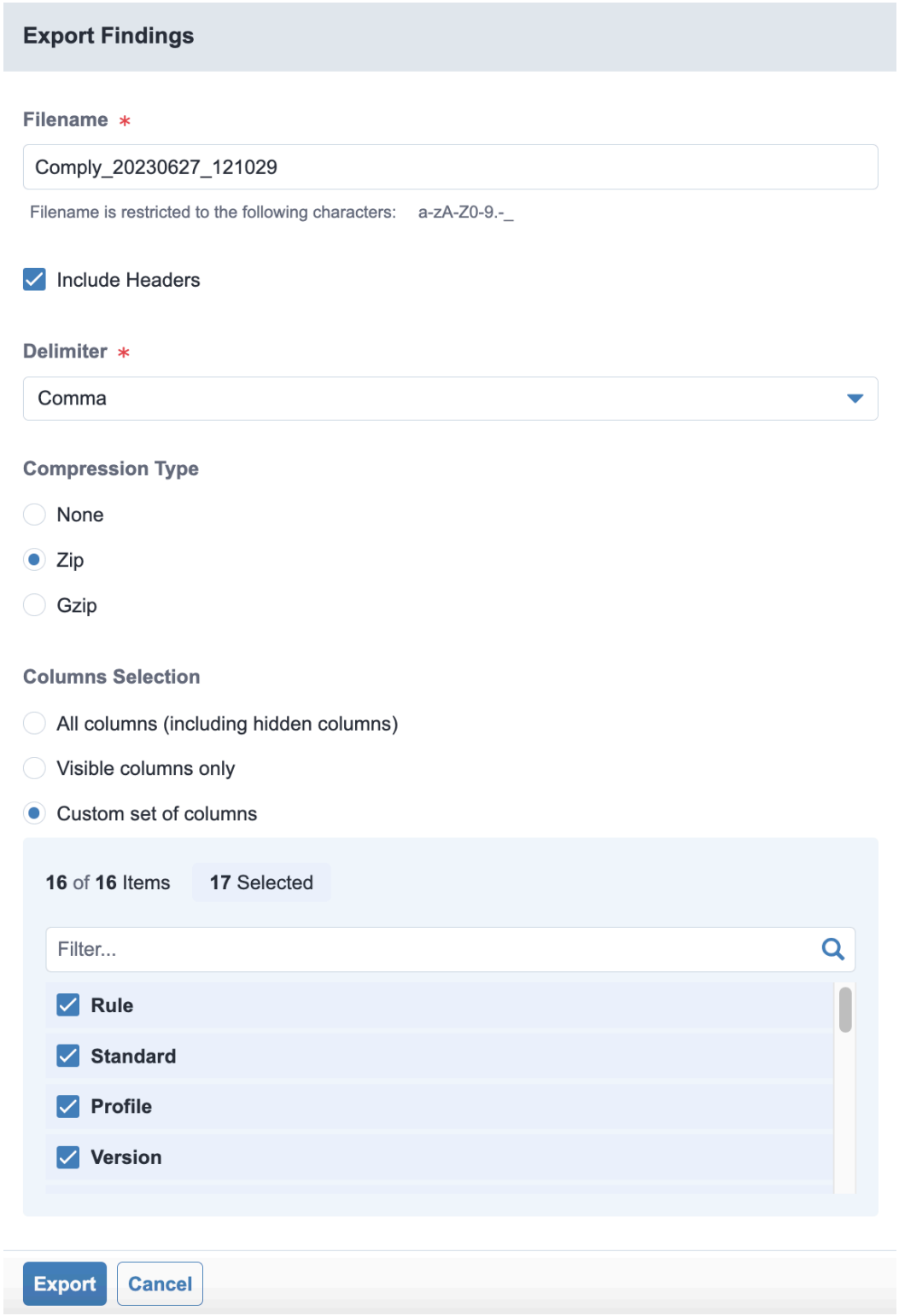
©2026 Tanium Inc. All Rights Reserved



Note: Choose the correct delimiter for your locale. If you select Tab as the delimiter, change the file extension to .tsv when opening in Microsoft Excel.

8. **Compression Type** - Choose None, Zip (default), or Gzip.
9. **Columns Selection**:
    - **All columns (including hidden columns)**-In addition to the columns available in the grid, select this option to also include columns from the Details view.
    - **Visible columns only**-Only include items visible in the grid.
    - **Custom set of columns**-Select this option to choose which columns to include from a provided list.
10. Click the **Export** button.
    The CSV file is downloaded to your local system and saved in the **Reports** > **Exports** tab.

©2026 Tanium Inc. All Rights Reserved



Result

©2026 Tanium Inc. All Rights Reserved

Create reports from findings

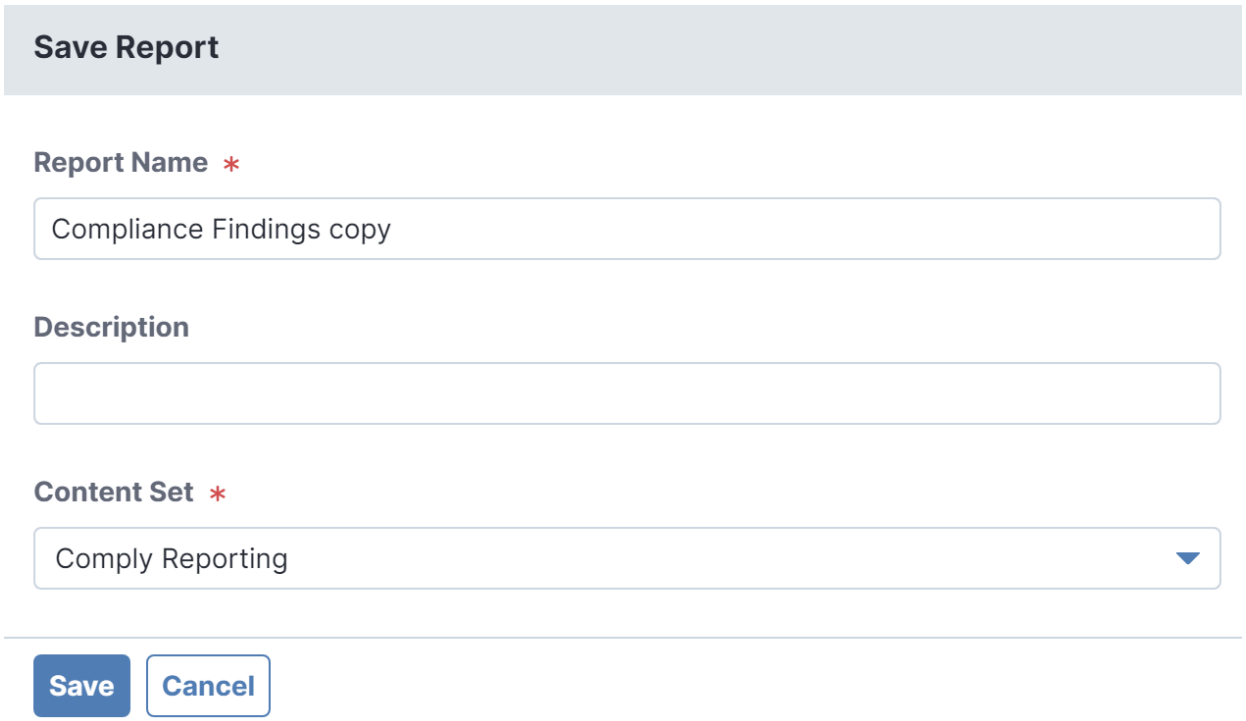
Create reports from the current findings view and save them with a name, description, and content set for later access.

About this task

Use the **Save As** button on the **Findings** page to create a report from the current view.

On the Save Report page, enter the following:

1. Enter a **Report Name**. A default name for the report is automatically generated.
2. Optionally, enter a description for the report.
3. Select a **Content Set**. For more information, see Tanium Core Platform User Guide: Managing RBAC.
4. Click **Save**.



Result

View reports by clicking on **Reports** in the **Comply** menu.

©2026 Tanium Inc. All Rights Reserved

Creating exceptions for findings

Use exceptions to exclude specific scan results from compliance and vulnerability findings when certain risks are acceptable or endpoints are not exploitable.

About this task

Use exceptions to exclude certain scan results from compliance and vulnerability findings. Exclusions may be needed in situations when endpoints aren't exploitable or certain risks are determined to be acceptable, and you no longer want to see those scan results in findings. Excepted configurations are still scanned for, but their results are hidden unless you select to show them. You can also configure reports and exports to exclude excepted findings.

Before you begin

Review required permissions and key behaviors of exceptions before creating or managing them in Comply.

- To view and edit exceptions, the following RBAC permissions are required: **Comply Exception Read** and **Comply Exception Write**.
- Exceptions are not intended to hide an overly large number of findings. They are intended to narrowly target specific findings that you no longer wish to see in reports.
- After an exception is created, if new endpoints are added that meet the criteria, those endpoints are automatically included in the exception. Although it may take several minutes for that to be reflected in findings.
- The number of endpoints listed in the data grid for each Exception may appear higher than expected. This number will likely be larger than the actual number of endpoints listed in the Preview and larger than the actual number of endpoints listed in Findings. This is because the total number of endpoints that match the Exception targeting criteria include managed and unmanaged endpoints as well as endpoints both with and without findings.

©2026 Tanium Inc. All Rights Reserved

Configure exceptions

Configure exceptions from compliance and vulnerability findings or from the **Exceptions** page in the Comply menu.

About this task

You can configure exceptions directly from the list of compliance and vulnerability findings. When you create an exception from findings, filtering and endpoint data (if available) are automatically included in the configuration. You can also create an exception from scratch by navigating to the **Exceptions** page in the Comply menu.

- Configure exceptions from Findings on page 217
- Configure exceptions from scratch on page 221

Configure exceptions from Findings

Configure exceptions for compliance and vulnerability findings, define filtering and targeting criteria, and control whether excepted findings appear in scans, reports, and exports.

About this task

For Compliance findings, you can create exceptions from the **Rule** tab and from the **All Findings** tab. For Vulnerability findings, you can create exceptions from the **Check ID tab** and the **All Findings** tab.

Important: If you create an exception from the All Findings tab, endpoint information is also automatically included in the exception. If you select multiple findings from the All Findings tab, and those findings have different endpoints, multiple exceptions will be created, one for each endpoint. For more information, see Configure exceptions from All Findings (multiple endpoints) on page 219.

1. From the Main menu, go to **Modules** > **Comply > Findings**.
2. On the **Findings** page, select the **checkbox** for one or more findings to which you want to create an exception. An exception means that the configurations are still scanned for, but their results are hidden unless you select to show them.
3. Click the **Create Exception** button.
4. In the **Details** section of the Create Exceptions window, provide the following:

©2026 Tanium Inc. All Rights Reserved

- Enter a unique **Name**
- Enter a **Description**.
- Select a **Reason** for the exception: Acceptable Use, Acceptable Risk, Compensating Control, False Positive, or Other. If you select Other, make sure to enter your reasoning in the Description field.
- Optionally, enter an **Expiration Date**. (Never is the default.)

5. The **Filtering Criteria** is automatically populated from the selected findings. Filters are the findings that will be excepted.
   If you select multiple findings, criteria from each selected finding is included. You can edit the filtering criteria, add rows and groups, or delete values.

6. In the **Target** section, if you created the exception from the All Findings tab, the endpoint is automatically added under Additional Filter Criteria. You can edit or add endpoints as follows:
   - Click **Select Computer Groups** and choose one or more groups.

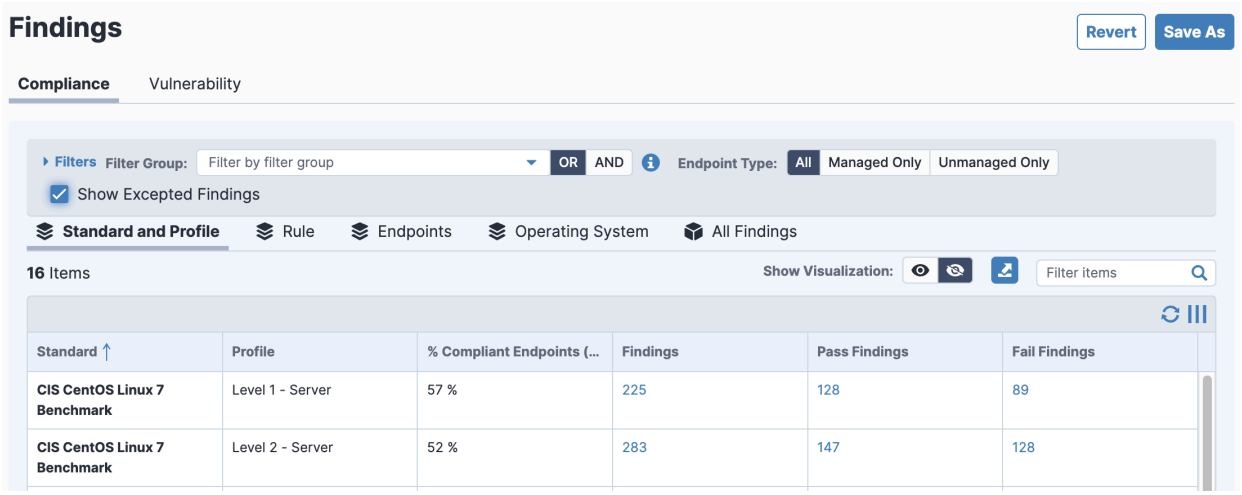
     
     Note: You might not have access to all computer groups that appear in the target list. Click **All** and **Available** in the target window to see every computer group or only the ones that you have permissions to view. Additionally, rules might limit your access to computers within the groups you select.

   - Optionally, select **Additional Filtering Criteria**: This further filters down from the selected computer groups.
     - **None**
     - **Ask a Question**: Enter a filter question.

       (Sensors used here must be registered in TDS. For more information, see Tanium Interact User Guide: Register or unregister sensors for collection.)
     - **Define a Rule**: Add rows and groupings to build a filter.
     - **Specify Individual Endpoints**: Enter or paste a comma-separated list of computer names into the provided field. This list must be no longer than 50 computers.

©2026 Tanium Inc. All Rights Reserved

7. Click **Show Preview** to review potential findings that match the filters and targeting criteria. Edit the criteria if necessary or click **Save** to create the exception. After you save the exception, you return to the Finding page and the newly created exception is applied. Any scans that meet the criteria will no longer appear in the list. They will not appear in reports or exports. Select the **Show Excepted Findings** checkbox to see all excepted findings again and include them in reports.



Navigate to **Exceptions** in the Comply menu to view or edit the exception you created. The side panel for each exception provides configuration and targeting details.

> **Note:** When you use Tanium Connect to export findings, you have the option to **Include excepted findings** in exports. For more information, see Exporting findings and assessments on page 259.

Configure exceptions from All Findings (multiple endpoints)

Configure exceptions for multiple findings with different endpoints, including base names and read-only criteria, when creating exceptions from the **All Findings** tab.

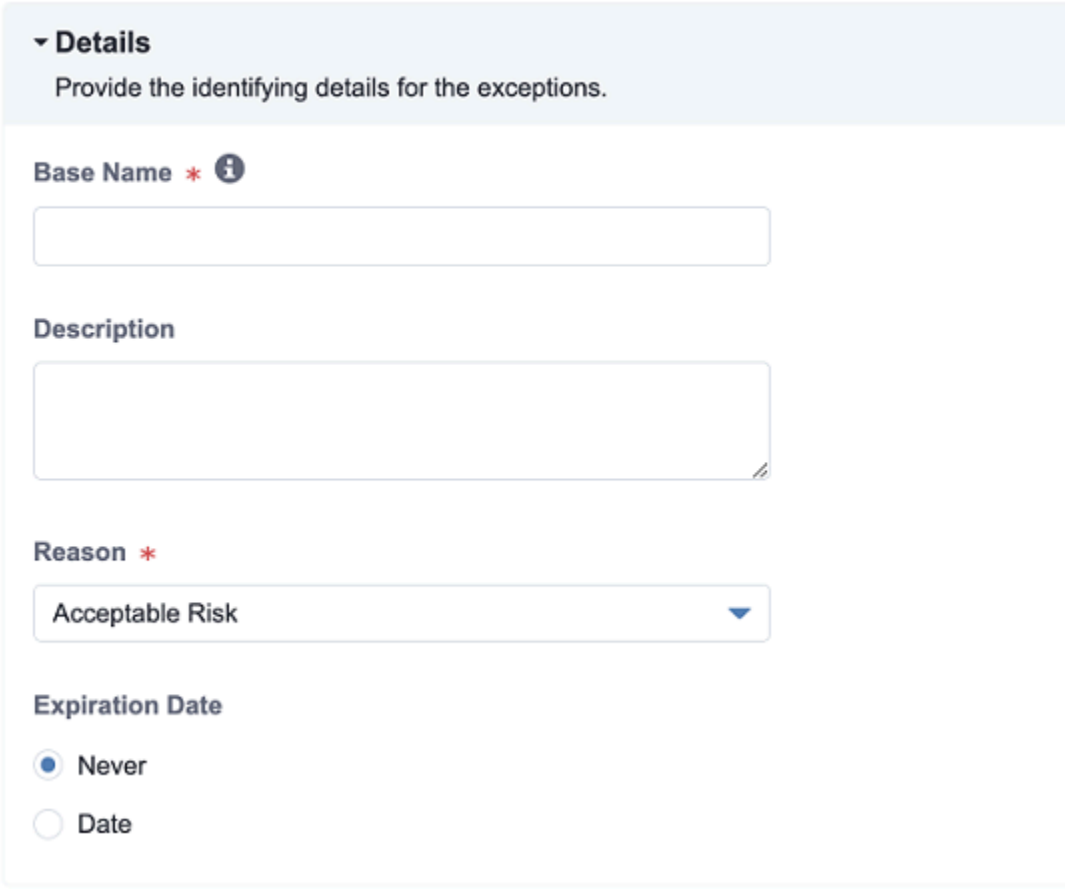
About this task

If you select multiple findings from the **All Findings** tab, and those findings have different endpoints, multiple exceptions will be created, one for each endpoint. The following configuration items are different for exceptions with multiple endpoints.

- Rather than configuring a Name, you configure a **Base Name.** With a base name, when the exceptions are created, each exception will be named as follows: <base name>-<endpoint>-<current timestamp>.

©2026 Tanium Inc. All Rights Reserved

- You cannot edit filtering criteria from the exception creation page. Endpoints are listed individually with along with read-only data from the findings. After you click **Save**, you are returned to findings and the newly created exceptions are applied. You can edit each individual exception from the **Comply** > **Exceptions** page.



©2026 Tanium Inc. All Rights Reserved



Configure exceptions from scratch

Configure exceptions from scratch to define details, filters, and targets so that specific compliance or vulnerability findings are excluded from results and reports.

About this task

To configure exceptions, do the following:

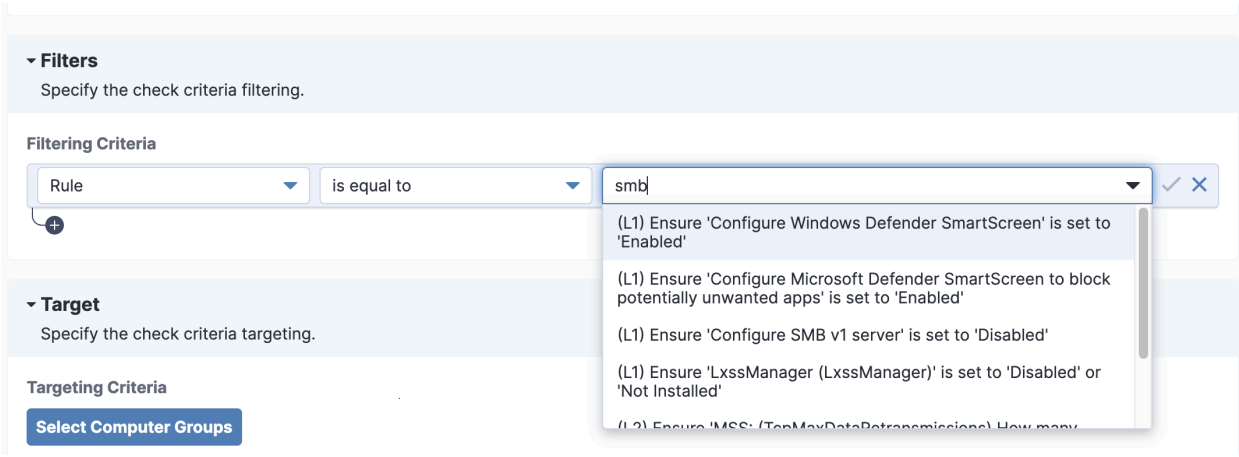
1. From the Main menu, go to **Modules** > **Comply >Exceptions**.
2. Click **Create Exception**.
3. On the **Create Exception** page, in the **Details** section, provide the following:
    - Enter a unique **Name**
    - Enter a **Description**.
    - Select the scan **Type** you are creating this exception for: **Compliance** or **Vulnerability**
    - Select a **Reason** for the exception: Acceptable Use, Acceptable Risk, Compensating

©2026 Tanium Inc. All Rights Reserved

Control, False Positive, or Other. If you select Other, make sure to enter your reasoning in the Description field.

- Optionally, enter an **Expiration Date**. (Never is the default.)
- Optionally, change the **State** from **Active** (the default) to **Inactive**. With Active, the exception goes into effect immediately. With Inactive, it does not go into effect upon creation, but you can save it to use at a later time.

4. In the **Filters** section, enter **Filtering Criteria**. These are the findings that will be excepted and are specific to either compliance or vulnerability assessments depending on which finding type is selected. Select an **Attribute**, **Operator**, and **Value**. Click the + plus sign to add another row or group. For the Value field, begin typing and potential matches appear.



5. In the **Target** section, do the following:
   - Click **Select Computer Groups** and choose one or more groups.

     Note: You might not have access to all computer groups that appear in the target list. Click **All** and **Available** in the target window to see every computer group or only the ones that you have permissions to view. Additionally, rules might limit your access to computers within the groups you select.

   - Optionally, select **Additional Filtering Criteria**: This further filters down from the selected computer groups.
     - **None**
     - **Ask a Question**: Enter a filter question.

       (Sensors used here must be registered in TDS. For more information, see

©2026 Tanium Inc. All Rights Reserved

Tanium Interact User Guide: Register or unregister sensors for collection.)

- **Define a Rule**: Add rows and groupings to build a filter.
- **Specify Individual Endpoints**: Enter or paste a comma-separated list of computer names into the provided field. This list must be no longer than 50 computers.

6. Click **Show Preview** to review potential findings that match the filters and targeting criteria. Edit the criteria if necessary or click **Save** to create the exception.
   After the exception is created, go to **Findings** for compliance or vulnerability scans. Any scans that meet the criteria will no longer appear in the list. They will not appear in reports or exports. Select the **Show Excepted Findings** checkbox to see all excepted findings again and include them in reports.

   Note: When you use Tanium Connect to export findings, you have the option to **Include excepted findings** in exports. For more information, see Exporting findings and assessments on page 259.

Export exceptions list

Export the list of exceptions to a CSV file or copy it to the clipboard from the Exceptions list view.

About this task

To export the list of exceptions, do the following:

1. From the Main menu, go to **Modules** > **Comply > Exceptions**.
2. From the list view, click the **Export** button and select **Export to CSV** or **Copy to clipboard**.

Result

Note: Filter the list of exceptions by clicking on **Filters** and entering filter criteria such as Name, Description, Type, Reason, Endpoints, Created On, Modified On.

©2026 Tanium Inc. All Rights Reserved

Exception examples

Examples of situations where you might use compliance and vulnerability exceptions.

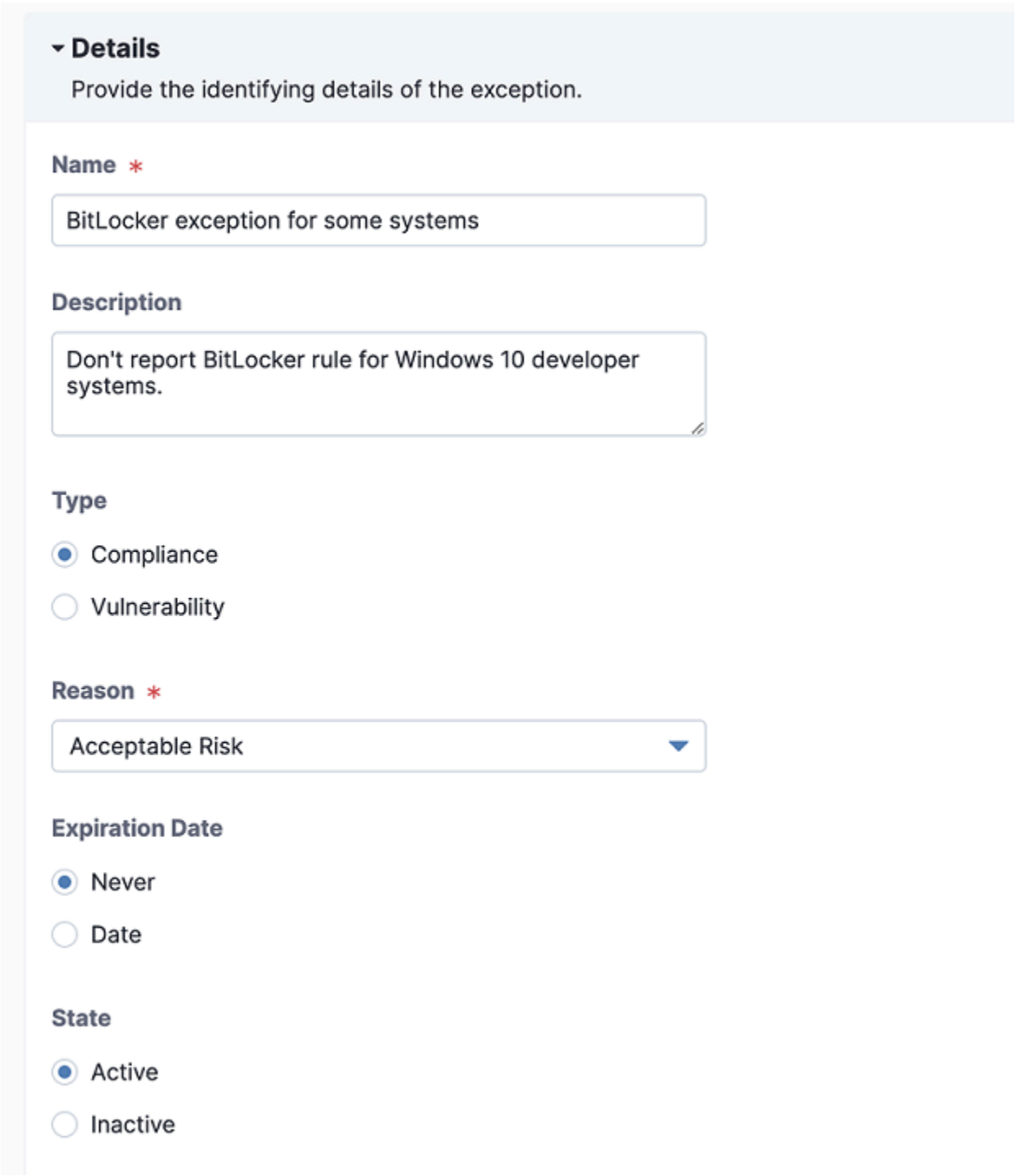
The following are possible situations for using compliance and vulnerability exceptions.

Compliance finding exception example

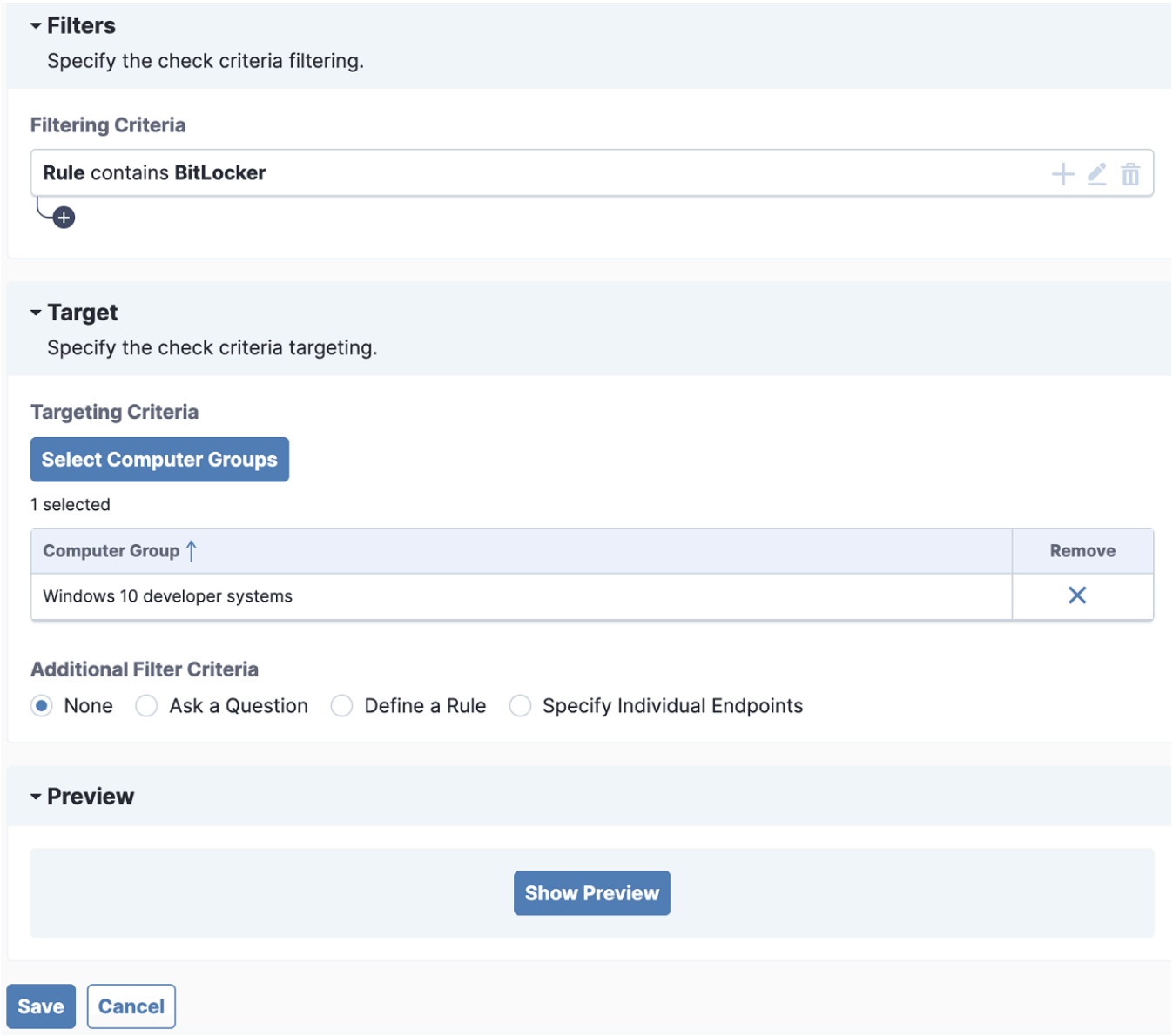
Use a compliance exception to exclude specific systems, such as Windows 10 developer machines without BitLocker, from applicable BitLocker rules in your compliance assessments.

You have a set of developer systems running Windows 10, but due to how they are used, you cannot configure BitLocker on these systems. Rather than creating a custom profile and a separate assessment for these endpoints, you create an exception for all BitLocker rules for compliance assessments on those Windows 10 developer systems.

©2026 Tanium Inc. All Rights Reserved



©2026 Tanium Inc. All Rights Reserved

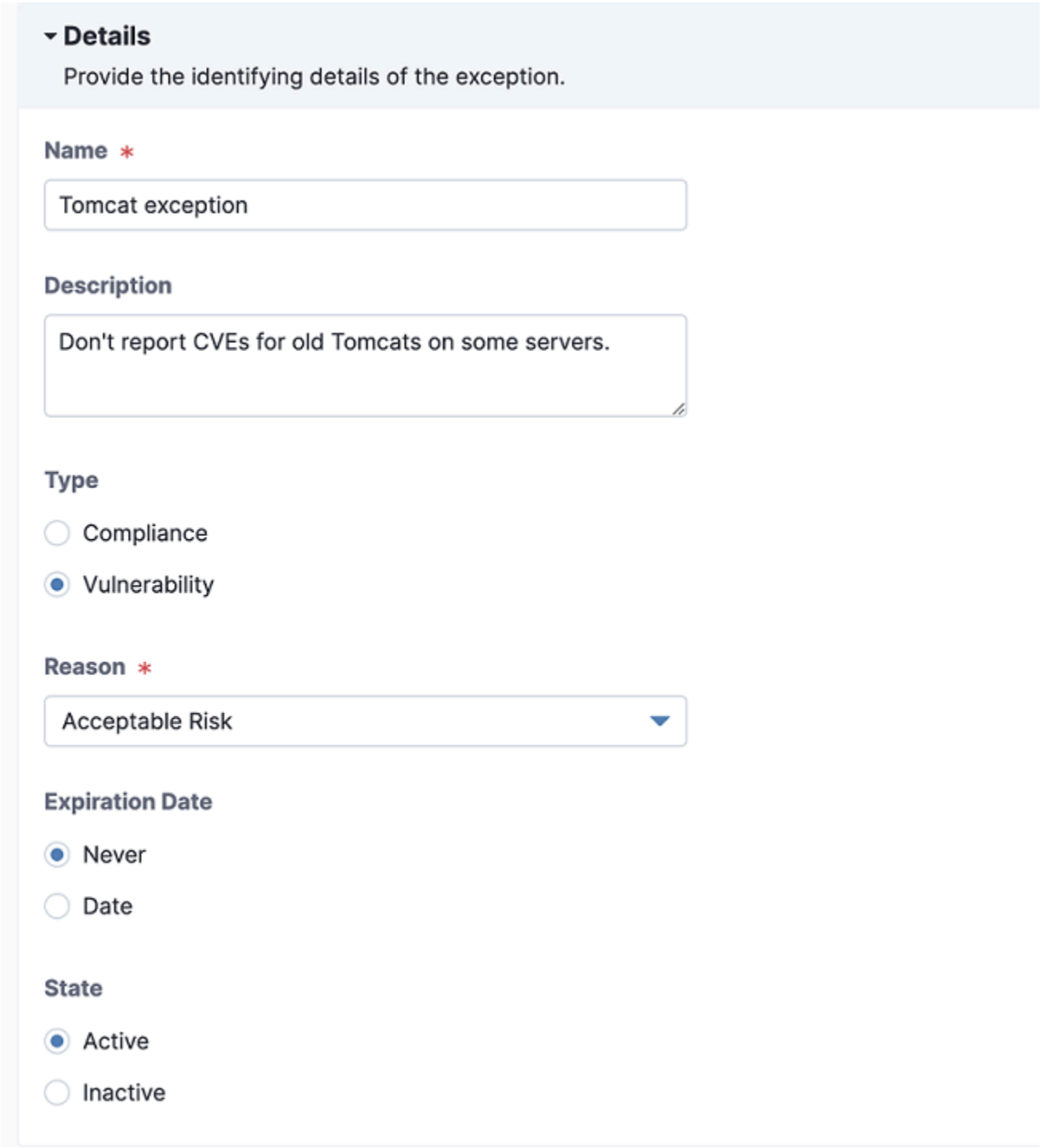


Vulnerability finding exception example

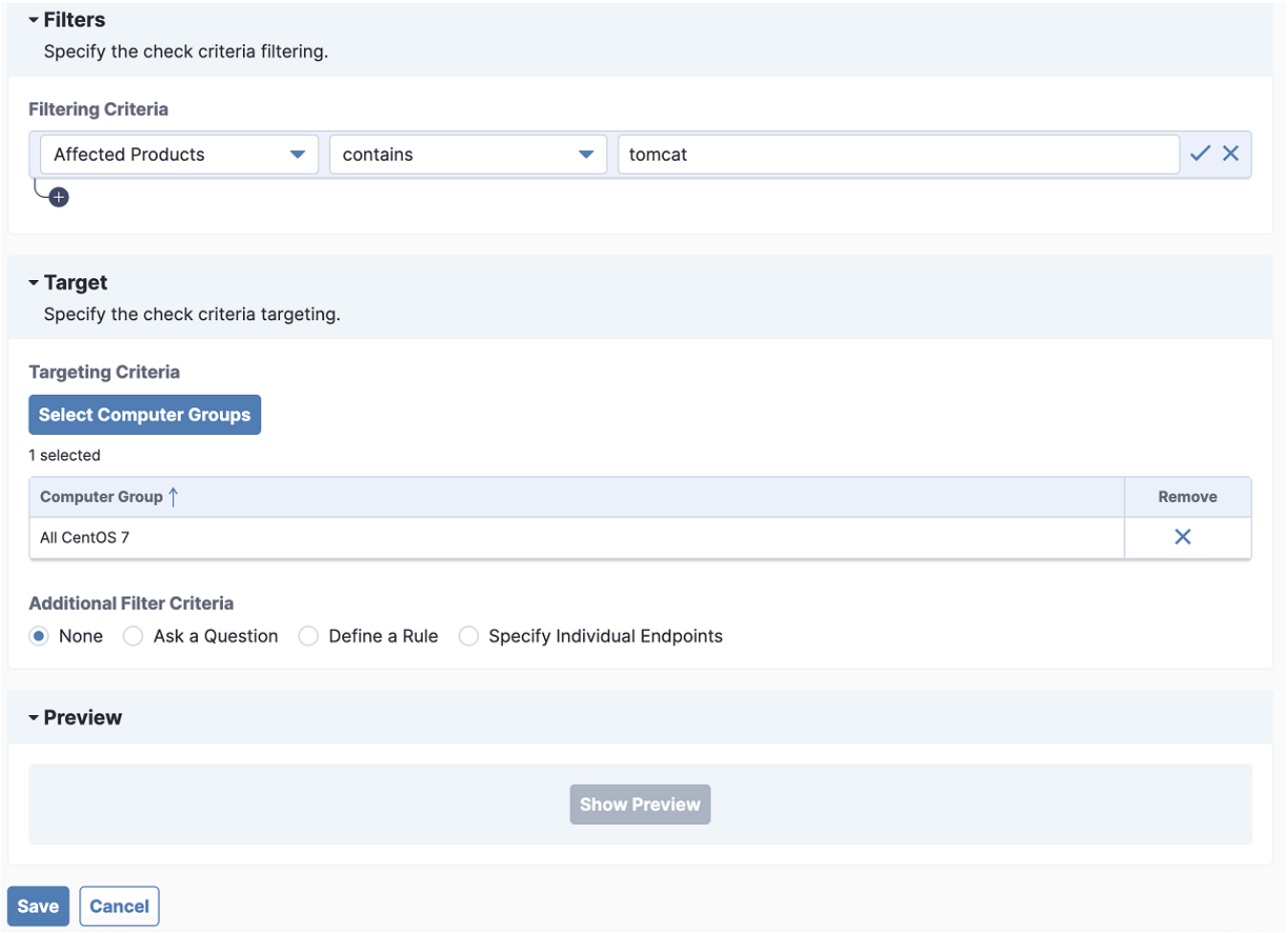
Example of creating a vulnerability finding exception to suppress recurring findings for an outdated Tomcat installation that cannot be upgraded.

You have a set of servers running an old version of Tomcat. You cannot update Tomcat because the custom application you are running will not work on newer versions of Tomcat. You're tired of seeing findings about Tomcat on those machines, therefore you create an exception that hides those findings.

©2026 Tanium Inc. All Rights Reserved



©2026 Tanium Inc. All Rights Reserved



©2026 Tanium Inc. All Rights Reserved

Investigating findings

Use the Investigate feature to analyze compliance checks or vulnerabilities by reviewing the actual endpoint values that caused the findings.

About this task

When a compliance check fails or a vulnerability is found, use the Investigate feature to find the actual values on the endpoints that caused the issue.

Before you begin

- Investigations are only supported:
    - With the Tanium Scan Engine
- Investigations are NOT supported:
    - In low resource mode
    - On unmanaged devices
    - For more than 5,000 devices in one investigation
- The following sensors are required and must be registered with TDS:
    - **Comply - CVE Investigation Details**
    - **Comply - Compliance Investigation Details**

      For more information, see Register or unregister sensors for collection.
- The following RBAC permission is required:
    - **Comply Investigation Execute**. For more information, see User role requirements on page 41.

©2026 Tanium Inc. All Rights Reserved

 **Important:** The Investigation feature only becomes available for existing assessments when they are redeployed or run again as part of a set schedule.

Investigate compliance findings

Investigate compliance findings by reviewing benchmark rules and their checks in the Compliance tab, filtering findings as needed, and opening rule details to compare expected check values with actual endpoint results.

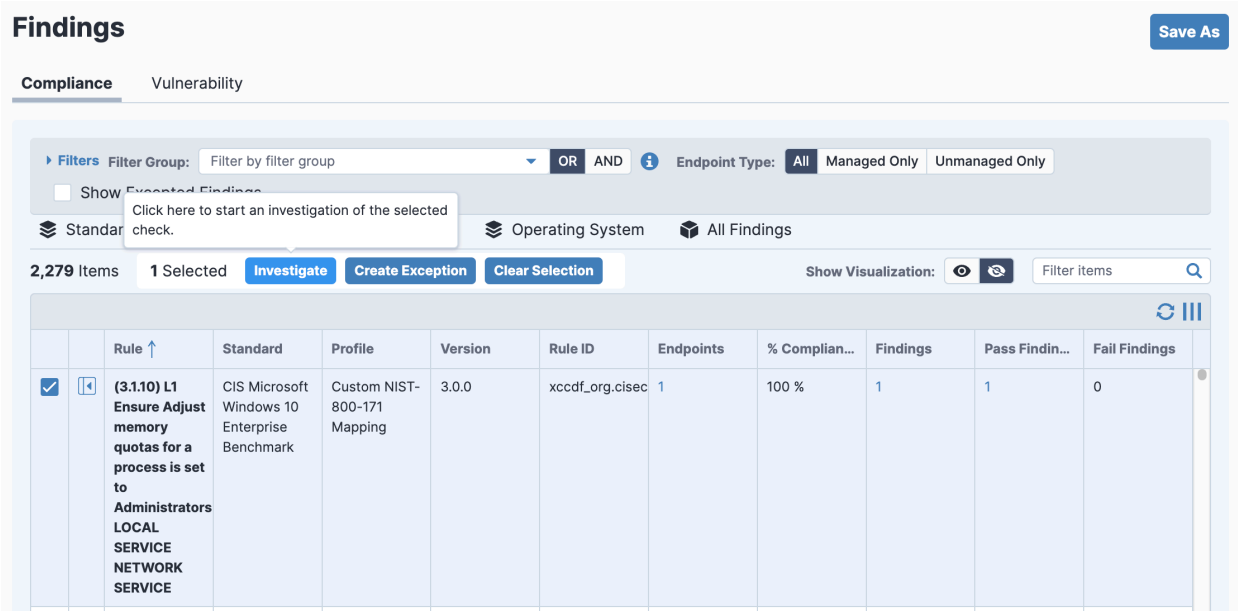
About this task

Compliance checks are defined through benchmarks, which are listed on the Standards page in Comply. Each benchmark contains a set of rules. Each rule contains a set of checks (criteria). When investigating compliance findings, you are examining the expected values for the checks of the selected rule and comparing them to the actual values that were the result of the rule being evaluated on the endpoint.

To investigate compliance findings,

1. From the Main menu, go to **Modules** > **Comply > Findings**.
2. In the **Compliance** tab, select the **Rule** or **All Findings** tabs.
   Filter the list if necessary either by **Computer Group** or by using any of the available filter items. You can also investigate findings from the **All Findings** tab.
3. Select the rule **checkbox** and click the **Investigate** button to open the Benchmark Rule Details window. (You can only investigate one rule at a time.) You can also click the **Get more details** arrow to open the flyout and click the Investigation button located there.

©2026 Tanium Inc. All Rights Reserved



Note: If you receive a **No rule checks** message after you click Investigate, that means there are no checks on the endpoints for the selected rule. This may be because the rule is defined for informational purposes only and therefore has no criteria and nothing to evaluate.

Compliance investigations

Review the Investigation/Benchmark Rule Details window to understand rule information and investigate compliance checks, including status, expected and actual values, and endpoint counts.

In the Investigation/Benchmark Rule Details window, there are several sections of information.

- The **Details** section has the general data about the rule, including the Benchmark, Description, Rational, and Remediation suggestion.

The table with the list of checks (also called tests) has several columns:

- **Status** - Indicates whether the endpoints listed for this check Pass, Fail, provided only Informational results, or experienced an Error. **Informational** means a rule was checked, but the output from the engine is only informational for auditors or administrators and is not a compliance category. There are two kinds of status errors. An OVAL **Error** indicates there was a problem collecting information or analyzing a check on the endpoint. An **Investigation Error** is a Tanium error, likely a Tanium Interact TSE-error. For more information, see Tanium Interact User Guide: Troubleshooting.

©2026 Tanium Inc. All Rights Reserved

- **Test Description** - This text is taken from the OVAL content for that check.
- **Expected Objects** - The type of object that is expected to be checked on the endpoint.

  Note: **No Expected Objects** may be displayed if the OVAL Test definition for the test that was evaluated did not specify any Object. This can occur when there was an error reported for the particular investigation.

- **Expected States** - The property of the object being checked on the endpoint.

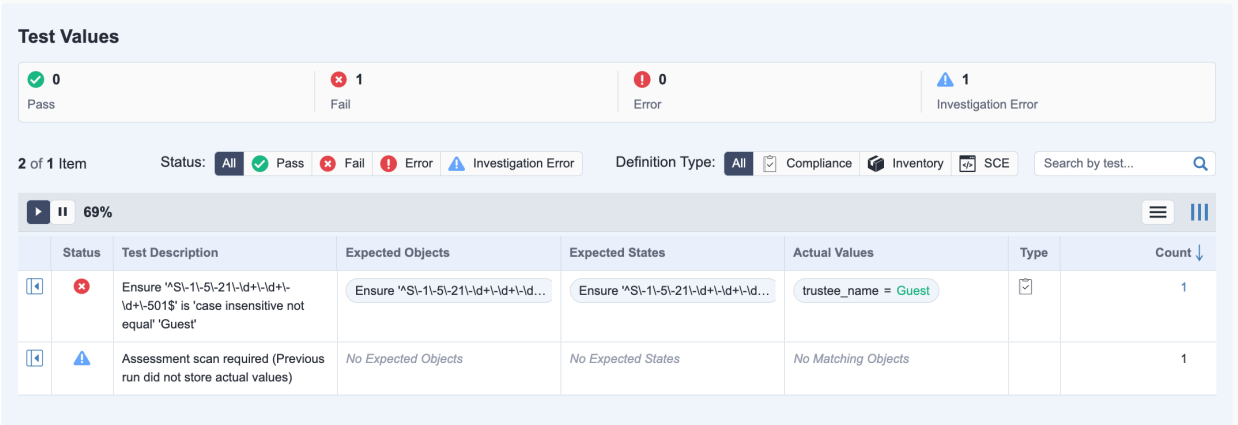
  Note: **No Expected States** may be displayed if the OVAL Test definition for the test that was evaluated did not specify any State (or property) of the Expected Object. Note that States are not a required attribute of a Test. To satisfy the Test, it may be sufficient to simply specify the Object. An example of this would be to check for the existence of a File (no state is needed in this case).

- **Actual Values** - The object found on the endpoint and all the associated properties of that object. The property names are in black and the actual values are in green.

  Note: **No Matching Objects** may be displayed if there was no matching object found on the endpoint that matched the specified Expected Object.

- **Type** - The type of check, Compliance, Inventory, or SCE. The difference between a Compliance check and an Inventory check is a field in the OVAL definition type. For **Compliance**, this checks if the system meets a predefined state. For **Inventory**, this checks if the required software installed on the system. The **SCE** (script check engine) checks items that OVAL cannot and is packaged together with the benchmark.
- **Count** - The number of endpoints that have the actual value listed for the check.

©2026 Tanium Inc. All Rights Reserved

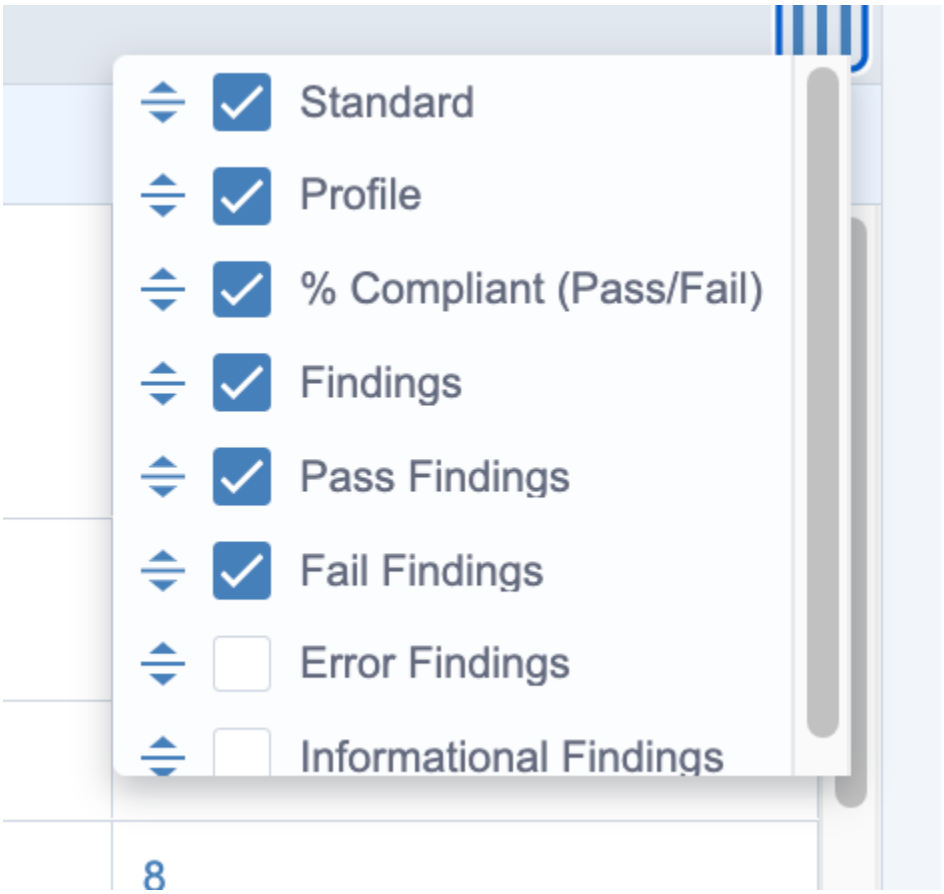


Filter tests list

Filter the tests list in the table by **Status**, **Definition Type**, or other available grid filters.

About this task

You can filter tests in the table by **Status**, **Definition Type**, or any of the other available grid filters.



©2026 Tanium Inc. All Rights Reserved

Expand Details

View detailed information about compliance checks, including endpoints with actual values, raw OVAL XML, and script details, from the Investigation/Benchmark Rule Details window.

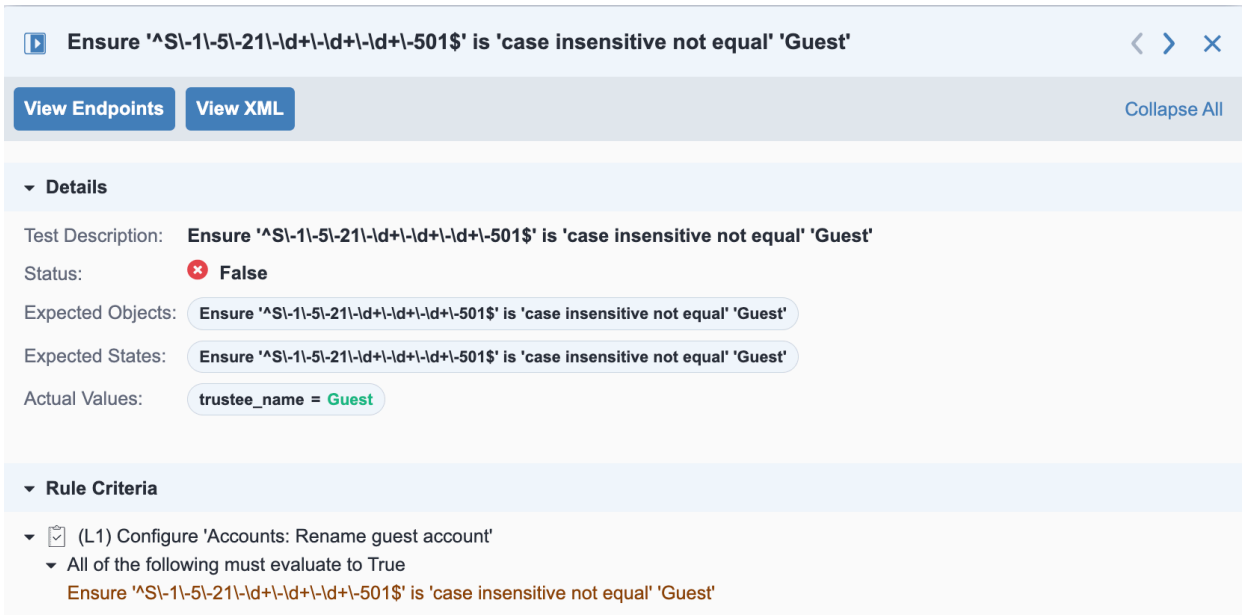
About this task

Click the arrow on a check in the Investigation/Benchmark Rule Details window to see details about that check. From this window, you can click the View Endpoints and View XML buttons.

- **View Endpoints** -

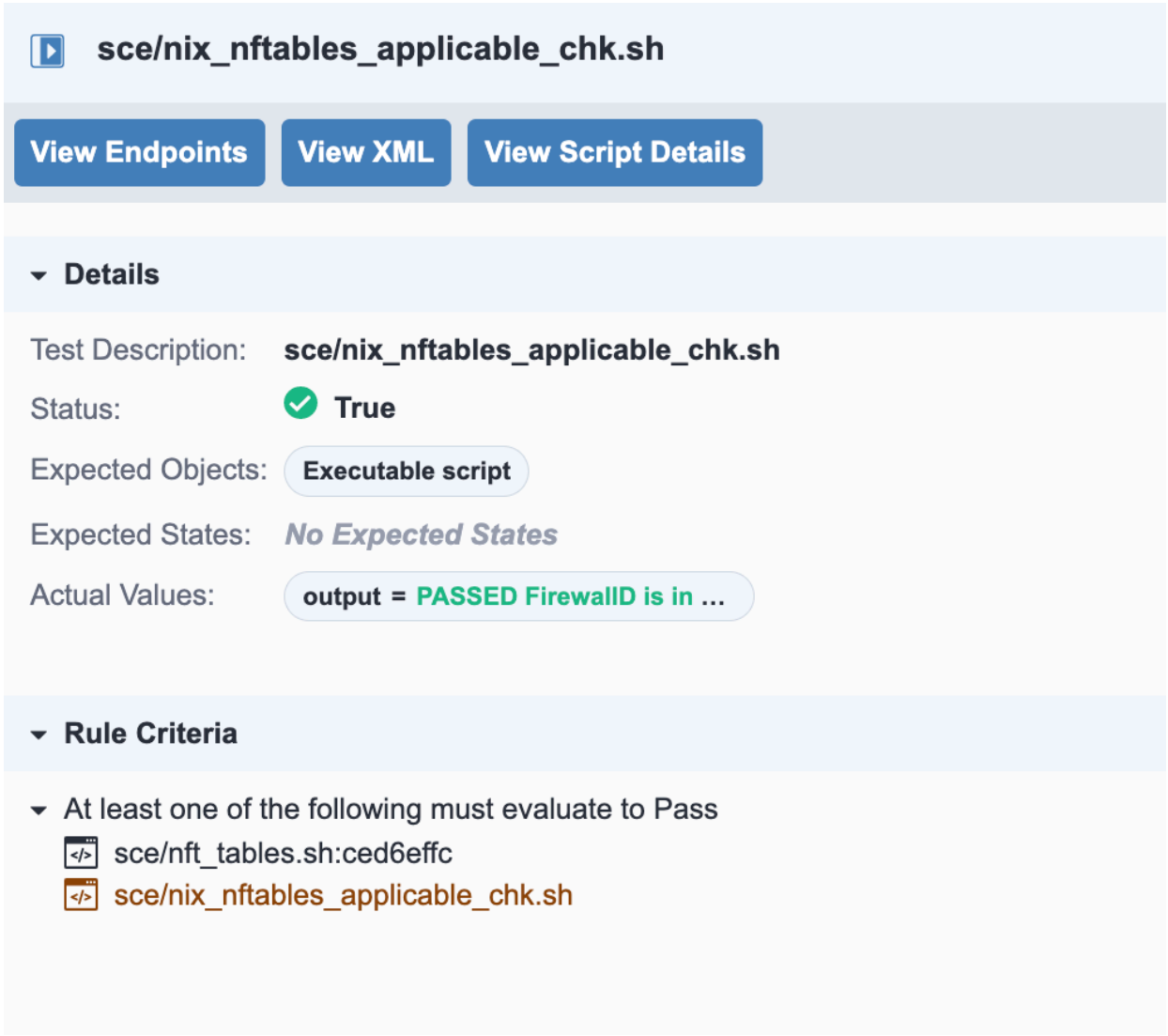
  Click this button to see all the endpoints that have the actual value for that check. This includes online and offline endpoints.

- **View XML** - Click this button to view the raw OVAL XML for this check. Viewing the XML shows you the details of what the check does. The first section is the test, and the next section is the expected object. The object has properties that are listed here. The next section is the expected state.



- **View Script Details** - Only SCE checks will have this additional button available. Click **View Script Details** to see the raw script that was run on the endpoint to find a specific check.

©2026 Tanium Inc. All Rights Reserved



Note: To collect actual values for compliance checks from an endpoint, you can use the **Comply - Compliance Investigation Details** sensor. This sensor has the following columns: Check ID, Test ID, and Actual Values.

- Check ID - A semicolon separated string that contains the Benchmark Name, Benchmark Version, Profile Name, Profile Version, and Rule ID.
- Test ID - The ID of the test that was evaluated on the endpoint.
- Actual Values - The values that were collected to evaluate the test with the specified Test ID.

©2026 Tanium Inc. All Rights Reserved

Investigate vulnerability findings

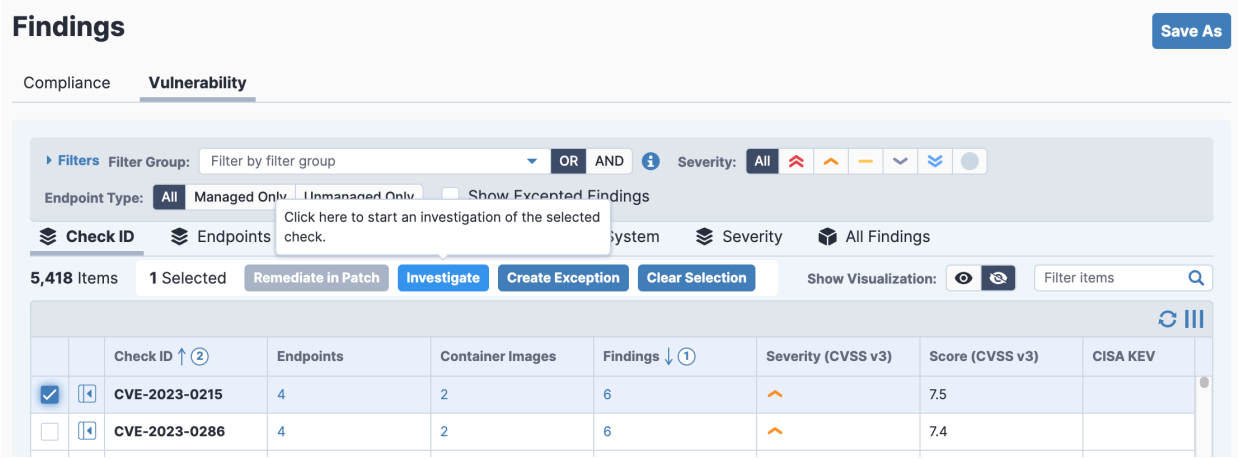
Investigate vulnerability findings by reviewing CVE details, comparing expected check values to actual endpoint values, and using the Vulnerability tab filters to focus on specific CVEs.

About this task

Vulnerability checks are defined through a vulnerability source, which is listed on the Standards page. Each source has a list of CVEs, and each CVE has vulnerability definitions and/or patch definitions. Each definition has a set of criteria or checks. When investigating vulnerability findings, you are examining the expected values for checks and comparing them to the actual values that were discovered on the endpoint.

To investigate vulnerability findings,

1. From the Main menu, go to **Modules** > **Comply > Findings**.
2. In the **Vulnerability** tab, from the **Check ID** or **All Findings** tabs, locate a particular CVE using any of the available filters.
3. Select the CVE **checkbox** and click the **Investigate** button to open the CVE Details window. (You can only investigate one CVE at a time.) You can also click the **Expand Details** arrow to open the flyout and click the Investigation button located there.



Vulnerability investigations

Review investigation details, check statuses, and analyze expected and actual values to understand how vulnerability and patch definitions apply to your endpoints.

In the Investigation/CVE Details window, there are several sections of information.

©2026 Tanium Inc. All Rights Reserved

- The **Details** section has the general data about the rule, including the CVE ID, the score and severity.

The table with the list of checks (also called tests) has several columns:

- **Status** - This indicates whether the endpoints listed for this check were found=**True**, not found=**False**, or experienced an **Error**. Note that it's the combination of checks that were found and not found that determine the vulnerability. There are two kinds of status errors. An OVAL **Error** indicates there was a problem collecting information or analyzing a check on the endpoint. An **Investigation Error** is a Tanium error, likely a Tanium Interact TSE-error. For more information, see Tanium Interact User Guide: Troubleshooting.

- **Test Description** - This text is taken from the OVAL content for that check.

- **Expected Objects** - The type of object that is expected to be checked on the endpoint.

  > Note: **No Expected Objects** may be displayed if the OVAL Test definition for the test that was evaluated did not specify any Object. This can occur when there was an error reported for the particular investigation.

- **Expected States** - The property of the object being checked on the endpoint.

  > Note: **No Expected States** may be displayed if the OVAL Test definition for the test that was evaluated did not specify any State (or property) of the Expected Object. Note that States are not a required attribute of a Test. To satisfy the Test, it may be sufficient to simply specify the Object. An example of this would be to check for the existence of a File (no state is needed in this case).

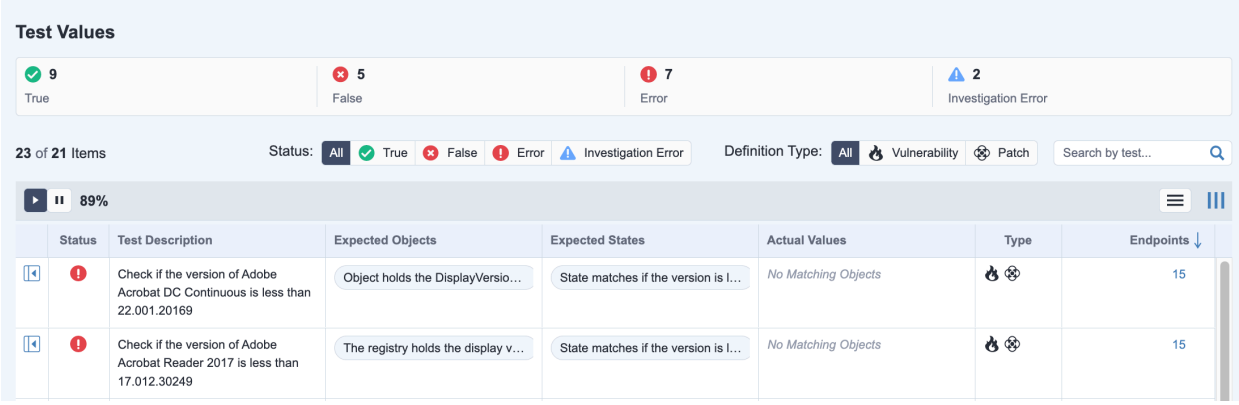
- **Actual Values** - The object found on the endpoint and all the associated properties for that object. The property names are in black and the actual values are in green.

  > Note: **No Matching Objects** may be displayed if there was no matching object found on the endpoint that matched the specified Expected Object.

- **Type** - This indicates the check was found in an OVAL **Vulnerability** definition or an OVAL **Patch** definition. Some check are found in both.

©2026 Tanium Inc. All Rights Reserved

- **Endpoints** - The number of endpoints that have the actual value listed for the check.

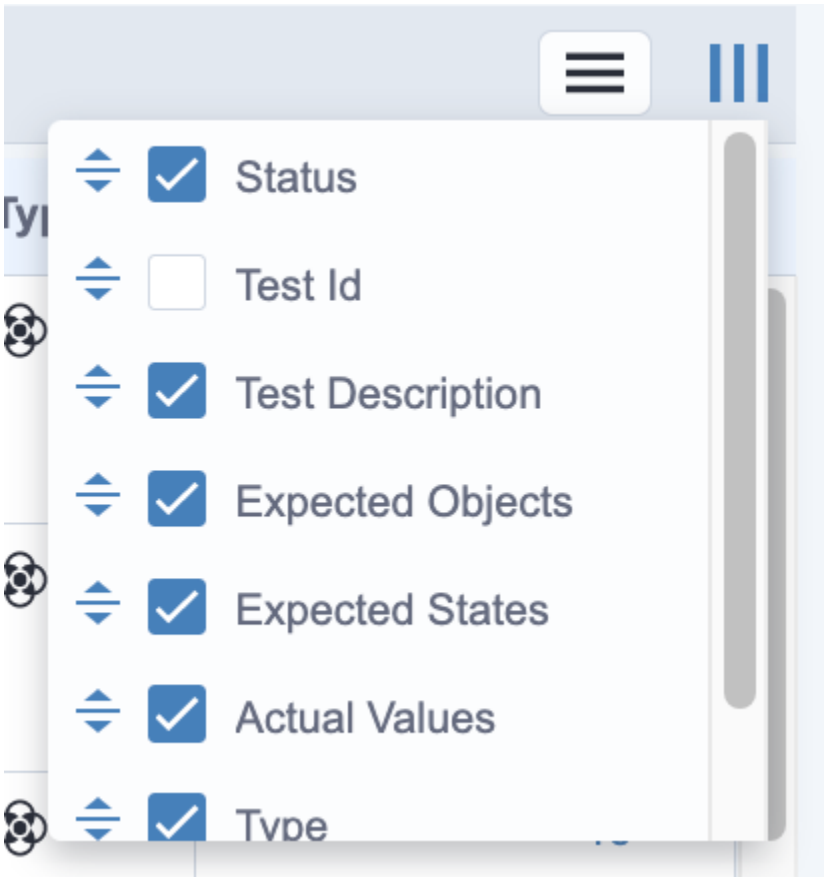


Filter tests list

Filter the tests list by status, definition type, or other available grid filters.

About this task

You can filter tests in the table by **Status**, **Definition Type**, or any of the other available grid filters.



©2026 Tanium Inc. All Rights Reserved

Expand Details

View detailed information about CVE investigation checks, related vulnerability and patch definitions, endpoints with actual values, and the raw OVAL XML used for each check.

About this task

Click the arrow on a check in the Investigation/CVE Details window to see details about that check, including the list of vulnerability definitions and/or patch definitions.

> **Note:** By default, only definitions that have the check are shown. If you want to see other definitions that are related to that CVE but do not include that check, you can deselect the **Has Test** checkbox and if there are any such definitions, they will be listed.

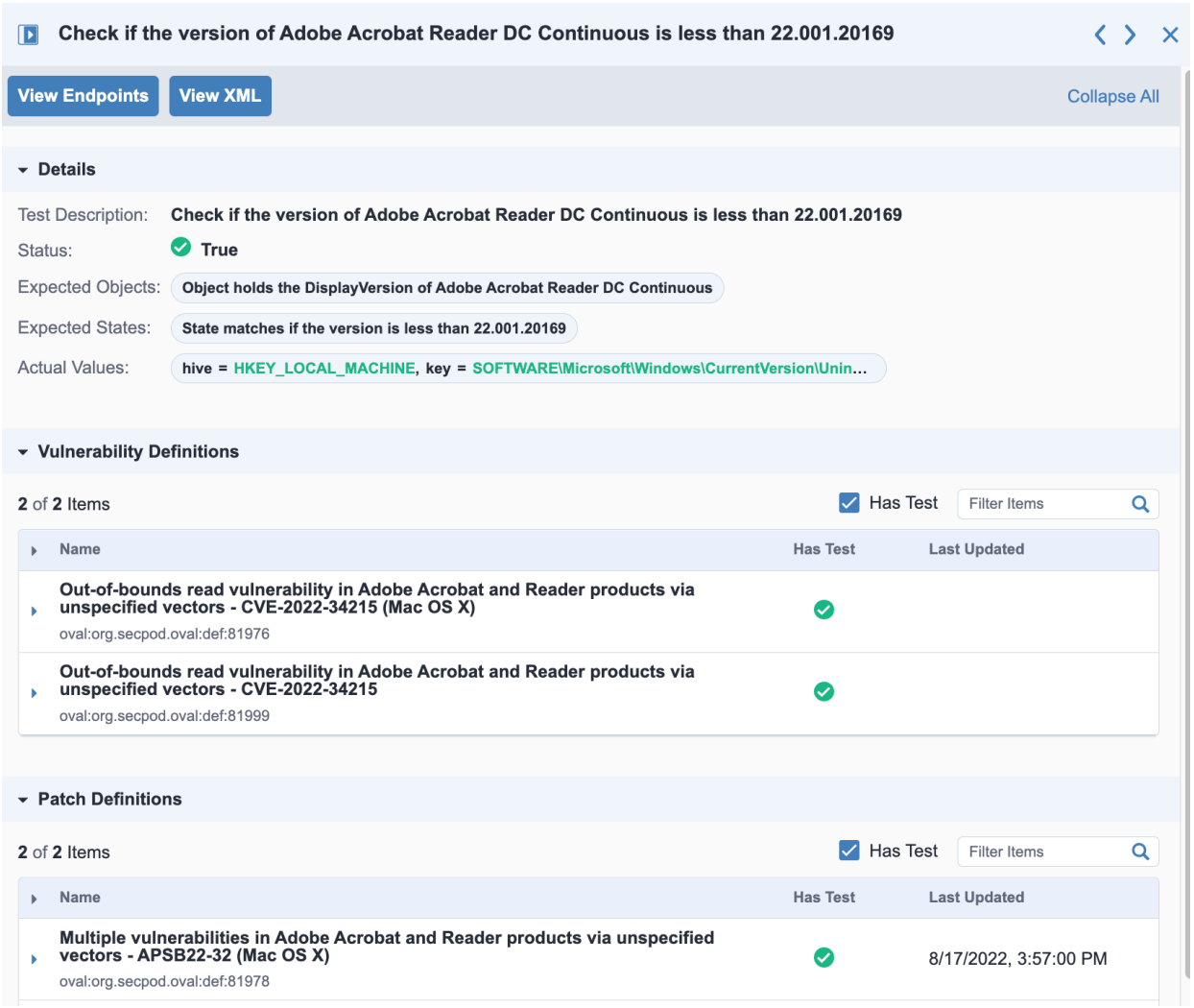
From this window, you can also click the **View Endpoints** and **View XML** buttons.

- **View Endpoints** -

  Click this button to see all the endpoints that have the actual value for that check.

- **View XML** - Click this button to view the raw OVAL XML for this check. Viewing the XML shows you the details of what the check does.

©2026 Tanium Inc. All Rights Reserved



Note: To collect actual values for vulnerability checks from an endpoint, you can use the **Comply - CVE Investigation Details** sensor. This sensor has the following columns: Check ID, Test ID, and Actual Values.

- Check ID - The CVE ID.
- Test ID - The ID of the test that was evaluated on the endpoint.
- Actual Values - The values that were collected to evaluate the test with the specified Test ID.

©2026 Tanium Inc. All Rights Reserved

Identify CVEs in error or unknown state

Use the **Comply - CVE Status** sensor to identify CVEs in an **error** or **unknown** state that might indicate false negatives and gaps in vulnerability coverage.

About this task

The **Comply - CVE Status** sensor returns CVEs from the Comply database that are in an **error** or **unknown** evaluation state. CVEs in these states are not included in findings, so they might represent false negatives — vulnerabilities that exist on an endpoint but are not reported. Use this sensor to identify gaps in vulnerability coverage across your environment at scale.

Common causes of error or unknown states include PowerShell or WMI timeouts and scan engine issues during definition evaluation.

The sensor returns the following columns:

- **CVE** - The CVE identifier, for example CVE-2020-0810.
- **Status** - The evaluation state: **error** or **unknown**.

To use this sensor, search for **Comply - CVE Status** in Tanium Interact. For more information, see Tanium Interact User Guide: Asking questions.

Export investigations

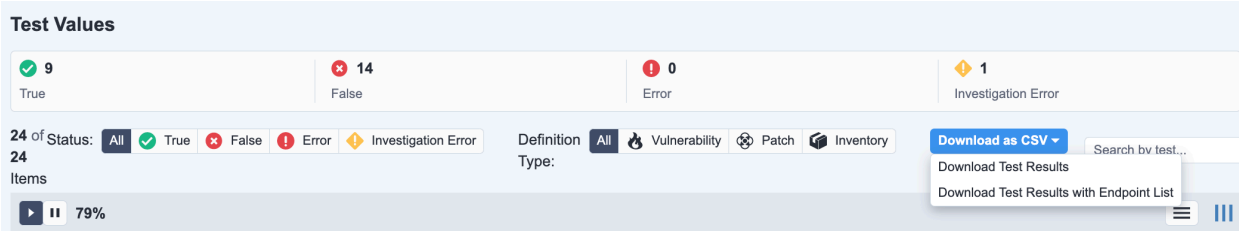
Export investigation results to a CSV file, customize the export options, and download the file when it is ready.

About this task

You can export investigations to a CSV file by doing the following:

1. Go to the Compliance or Vulnerability Investigation window, click the **Download as CSV** button.
2. Select **Download Test Results** or **Download Test Results with Endpoint List**. Downloading results with endpoints takes longer than downloading without that information.

©2026 Tanium Inc. All Rights Reserved

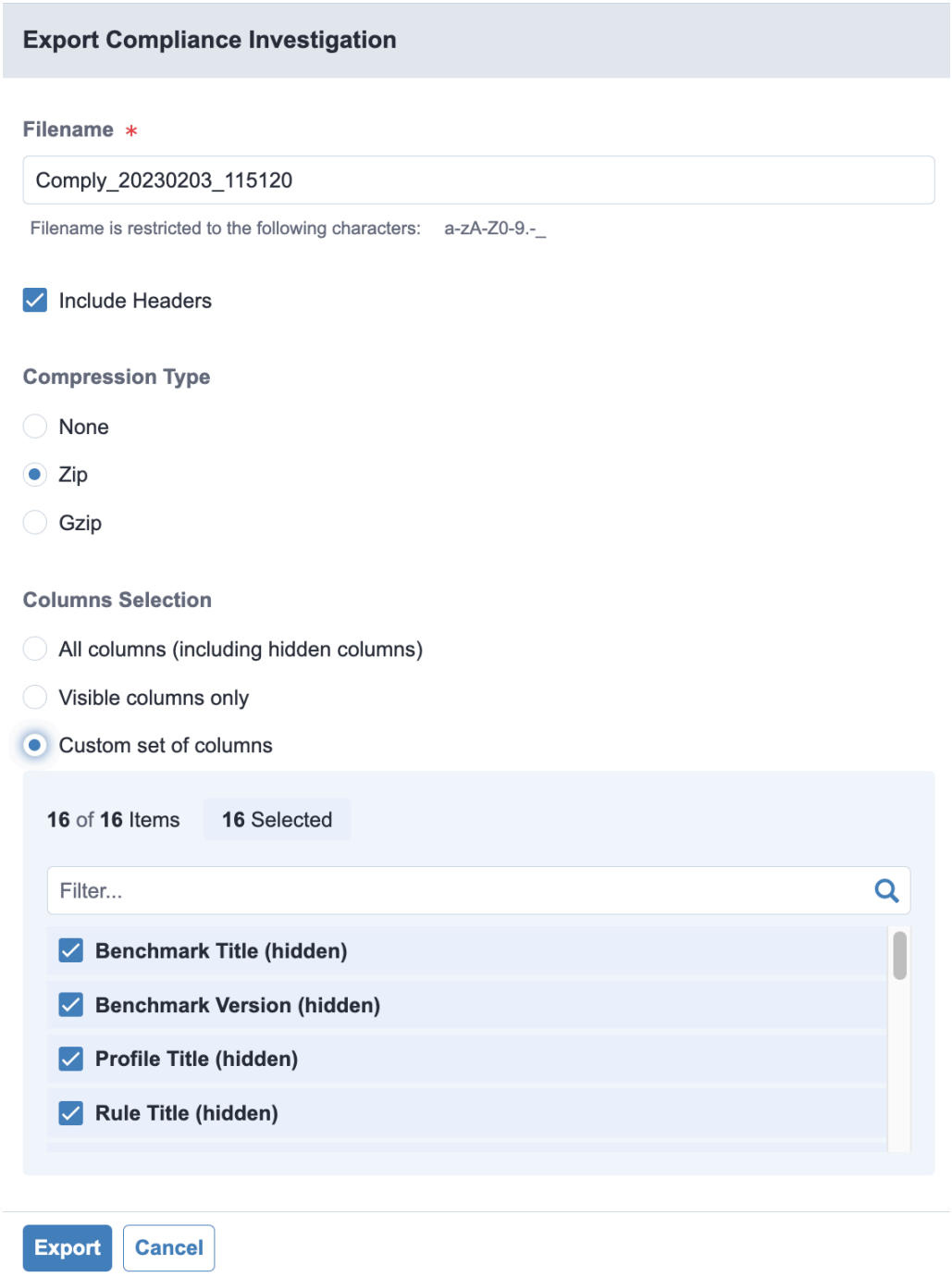


3. Enter the following information into the **Export** window.
    - **Filename**-

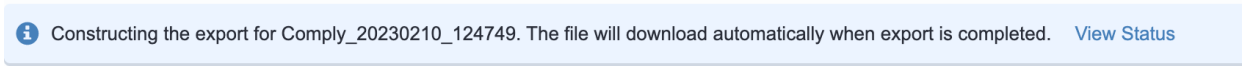
      Use the default filename or enter your own name.

    - **Include Headers**-This is selected by default.
    - **Compression Type** - Choose None, Zip (default), or Gzip.
    - **Columns Selection**:
        - **All columns (including hidden columns)**-In addition to the columns available in the Test Values grid, select this option to also include columns from the Details view.
        - **Visible columns only**-Only include items visible in the Test Values grid.
        - **Custom set of columns**-Select this option to choose which columns to include from a provided list.

©2026 Tanium Inc. All Rights Reserved



4. Click the **Export** button.
   When the CSV file is ready, it is automatically downloaded. A message at the top of the Investigation window lets you know the export file is building.



   Click **View Status** in the message to go to the **Reports** > **Exports** tab. The status will display on the Exports tab and then disappear once the file is ready.

©2026 Tanium Inc. All Rights Reserved

Important: Unlike other exports, this file is not saved in the **Reports** > **Exports** tab.

©2026 Tanium Inc. All Rights Reserved

Remediating findings

Use Tanium Comply with Tanium Patch or Tanium Deploy to remediate vulnerability findings on endpoints within a single workflow.

About this task

Remediation visibility uses Tanium Comply to scan for vulnerabilities on endpoints and Tanium Patch or Tanium Deploy to remediate discovered vulnerabilities as part of one workflow.

Tanium Patch is required for OS patch remediations. If a Comply scan finds that an endpoint is vulnerable to a CVE and there is a patch that remediates the CVE on the endpoint operating system, you can use the provided workflow to apply the patch. For OS patch remediations, a direct match is made between the CVE and the patch that is known to remediate it. After the patch is applied, the finding should no longer appear in Comply. For more information, see Configure an OS patch remediation on page 245.

Tanium Deploy is required for software update remediations. If a Comply scan finds that an endpoint is vulnerable to a CVE in a software application, you can use the provided workflow to deploy a software update. Remediating with a software update is different from remediating with an OS patch in that there is an association made between the software and the CVE, but there is no direct match made between the CVE and a particular software version. Therefore, the software update you deploy may or may not remediate the CVE. When you run another scan, the finding could still be present. For more information, see Configure a software update remediation on page 252.

Configure an OS patch remediation

Configure OS patch remediations in Tanium Comply using Tanium Patch data, required sensors, and appropriate RBAC permissions.

About this task

Before you begin

- OS patch remediation requires the following Tanium modules:
    - Tanium™ Patch

©2026 Tanium Inc. All Rights Reserved

    - Tanium™ Interact
    - Tanium™ Connect
- Remediating with OS patches requires that both Tanium Comply scans and Tanium Patch scans are running on endpoints.
- The following sensors are required and are registered with TDS by default:
    - **Patch - Applicable Patch Status by CVE**. This sensor is hidden by default. It has a 12 hour max age. Therefore if you make changes in Patch, it takes time for those changes to appear in the Remediations view. If you install Patch after Comply, it also takes some time before data appears on the Remediations page, even though the Remediations page itself might appear fairly quickly. For more information, see Register or unregister sensors for collection.
    - **Comply - Vulnerability Findings Details**
    - **Operating System Generation**
    - **OS Platform**
- RBAC privileges:
    - You must have the required Patch permissions for viewing and configuring Patch lists and Block lists. For more information, see Patch User Guide: User role requirements.
- Only findings from client-based OVAL scans are available in Remediations.
- Excepted findings are not included in Remediations. For more information, see Creating exceptions for findings on page 216.

View findings

Learn how to view Comply scan findings for OS patches, including aggregated patch information and detailed vulnerability and endpoint data in the **RemediationsOS Patches** tabs.

If a Comply scan shows that an endpoint is vulnerable to a CVE, and there is an unscheduled patch that would remediate that CVE, a finding with information on the CVE, the vulnerable endpoint(s), and the unscheduled patch appears on the **Remediations** > **OS Patches** tab as described in the following sections.

©2026 Tanium Inc. All Rights Reserved

In the **Remediations** > **OS Patches** tab, there are two tabs as follows:

Patches - This tab contains the information found in the **Actionable Findings** tab and aggregates it into categorized lists. The total number of findings with CVEs that can be remediated by the same patch are listed together as a line item where you can take Patch Action. Click the number in the **Total Findings** column to see all the individual findings listed for that patch.

- **Top 5 unscheduled patches** - The top 5 patches listed on the **Patches** tab are determined by Patch Severity sorted by CVE severity for each severity category from Critical to Unscored.

Actionable Findings - This tab contains the raw findings from scans, including the following information:

- **Check ID** - The check ID of the vulnerability known to be resolved by the corresponding patch.
- **Patch Title and Severity** - The name of the patch and its known severity.
- **Patch UID** - (hidden by default) The latest superseding patch applicable to the CVE (if the supersedence chain is available).
- **CVE information** - The year, score, and if the vulnerability is on the CISA KEV list.
- **Endpoint information** - Details for the endpoint with the discovered vulnerability.
- **Endpoint criticality** (Hidden by default) - The criticality level, low, medium, high, critical, of the endpoint.

Filter findings

Filter findings by computer group, severity, operating system, and other criteria, or use the Filter Builder with Tanium Data Service to create custom filters.

About this task

You can filter the findings view as follows:

- **Standard Filter** - At the top level, you can filter by **Computer Group**. Click within the edit field to add multiple groups to the filter. You can also apply the **OR** and **AND** buttons to the selected computer groups.

©2026 Tanium Inc. All Rights Reserved

You can also filter by **Patch Severity** and **CVSS Base Severity**.

- Expand **Filters** to filter findings by **Check ID**, Show/Hide **CISA Known Exploited Vulnerabilities (KEV)**, **CVE Year**, **Endpoint** name, **IP Address**, **Operating System Generation**, **Operating System**, **Patch Title**, **Patch UID**, **Patch Status**, **CVSS Base Score (CVSS 3)**, and **EPSS Score**.

- **Filter Builder** - Click **Filter Builder** in the **Filters** section to create your own filter. With the filter builder, you can filter findings using Comply Tanium Data Service (TDS) and additional TDS harvested sensors, including the **Patch - Applicable Patch Status by CVE** sensor. For more information, see Filter builder on page 201.

Remediate actionable findings

Use the **Patch Actions** options in the **OS Patches** tab to create or update patch and block lists in Tanium Patch and deploy remediations to applicable endpoints.

About this task

From the **Remediations** > **OS Patches** tab, you can take an action on the aggregated findings listed in the **Patches** tab, such as adding the unscheduled patch to a Patch list or a Block list. This action takes you into Tanium Patch where you can then target and deploy the remediation to endpoints.

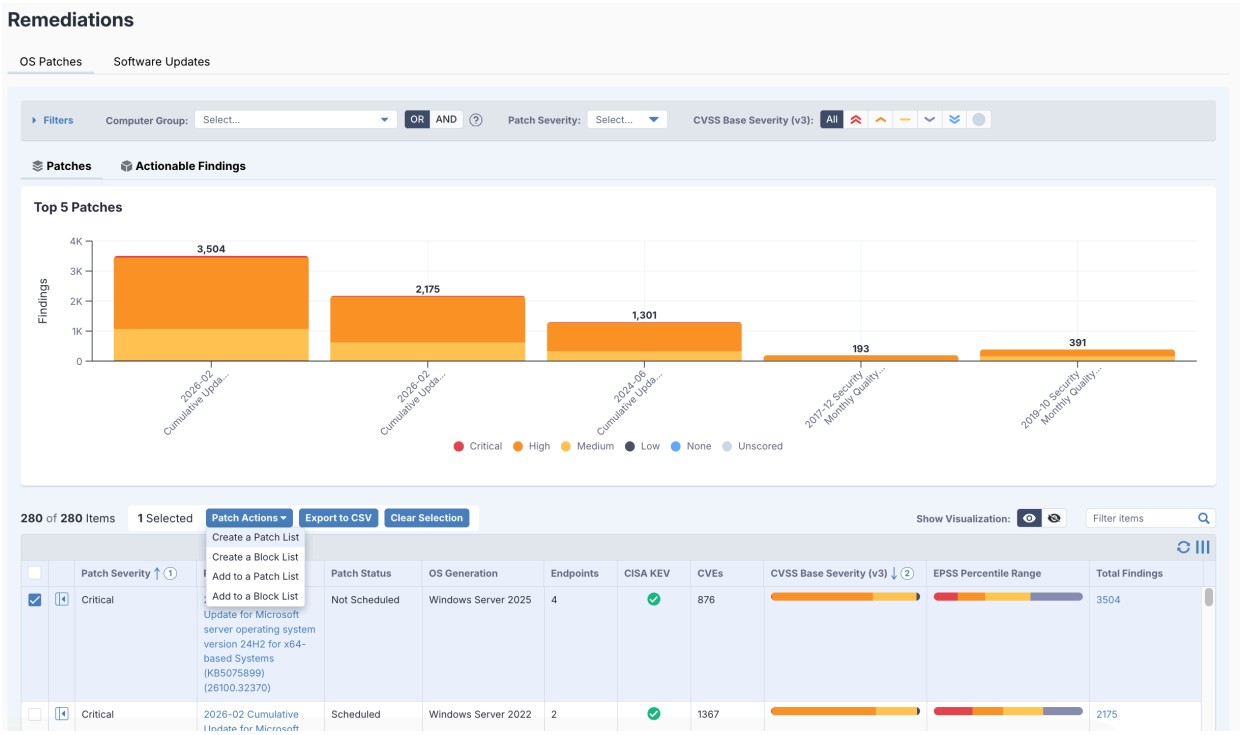
Note: You must have the appropriate Patch RBAC permissions for viewing and creating Patch Lists and Block Lists.

Important: The Patch Actions you configure in Comply are applied to the patch, not to the endpoint.

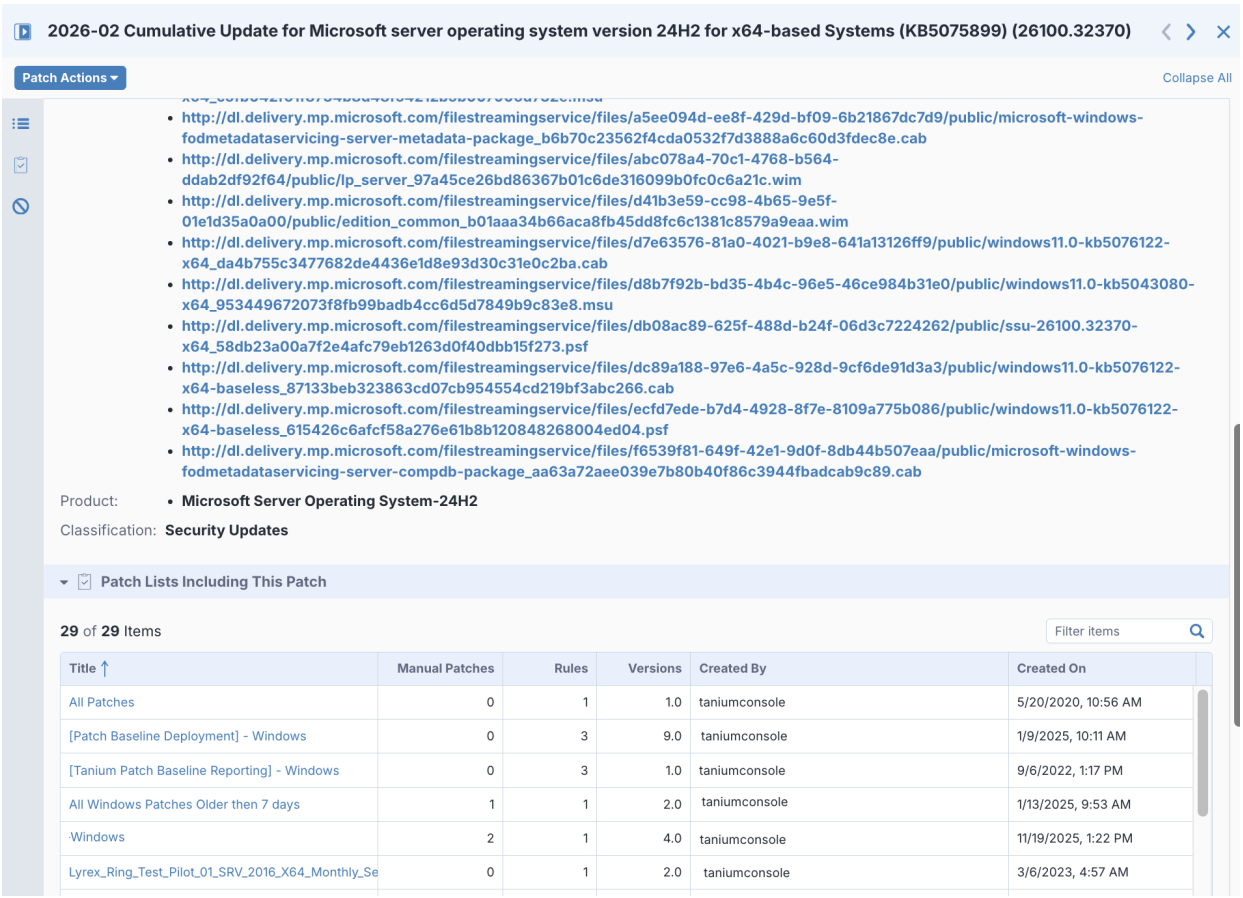
To perform a Patch action, do the following:

1. From the Main menu, go to **Modules** > **Comply > Remediations** > **OS Patches**.
2. In the **Patches** tab, items are listed by total number of findings with CVEs that can be remediated by the same patch. Select the checkbox next to a finding or open the side panel to access the **Patch Actions** button.

©2026 Tanium Inc. All Rights Reserved



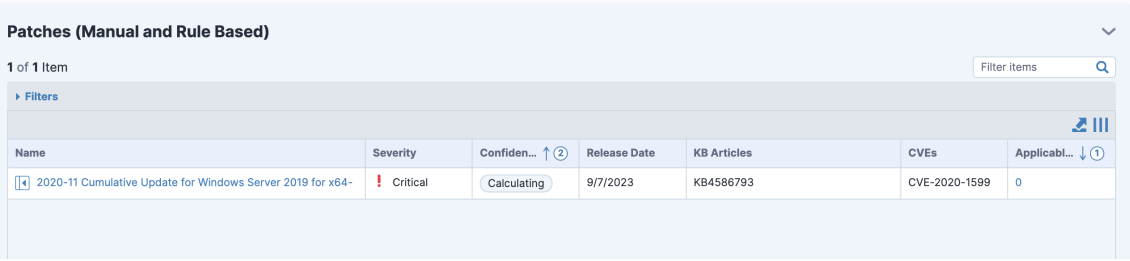
The side panel for an item in the **Patch** tab shows you if this patch is already part of an existing patch list.



©2026 Tanium Inc. All Rights Reserved

3. From the **Patch Actions** button, select **Create a Patch List**, **Create a Block List**, **Add to a Patch List**, or **Add to a Block List**. A pop-up for configuring your selection appears.
    - **Create a Patch List** - To create a patch list, enter a **Name** for the list and select a **Patch Content Set**. Click **Create Patch List**. This takes you to the **Patch** module > **Patch Lists** page where you can perform various actions on your newly created patch list. On the Patch Lists page in Tanium Patch, you can see the unscheduled patch Name, Severity, Confidence Score, Release Date, KB Articles, CVEs, and Applicable Endpoints.

      Note: After you perform a Patch Action and pivot to the Patch module, it takes time for the Applicable Endpoints column to update in Patch and may appear as 0 Applicable Endpoints at first. Also note that the number of Applicable Endpoints may fluctuate as endpoints come on and offline.

    - **Create a Block List** - To create a block list, enter a **Name** for the list and select a **Patch Content Set**. Click **Create Block List**. This takes you to the **Patch** module > **Block Lists** page where you can perform various actions on your newly created block list.
    - **Add to a Patch List** - To add to an existing patch list, select a **Patch List** from the provided options. Click **Add to Patch List**. This takes you to the Patch List you selected in the **Patch** module > **Patch Lists** page.
    - **Add to a Block List** - To add to an existing block list, select a **Block List** from the provided options. Click **Add to Block List**. This takes you to the Block List you selected in the **Patch** module > **Patch Lists** page.

Result

Note: See the Tanium Patch User Guide for more information about patch lists, block lists, and deploying patches to endpoints.

©2026 Tanium Inc. All Rights Reserved

Export remediation findings

Export remediation findings to a CSV file from the Patches or Actionable Findings tabs, and configure filename, headers, delimiter, and compression options.

About this task

You can export remediation findings by doing the following:

1. From the **Patches** tab or the **Actionable Findings** tab, select the checkbox next to one or more findings or open the side panel for a specific finding to access the **Export to CSV** button, or you can use the **Export All** button.
2. Click **Export to CSV** or **Export All** and enter the following information into the **Export Findings** window.
    a. **Filename** - Use the default filename or enter your own filename.
    b. **Include Headers** - This is selected by default.
    c. Select a **Delimiter** type: Comma, Semicolon, Single space, or Tab.
    d. Choose a **Compression Type** - None, Zip (default), or Gzip.
3. Click **Export**.

Result

Note: Patch columns are not available in Comply reports.

Investigate remediation findings

Use the Investigate feature to review remediation findings and identify the endpoint values that caused each issue.

About this task

For a remediation finding, you can use the Investigate feature to find the actual values on the endpoints that caused the issue.

From the **Actionable Findings** tab, select the checkbox next to a finding or open the side panel for a finding to access the **Investigate** button.

For more information, see Investigate vulnerability findings on page 236 and Investigating findings on page 229.

©2026 Tanium Inc. All Rights Reserved

Configure a software update remediation

Configure software update remediations that use Tanium Comply and Tanium Deploy scans, required sensors, and appropriate RBAC permissions to remediate client-based OVAL findings.

About this task

Before you begin

- Software update remediation requires the following Tanium modules and toolset:
    - Tanium™ Deploy
    - Tanium™ Endpoint Configuration Toolset version 2.28.89 or higher
    - Tanium™ Interact
- Remediating with software updates requires that both Tanium Comply scans and Tanium Deploy scans are running on endpoints.
- The following sensors are required and are registered with TDS by default:
    - **Deploy - CVE Software Packages, Deploy - CVE Software Packages Details** - Retrieves confidence level for software deployments.
    - **Comply - Vulnerability Status, Comply - Vulnerability Findings Details** - Retrieves CVEs on the endpoint.
    - **Note:** Deploy - CVE Software Packages and Comply - Vulnerability Findings Details are combined to retrieve deployment information and CVE information from the endpoint.
- RBAC privileges:
    - You must have the required Deploy permissions for viewing and configuring software updates. For more information, see the Tanium Deploy User Guide: User role requirements.
- Only findings from client-based OVAL scans are available in Remediations.

©2026 Tanium Inc. All Rights Reserved

- Excepted findings are not included in Remediations. For more information, see Creating exceptions for findings on page 216.

View findings

Use the **RemediationsSoftware Updates** tab to view CVE findings, related software packages, and deployment status so you can prioritize and remediate vulnerable endpoints.

If a Comply scan shows that an endpoint is vulnerable to a CVE, and there is a software update that could remediate that CVE, a finding with information on the CVE, the vulnerable endpoint(s), and the unscheduled software update appears on the **Remediations** > **Software Updates** tab as described in the following sections.

In the **Remediations** > **Software Updates** tab, there are two tabs as follows:

Software Packages - This tab contains the information found in the **Actionable Findings** tab and aggregates it into categorized lists based on software package and its deployment progress. Click on the number in the **Total Findings** column and you can see all the individual findings listed for that software package.

- **Top 5 Software Packages** - The top 5 software packages listed on the **Software Packages** tab are determined by available software packages sorted by CVE severity for each severity category from Critical to Unscored.

Actionable Findings - This tab contains the raw findings from scans, including the following information:

- **Check ID** - The check ID of the vulnerability that may be resolved by the corresponding software package.
- Software **Vendor** and Package **Title** - Click on the **Title** to go to the Deploy software package gallery.
- **Confidence** - The confidence rates the probability that a gallery package deployment will succeed. Tanium bases the score on execution success and performance metrics that endpoints across all Tanium environments returned for previous deployments of the package.
- **Deploy Progress** - The status may be any of the following:

©2026 Tanium Inc. All Rights Reserved

- **Scheduled** - A deployment is already targeting the endpoint to update the software package.
- **Not Scheduled** - There is currently no deployment targeting the endpoint to update the software package. This is the status you would target for a Deploy action in Comply.
- **Pending** - A deployment to update the software package using Deploy's automatic deployment configuration is already targeting the endpoint. This means it will deploy once the ring criteria is met. For more information, see the Tanium Deploy User Guide: Automatically deploying software.

- **Update eligibility** - **Eligible** indicates that the endpoint meets the system requirements and applicability rules defined in the software package. **Ineligible** indicates that the endpoint does not meet the requirements.. For more information, see the Tanium Deploy User Guide: View software package applicability.
- **Endpoint criticality** (Hidden by default) - The criticality level of the endpoint: low, medium, high, or critical.

Filter findings

Filter findings by computer group, severity, deployment status, eligibility, and advanced criteria using standard filters or the Filter Builder.

About this task

You can filter the findings view as follows:

- **Standard Filter** - At the top level, you can filter by **Computer Group**(s). Click within the edit field to add multiple groups to the filter. You can also apply the **OR** and **AND** buttons to the selected computer groups.

  You can also filter by **CVSS Base Severity**, **Deploy Progress**, and **Update Eligibility**.
- Expand **Filters** to filter findings by **Check ID**, **CISA Known Exploited Vulnerabilities (KEV)**, **CVE Year**, **Endpoint** name, **IP Address**, **Operating System Generation**, **Operating System**, **Platform**, **Vendor**, **Title**, **Version**, **Confidence**, **CVSS Base Score (CVSS 3)**, and **EPSS Score**.
- **Filter Builder** - Click **Filter Builder** in the **Filters** section to create your own filter. With the

©2026 Tanium Inc. All Rights Reserved

filter builder, you can filter findings using Comply Tanium Data Service (TDS) and additional TDS harvested sensors, including the **Deploy - Software Packages** sensor. For more information, see Filter builder on page 201.

Remediate actionable findings

Use Deploy actions in the Comply Remediations and the Software Updates workflow to bundle or automatically deploy software updates that remediate actionable findings on endpoints.

About this task

From the **Remediations** > **Software Updates** tab, you can take a Deploy action on the aggregated findings, such as adding the unscheduled software update to an Automatic Deployment Configuration or adding to an existing software bundle. When you select a Deploy Action, this takes you into Tanium Deploy where you can then target and deploy the software updates to endpoints.

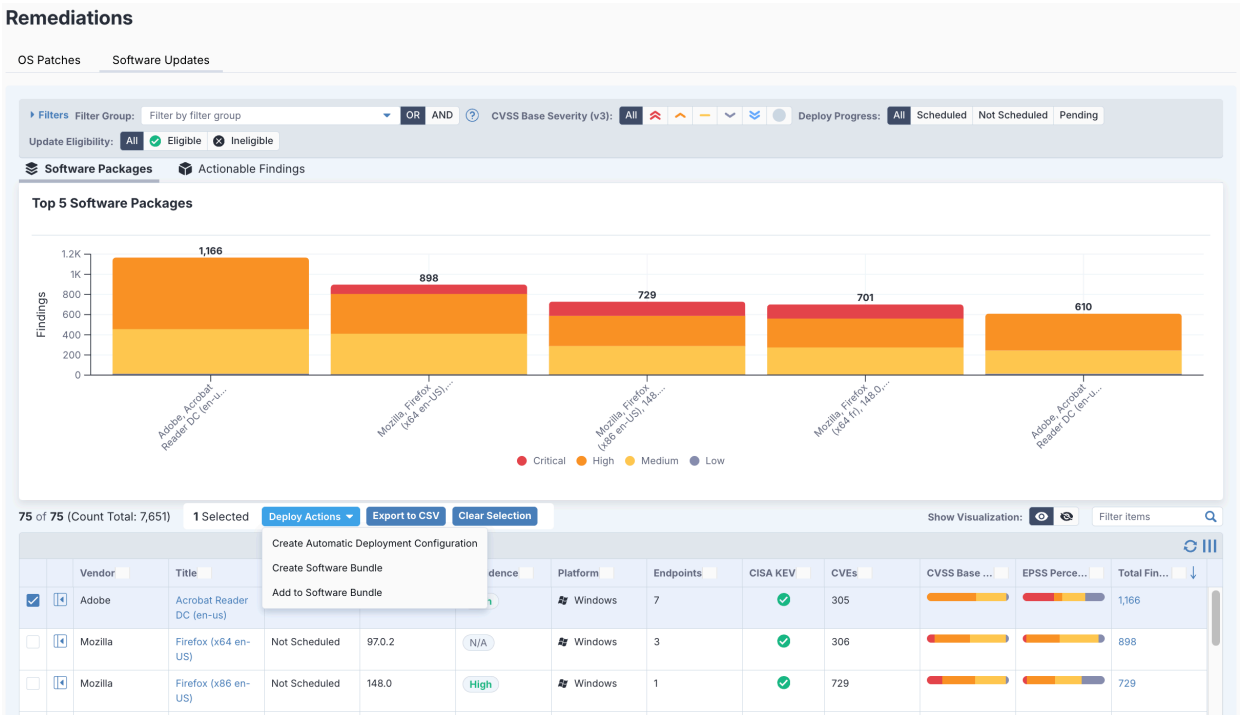
Note: You must have the appropriate Deploy RBAC permissions for viewing and creating Deploy Actions.

Important: The Deploy Actions you configure in Comply are applied to the software update, not to the endpoint.

To perform a Deploy action, do the following:

1. From the Main menu, go to **Modules** > **Comply > Remediations** > **Software Updates**.
2. In the **Software Packages** tab, items listed by total number of findings with CVEs may be remedied by the same software update, listed by **Vendor** and **Title**. Select the checkbox next to a software update or open the side panel to access the **Deploy Actions** button.
3. In the **Actionable Findings** tab, items listed by individual CVEs may be remedied by deploying a software update to a particular endpoint. Select the checkbox next to a finding or open the side panel to access the **Deploy Actions** button.

©2026 Tanium Inc. All Rights Reserved



4. From the **Deploy Actions** button, select **Create Automatic Deployment Configuration**, **Create Software Bundle**, or **Add to Software Bundle**.
    - **Create Automatic Deployment Configuration** - Select this option to pivot to the **Deploy** module > **Create Automatic Deployment Configuration** page. The software package and target endpoints are pre-populated in the Deploy form. For more information, see Deploy User Guide: Create an automatic deployment configuration.
    - **Create Software Bundle** - Select this option to pivot to the **Deploy** module > **Create Software Bundle** page. The software package and target endpoints are pre-populated in the Deploy form. For more information, see Deploy User Guide: Create a software package.
    - **Add to Software Bundle** - To add to an existing software bundle, select a **Software Bundle** from the provided options in the pop-up window. Click **Add to Bundle**. This takes you to the **Deploy** > **Edit Software Bundle** page where the software package you selected in Comply is added to an existing software bundle.
5. You can select multiple software updates or findings for Deploy actions, but they must be the same platform or some Deploy actions are not available.
6. If the software package that resolves the vulnerability is not already imported into Deploy, after you choose a Deploy Action, a pop-up appears and you must select which **Content Set** you want to import the software package into. After you make a selection, you are taken to

©2026 Tanium Inc. All Rights Reserved

the Deploy page that corresponds to the Deploy Action you selected.

7. Comply might find a vulnerability in a software application that is installed in multiple locations, and Deploy does not target those multiple locations for installations. Therefore, Deploy could display that there is an eligible software update, but not install that update in the directory where Comply found the vulnerability. In that case, the finding would still appear after the update is installed. You can use the **Investigate** feature in the **Actionable Findings** tab to compare locations to see if this is the issue.
8. See the Deploy User Guide for more information about deploying software packages.

Export remediation findings

Export remediation findings to a CSV file from the Software Updates or Actionable Findings tabs, and configure filename, headers, delimiter, and compression options.

About this task

You can export remediation findings by doing the following:

1. From the **Software Updates** tab or the **Actionable Findings** tab, select the checkbox next to one or more findings or open the side panel for a specific finding to access the **Export to CSV** button, or you can use the **Export All** button.
2. Click **Export to CSV** or **Export All** and enter the following information into the **Export Findings** window.
    a. **Filename** - Use the default filename or enter your own filename.
    b. **Include Headers** - This is selected by default.
    c. Select a **Delimiter** type: Comma, Semicolon, Single space, or Tab.
    d. Choose a **Compression Type** - None, Zip (default), or Gzip.
3. Click **Export**.

Result

Note: Deploy columns are not available in Comply reports.

Investigate remediation findings

Use the Investigate feature from the **Actionable Findings** tab to view endpoint values that caused remediation findings and access related investigation tasks.

©2026 Tanium Inc. All Rights Reserved

About this task

For a remediation finding, you can use the Investigate feature to find the actual values on the endpoints that caused the issue.

From the **Actionable Findings** tab, select the checkbox next to a finding or open the side panel for a finding to access the **Investigate** button.

For more information, see Investigate vulnerability findings on page 236 and Investigating findings on page 229.

©2026 Tanium Inc. All Rights Reserved

Exporting findings and assessments

Export compliance and vulnerability findings and assessments from Tanium Comply to Connect destinations.

About this task

Create a connection in Tanium Connect to export compliance and vulnerability findings to Connect destinations, such as Email, File, HTTP, Socket Receiver, Splunk, and SQL Server.

Note: To export one assessment at a time, see Export an assessment on page 141.

Note: You can export findings and assessments using the API. For more information, see Reference: Gateway examples for Comply on page 365.

Before you begin

You must have access to Tanium™ Connect with the **Connect User** role and ensure scheduled connections do not run during Tanium upgrades.

You must have access to Tanium™ Connect with the **Connect User** role.

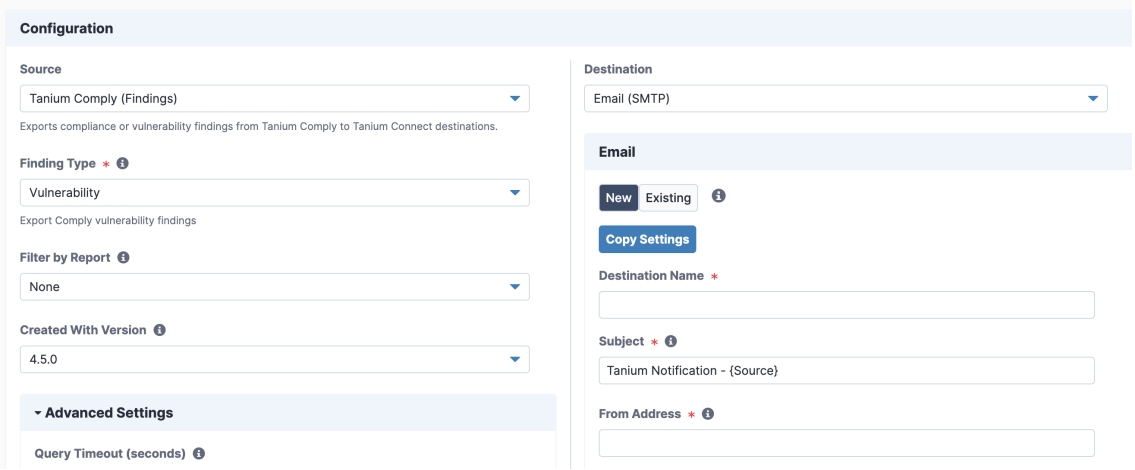
Important: Connections scheduled to run during an upgrade of Connect, or any Tanium solution configured as a connection source, might be interrupted or fail. Schedule your connections to run at a different time than your Tanium upgrades.

Exporting findings

Configure a Tanium Connect connection to export Comply findings data, customize columns and filters, and schedule the export to your chosen destination.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Connect**. Click **Connections** and then click **Create Connection**.
2. Enter a name and description for your connection in the **General Information** section.
3. In the **Advanced** section, set the following:
    - **Log level**: By default, the logging is set to **Information**. To reduce the amount of logging, you can set the log level to **Warning**, **Error**, or **Fatal**.
    - **Minimum Pass Percentage**: Minimum percentage of the expected rows that must be processed for the connection to succeed.
4. In the Configuration section set the **Source and Destination** as follows:
    a. Select **Tanium Comply (Findings)** as the **Source**.



    b. In the **Finding Type** list, select **Compliance**, **Vulnerability** (includes Remote Authenticated) or **Network Unauthenticated**.
    c. In the **Filter by Report** field, select a report to export only the findings that match the filters saved in that report. If you select **None**, all findings of the selected finding type are exported.
        - To export a subset of findings, such as the findings for a specific computer group, filter the findings on the **Findings** page, save the filtered findings as a report, and then select that report here. For more information, see Create a new Comply report on page 275.
        - The report type must match the **Finding Type**. A Compliance connection lists compliance reports, a Vulnerability connection lists vulnerability reports, and a Network Unauthenticated connection lists network unauthenticated reports.
        - For compliance and vulnerability reports, the filters saved in the report,

©2026 Tanium Inc. All Rights Reserved

including computer group filters, determine which findings are exported. The columns that you select in the **Columns** section of the connection determine the data exported for each finding.

- Tanium Connect reads the report each time the connection runs. Changes that you make to the report apply to the next run. If you delete the report, the connection fails until you select a different report.

d. In the **Created With Version** field, the version of the Comply findings source used to created the connection is displayed.
e. If needed, modify the **Advanced Settings** for the source:
   - **Query Timeout**: Specifies the timeout for the request.
   - **Batch Size**: Specifies how many rows are exported.

5. Configure the connection destination. Select a connection destination from the **Destination** list. Provide the configuration information for the destination you select. For more information, see Tanium Connect User Guide: Connection destinations.

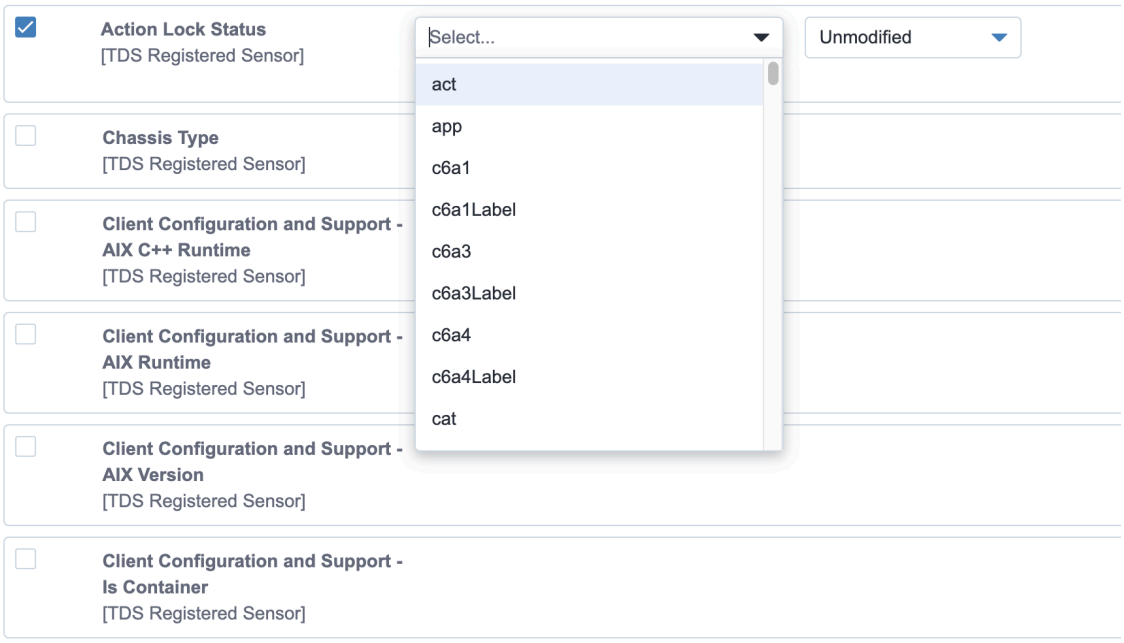
6. (Optional) In the Configure Output section, configure a **Filter**.
   You can use filters to modify the data that you are getting from your connection source before it is sent to the destination.

   For more information, see Tanium Connect User Guide: Configure filters.

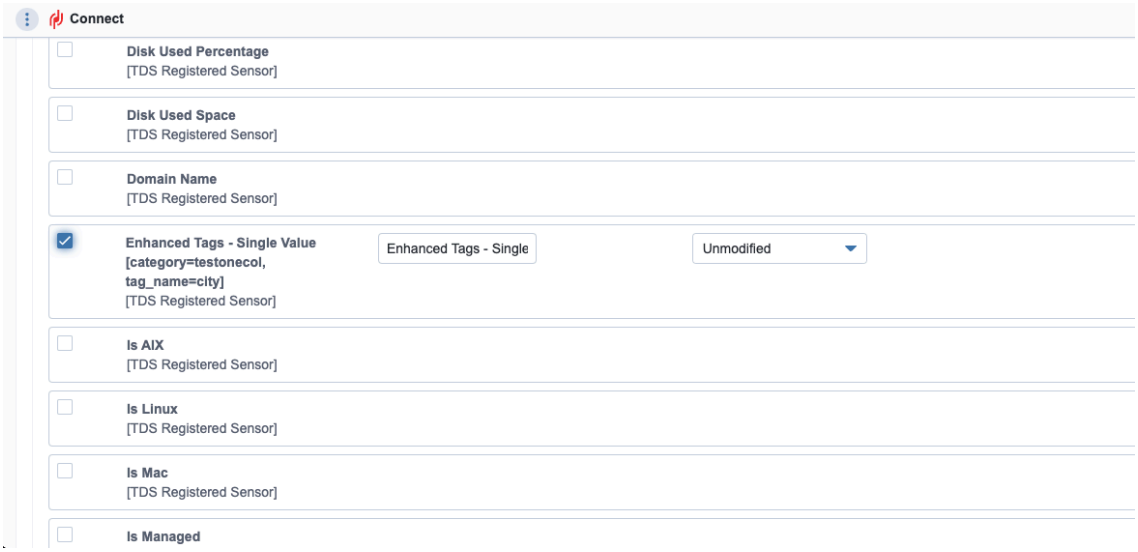
7. Configure the **Format** for the data. For information on configuring the format, see the section on the destination type that you selected in the Tanium Connect User Guide.

8. (Optional) You can customize columns for the exported data. In the **Columns** section, select the available **Source** items and configure the **Destination Label**, **Value Type**, and **Customization**, see Tanium Connect User Guide: Format data for emails. Note that customizing columns doesn't add new rows. It adds columns to existing rows.
   - Any sensor that is registered in TDS and only has a single column in its sensor definition will appear as an option under Columns with a **TDS Registered Sensor** label.

©2026 Tanium Inc. All Rights Reserved



- You can use Enhanced Tags to add labels to endpoints. If you are using an enhanced tag, it must be a single column sensor (Enhanced Tags - Single Value) and be harvested by TDS. For more information, see Enhanced Tags Documentation. (Also note that "Evaluation Terms" in enhanced tags are reserved values to use for column headers.)



Best Practice: For the best results, if you use any sensors with a TDS Registered Sensor label as a column customization, rather than updating an existing connection, create a new connection with these custom columns, then disable and delete your existing connection.

9. Configure the **Schedule** for the connection. For more information, see Tanium Connect User Guide: Schedule connections. Enable the connection to run on a schedule. Select **Enable**.

©2026 Tanium Inc. All Rights Reserved

You can set up the schedule when you configure the rest of the connection. If the schedule is not enabled, the connection only runs when you manually run it.

10. Click **Save** or **Save and Run**.

Result

Note: For more information, see Exported columns on page 267

Exporting vulnerability assessments

Export vulnerability or network unauthenticated assessment data from Tanium Comply to Tanium Connect destinations. This feature is deprecated; use Tanium Comply (Findings) as the source instead.

About this task

Create a connection in Tanium Connect to export data from vulnerability or network unauthenticated assessments to Connect destinations, such as Email, File, HTTP, Socket Receiver, Splunk, and SQL Server.

Note: SBOM findings can be exported using Tanium Connect, but exporting SBOM assessments is not supported.

Important: Exporting vulnerability assessments through Tanium Connect is a deprecated feature starting with Comply 2.22.15, which means it is available but is no longer receiving updates or active development. It is recommended you use **Tanium Comply (Findings)** as the source instead.

Create a connection

Create a connection to export vulnerability assessment findings, configure advanced settings and filters, and define the format, columns, and schedule for the exported data.

1. From the Main menu, go to **Modules** > **Connect**. Click **Connections** and then click **Create Connection**.
2. Enter a name and description for your connection in the **General Information** section.

©2026 Tanium Inc. All Rights Reserved

3. In the **Advanced** section, set the following:
    - **Log level**: By default, the logging is set to **Information**. To reduce the amount of logging, you can set the log level to **Warning**, **Error**, or **Fatal**.
    - **Minimum Pass Percentage**: Minimum percentage of the expected rows that must be processed for the connection to succeed.

4. In the Configure section set the **Source and Destination** as follows:
    a. Select **Tanium Comply (Assessments) - Deprecated** as the **Source**.
    b. In the **Assessment Type** list, **Vulnerability** is selected by default and is the only report type supported for use with Connect.
    c. Select an assessment from the **Assessment Name** list.
    d. If needed, modify the **Advanced Settings** for the source:
        - **Question Timeout**: Specifies the timeout for the request.
        - **Polling Interval**: Specifies how often Comply is polled for updated data while the connection is active.
        - **Batch Size**: Specifies how many rows are exported.
        - Optionally, select to **Include Errors** in the output.
        - **Question completion percentage**: The percentage of endpoints to provide responses from before exporting findings.

    e. Configure the connection destination. Select a connection destination from the **Destination** list. Provide the configuration information for the destination you select. For more information, see Tanium Connect User Guide: Connection destinations.

5. (Optional) Configure a **Filter**.
   You can use filters to modify the data that you are getting from your connection source before it is sent to the destination.

   For more information about the types of filters you can configure, see Tanium Connect User Guide: Configure filters.

6. Configure the **Format** for the data. For information on configuring the format, see the section on the destination type that you selected in the Tanium Connect User Guide.

7. (Optional) You can customize columns for the exported data. In the **Columns** section, select the available **Source** items and configure the **Destination Label**, **Value Type**, and **Customization**, see Tanium Connect User Guide: Format data for emails. Note that

©2026 Tanium Inc. All Rights Reserved

customizing columns doesn't add new rows. It adds columns to existing rows.

8. Configure the **Schedule** for the connection. For more information, see Tanium Connect User Guide: Schedule connections. Enable the connection to run on a schedule. Select **Enable**. You can set up the schedule when you configure the rest of the connection. If the schedule is not enabled, the connection only runs when you manually run it.
9. Click **Save** or **Save and Run**.

Result



Note: For more information, see Exported columns on page 267

Findings field descriptions

Use these field descriptions to understand how Comply sensors report compliance and vulnerability findings, including dates, states, and other attributes in exports.

The following fields have distinct differences. If you select to include **First Found Date, Last Found Date**, **Absolute First Found Date**, and **Last Scan Date** columns in exports, you should understand the distinctions with each sensor.

Sensor descriptions

Sensor	Description
Comply – Compliance Status	You should use this sensor to return the following data: • **Check ID** -The unique identifier for a Compliance rule. It is made up of the benchmark name, benchmark version, profile name, profile version, and rule id. • **State** - The result of the scan engine evaluation of the rule. (Many, but not all, of these are the same as Status Category). • **Category** - A computed value based on the state. The possible values for category are: fail, pass, error, informational. • **Rule ID** - The rule identifier for the benchmark rule. • **First Found Date** - This returns the first found date for all the unique compliance findings present on an endpoint. If the compliance finding state changes (from Pass to Fail, for example), this date is reset to the new discovery date. • **Last Scan Date** - This returns the last scan date for all the unique compliance findings present on an endpoint.

©2026 Tanium Inc. All Rights Reserved

Sensor	Description
	• **Excepted** - This returns true or false indicating whether it is an excepted finding. • **Scan Type** - Scan Method (Client-Based, Remote Authenticated) • **Max Cache Age** - The maximum age of the index cache, in seconds, that was acceptable when the scan ran. A value of 0 means the scan required a fresh index.
Comply – Vulnerability Status	You should use this sensor to return the following data: • **Check ID** - The CVE ID. For example, CVE-2020-0810. • **First Found Date** - This returns the first time a vulnerability is identified in an environment. Note that if a vulnerability is found and remediated and then found again, the first found date is set to the date of the most recent first finding. • **Last Found Date** - This returns the last found date for all observed vulnerabilities that the endpoint is currently vulnerable to. • **Absolute First Found Date** -This returns the very first time a vulnerability is found on an endpoint, and this date is not reset if the vulnerability is remediated. • **Last Scan** - This returns the last scan date for all observed vulnerabilities that the endpoint is currently vulnerable to. • **Scan Type** - Scan method, for example Client-Based, Remote Authenticated, Network Unauthenticated, SBOM (Software Bill of Materials), or Container Registries. • **Excepted** - This returns true or false indicating whether it is an excepted finding. • **Detected Products** - The list of vulnerable products associated with a finding on an endpoint. • **Detected CPEs** - The list of vulnerable CPEs associated with a finding on an endpoint. • **Max Cache Age** - The maximum age of the index cache, in seconds, that was acceptable when the scan ran. A value of 0 means the scan required a fresh index.

Test a connection and review data

Test a connection for a Comply report and review the resulting data and findings.

1. From the Main menu, go to **Modules** > **Connect**. Click **Connections**.
2. Click the connection that you created for your Comply report.
3. Click **Run Now**. Confirm that you want to run the connection.

©2026 Tanium Inc. All Rights Reserved

4. View the summary of the run.
5. View the assessment or finding in the destination that you configured for the connection.

Exported columns

Lists the columns included in CSV exports for each finding and assessment type, along with notes and limitations for specific fields.

The following columns are exported for each finding and assessment type.

Exported columns for findings and assessments

Compliance findings	Vulnerability findings	Network unauthenticated findings	Vulnerability assessments (deprecated as of Comply 2.22.15)
Computer Name	Computer Name	IP Address	computerName
IP Address	IP Address	MAC Address	ipAddress
Operating System Generation	Operating System Generation	MAC Vendor	CVE
Operating System	Operating System	Service Name	first_found_date
Rule	CVE	Service Port	absolute_first_found_date
Rule ID	Scan Type	Service Version	last_found_date
Standard	CVE Year	OS Name	last_scan_date
Standard Version	First Found Date	OS Version	score
Profile	Absolute First Found Date	CVE	title
Version	Last Found Date	CVE Summary	severity
Status Category	Last Scan Date	CVE Published	attack_vector
Status	Title	CVE Updated	oval_source
Description	Severity	CVE CVSS Score	oval_definition

©2026 Tanium Inc. All Rights Reserved

Compliance findings	Vulnerability findings	Network unauthenticated findings	Vulnerability assessments (deprecated as of Comply 2.22.15)
Rationale	CVSS Score	CVE Links	mitre_link
Fix Text	CVSS Vector	CISA KEV	nist_link
CCE	CVSS V2 Score	CISA Vendor	secpod_link
CCI	CVSS V2 Vector	CISA Product	solution_links
Severity	CVSS V2 Severity	CISA Vulnerability Name	created_date
First Found Date	CVSS V3 Score	CISA Short Description	last_modified_date
Last Scan Date	CVSS V3 Vector	CISA Required Action	remediations
Test ID [2] [3]	CVSS V3 Severity	CISA Notes	details
Expected Objects [2] [3]	CVE Created	CISA Date Added	criteria [1]
Expected States [2] [3]	CVE Modified	CISA Due Date	score_mapping
Actual Values [3]	MITRE Link		id_mapping
Scan Type	NIST Link		
Endpoint ID	Secpod Link		
Endpoint Criticality	Definition Title		
	Definition Last Modified		
	OVAL Definition		
	OVAL Source		

©2026 Tanium Inc. All Rights Reserved

Compliance findings	Vulnerability findings	Network unauthenticated findings	Vulnerability assessments (deprecated as of Comply 2.22.15)
	Solution Links		
	Remediations [3]		
	Remediation Details		
	Criteria [1]		
	Details		
	Detected Products [3]		
	Detected Common Platform Enumerations [3]		
	Common Platform Enumerations [3]		
	Affected Products [3]		
	Affected Platforms [3]		
	Test ID [2 3]		
	Expected Objects [2 3]		
	Expected States [2 3]		
	Actual Values [3]		
	CISA KEV		
	CISA Vendor		
	CISA Product		

©2026 Tanium Inc. All Rights Reserved

Compliance findings	Vulnerability findings	Network unauthenticated findings	Vulnerability assessments (deprecated as of Comply 2.22.15)
	CISA Vulnerability Name		
	CISA Short Description		
	CISA Required Action		
	CISA Notes		
	CISA Date Added		
	CISA Due Date		
	Endpoint ID		
	Image Hash		
	Image Name		
	Label		
	Registry		
	Patch Status		
	Patch Title		
	Patch UID		
	Patch Severity		
	Alias		
	CVSS v3 Temporal Score		
	CVSS v4 Score		
	CVSS v4 Severity		

©2026 Tanium Inc. All Rights Reserved

Compliance findings	Vulnerability findings	Network unauthenticated findings	Vulnerability assessments (deprecated as of Comply 2.22.15)
	CVSS v4 Threat Score		
	CVSS v4 Vector		
	EPSS Score		
	EPSS Percentile Range		
	EPSS Percentile		
	Max Maturity		
	Common Weakness Enumeration IDs		
	Common Weakness Enumeration Names		
	MITRE ATT&CK IDs		
	MITRE ATT&CK Names		
	Exploit Types		
	Ransomware Count		
	Botnet Count		
	Endpoint Criticality		

[1] Microsoft Excel does not properly handle line breaks in vulnerability CSV file exports. As a workaround, you can view the file with another tool or exclude the **criteria** column from the CSV export.

[2] Test ID, Expected Objects, and Expected States are hard-coded into the benchmark or OVAL definition and will not reflect user defined values.

[3] For endpoints in low resource mode, these columns may have no data due to Investigations not supporting low resource mode or due to other errors. Service versions can determine whether data appears in these columns, as well. For instance, the definitions

©2026 Tanium Inc. All Rights Reserved

Compliance findings	Vulnerability findings	Network unauthenticated findings	Vulnerability assessments (deprecated as of Comply 2.22.15)
of Affected Products and Affected CPEs were updated between versions.			

©2026 Tanium Inc. All Rights Reserved

Working with Comply reports

Learn how to access, interpret, and manage Comply reports to monitor compliance activities and support informed decision-making.

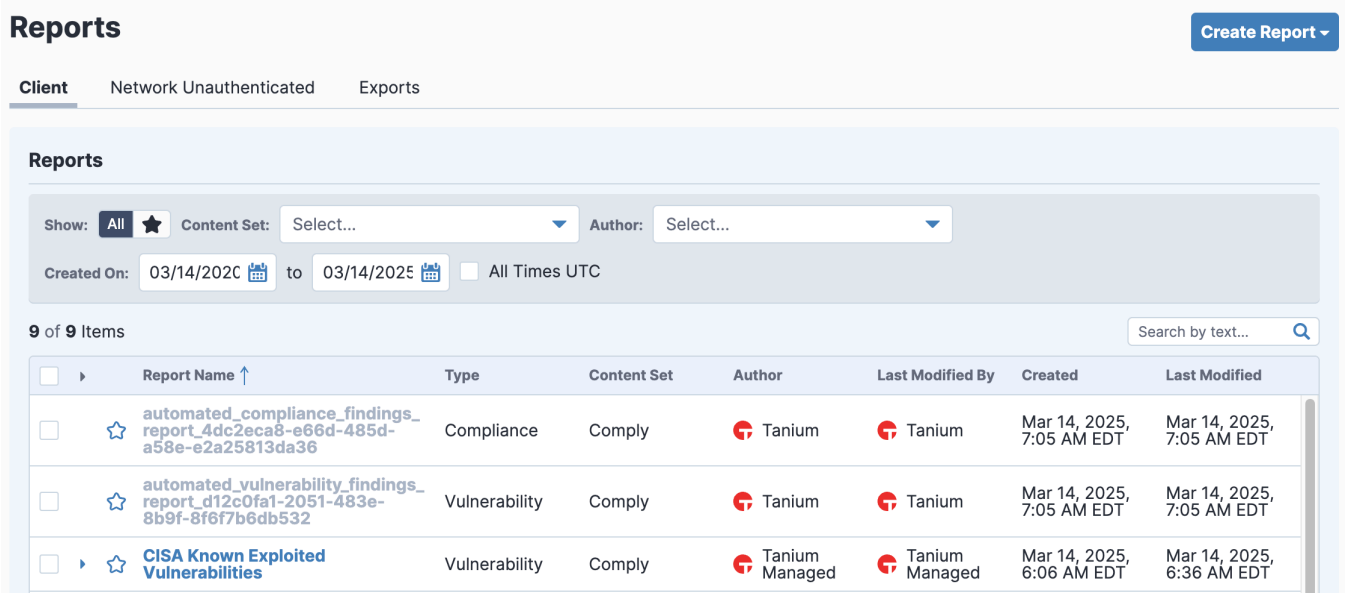
Viewing reports

Learn where different types of Comply reports appear in the console and how management rights are preserved for reports.

A report is a set of saved filters and groupings on a set of findings. You can create reports from findings, and you can create a report from another report.

- Compliance and vulnerability reports appear on the **Client** tab.
- Network unauthenticated reports appear on the **Network Unauthenticated** tab.

Comply provides some default reports:



©2026 Tanium Inc. All Rights Reserved

Note:

The **Management Rights: Preservation** setting is set to **On** by default. When this is set to **On**, the management rights of a report's original creator are preserved when the saved action for the report is recreated. The saved action is recreated when the report schedule is edited or when a report vulnerability feed is updated. With this setting, users who are not administrators can only change the schedule for reports they create.

Compliance report results

The compliance report results page displays report findings and lets you refine, save, or revert reports using filters, exception options, and action buttons.

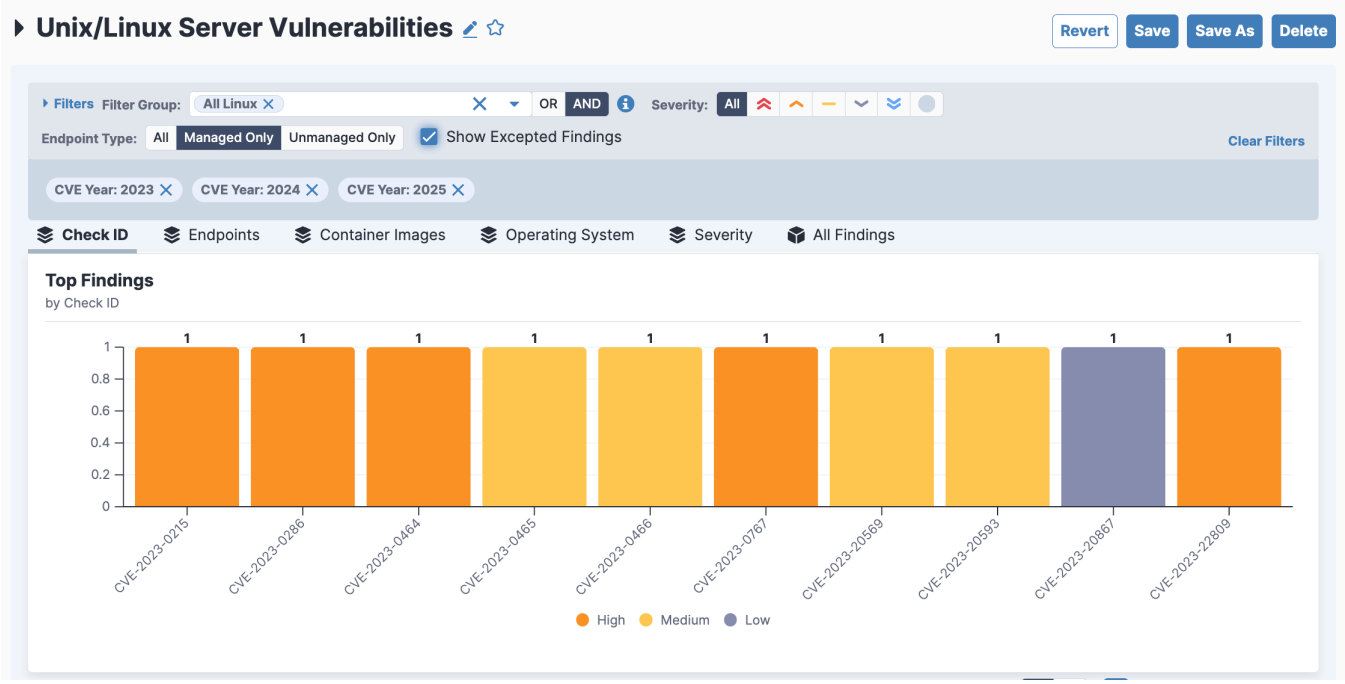
Click on a compliance report in the list to view the report details page. The details page is another view of the findings that were used to create the report. You can further refine or change the report by using the available filters and fields.

Optionally, select the checkbox to **Show Excepted Findings** if you have configured exceptions. For more information, see Creating exceptions for findings on page 216.



©2026 Tanium Inc. All Rights Reserved

Click the **Revert** button to undo changes and return to the original report. Click the **Save As** button to create a new report using the applied filters.



Vulnerability report results

View and refine vulnerability report findings, including excepted findings and detailed remediation instructions and solutions.

Click on a vulnerability report in the list to view the report details page. The details page is another view of the findings that were used to create the report. You can further refine or change the report by using the available filters and the **Save As** button to create a new report.

Optionally, select the checkbox to **Show Excepted Findings** if you have configured exceptions. For more information, see Creating exceptions for findings on page 216.

Click the **Get More Details** icon on a finding in a report for **Remediation Instructions** and a **Solution**.

Create a new Comply report

Create a new Comply report from the **Comply** > **Reports** > **Client** or the **Network Unauthenticated** tab, then choose a report type to open the related **Findings** page.

About this task

©2026 Tanium Inc. All Rights Reserved

Create a new report from the **Comply** > **Reports** > **Client** or **Network Unauthenticated tab**. Click the **Create Report** button and select a report type. This takes you to the **Findings** page for your selection. For more information, see Create reports from findings on page 215. Also see Creating vulnerability assessments on page 146.

Exporting Comply network unauthenticated reports

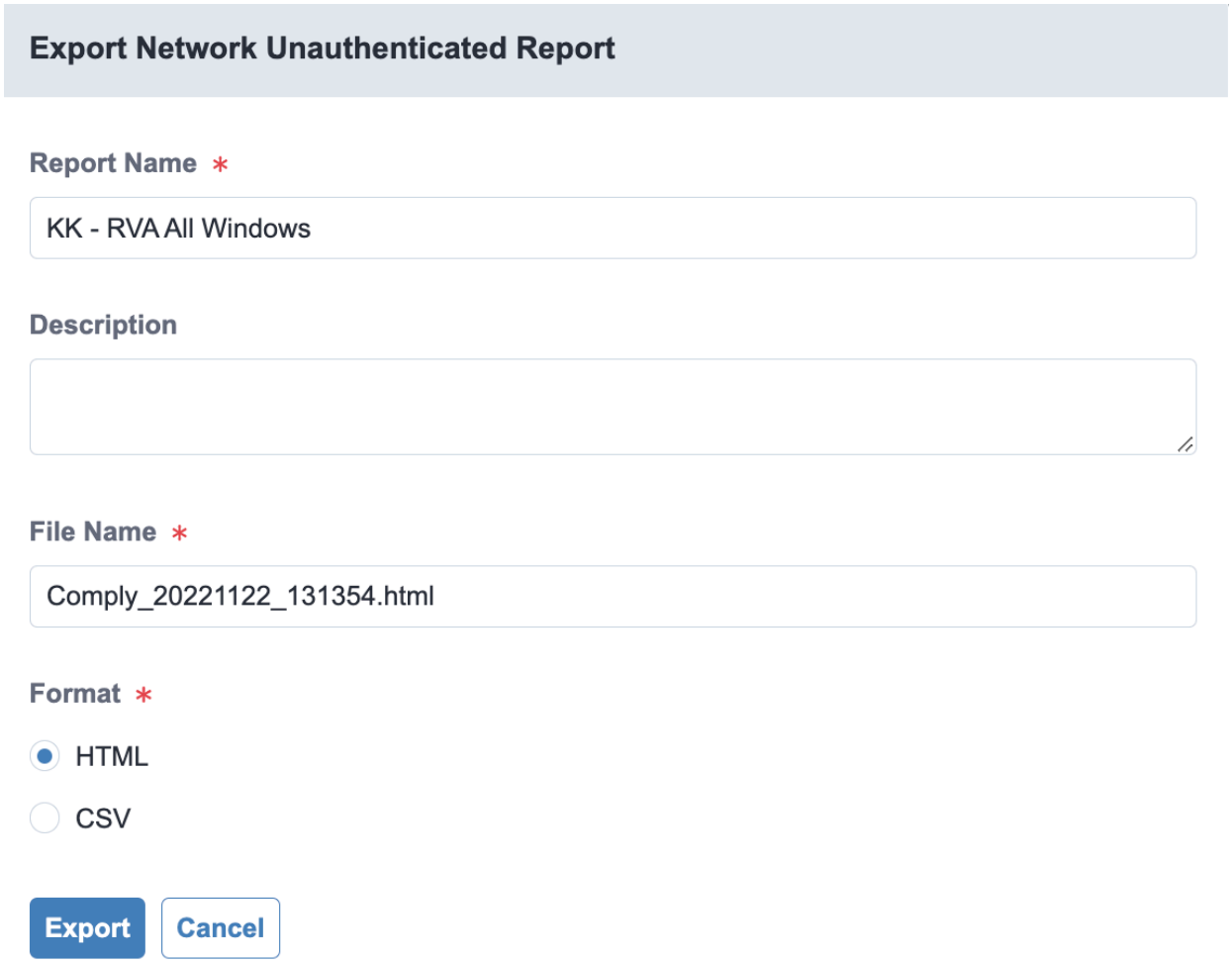
Export a Comply network unauthenticated report, configure its details, and monitor the export status.

About this task

Do the following to export a report.

1. From the Main menu, go to **Modules** > **Comply** > **Reports**. Select the **Network Unauthenticated** tab.
2. Select a report and click the **Export** icon . You can only export one report at a time. If you have more than one report selected, the Export icon is not displayed.
3. In the **Export Report** window, provide the following for each report type:

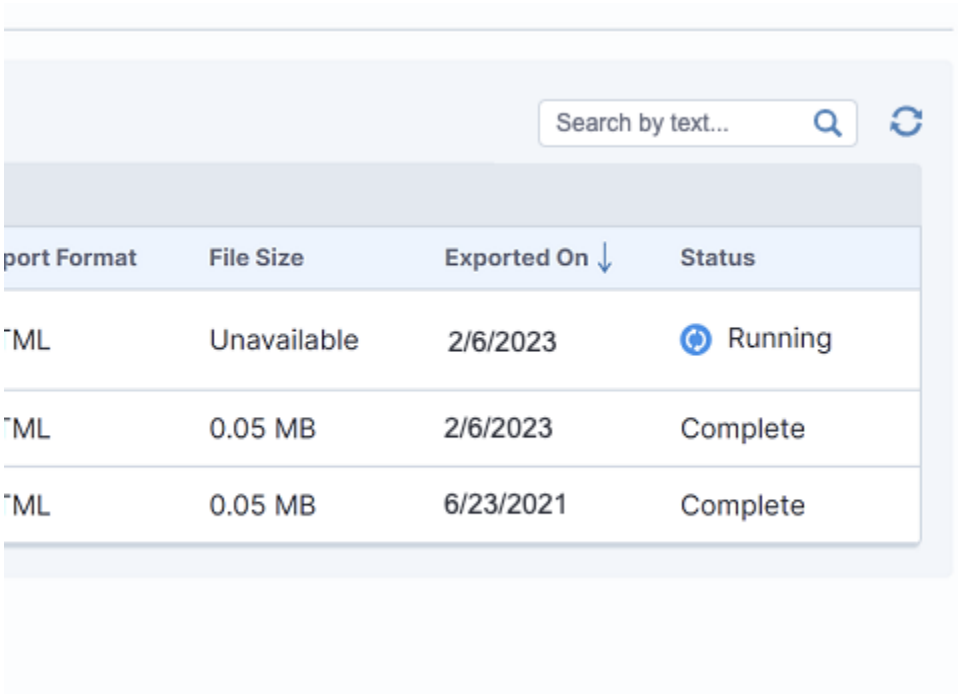
©2026 Tanium Inc. All Rights Reserved



4. Enter a **Report Name**.
5. Optionally, enter a **Description**.
6. Enter a **File Name** or use the pre-populated name.
7. Select a **Format**: **HTML** or **CSV**.
8. Click **Export**.

Click the **Exports** tab to view the status of the exported report. It will appear as **Running** until it's **Complete**. Click the Refresh button to update the Status column manually.

©2026 Tanium Inc. All Rights Reserved

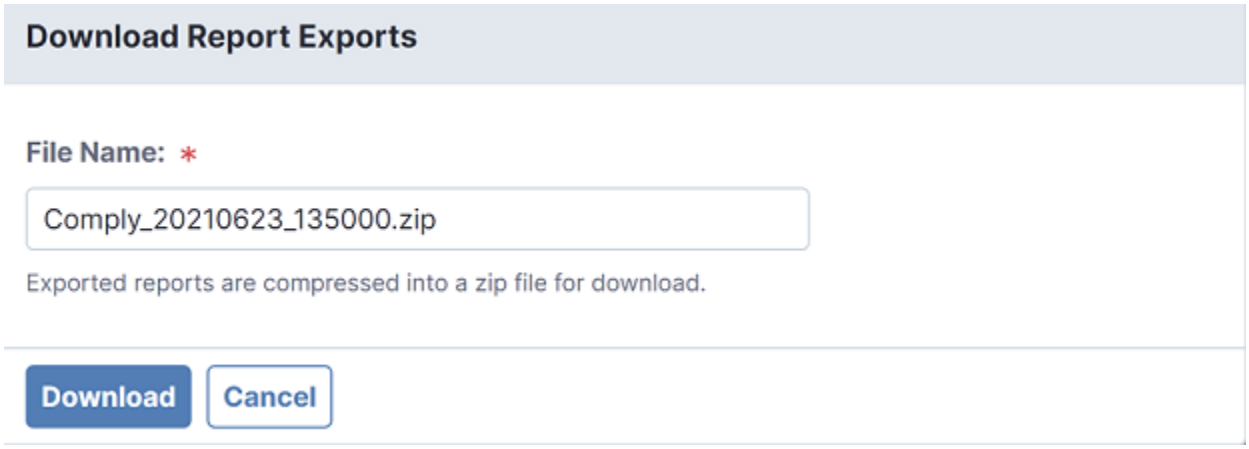


Downloading exported Comply reports

Download exported Comply reports as ZIP files.

About this task

1. From the Main menu, go to **Modules** > **Comply**. Then go to the **Reports** > **Exports** tab.
2. Select an exported report and click Download.
3. Click the **Download** button to download a zip file containing the report.



©2026 Tanium Inc. All Rights Reserved

Customizing compliance results

You can customize compliance results if you have the Comply Report Content Administrator role.

About this task

You must have the Comply Report Content Administrator role to customize compliance results. For more information, see User role requirements on page 41.

Custom profiles

Custom profiles define a tailored set of compliance checks and parameters, allowing you to create or upload profiles that implement only the rules you need.

A profile defines a set of rules to be evaluated and the parameters for those rules. Custom profiles allow you to specify just a subset of the checks available in a standard to be deployed.

From the Main menu, go to **Modules** > **Comply > Setup** > **Compliance**.

You can either create a custom profile or upload one from a tailoring file.

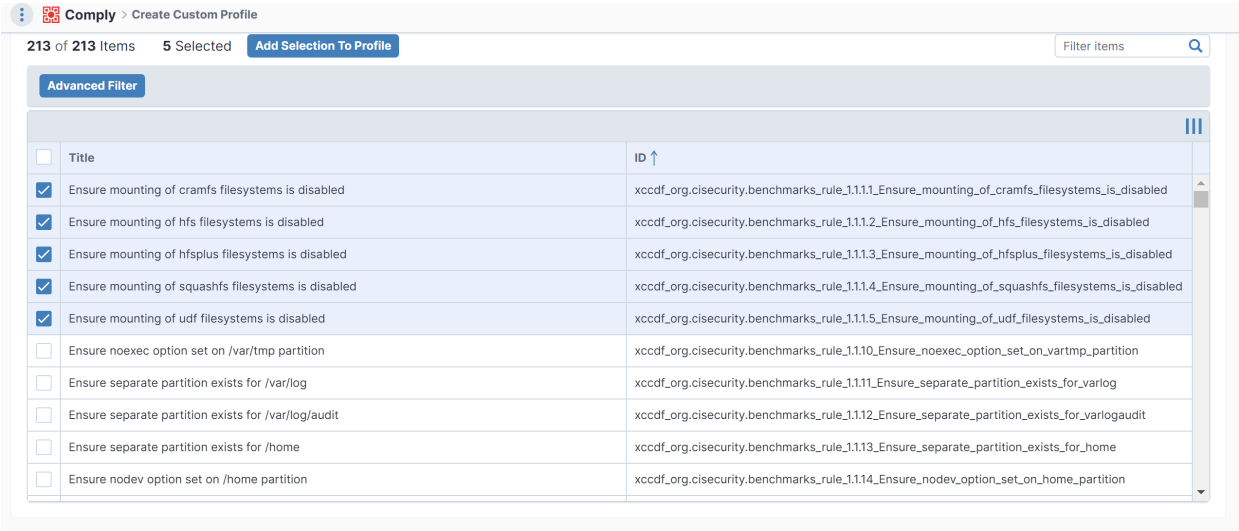
Create a new custom profile

Create a custom profile by selecting rules from a standard, configuring selectors and values, and saving the profile for use in assessments.

1. In the **Custom Profiles** tab, click the **Create** button.
2. On the **New Custom Profile** page, enter a **Name** and **Description**.
3. In the **Rules** section, select a standard from the **Standard** list.
4. Select each rule you would like to include in your custom profile.

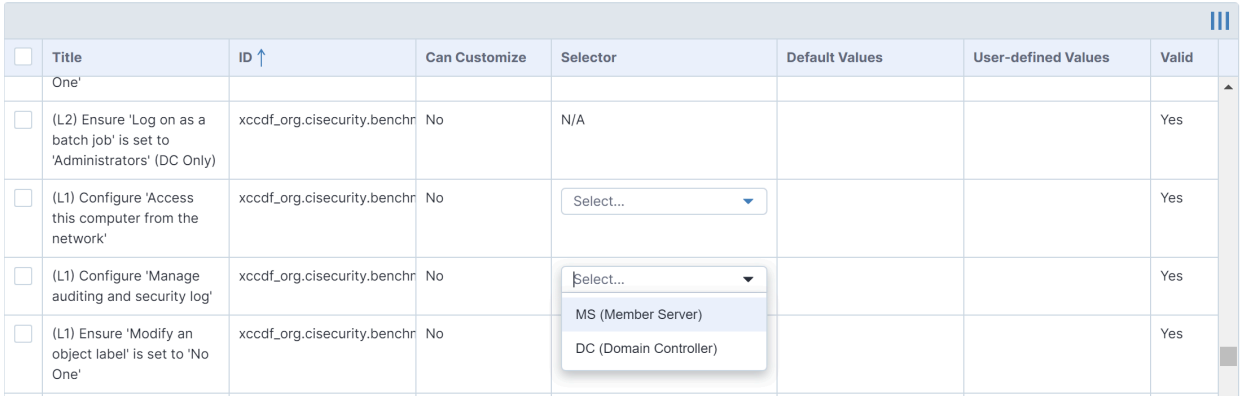
Tip: Click **Advanced Filter** to filter the rules by category.

©2026 Tanium Inc. All Rights Reserved



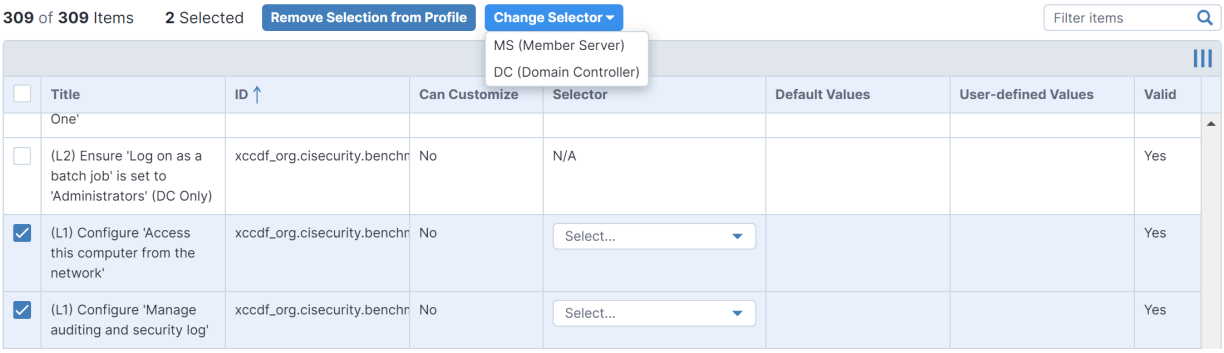
5. Click **Add Selection To Profile** to move the selected rules to the **Selected Rules** section.
   To remove a rule that you added, select the rule and click **Remove Selection From Profile**.

6. Some standards (for example, CIS Microsoft Windows Server 2008 and 2012) require you to choose a selector for certain rules.
   In the **Selected Rules** section, these rules have a selection list in the **Selector** column. In the CIS Windows example, set the **MS (Member Server)** or **DC (Domain Controller)** selector for each rule.



   To set or change the selector for multiple rules, select the rules and click **Change Selector**.

©2026 Tanium Inc. All Rights Reserved



7. Click **Create** to create the new custom profile.

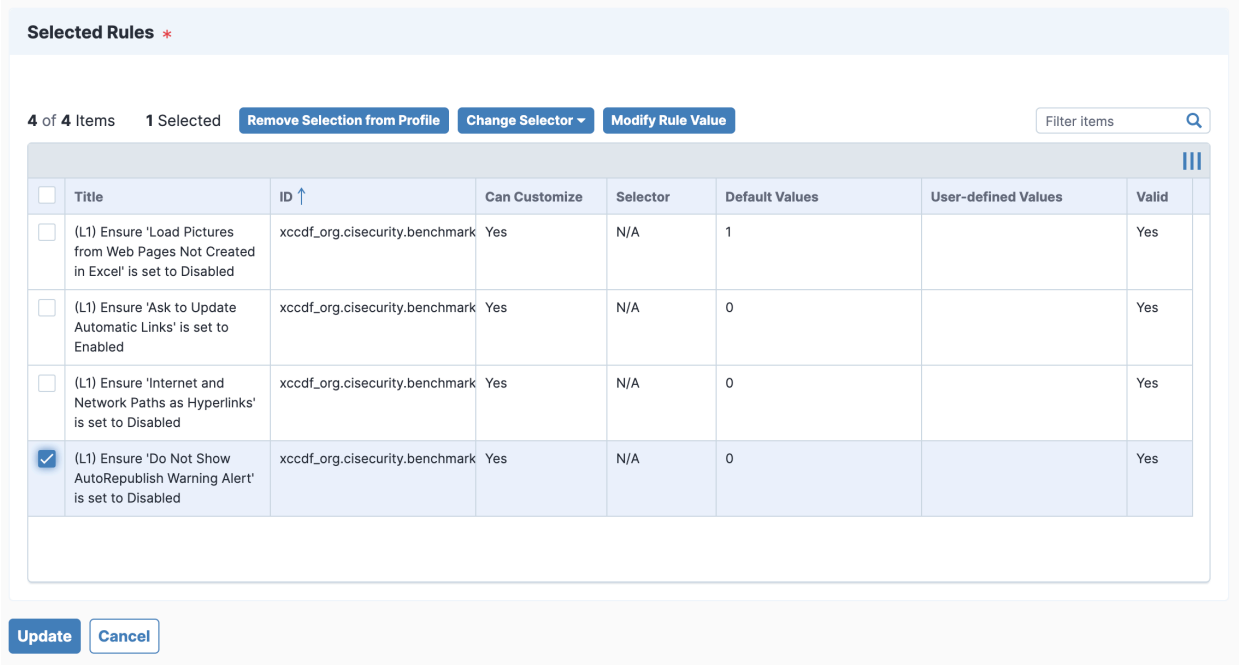
Result

You can also modify some rule values within your custom profile. If a rule value is customizable, a value of **true** displays in the **Can Customize** column along with the default value for the rule in the **Default Values** column.

> **Note:** You cannot delete a custom profile that is used in an assessment. You must delete the assessment first, and then you can delete the custom profile.

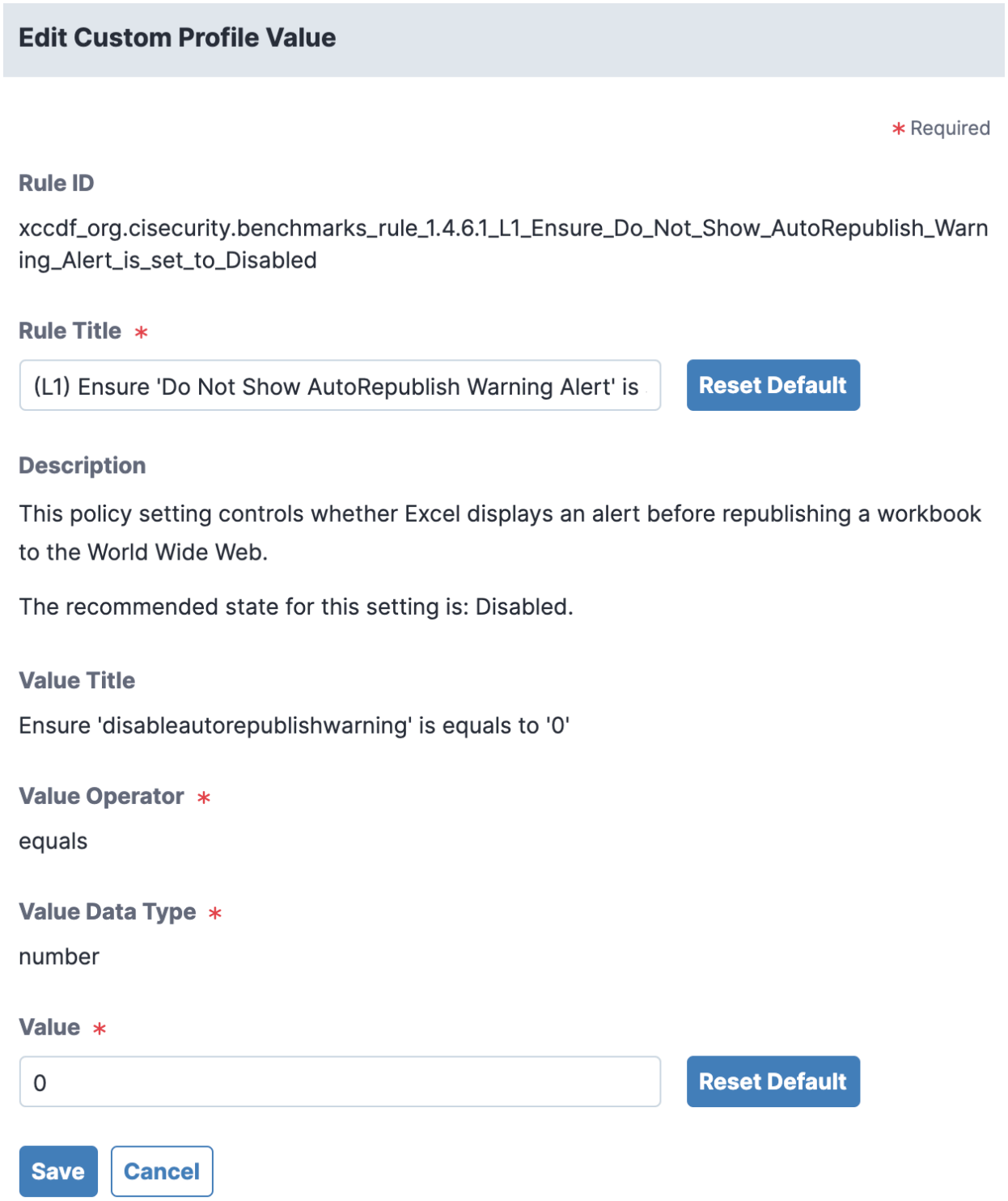
Customize a rule value

1. Select the rule and click **Modify Rule Value**.



©2026 Tanium Inc. All Rights Reserved

2. In the **Modify Custom Profile Value** window, enter a **Custom Rule Title** and change the **Custom value** field.



©2026 Tanium Inc. All Rights Reserved

> **Note:** Rule titles occasionally include the value used in the rule. Customize the title of rules for which values have been changed. The customized rule titles will then show up in report results, question answers, and report exports. For example, If you provide a new value for the rule **(L1) Ensure 'Enforce password history' is set to '24 or more password(s)'**, you can change **24** to match the custom value.

3. Click **Save**. The new value will appear in the **User-defined Values** column. You can return to the **Default Value** of a rule by clicking **Use Default**.

On the **Custom Profiles** page, click a custom profile to view its details.

You will see the rules included in the custom profile as well as those for which the values have been modified.

IMPORT A NEW CUSTOM PROFILE

Import a new custom profile by selecting a standard, adding a description, and uploading the tailoring file.

1. Click **Import** > **Custom Profile**.
2. In the **Import Custom Profile** window, enter a **Description**.
3. Select a standard from the **Standard** list.
4. Click **Select File** and locate the tailoring file for the new profile.

> **Note:** A custom profile can also be specified with a tailoring file, which is supported in SCAP 1.2 and later.

Cloning custom profiles

Clone an existing custom profile, update its title, description, and rules, and then create the new profile.

1. Select a custom profile and click **Clone**.
2. Provide a new **Title** and **Description** for the duplicate custom profile.
3. Make any necessary changes to the rules included in the custom profile.

©2026 Tanium Inc. All Rights Reserved

4. Click **Create**.

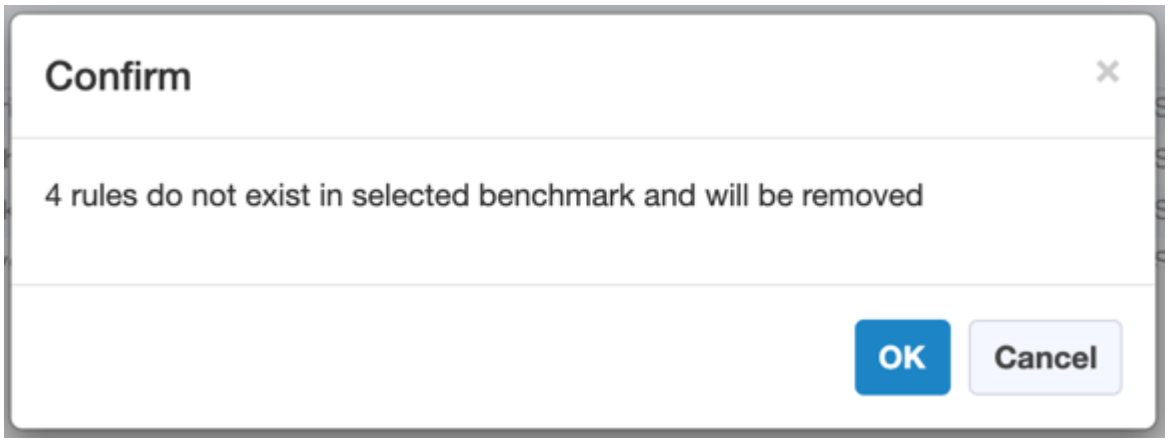
Editing custom profiles

Edit an existing custom profile, update its details and rules, and confirm any changes to associated assessments.

1. Select a custom profile and click **Edit** .
2. In the **Details** section, you can edit the **Title** and **Description**.
3. In the **Rules** section, choose additional rules or select a new standard from the **Standard** list to select other rules.

   > **Note:** If you choose to select a new standard, previously selected rules might no longer be valid. If a rule is invalid, No will be displayed as the value in the **Valid** column of the **Selected Rules** list. A warning also appears, indicating that invalid rules are selected.

4. Click **Update**.
5. If any of the selected rules are invalid, a confirmation window appears that invalid rules will automatically be removed from the custom profile.
   Click **OK**.



6. If one or more assessments currently use this custom profile, a confirmation window appears. If you want to redeploy these assessments immediately, click **Redeploy and Continue**; otherwise, click **Continue**. Assessments with changes that are not redeployed will show a Warning ⚠ next to them.

©2026 Tanium Inc. All Rights Reserved

Custom checks

Create and manage custom checks in Comply by uploading or writing scripts for supported platforms, configuring check criteria, and interpreting case-sensitive results.

You can create custom checks in Comply to check a condition on endpoints that might not be included in any standard. For custom checks, rather than running the scan engine on downloaded content, Comply CX directly executes a user-provided script.

The following scripts are supported for each platform:

Windows:

- VBScript (.vbs)

  executed with `cmd.exe /d /c cscript custom_script.vbs`

- PowerShell (.ps1) executed with `powershell -NonInteractive -ExecutionPolicy bypass -File custom_script.ps1`

Linux/Unix/MacOS:

- Bourne / Posix shell (.sh) executed with `/bin/sh custom_script.sh`

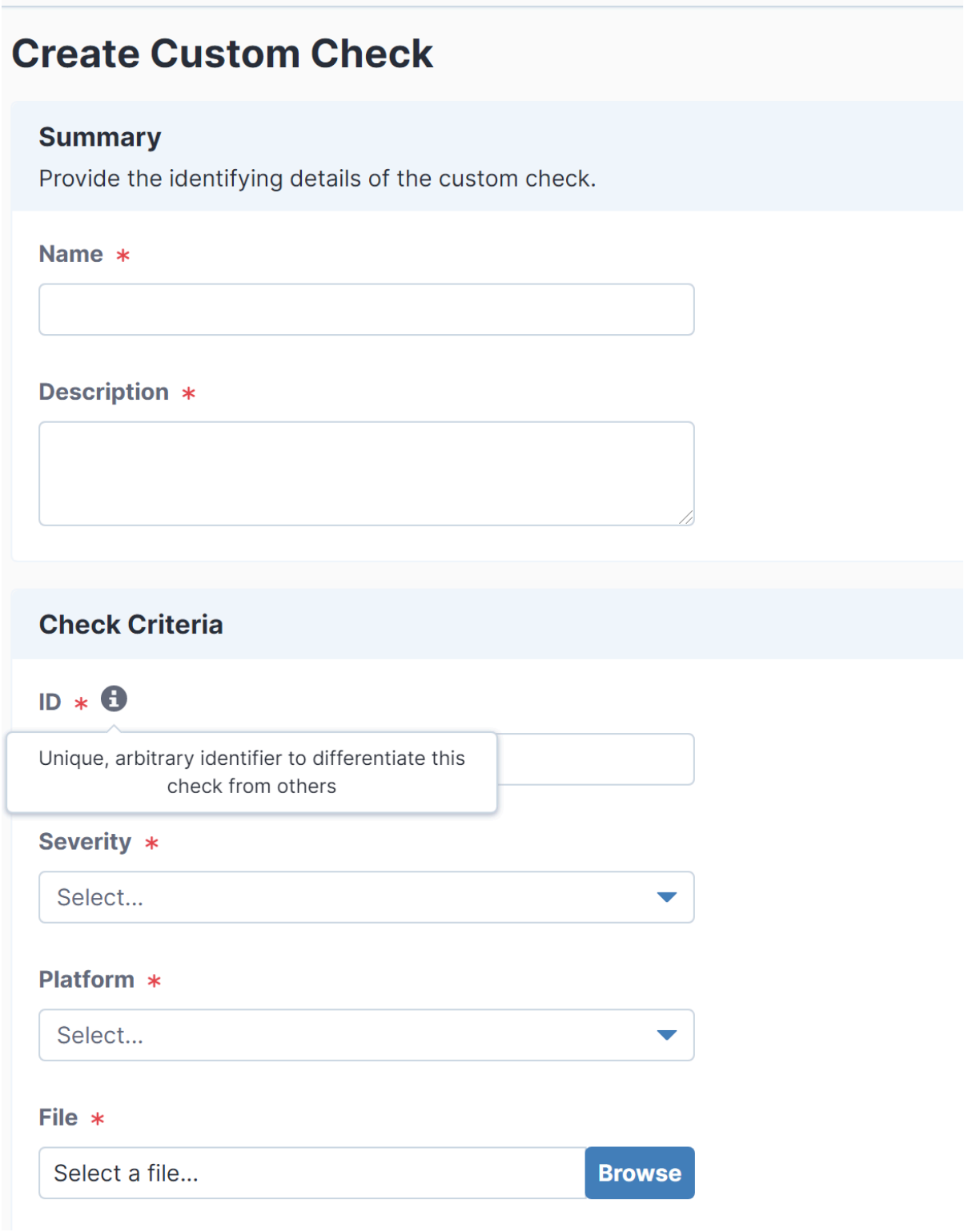
For more information, see Reference: Troubleshoot custom script issues on page 288.



CAUTION: You must have the **Comply Custom Check Writer** role to write custom checks. Apply this role cautiously. Users with the Comply Custom Check Writer permission can obtain high-privileged code execution rights on all Comply endpoints.

1. From the Main menu, go to **Modules** > **Comply > Setup** > **Compliance**.
2. On the **Custom Checks** tab, click the **Create** button.

©2026 Tanium Inc. All Rights Reserved



3. In the **New Custom Check** window, enter a **Name** and **Description**.
4. In the Check Criteria section, enter and identifier, **ID**, for this check.
5. Select the appropriate **Severity** and **Platform**.

©2026 Tanium Inc. All Rights Reserved

6. Add the custom check script using one of the following methods:

    - **Upload a file**: Click **Select File** and locate the script file on your computer. The maximum file size of a custom check is 1 MB.
    - **Write inline**: Enter or paste the script directly in the script editor field. This method does not require a separate file.

    Both methods support the same script types for each platform.

7. Enter a **Rationale** for the check in the edit field.
8. In the **Fix Text** field, enter information for remediating the check.
9. Click **Create**. Your custom check will now show under **Custom Checks** and be available in the **Custom Checks** section of the page when you create a new compliance report.



Note: You cannot delete a custom check that is used in an assessment. You must delete the assessment first, and then you can delete the custom check.

The result of a custom check is indicated by the last line of output from the custom check. This value should appear on a line by itself after all other output and should return one of the following results:



Important: Results are case-sensitive.

Custom check results

Result	Description
pass	All conditions are satisfied.
fail	All conditions are not satisfied.
error	Compliance evaluation could not be completed; therefore, the status of the endpoint(s) compliance has not been confirmed.
unknown	The result is unknown.

©2026 Tanium Inc. All Rights Reserved

Reference: Troubleshoot custom script issues

Troubleshoot common issues with custom shell scripts in Comply CX, including environment differences, invalid /bin/sh syntax, and how to locate runtime error output.

Issue: There are errors when the script is run by CX, but it runs without errors when tested elsewhere.

This could be due to the shell script being written with enhanced bash script syntax that is not valid for /bin/sh. This occurs because the shebang line in any custom check script will be ignored. The shebang line is only evaluated when a script is run directly from the command line (`./custom_script.sh`). Comply CX invokes the script with /bin/sh and will ignore the shebang.

Issue: The shell script works fine on some machines, but does not work on others.

This issue may occur if the shell script is written for bash and some endpoints have /bin/sh redirected to /usr/bin/bash, while others do not. Comply CX will always run /bin/sh.

Issue: How to check for runtime execution errors

You cannot use Debug mode to check for custom shell script errors. Debug mode only applies to scan engine output, not custom checks.

To check for custom script errors, do the following:

1. Go to the Comply results directory, <Tanium Client>/extensions/comply/data/results.
2. Locate the sub folder for the assessment in the results folder

   . Result files are located there and sequentially numbered (0-results.xml, 1-results.xml). The custom check shell script output and STDERR output are in the relevant result file.

Custom ID mappings

Use custom ID mappings to associate compliance checks and rules with your own identifiers and display them in assessment results.

Use custom ID mappings to create a custom column on results that associates a specific tag with a custom check or rule identifier.

1. From the Main menu, go to **Modules** > **Comply > Setup** > **Compliance**.

©2026 Tanium Inc. All Rights Reserved

2. On the **Custom ID Mappings** tab, click the **Import** button.
3. In the **New Custom ID** window, enter a **Name** and **Description**.
4. Click **Browse** and locate the custom ID mapping file.
5. Click **Import**. Your custom ID will now show under **Custom ID Mappings** and be available in the **Advanced Settings** section when you create a new Compliance assessment.

> **Note:** You cannot delete a custom ID that is used in an assessment. You must delete the assessment first, and then you can delete the custom ID.

Use the following file format for a custom ID mapping: `Rule id|custom id`

Example:

```
xccdf_org.cisecurity.standards_rule_1.1.1_Create_Separate_Partition_for_tmp|company_policy_rule_42
```

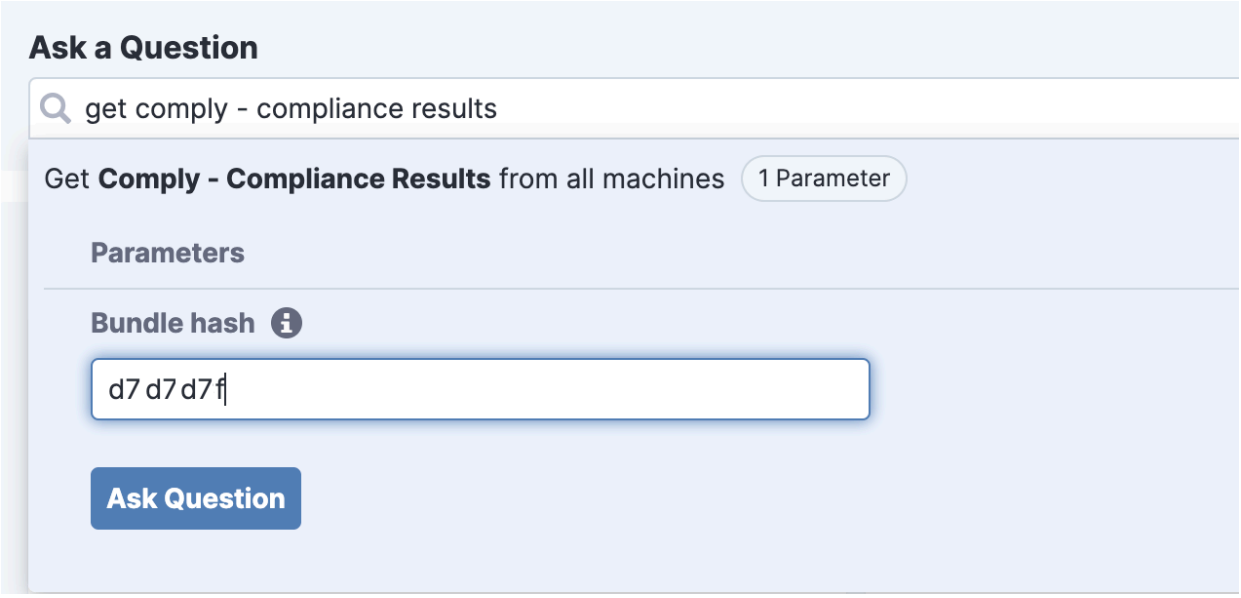
> **Note:** An assessment can only have a single custom ID mapping associated with it; however, it can have multiple standards and custom checks. When selecting the standards and custom checks, be aware that an assessment is targeted to a single action group.

View ID Mappings and Score Mappings in Interact

Use the custom ID hash from a Comply assessment in Interact to view the corresponding ID and score mappings in the results grid.

1. Obtain the hash for the custom ID for a report by clicking on the assessment name on the **Compliance Assessments** page and expanding **Get Details**. You can click **Copy** to copy the hash.
2. In Interact, ask a question such as `Get Comply - Compliance Results from all machines` and paste the hash in the **Bundle hash** field.

©2026 Tanium Inc. All Rights Reserved



Use the appropriate Comply sensor:

- **Comply - Compliance Results**
- **Comply - Compliance Status**

3. Click **Ask Question**.
4. The **ID Mappings** and **Score Mappings** columns in the results grid show these mappings.

Export custom check or ID mapping

Export a custom check or ID mapping from one Tanium Console and import it into another to reuse the same configuration.

About this task

To view, edit, or reuse a custom check or ID mapping, you can export it by doing the following:

1. From the Main menu, go to **Modules** > **Comply > Setup** > **Compliance**. Click the **Custom Checks** tab.
2. Select a custom check and click **Export** . You will select this exported file from the other Tanium console.
3. Sign in to Tanium Console where you want to import the custom check and navigate to the **Custom Checks** tab.
4. Click the **Create** button and select **Custom Check**.

©2026 Tanium Inc. All Rights Reserved

5. In the **New Custom Check** window, fill out the fields using the same information you entered for the exported file in the first Tanium console.
6. Click **Browse** and choose the file you exported in the second step.
7. Click **Create**.

Result

If you have custom IDs to go along with the custom check, export and import them using the previous steps, but from the **Custom ID Mappings** tab.

©2026 Tanium Inc. All Rights Reserved

Customizing vulnerability results

Customize vulnerability results using custom ID mapping and custom scoring to align CVEs with the frameworks on which you report.

About this task

You must have the Comply Report Content Administrator role to customize vulnerability results. For more information, see User role requirements on page 41.

Best Practice: Use custom ID mapping and custom scoring to align CVEs to the frameworks on which you report.

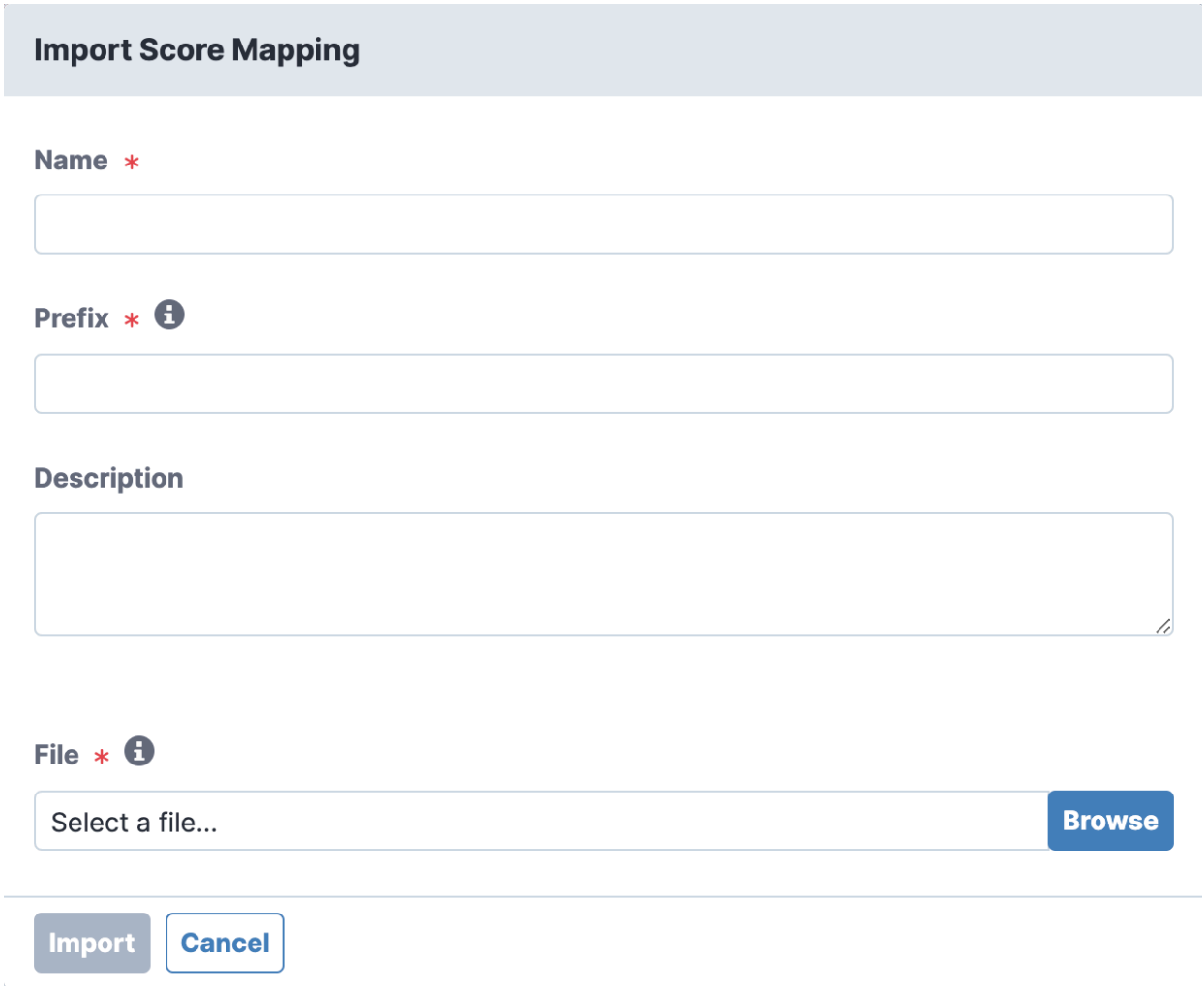
Custom scores

Use custom vulnerability scores in Comply to import CVE score mappings, apply them to assessments, and manage custom score configurations.

Comply allows you to specify a score to an individual CVE. By default, Comply shows the CVSS score.

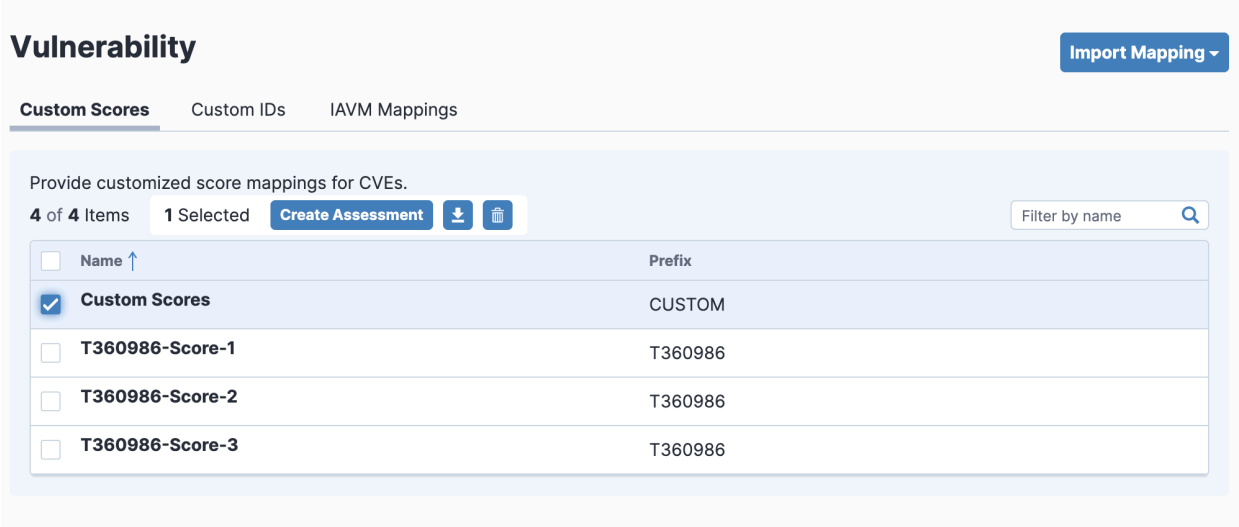
1. From the Main menu, go to **Modules** > **Comply > Setup** > **Vulnerability**.
2. On the **Custom Vulnerability Scores** tab, click the **Import Mapping** button and select **Custom Score**.
3. In the **Import Score Mapping** window, enter a **Name**, **Prefix**, and **Description**.

©2026 Tanium Inc. All Rights Reserved



4. Click **Browse** and locate the score mapping file.
5. Click **Import**. Your custom score will now show under **Custom Scores**.
6. Select your custom score and click the **Create Assessment** button to create a new assessment directly from the **Custom Score** tab.

©2026 Tanium Inc. All Rights Reserved



Note: You cannot delete a custom score that is used in an assessment. You must delete the assessment first, and then you can delete the custom score.

Use the following file format for a custom score mapping: `CVE|score`

Example: `CVE-2017-8789|11.5`

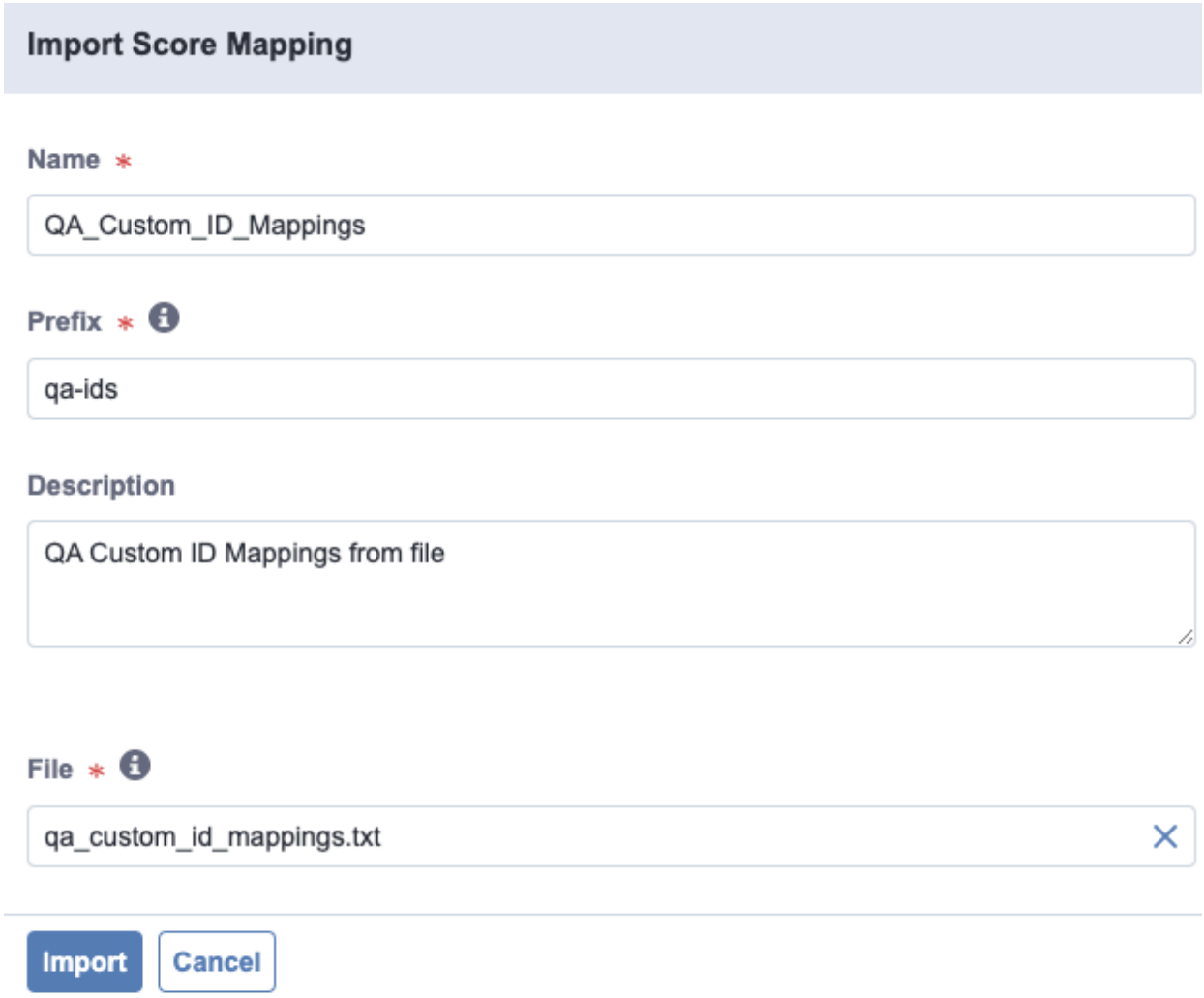
Custom ID mappings

Learn how to create and import custom ID mappings that associate your own identifiers with CVEs, and use them to create vulnerability assessments.

Custom ID mappings allow you to create a custom column on results that associates a specific tag with a CVE.

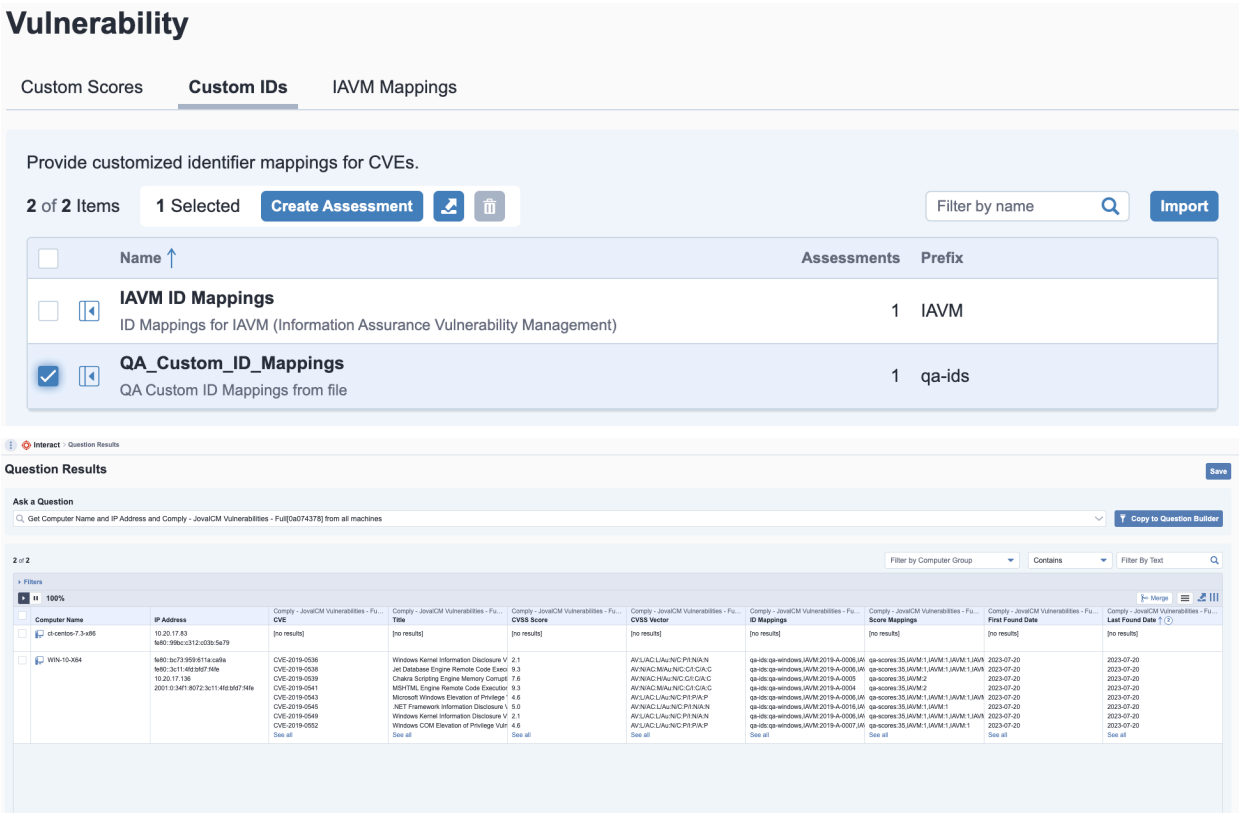
1. From the Main menu, go to **Modules** > **Comply > Setup** > **Vulnerability**
2. On the **Custom IDs** tab, click the **Import Mapping** button and select **Custom ID**.
3. In the **Import Custom ID Mapping** window, enter a **Name**, **Prefix**, and **Description**.

©2026 Tanium Inc. All Rights Reserved



4. Click **Browse** and locate the custom vulnerability ID mapping file.
5. Click **Import**. Your custom ID will now show under **Custom IDs**.
6. Select your custom ID and click the **Create Assessment** button to create a new assessment directly from the **Custom ID** tab.

©2026 Tanium Inc. All Rights Reserved



Note: You cannot delete a custom ID mapping that is used in an assessment. You must delete the assessment first, and then you can delete the custom ID mapping.

Use the following file format for a custom ID mapping: `CVE|custom id`

Example: `CVE-2014-2814|KB297262`

Upload IAVM mapping definitions

Upload custom Information Assurance Vulnerability Management (IAVM) mapping definitions to Comply and replace existing mappings used in vulnerability assessments.

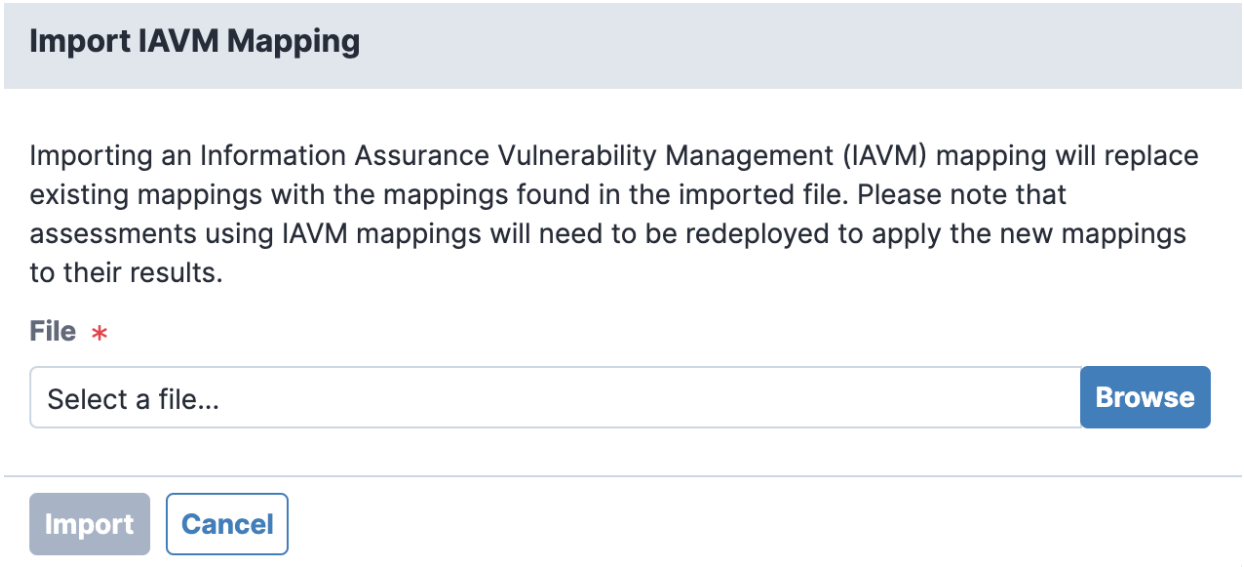
About this task

Information Assurance Vulnerability Management (IAVM) is a vulnerability source that is managed by the Department of Defense (DOD) and is accessible only with a common access card (CAC).

If you use IAVM mappings, you can upload IAVM mapping definitions in Comply.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Comply > Setup** > **Vulnerability**.
2. On the **IAVM Mappings** tab, click the **Browse** button and select the custom IAVM file.



3. Click **Import**. The last upload time and the count of IAVM ID and score mappings will be listed on the **IAVM Mappings** page.

Result

Note: When you import new IAVM mapping definitions, they will replace any existing mapping definitions.

Note: You cannot delete an IAVM mapping that is used in an assessment. You must delete the assessment first, and then you can delete the IAVM mapping.

Important: To apply the IAVM mappings, you must add both the IAVM ID and score mappings when you create a vulnerability assessment. Assessments using IAVM mappings will need to be redeployed to apply the new mappings to their results.

View ID Mappings and Score Mappings in Interact

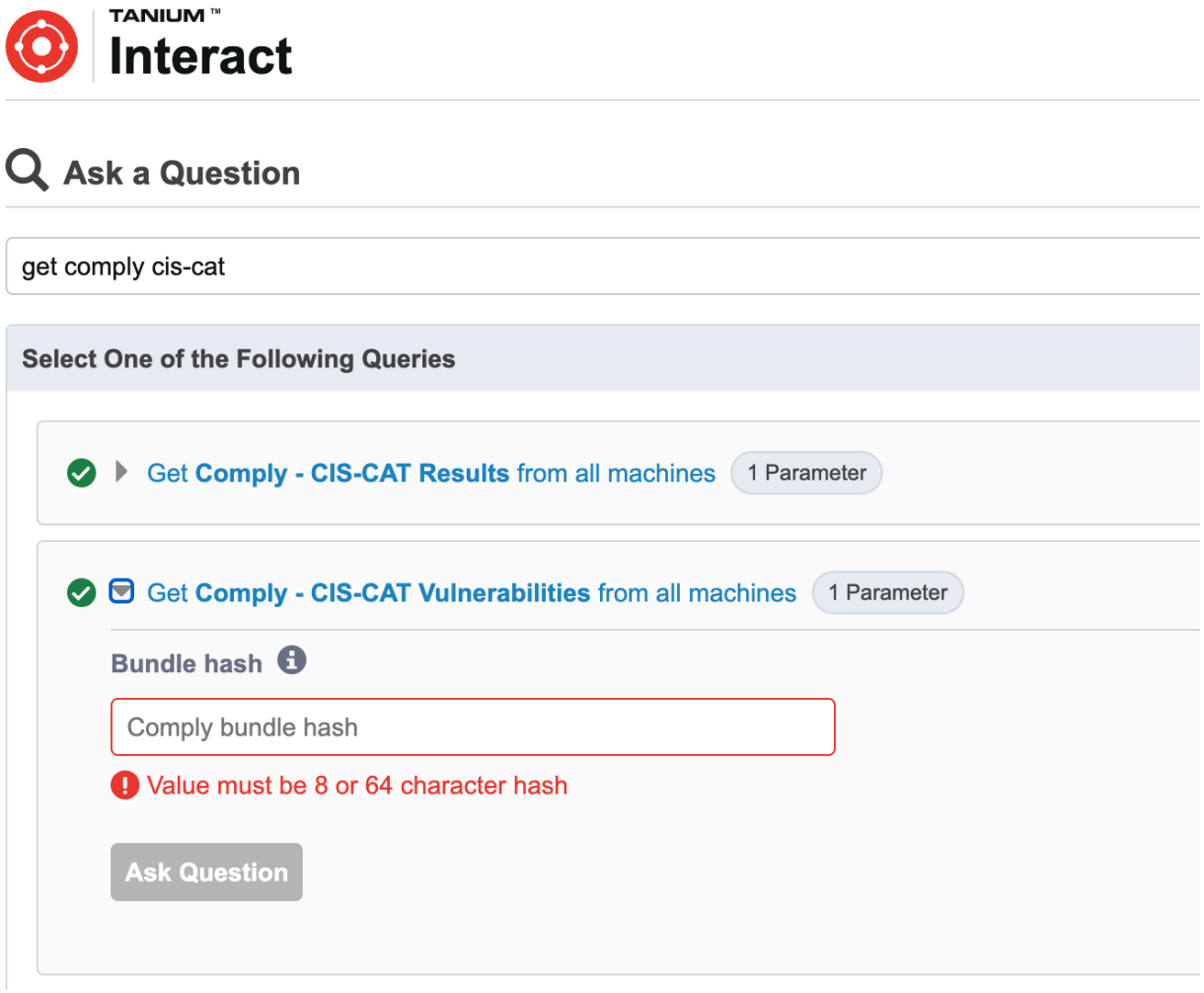
View ID mappings and score mappings in Interact by obtaining the custom ID hash from a vulnerability assessment, using it in an Interact Comply question, and reviewing the ID Mappings and Score Mappings columns in the results.

1. Obtain the hash for the custom ID for a report by clicking on the assessment name on the **Vulnerability Assessments** page and expanding **Get Details**. You can click **Copy** to copy the

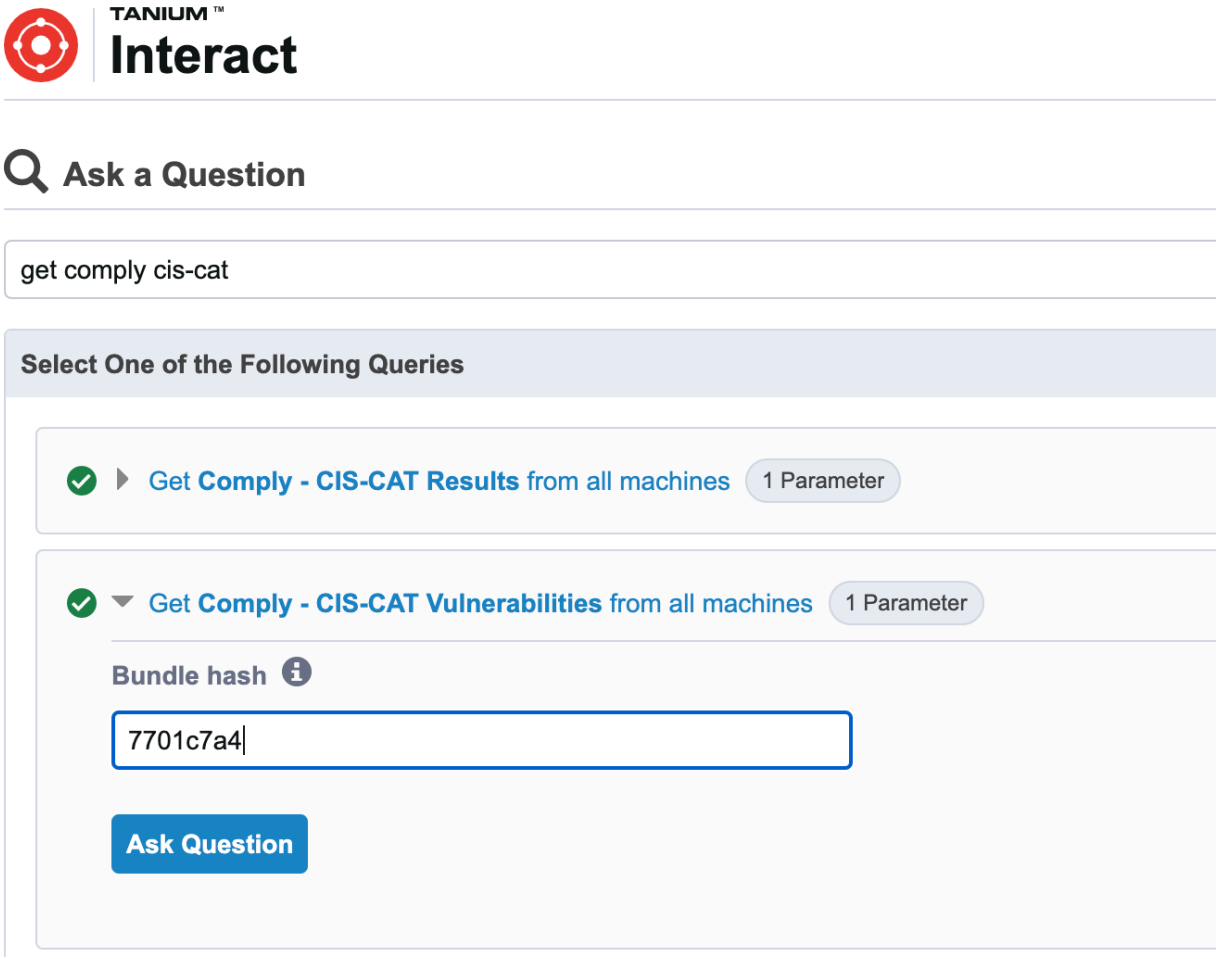
©2026 Tanium Inc. All Rights Reserved

hash.

2. In Interact, ask the question that matches the engine type such as `Get Comply - CIS-CAT Vulnerabilities from all machines` and paste the hash in the **Bundle hash** field.



©2026 Tanium Inc. All Rights Reserved



Use the appropriate Comply sensor for the engine type:

- **Comply - CIS-CAT Vulnerabilities**
- **Comply - Vulnerability Status**
- **Comply - SCC Vulnerabilities**

> **Note:** If you are using a Tanium Console version older than 7.5.2 with Comply 2.11, the sensors listed here are deprecated and hidden. For instructions on un-hiding sensors, see Tanium Console User Guide: View sensor details.

3. Click **Ask Question**.
4. The **ID Mappings** and **Score Mappings** columns in the results grid show these mappings.

Download custom ID mapping

Download a custom ID mapping so you can view, edit, or reuse it.

©2026 Tanium Inc. All Rights Reserved

About this task

To view, edit, or reuse a custom ID mapping, you can download it.

Select a custom ID mapping and click **Export**.

©2026 Tanium Inc. All Rights Reserved

Managing application settings

View and update default Comply application settings for on-premises and cloud deployments.

About this task

CAUTION: Any changes to the default values for the Comply application settings must be tested first in a lab or staging environment so that you understand the implications of the change. You must have the **Comply Administrator** role to modify application settings. For more information, see User role requirements on page 41.

1. From the Main menu, go to **Modules** > **Comply**. On the Comply **Overview** page, click Settings .
2. Click **Edit** for a setting, enter a **Value**, and click **Save**.

Result

The following settings are available:

Available Comply settings

General Settings	Default Value	Definition
Assessment Question Reissue Seconds	18000	How frequently to reissue assessment saved questions.
Is Airgapped	Off	Whether this module server is airgapped from the internet.
Management Rights: Filtering	Off	Enable filtering of assessments based on user management rights.
Management	On	Preserve management rights when assessments are updated.

©2026 Tanium Inc. All Rights Reserved

General Settings	Default Value	Definition
Rights: Preservation		
Tanium Request Timeout Seconds	60 Seconds	Number of seconds to wait for a response from the Tanium server before raising an error.
Log Level	Debug	Effective logging level (trace, debug, info, warn, error, fatal).
Threshold: Error Status	5%	Set assessments to an Error state when the percentage of endpoints with errors exceeds this threshold. This corresponds to the **Assessments with Issues** status on the Assessments list page.
Threshold: Pending Status	5%	Set assessments to a Pending state when the percentage of pending results exceeds this threshold.
Threshold: Scan Timeout	5%	Include a scan timeout when the percentage of assessment issues exceeds this threshold. **Note:** This setting applies to the legacy Tanium Scan Engine, CIS-CAT, and SCC only. Tanium Scan Engine 7.0 uses a timeout managed by Tanium and is not affected by this setting.
Saved Action Duration	60 minutes	Set when to reissue Saved Actions for age-based assessments. **Note:** This setting appears the first time Comply issues a saved action for an age-based assessment (one with a schedule that uses **Repeat: Using assessment age**). Until then, Saved Action Duration does not appear in the settings list. Even though **Repeat: Interval** also produces a recurring saved action, assessments scheduled with **Repeat: Interval** or **Repeat: Never** do not cause Saved Action Duration to appear.
Investigations Tab	On	Launch an investigation in a new tab instead of the current tab.
File Upload:	2048 MB	Set the maximum size of any incoming request's payload. By implication, all file uploads must be

©2026 Tanium Inc. All Rights Reserved

General Settings	Default Value	Definition
Payload Size		smaller than this value.
File Upload: Zip File Entries	5000 entries	Set the maximum number of entries allowed in a zip file.
CVE Definitions Banner	Off	Whether the CVE Definitions Type banner has been dismissed by the user. After it has been permanently dismissed, this setting automatically changes to On, and the banner will not appear again. To make the banner reappear to access the Update CVEs Definitions Type bulk edit window again, change this setting back to Off.
Automatic Assessments: Compliance	Auto	When set to Auto, Comply checks the operating systems on your managed endpoints. For each operating system that does not have a compliance assessment, Comply creates and deploys a compliance assessment. To stop automatic creation, select Off. Assessments that Comply already created remain.
Automatic Assessments: Vulnerability	Auto	When set to Auto, Comply checks the operating systems on your managed endpoints. For each operating system that does not have a vulnerability assessment, Comply creates and deploys a vulnerability assessment. To stop automatic creation, select Off. Assessments that Comply already created remain.

Note: You cannot add a new application setting or delete any of the existing application settings. You can only update the default values for these settings. If you click Delete , the setting returns to the default value. The setting is not deleted.

©2026 Tanium Inc. All Rights Reserved

Maintaining Comply

Perform regular maintenance tasks to ensure that Comply runs scheduled activities reliably on all targeted endpoints without overusing endpoint or network resources.

About this task

Perform regular maintenance tasks to ensure that Comply successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Comply is not performing as expected, you might need to troubleshoot issues or change settings. For more information, see Troubleshooting Comply on page 310.

Comply monthly maintenance

1. From the Main menu, go to **Modules** > **Comply** > **Overview**.
2. Scroll to the **Health** dashboard to review any Tanium™ Comply health check errors on endpoints.
   The **Comply Health Checks** panel shows a bar graph with the number of affected endpoints for each type of error, such as outdated tools, scan failures, or insufficient disk space.
3. To investigate a health check error, click one of the error bars. The Tanium Server issues a question that returns the computer name, operating system, IP address, coverage status, and client extensions status for the affected endpoints.
4. To troubleshoot health check errors, see Tanium Comply User Guide: Reference: Common errors in Comply.

Result

Note: Review and update Comply assessments when you perform Comply quarterly maintenance on page 304.

Comply quarterly maintenance

1. From the Main menu, go to **Modules** > **Comply > Assessments** and review the **Status** of

©2026 Tanium Inc. All Rights Reserved

assessments for errors or warnings. For more information, see Tanium Comply User Guide: Status definitions.

2. Investigate the error for each assessment.

   Tip: To issue a question that returns details about all the endpoints associated with scan errors, click the **Scan Errors** value above the grid.

   a. In the assessment row, click Additional Data, scroll to **Endpoint Statistics**, and click the **Scan Errors** value.
   b. Click the **Endpoints** value to issue a question that returns details about the affected endpoints. You can then review the results and, optionally, issue a drill-down question to investigate the errors. For more information, see Tanium Console User Guide: Managing question results.

3. Troubleshoot assessments if necessary to resolve issues related to endpoint compliance distribution. For more information, see Tanium Comply User Guide: Troubleshooting.

4. Edit assessments if necessary to resolve issues. For more information, see Tanium Comply User Guide: Edit an assessment.

5. Delete outdated assessments and create new assessments if updated versions of configuration compliance standards are released. For more information, see Tanium Comply User Guide: Creating compliance assessments.

   Note: Assessments that you delete on the **Assessments** page are removed from the Tanium Server but not from endpoints. Delete stale assessments from endpoints if retaining the associated data is no longer necessary. Otherwise, delete assessments from endpoints at intervals that preserve the data for a useful period without allowing the assessments to use too much disk space on endpoints. Base the intervals on how often users delete assessments from the server. For more information, see Tanium Comply User Guide: Delete stale assessments from endpoints.

Monitor and troubleshoot Comply coverage

Use the coverage metric to identify endpoints that show as **Needs Attention** and review contributing factors and corrective actions to restore Comply coverage.

The following table lists contributing factors into why the Comply coverage metric reports endpoints

©2026 Tanium Inc. All Rights Reserved

as **Needs Attention**, and corrective actions you can make.

Contributing factors and corrective actions for Tanium Comply metric 1

Contributing factor	Corrective action
Endpoints do not have the latest scan engine installed	• Ensure that the computer groups targeted by each deployment include all applicable endpoints. Review the deployments to confirm that no computer groups are missing. • Ensure the latest engine is installed. When updates are available for the Legacy Tanium Scan Engine or Amazon Corretto JREs that are included with Comply, a yellow banner displays on the Comply Main page that says Updates are available for one or more engines.
Endpoints do not have the latest Comply tools installed	Ensure that the Comply Action Group targets All Computers.
Specific endpoints missing Comply tools, scan engines, or JREs	Ensure that existing deployments include all possible architectures (bitness) and platforms. For example, some environments still contain 32-bit Linux and Windows endpoints. These endpoints require specific deployments.
Issue with a specific endpoint that might prevent Comply from running successfully	Check for issues with the endpoint that might prevent Comply from running successfully, such as having less than the minimum required available disk space (200 MB).
Comply tools are not successfully deployed to endpoints	Ensure that the Comply Action Group targets All Computers. Comply actions are always explicit, so the action group targeting does not need to be restrictive.

Monitor and troubleshoot endpoint compliance distribution

Use this table to identify common causes of low endpoint compliance distribution and apply corrective actions to improve assessment coverage and accuracy.

The following table lists contributing factors into why the endpoint compliance distribution metric might be lower than expected, and corrective actions you can make.

©2026 Tanium Inc. All Rights Reserved

Contributing factors and corrective actions for metric 2

Contributing factor	Corrective action
Endpoints are missing from compliance reports	Ensure that those endpoints exist in correctly targeted computer groups and that those computer groups are explicitly targeted for compliance reports. Make sure that compliance reports run on a periodic schedule.
Configuration compliance assessments do not include endpoints that were offline at the time of the initial report schedule	Change your configuration compliance assessment scheduling to use **Using report age** , and instead of running a weekly report, set the assessment result maximum age to 7 days. For more information, see Creating compliance assessments on page 121 . With this configuration, Comply continuously checks for and attempts to assess endpoints as they come online, as long as they do not already have findings that are newer than 7 days. This setting allows global organizations and "follow the sun" models to continuously scan managed endpoints as they come online around the world, regardless of timezone or the original scan execution time.
Systems that were included in the original report do not have any results	Make sure that the targeted endpoints are the correct operating system and platform for the configured report. For example, some compliance standards are specific to Windows Server 2008 and not Windows Server 2008 R2. Compliance standards can be specifically developed for the targeted operating systems, and in some cases will not function if the wrong operating system is targeted.
Standards content does not meet local requirements	• Use custom profiles or import a tailoring file to customize compliance checks to meet your business needs. • Develop custom checks to assess things not covered by an existing standard. • Use custom ID mapping to align checks to local guidance or frameworks. For more information, see Customizing compliance results on page 279 and Customizing vulnerability results on page 292 .
Third-party content compatibilities and bugs	Ensure any imported content meets the defined requirements, such as: • Compliance standards must follow SCAP standards and contain OVAL definitions. For more information, see Importing individual standards and assigning categories on page 110. • Tailoring is supported only in SCAP 1.2 and later. For more information, see Import a new custom profile on page 283.

©2026 Tanium Inc. All Rights Reserved

Monitor and troubleshoot endpoints with critical or high vulnerabilities

Identify common causes for a low Comply endpoints with critical or high vulnerabilities metric and the corrective actions you can take to address them.

The following table lists contributing factors into why the Comply endpoints with critical or high vulnerabilities metric might be lower than expected, and corrective actions you can make.

Contributing factors and corrective actions for metric 3

Contributing factor	Corrective action
Endpoints are missing from vulnerability reports	Ensure that those endpoints exist in correctly targeted computer groups and that those computer groups are explicitly targeted for vulnerability reports. Make sure that vulnerability reports run on a periodic schedule.
OVAL checks do not align with locally developed guides or industry frameworks	Use custom ID mapping and custom scoring to align CVEs to the frameworks on which you report. For more information, see Customizing vulnerability results on page 292 .

Monitor and troubleshoot mean time to identify vulnerability findings

Identify common causes of higher-than-expected mean time to identify vulnerability findings and apply recommended corrective actions to improve detection and assessment effectiveness.

The following table lists contributing factors into why the Comply mean time to identify vulnerability findings metric might be higher than expected, and corrective actions you can make.

Contributing factors and corrective actions for metric 4

Contributing factor	Corrective action
Newly released or discovered vulnerabilities are	Ensure that the Tanium Vulnerability Library (TVL) is configured to automatically update. For more information, see Default vulnerability sources on page 114 . Comply automatically updates assessments to use new definitions, but those assessments must run again

©2026 Tanium Inc. All Rights Reserved

Contributing factor	Corrective action
not being detected in vulnerability assessments	using the new definitions.
Newly released or discovered vulnerabilities are being detected, but not as quickly as needed	For best results, run general assessments that address all known vulnerabilities once a month or bi-monthly. In addition to that large general assessment, configure a small lightweight assessment that uses only high and critical severity vulnerability definitions from the current year so that you can run it frequently without negative performance impact. For example, you might run the lighter assessment weekly or every 3 days.
Vulnerability assessments are not targeting the desired vulnerabilities	Verify that the assessment configuration includes the appropriate severity, CVE years, and computer group targeting that was intended for the assessment.
CVEs have been published, but no OVAL definition is available	Check the Tanium Community for guidance on using Tanium to find and remediate a particular CVE.

©2026 Tanium Inc. All Rights Reserved

Troubleshooting Comply

Troubleshoot issues with Tanium Comply without manually deleting any Tanium content that includes `Comply` in its name.

About this task

CAUTION: Do not manually delete any Tanium content that includes `Comply` in the name for any reason. Deleting Tanium content can cause Comply to stop working correctly.

Collect logs

Collect troubleshooting log bundles as ZIP files and download them from the Tanium Console to share with Tanium Support.

About this task

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

1. From the Main menu, go to **Modules** > **Comply > Overview**. Click Help ?, then the **Troubleshooting** tab. Select the solutions for which to gather troubleshooting packages. All available solutions are selected by default.
2. Click **Create Package**.
3. When the packages are ready, click **Download Support Bundle**. A productname-support.[timestamp].zip file downloads to the local download directory for each selected package.

   Tip: Some browsers might block multiple downloads by default. Make sure to configure your browser to permit multiple downloads from the Tanium Console.
4. Contact Tanium Support to determine the best option to send the ZIP file(s). For more information, Contact Tanium Support on page 332.

©2026 Tanium Inc. All Rights Reserved

Collect troubleshooting information from endpoints

About this task

You can use Client Management to directly connect to an endpoint and collect a bundle of logs and other artifacts, sometimes referred to as an *Endpoint Must Gather* (EMG).

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Single Endpoint View** search box, enter all or part of an IP address or a computer name.
   Matching results appear after the search completes.
4. From the search results, click the computer name.
   Client Management opens the Endpoint Details page in Single Endpoint View (SEV).
5. Click the **Client Health** tab and, if the endpoint is not yet **Connected**, click **Direct Connect**.
6. In the **Available Steps** grid, select the domains (types of logs and artifacts) for which you want to gather troubleshooting information.
   For Patch information, select the **Core** and **Patch** domains.

   For Comply information, select the **Comply** domain and then select **Comply Database**, **Comply Extension Data**, and **Comply Intel**.

   For Endpoint Management for Operational Technology entity provider information, select the **Core** domain and then select **Tanium Client Logs**. Select the **Entity** domain and then select **Config Data**, **Entity Log**, and **Entity Provider Metadata**.
7. Click **Gather from Endpoint**.
   The selected logs and artifacts are gathered from the endpoint. The package appears in the **Must Gathers** section, and the name of the package corresponds with its time stamp.
8. When **Finished** appears in the **Run State** column, select the package and click **Download** to download a ZIP file that contains the troubleshooting information.
   For more information about collecting troubleshooting information in Single Endpoint View, see Tanium Reporting User Guide: Collect troubleshooting information.

   For more information about how to connect directly to endpoints, see Tanium Direct Connect

©2026 Tanium Inc. All Rights Reserved

User Guide.

For more information about Client health features in Client Management, see Tanium Client Management User Guide: Monitor the Client health overview in Client Management and Tanium Client Management User Guide: Access detailed Client health and troubleshooting information on an endpoint.

Locate log files

Locate log files on your endpoint or on the Tanium Module Server for troubleshooting with technical support.

About this task

You might need to locate log files on your endpoint or on the Tanium Module Server for troubleshooting purposes when working with technical support.

Endpoint log files

Comply creates and stores endpoint scan log files in specific directories on the client system.

When the scan is running, Comply log files are created on endpoints at the following path: *<Tanium Client>*\extensions\comply\data\results\<assessment scan name>*-stdout.txt

When the scan is complete, Comply log files are stored on endpoints at the following path: *<Tanium Client>*\extensions\comply\data\archived-results\<assessment scan name>*-stdout.txt

Tanium Module Server log files

Locate Comply service log files on the Tanium Module Server for on-premises deployments.

Comply log files are created on the Tanium Module Server at the following path: *<Module Server>*\services\comply-service-files\logs

Service log files are found here.

©2026 Tanium Inc. All Rights Reserved

Database corruption issue upgrading from Comply 2.19 or earlier to Comply 2.23

Upgrading directly from Comply 2.19 or earlier to Comply 2.23 can corrupt the Comply CX database and cause data loss. To avoid this issue, first upgrade to Comply 2.20 before upgrading to Comply 2.23.

Upgrading from Comply 2.19 or earlier to Comply 2.23 will result in Comply CX database corruption and data loss. A secondary effect is that after the database is re-created, all scans with age-based scheduling will run immediately, potentially resulting in a resource impact.

You can avoid this problem by upgrading in two steps. First upgrade to Comply 2.20 and then upgrade to Comply 2.23. Upgrading to Comply 2.21 is not recommended as it may introduce a known issue that causes assessments to fail.

SBOM false positives

Learn how to identify and resolve SBOM false positives to ensure accurate compliance reporting.

Due to limitations in NVD's CPE to vulnerability mapping

Learn how limitations in NVD's CPE-to-vulnerability mapping can lead to SBOM false positives and how to interpret these results accurately.

SBOM Assessment Information

Software Bill of Materials (SBOM) assessments examine the inventory of existing applications and their associated software components on an endpoint and match the identified software components to known vulnerabilities. SBOM scanning helps provide visibility over the entire software supply chain to identify vulnerabilities and unknown security risks.

How is an SBOM Finding Identified?

Tanium SBOM maps software components found on an endpoint to known vulnerabilities using a Common Platform Enumeration (CPE). The CPE to vulnerability mapping that is used comes primarily from the National Institute of Science and Technology (NIST) National Vulnerability Database (NVD).

©2026 Tanium Inc. All Rights Reserved

Limitations in NVD's CPE to Vulnerability Mapping

In most cases, the CPEs listed in NVD are accurate; however, some older vulnerabilities are no longer updated by NVD. Therefore changes to vulnerable CPEs are not reflected. These CVEs have a status of **Deferred** in NVD. For Deferred CVEs, Tanium will continue to use the most recent CPEs listed in NVD. On a few occasions, Tanium has observed that the CPEs listed in a Deferred CVE, especially for older vulnerabilities, are no longer accurate. In these cases, because NVD is not updating the source information, Tanium may show false positives or false negatives for these CVEs.

If you are seeing SBOM false positives or false negatives for these CVEs, you can create exceptions to those findings by excluding those CVEs from being reported on a specific set of endpoints. For more information, see Creating exceptions for findings on page 216.

Due to backporting

Backporting is the practice of applying a targeted fix to an older version of software without upgrading to the newer release that contains the fix. SBOM scans depend largely upon Common Platform Enumeration (CPE) identifiers, which function by retrieving the version of software components to identify known vulnerabilities. In the presence of backporting, SBOM scans can produce false positives because backported fixes do not change the old version number of the software components.

If you are seeing SBOM false positives due to backporting, you can create exceptions to those false positive findings by excluding specific CVEs from being reported on a specific set of endpoints. For more information, see Creating exceptions for findings on page 216.

Note: These types of false positives do not occur with OVAL scans. OVAL scans are able to identify precise indicator values that confirm the presence of a vulnerability. They do not rely on software version numbers.

Delete stale assessments from endpoints

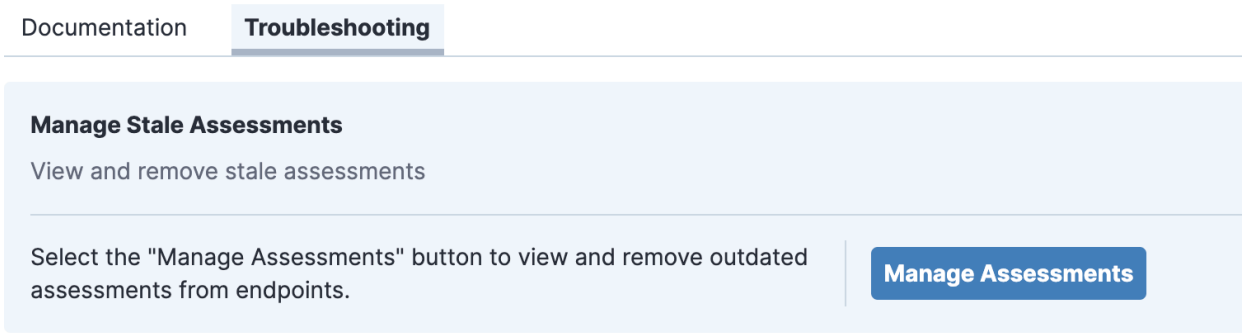
Schedule deletion actions to remove stale assessment data from endpoints after the assessments are deleted from the console.

About this task

©2026 Tanium Inc. All Rights Reserved

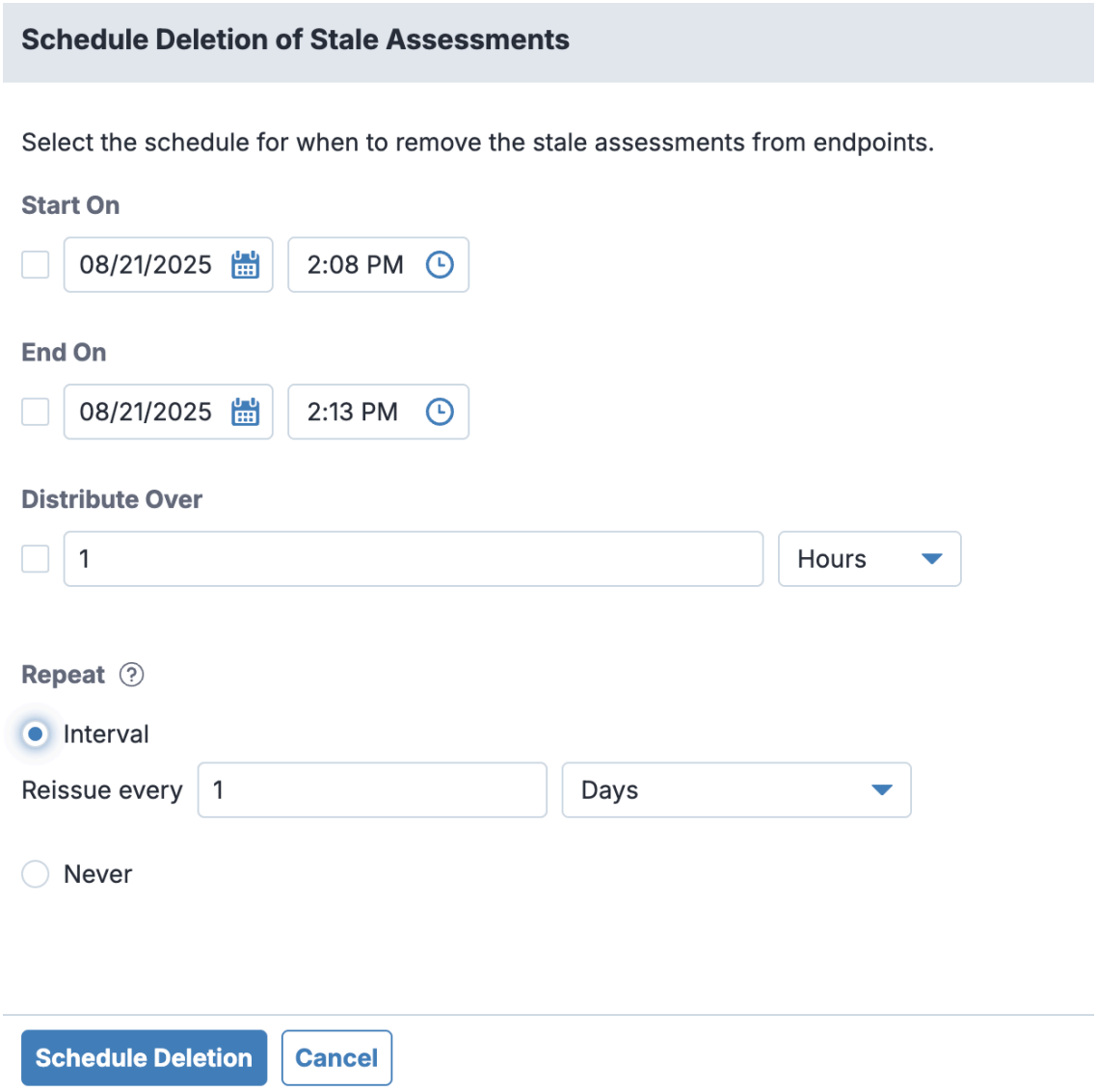
If you delete an assessment, that assessment is removed from the console but it remains on the endpoint. To delete stale assessments from endpoints, do the following.

1. From the Main menu, go to **Modules** > **Comply > Overview**. Click **Help** ?.
2. On the **Troubleshooting** tab, click **Manage Assessments**.



3. On the **Stale Assessments** page, select one or more and click **Schedule Deletion**.
4. Select and edit the following fields to schedule the removal action:
    - Select **Start On** and complete the date and time value to schedule the removal to begin at a specific time. The date and time displayed by default is the local browser time. For details on how this time is used to deploy the scheduled action, see Tanium Console User Guide: Deploying actions.
    - Select the **Distribute Over** and enter values to run the removal over minutes, hours, or days. Also select whether this deletion will recur on a configured interval.
    - Click **Schedule Deletion**.

©2026 Tanium Inc. All Rights Reserved



Next steps

Important:

Stale assessment tracking records are automatically and permanently removed from the server 90 days after an assessment is marked stale (that is, 90 days after you delete it from the **Assessments** page), whether or not you ran **Schedule Deletion** to remove the corresponding data from endpoints. After this automatic removal, the assessment no longer appears on the **Stale Assessments** page, and **Schedule Deletion** is no longer available for it. If endpoint-side result data still needs to be removed at that point, use the **Comply - Report Hashes** sensor and the **Comply - Remove Selected Hashes** package instead.

©2026 Tanium Inc. All Rights Reserved

Manually remove Comply content from endpoints

Use the Comply report and removal tools to identify and manually delete stale assessment data from endpoints when it no longer appears on the Stale Assessments page.

> **Note:**
>
> Stale assessment tracking records are automatically and permanently removed from the server 90 days after an assessment is marked stale, whether or not **Schedule Deletion** was run for it. After that removal, the assessment can no longer appear on the **Stale Assessments** page, which is why the following method might be your only remaining option.

If stale assessments do not appear in the **Stale Assessments** page, you can use the **Comply - Report Hashes** sensor to identify assessment data on endpoints and then use the **Comply - Remove Selected Hashes** package (for the respective platform) to manually remove assessment data from endpoints.

Java tool options when executing java

Learn how Comply uses the system JAVA_TOOL_OPTIONS environment variable when executing Java and how to configure this behavior.

Starting with Comply 2.14, JAVA_TOOL_OPTIONS has the following config setting.

CX.comply.UseSystemJavaToolsOption Use the system environment variable JAVA_TOOL_OPTIONS when executing java. The default is 1. Set to 0 and ComplyCX will ignore any system set JAVA_TOOL_OPTIONS environment variable.

Scans do not run as expected

Comply cannot run scans or clean up old results on endpoints that have action locks enabled.

About this task

Comply cannot run scans or clean up old results on endpoints with actions locks turned on. For more information, see Tanium Console User Guide: Managing action locks.

©2026 Tanium Inc. All Rights Reserved

Remote vulnerability source fails in proxied environment

In proxied environments, you may need to update the Tanium Module Server hosts file to ensure proper resolution of the remote vulnerability source URL.

In a proxied environment, an entry to the hosts file on the Tanium Module Server may be needed to ensure proper resolution of the remote source URL.

- On a Windows-based TMS, the hosts file must be edited via the operating system by a privileged OS account.
- On a TanOS-based TMS, this is done through Appliance Configuration in the TanOS management interface. For more information, see Tanium Appliance User Guide: Configuring appliance connections.

Update the Tanium Vulnerability Library for CVSS v3 support

Manually update the Tanium Vulnerability Library to ensure Comply 2.13 and later support CVSS v3 when recurring or airgapped updates are disabled.

About this task

Starting with Comply 2.13, Tanium Vulnerability Library files on content.tanium.com now support CVSS v3. If you are upgrading from a previous version, and you have disabled recurring updates or are running in airgap mode, you must manually upgrade to the latest TVL for Comply features to function properly. For more information, see Upload the Tanium Vulnerability Library files on page 61.



Note: After upgrading to Comply 2.13, until the TVL is updated based on the configured update schedule, a message may appear in Tanium Console instructing you to upgrade to the latest TVL.

Restart Connect service after upgrade

Restart the Connect service after upgrading to Comply 2.13.

About this task

©2026 Tanium Inc. All Rights Reserved

It is recommended that you restart the Connect service after upgrading to Comply 2.13.

RBAC synchronization with SUS adoption after upgrade

After upgrading to Comply 2.12 and adopting the System User Service, RBAC privileges and related updates may take time to synchronize, temporarily causing console query errors that resolve once migration completes.

In Comply 2.12, the steps required to configure the service account are no longer necessary due to the adoption of the System User Service, which performs these tasks automatically. Consequently, after upgrading to Comply 2.12, it might take time for the database migration to complete and for RBAC privileges and other updates to sync properly. This could lead to issues and error messages when first querying the Tanium Console. These issues should resolve on their own after a few minutes, but could take longer depending on system resources and the amount of data to migrate.

Remote authenticated scan timeout failure

Increase the remote authenticated scan (RAS) timeout in Comply 2.17 by updating the CX.comply.JovalMinCommandTimeoutMs client setting on the satellite.

If RAS scans are timing out, starting in Comply 2.17, you can increase the timeout value in one of the following ways:



Note: The default timeout value is 90000 milliseconds

- Option 1: Increase the timeout setting on the satellite by deploying the **Modify Tanium Client Setting** package and setting `CX.comply.JovalMinCommandTimeoutMs` to `<value in milliseconds>`
- Option 2: Log into the satellite performing the RAS scan and enter the following from a command line: `./TaniumClient config set CX.comply.JovalMinCommandTimeoutMs <value in milliseconds>`

Remote authenticated scans fail on ESXi and vCenter devices

Remote authenticated scans of ESXi and vCenter devices can fail because of an untrusted self-signed

©2026 Tanium Inc. All Rights Reserved

certificate or because the scan engine and vCenter cannot agree on a TLS cipher suite. You can resolve each issue by changing a Tanium client setting on the satellite.

Certificate errors

With Legacy Tanium Scan Engine version 6.4.2 and later, RAS scans of ESXi and vCenter devices fail when using a self-signed certificate that is not from a trusted certificate authority. In previous versions of the Legacy Tanium Scan Engine, the TLS certificate provided by the endpoint was not authenticated. This behavior changed in version 6.4.2 and now trusted certificates must be used.

The scan log shows an error similar to the following:

```
SSLHandshakeException: PKIX path building failed
```

If RAS scans are failing on ESXI and vCenter devices for this reason, you have the option to disable TLS validation. You can accomplish this by deploying a package to modify Tanium client settings on the satellite or by logging into the satellite directly and using a command line flag to restore the previous behavior.

- Option 1: Disable TLS validation on the satellite by deploying the **Modify Tanium Client Setting** package and setting `CX.comply.RasDisableTlsValidation` to `1`
- Option 2: Log into the satellite performing the RAS scan and enter the following from a command line: `./TaniumClient config set CX.comply.RasDisableTlsValidation 1`

TLS handshake failures

RAS scans of vCenter can also fail when the scan engine and vCenter cannot agree on a TLS cipher suite. In this case, the scan log shows the following error and the scan ends with no results:

```
SSLHandshakeException: Received fatal alert: handshake_failure
```

The Java runtime used by the scan engine disables `TLS_RSA_*` cipher suites by default. If vCenter does not accept any other cipher suite that the scan engine offers, the handshake fails. Disabling TLS validation does not resolve this error.

To resolve this issue, enable the `TLS_RSA_*` cipher suites on the satellite. The satellite must run comply-cx 1.33.621 or later.

1. On the satellite performing the RAS scan, enter the following from a command line:

©2026 Tanium Inc. All Rights Reserved

```
TaniumClient config set CX.comply.RasEnableTlsAlgorithms "TLS_RSA_*"
```

2. Run the assessment again.

Results directory on endpoint after upgrade

Describes how Comply 2.11 migrates endpoint results directories and how long legacy results and benchmark folders are retained before automatic deletion.

When upgrading to Comply 2.11, the Tools/Comply/results directory on the endpoint is migrated to extensions/comply/data/results.

By default the legacy results will remain for 7 days unless they are migrated by the service and there is an ECF configuration

Note that the Tools/Comply/results and Tools/Comply/benchmarks folders are automatically deleted after 30 days.

Incomplete findings for endpoints after upgrade

After upgrading Tanium Comply, findings for endpoints might appear incomplete while tools are deploying and data is migrating.

After upgrading Tanium Comply, while tools are deploying and data is migrating, it may take time for Findings to be complete.

Incorrect or missing findings for reports with custom profiles after upgrade

After upgrading Tanium Comply, assessments that were migrated from compliance reports using custom profiles or tailoring files might show missing or incorrect findings until you re-deploy them and verify results.

After upgrading Tanium Comply, compliance reports from previous versions are automatically migrated to assessments. If you had compliance reports that used custom profiles or tailoring files, you must re-deploy those assessments after upgrading. Otherwise, the corresponding findings may be missing or displayed correctly.

©2026 Tanium Inc. All Rights Reserved

Note: You may need to disable **Hide error results** from questions in **User Preferences** to validate that you have missing or incorrect findings.

Note: Ensure Comply tools on the endpoints have been upgraded to the latest version before re-deploying assessments.

Missing vulnerability reports after upgrade

After upgrading from Comply 2.9, compliance reports are migrated but vulnerability reports are not, because older query filters may not produce consistent results in newer versions. Use the OS-based vulnerability reports available in Comply 2.10 and later instead.

About this task

After upgrading from Comply 2.9 to a later version of Comply, compliance reports are migrated to the new version but vulnerability reports are not. This is intended due to the inability to ensure that query filters would provide the same results in newer versions of Comply that were seen in Comply 2.9 and earlier reports. Instead, there are some high-level, OS-based vulnerability reports provided with Comply 2.10 and later.

Deployments do not run as expected

Review common deployment error messages and their causes to ensure endpoints meet Comply requirements for disk space and required UNIX utilities.

Check for the following error messages if a deployment does not run as expected:

```
Some machines included in this deployment cannot be deployed to.
```

Ensure that targeted endpoints have enough disk space to accommodate deployments.

```
Some machines included in this deployment don't have the system
utilities required to complete a scan.
```

Linux or macOS endpoints do not have the UNIX utilities installed that are required for Comply to work correctly.

©2026 Tanium Inc. All Rights Reserved

License expiration impact

Understand how expired licenses affect Comply operation, SBOM data retention, and related endpoint tooling.

Comply will continue to operate with an expired license, but you cannot perform software updates.

For SBOM, once the SBOM license expires, there is a 30 day grace period before SBOM assessments and findings are deleted.

See Identify and resolve issues with Client Extensions.

See Remove Comply tools from endpoints on page 327.

Identify and resolve issues with Client Extensions

Use these steps to investigate and resolve errors with the Client Extensions that Comply installs and uses, including reviewing sensor results, uninstalling and reinstalling tools, checking dependency and blocker status, and analyzing Extensions logs on endpoints.

About this task

Use the following steps to troubleshoot issues with the Client Extensions that Comply installs and uses. During troubleshooting, consider environmental factors such as security exclusions, file locks, CPU usage, RAM usage, and disk failures.

Tip: For more information about the Client Extensions that Comply installs and uses, see Client Extensions on page 29.

1. If endpoints have Client Extension shared process mode enabled and you need to troubleshoot resource usage or crashes in the combined TaniumCX.exe or TaniumCX process, disable shared process mode on the affected endpoints, and then reproduce the issue if possible. For more information, see Endpoint Configuration User Guide: Manage Client Extension shared process mode.
2. To review the health of Client Extensions or to start an investigation into an existing error, ask a question using the `Client Extensions - Status` or Comply `- Tools Version`

©2026 Tanium Inc. All Rights Reserved

sensor.

The results of these questions help to identify endpoints with errors and provide a starting point to deploy actions that might help correct the issue. Filter the results and drill down as necessary to investigate results that indicate errors.

Tip: Consider whether endpoints with errors share common characteristics, such as operating system, domain or organization unit, or the antivirus software that is installed.

3. Target one or more endpoints with errors, and uninstall tools that report errors without blocking reinstallation. For more information, see Remove Comply tools from endpoints on page 329 and Endpoint Configuration User Guide: Uninstall a tool installed by Endpoint Configuration.



CAUTION: When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

Wait for automatic reinstallation of the tool. If the reinstallation does not resolve the issue, continue to the next step.

4. Ask a question using the `Endpoint Configuration - Tools Status Details` sensor, and include filters to limit the results to the tool that you are investigating. For example:
`Get Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains` Comply `from all machines with Endpoint Configuration - Tools Status:Tool Name contains` Comply

Review the columns in the results for specific information about errors. The following table provides guidance for some common error conditions:

Potential errors returned by the Endpoint Configuration - Tools Status Details sensor

Error Condition	Possible Resolution
No error appears, but an available new version has	Review the **Targeted Version** column to make sure that the endpoint has received the latest manifest. If the targeted version does not yet show the updated version, the

©2026 Tanium Inc. All Rights Reserved

Error Condition	Possible Resolution
not been installed	Endpoint Configuration manifest has not updated on the endpoint, usually for one of the following reasons: • The manifest update is still pending. Either wait for the manifest to update and then review the results again, or follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest. • Action lock is enabled on the endpoint. Follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest to identify endpoints with action lock turned on. • Comply is no longer installed, or it is no longer targeting the endpoint. In some cases, Comply might stop targeting an endpoint because it no longer needs the endpoint for a particular workload. Consider whether Comply should still target the endpoint: • If it is expected or intentional that Comply no longer targets the endpoint, you can optionally uninstall Comply tools and dependencies. For more information, see Remove Comply tools from endpoints on page 329. • If Comply should still target the endpoint, make sure that the Comply action group includes the endpoint, and make sure Comply targets the endpoint in any expected configurations or profiles. Then, either wait for the manifest to update and then review the results again, or follow the steps in Endpoint Configuration User Guide: Verify and manually update the Endpoint Configuration manifest.
Installation Blocker: `Unmet Dependencies: [Tool name]`	If no **Failure Message** or **Failure Step** appears, the endpoint might be waiting for the dependencies to install. Wait to see if the condition resolves on its own. If this condition remains for an extended period, ask the question again and review any error information in other columns, especially the **Failing Dependency** column.
Failing Dependency: `[Tool name]`	Ask the question: `Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains [Tool name] from all machines with Endpoint Configuration - Tools Status:Tool Name contains [Tool name]` Investigate further errors with the tool. If the dependency has not been installed on an endpoint, ask the question: `Get Endpoint Configuration - Tools Retry Status from all machines with Computer Name equals Computer_Name` to review the retry status for the

©2026 Tanium Inc. All Rights Reserved

Error Condition	Possible Resolution
	tool installation. For more information, see Endpoint Configuration User Guide: Review tool installations that are scheduled for a retry .
Manually Blocked: `blocked`	The tool was previously blocked, either manually or during a previous uninstallation. Unblock the tool. For more information, see Endpoint Configuration User Guide: Block or unblock tools from installing on an endpoint .

5. Review the Extensions logs on the endpoint. Take note of entries that include `fail` or `error`. For more information, see Review the Extensions log for an endpoint on page 326.

Result

For additional help, collect all logs for Tanium Comply on page 311, and contact Tanium Support on page 332.

Review the Extensions log for an endpoint

Use Client Management to directly connect to an endpoint and view and download extension logs.

1. From the Main menu, go to **Shared Services** > **Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Direct Connect** search box, enter all or part of an IP address or a computer name.

   Matching results are displayed after the search completes.
4. From the search results, click the computer name to connect to the endpoint.
5. Click the **Logs** tab, and select an **extensions[#].log** file.
6. (Optional) To download the log, click **Download**.

For additional help, collect all logs for Tanium Comply on page 311, and contact Tanium Support on page 332.

Verify endpoint tools

If you are experiencing issues such as a feature not working on an endpoint or seeing incorrect data

©2026 Tanium Inc. All Rights Reserved

in the workbench, confirm that your endpoints have the latest toolset version.

For more information, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or Client Extensions and Reference: Client extensions and endpoint tools used for Tanium solutions.

Remove Comply tools from endpoints

About this task

You can deploy an action to remove Comply tools from an endpoint or computer group. Separate actions are available for Windows and non-Windows endpoints.

1. In Interact, target the endpoints from which you want to remove the tools. For example, ask a question that targets a specific operating system:`Get Endpoint Configuration - Tools Status from all machines with Is Windows equals true`
2. In the results, select the row for Comply, drill down as necessary, and select the targets from which you want to remove Comply tools. For more information, see Tanium Interact User Guide: Drill Down.
3. Click **Deploy Action**.
4. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
5. For **Tool Name**, select Comply.
6. (Optional) By default, after the tools are removed they cannot be reinstalled. To allow tools to be automatically reinstalled, clear the selection for **Block reinstallation**. Re-installation occurs almost immediately.

©2026 Tanium Inc. All Rights Reserved

> **Note:**
> If reinstallation is blocked, you must unblock it manually:
>
> - To allow Comply to reinstall tools, deploy the **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]** package (depending on the targeted endpoints).
> - If you reinstall tools manually, select **Unblock Tool** when you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package.

7. (Optional) To remove all Comply databases and logs from the endpoints, clear the selection for **Soft uninstall**.

   > **CAUTION:** When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

8. (Optional) To also remove any tools that were dependencies of the Comply tools that are not dependencies for tools from other solutions, select **Remove unreferenced dependencies**.

9. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   > **Tip:** If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

10. Click **Show preview to continue**.

11. A results grid appears at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

    > **Note:** If you have enabled Endpoint Configuration approval, tool removal must be approved in Endpoint Configuration before tools are removed from endpoints.

©2026 Tanium Inc. All Rights Reserved

Uninstall Comply

Learn how to uninstall Comply by removing endpoint artifacts and then uninstalling Comply from the server.

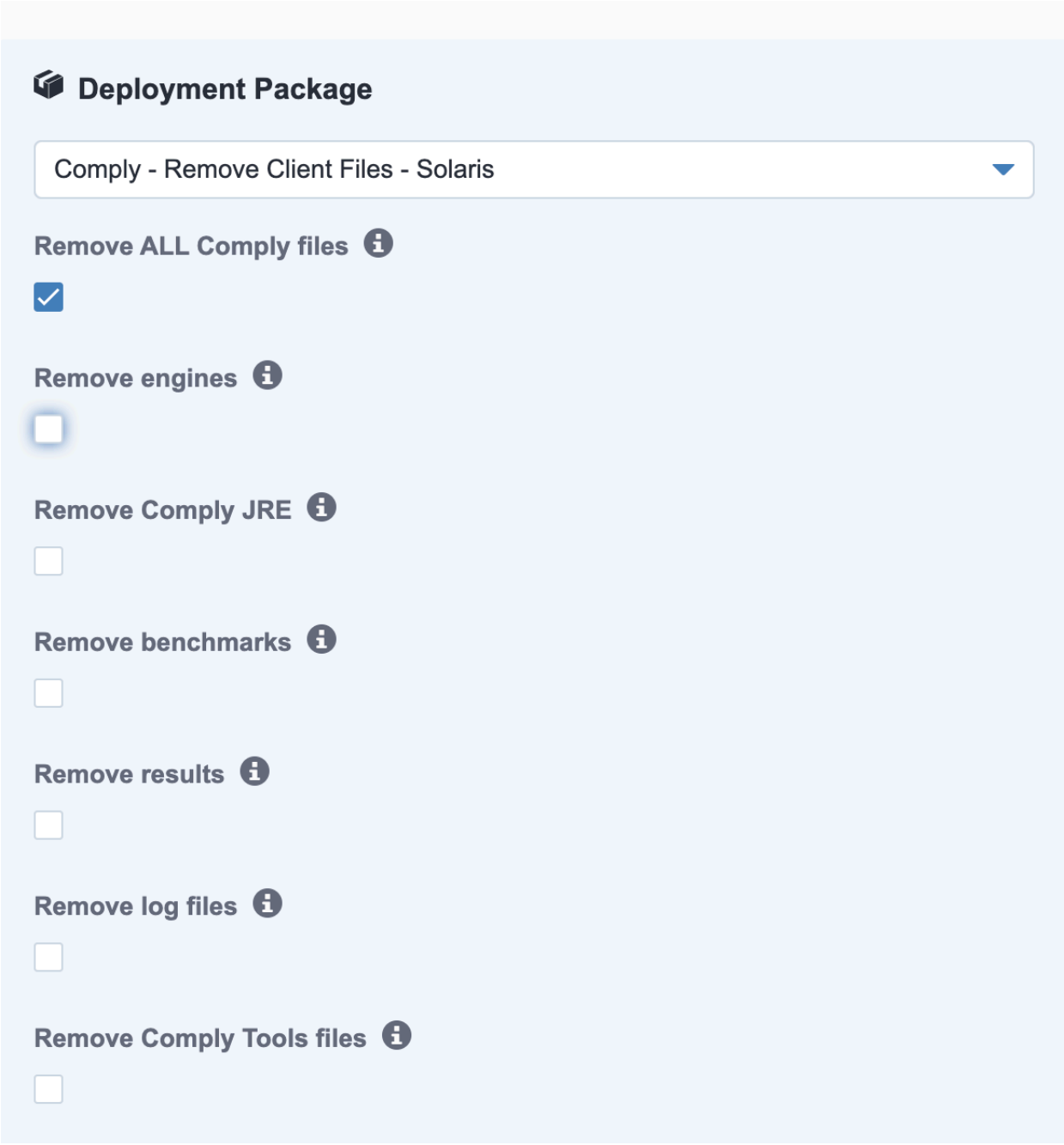
If you need to uninstall Comply, clean up the Comply artifacts on endpoints and then uninstall Comply from the server.

Remove Comply content from endpoints

Remove Comply content and tools from selected endpoints by deploying the appropriate Comply removal action package.

1. From the Main menu, go to **Modules** > **Interact**.
2. Ask a question to target the endpoints from which you want to remove Comply content and tools. For example, `Get Endpoint Configuration - Tools Status from all entities` returns all endpoints with the Comply tools installed.
3. Select the endpoints from which you want to remove Comply content and tools.
4. Click **Deploy Action**.
5. On the **Deploy Action** page, select either the **Comply - Remove Client Files - Windows**, **Comply - Remove Client Files - Solaris**, or **Comply - Remove Client Files - Unix** action, as appropriate. For more information, see Tanium Platform User Guide: Managing Scheduled Actions.
6. Check **Remove ALL Comply files** if you want to remove all Comply content or select only the content and tools you want to remove.

©2026 Tanium Inc. All Rights Reserved



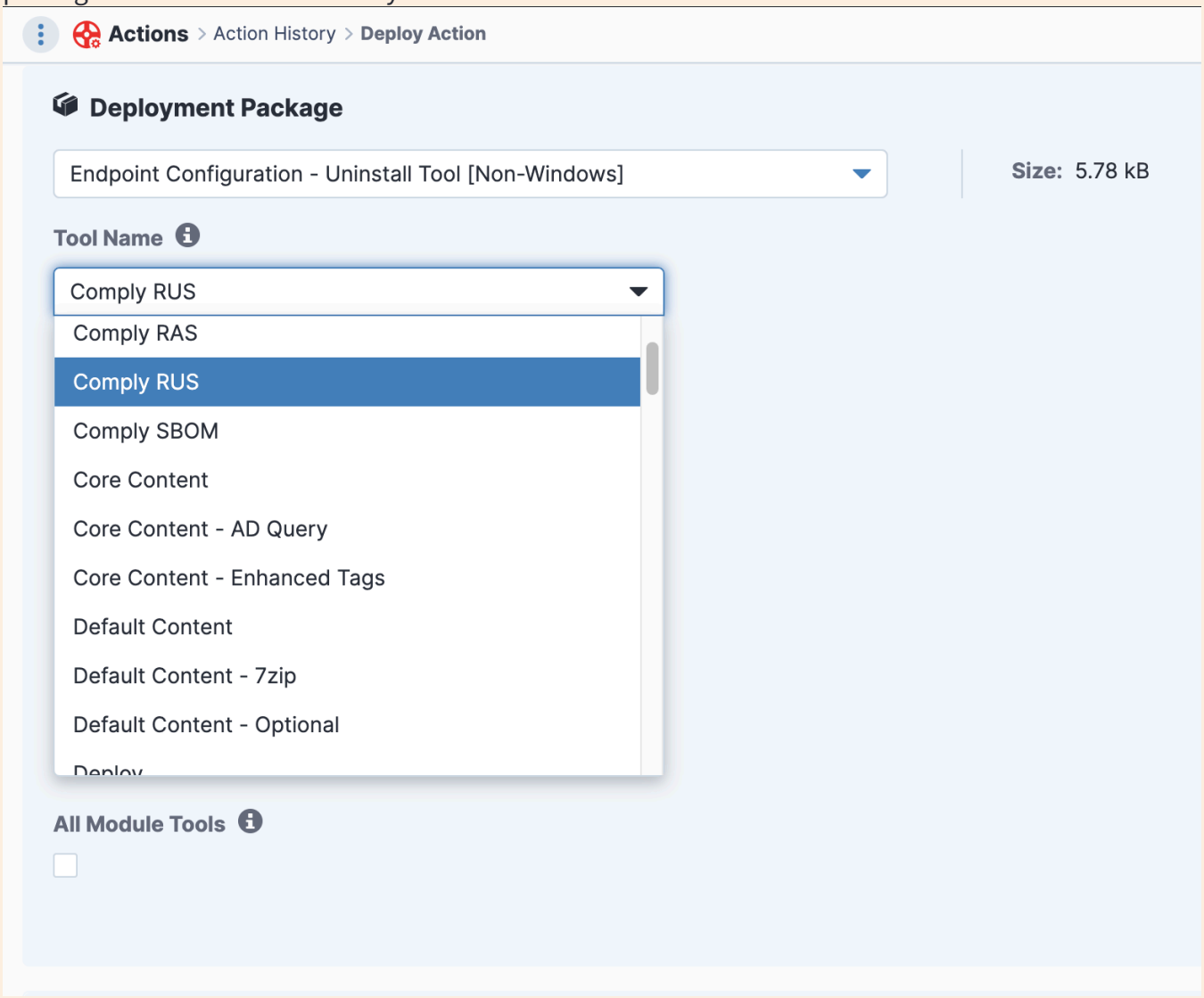
7. In the **Action Details** section, the package name is automatically added to the **Name** field.
8. Set a **Deployment Schedule**, **One Time** or **Recurring**.
9. Under **Targeting Criteria**, select endpoints to target for the uninstall.
    - The default **Action Group** is **All Computers**. You can select a different group here and further filter the list based on your selection.
    - You can also enter a manual list.
10. Click **Save** and **Show preview to continue**.

©2026 Tanium Inc. All Rights Reserved

11. A results grid displays at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

Result

Important: Uninstalling Comply does not remove Remote Authenticated Scanning (RAS), Network Unauthenticated Scanning (RUS), or Software Bill of Materials (SBOM). You must deploy a package for each one individually.



Remove the Comply solution from the Tanium Module Server

Uninstall the Comply solution from the Tanium Module Server and optionally remove the associated database.

1. From the Main menu, go to **Administration** > **Solutions**.

©2026 Tanium Inc. All Rights Reserved

2. In the Comply section, click **Uninstall**.
3. Review the content that will be removed and click **Uninstall**.
4. Depending on your configuration, enter your password or click **Yes** to start the uninstall process.
5. Return to the **Solutions** page and verify that the **Import** button is available for Comply.

Result

Note: When you uninstall Comply, the database and service files are not removed. This allows future installations to retain the previous state. On uninstall, the <Module Server>\services\comply-service-files are moved to <Module Server>\services\comply-service-files_<timestamp>.

To uninstall the database, you must run the following command on the Tanium Module Server:

- Windows

  : C:\Program Files\Tanium\TaniumModuleServer\services\rdb-service\TaniumRdbService.exe clear comply

- Linux/TanOS:

  /opt/Tanium/TaniumModuleServer/services/rdb-service/TaniumRdbService clear comply

Contact Tanium Support

To contact Tanium Support for help, sign in to the Tanium Customer Community.

For more information about submitting a support case, see Case Submission Form.

©2026 Tanium Inc. All Rights Reserved

Reference: Supported engines and JREs

This topic lists the engines and Java Runtime Environments (JREs) that are validated and supported for use with Comply.

The following engines and JREs are supported in Comply.

Note: Supported engines and JREs are published after internal validation. Regular updating is recommended.

CIS-CAT

CIS-CAT engine support

Version
4.0 through 4.62.0

Note: CIS-CAT versions later than 4.62.0 require Java 21 and are not supported.

SCC

SCC engine support

Version	Filename
5.4	scc-5.4_Windows_bundle.zip
	scc-5.4_ubuntu16_amd64_bundle.zip
	scc-5.4_macosx10_x86_64_bundle.zip

©2026 Tanium Inc. All Rights Reserved

Version	Filename
	scc-5.4_rhel6_i686_bundle.zip
	scc-5.4_rhel6_x86_64_bundle.zip
	scc-5.4_rhel7_x86_64_bundle.zip
5.4 (embedded*)	scc-5.4_Windows_bundle.zip
	scc-5.4_ubuntu16_amd64_bundle.tar.gz
	scc-5.4_macosx10_x86_64_bundle.tar.gz
	scc-5.4_rhel6_i686_bundle.tar.gz
	scc-5.4_rhel6_x86_64_bundle.tar.gz
	scc-5.4_rhel7_x86_64_bundle.tar.gz
5.4.2	scc-5.4.2_Windows_bundle.zip
	scc-5.4.2_ubuntu16_amd64_bundle.tar.gz
	scc-5.4.2_macosx10_x86_64_bundle.tar.gz
	scc-5.4.2_rhel6_i686_bundle.tar.gz
	scc-5.4.2_rhel6_x86_64_bundle.tar.gz
	scc-5.4.2_rhel7_x86_64_bundle.tar.gz
5.4.2 (*embedded)	scc-5.4.2_Windows_bundle.zip
	scc-5.4.2_ubuntu16_amd64_bundle.tar.gz
	scc-5.4.2_macosx10_x86_64_bundle.tar.gz
	scc-5.4.2_rhel6_i686_bundle.tar.gz
	scc-5.4.2_rhel6_x86_64_bundle.tar.gz
	scc-5.4.2_rhel7_x86_64_bundle.tar.gz
5.5	scc-5.5_Windows_bundle.zip
	scc-5.5_ubuntu16_amd64_bundle.zip
	scc-5.5_macosx10_x86_64_bundle.zip
	scc-5.5_rhel6_i686_bundle.zip
	scc-5.5_rhel6_x86_64_bundle.zip
	scc-5.5_rhel7_x86_64_bundle.zip
5.5 (*embedded)	scc-5.5_Windows_bundle.zip
	scc-5.5_ubuntu16_amd64_bundle.zip
	scc-5.5_macosx10_x86_64_bundle.zip
	scc-5.5_rhel6_i686_bundle.zip
	scc-5.5_rhel6_x86_64_bundle.zip
	scc-5.5_rhel7_x86_64_bundle.zip

©2026 Tanium Inc. All Rights Reserved

Note: **Embedded* files are the zip/tar.gz files found within each corresponding SCC zip file.

Tanium Scan Engine 7.0

Tanium distributes TSE 7.0 to endpoints automatically through Tanium Endpoint Configuration. When an endpoint runs a Comply-CX version that meets the required threshold, Comply routes vulnerability scans to TSE 7.0.

Comply-CX version support for Tanium Scan Engine 7.0

Minimum Comply-CX version for Tanium Scan Engine 7.0 support		
Comply 2026H2	comply-cx 1.33.636	Tanium Scan Engine 7.0 for client-based vulnerability scans only
Comply 2026H1 MR11 and later	comply-cx 1.31.418	Tanium Scan Engine 7.0 for client-based vulnerability scans only
Upgrading to 2026H2 from 2026H1 MR11 and later will keep the minimum Comply-CX version needed for TSE 7.0 support at 1.31.418.		

Legacy Tanium Scan Engine (Joval)

Comply includes the Tanium Scan Engine and JREs with the Comply toolset to be managed through ECM. For more information, see Deploying the legacy Tanium Scan Engine and JRE using ECM on page 85.

Note: You cannot change default targeting for the Comply Engines tool. You can only change what endpoints are targeted. For more information, see Managing Tanium Client and endpoint tool upgrade rollouts.

Comply toolset version support for Tanium Scan Engines and JREs

Toolset	Tanium Scan Engines	JREs
2.39.125	TSE 6.6.5.1, TSE 6.4.6	Amazon Corretto JRE 11.0.30.7.1

©2026 Tanium Inc. All Rights Reserved

Toolset	Tanium Scan Engines	JREs
2.39.19	TSE 6.5.5.1, TSE 6.4.6	Amazon Corretto JRE 11.0.30.7.1

Default targeting for Tanium Scan Engines in ECM

Tanium Scan Engine	Default Targeting
6.6.5.1	All Computers (in the Comply action group) except for CentOS 5, RHEL 5, Oracle Linux 5, AIX, and Solaris.
6.4.6	CentOS 5, RHEL 5, Oracle Linux 5, AIX, and Solaris computers (in the Comply action group).

Note: The following version and support information applies to the Legacy Tanium Scan Engine (the Joval-based engine). For information about Tanium Scan Engine 7.0, see the Comply release notes.

The Legacy Tanium Scan Engine is packaged and distributed with a license file via ECF. Beginning with version 6.3.5, the license file format changed, and the new license is not backwards compatible with older versions of the engine. Each version of the engine is supported for a little more than a year after the release date.

The following table provides Legacy Tanium Scan Engine version and support information.

Legacy Tanium Scan Engine support information

Version	Release	Support EOL
6.6.5.1	4/24/2026	TBD
6.5.5.1 [1]	12/6/2024	TBD
6.4.6	10/22/2024	TBD
6.4.5.1-L	The 6.4.5.1 engine repackaged with a 3 year license.	
6.4.5.1	6/30/2023	8/15/2024

©2026 Tanium Inc. All Rights Reserved

Version	Release	Support EOL
6.4.4.3 [1]	5/9/2023	6/30/2024
6.4.4.1	9/29/2022	6/30/2024
6.4.2	3/11/2022	5/25/2023

[1] Joval 6.5 and later drops support for Java 8 and uses Tanium-provided Amazon Corretto JRE v11.x .

Joval 6.5.5.1 is available for targeting on endpoints that can run the Tanium-provided Amazon Corretto JRE v11.x. For endpoints that cannot run this version, such as Red Hat Enterprise Linux 5, Oracle Linux Server 5, CentOS 5, Solaris, AIX, Windows 7, and Server 2008 R2 targeting will default to the next engine in the Tanium Scan Engine priority list that supports earlier versions of JRE.

Java Runtime Environment (JRE)

The JRE information in this section applies to the legacy Tanium Scan Engine (Joval-based) only. Tanium Scan Engine (TSE) 7.0 client-based vulnerability scans do not require a Java runtime. The legacy engine is still used for compliance scans, remote authenticated scans (RAS), and endpoints that have not transitioned to TSE 7.0.

Note: Amazon Corretto Java Runtime Environment (JRE) version 11.x is provided for use with supported Windows, Linux, and macOS endpoints. JRE version 11.0.15.9.1 and later also support Mac on Apple silicon (M1 and later) and Amazon Linux 2 EC2.

A JRE that you upload must be Java 8.

Supported JRE distributions by operating system (legacy Tanium Scan Engine)

Operating system	Operating system version	Supported JRE distributions and versions	Can deploy using Comply?
Microsoft Windows Server	Microsoft Windows Server 2008 R2	Java version 8 distributions provided by Oracle	Yes [4]
	Microsoft Windows Server 2012	• JRE provided with Comply	Yes

©2026 Tanium Inc. All Rights Reserved

Operating system	Operating system version	Supported JRE distributions and versions	Can deploy using Comply?
	and 2012 R2	• Java version 8 distributions provided by either Oracle or Amazon	
	Microsoft Windows Server 2016 and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
Microsoft Windows Workstation	Microsoft Windows 7	Java version 8 distributions provided by Oracle	Yes [4]
	Microsoft Windows 10 and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
macOS	macOS 10.15 Catalina and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
Linux	Amazon Linux 2023	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	Amazon Linux 1 AMI (2016.09, 2018.03)	• JRE provided with Comply • Java version 8 distributions provided by Amazon	Yes
	Amazon Linux 2 LTS	• JRE provided with Comply • Java version 8 distributions provided by Amazon	Yes
	Debian 8.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	Red Hat Enterprise Linux (RHEL)	Upload your own version of Java 8	No [5]

©2026 Tanium Inc. All Rights Reserved

Operating system	Operating system version	Supported JRE distributions and versions	Can deploy using Comply?
	5.x		
	Red Hat Enterprise Linux (RHEL) 6.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	AlmaLinux 8.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	Rocky Linux 8.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	Oracle Linux 5.x and later	Java version 8 distributions provided by either Oracle or Amazon	Yes
	CentOS 6.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	SUSE Linux Enterprise Server (SLES) 12.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	openSUSE 12.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
	Ubuntu 14.x and later	• JRE provided with Comply • Java version 8 distributions provided by either Oracle or Amazon	Yes
AIX	IBM AIX 7.1 TL1SP10 and later [1]	IBM JRE 8	Yes [2]

©2026 Tanium Inc. All Rights Reserved

Operating system	Operating system version	Supported JRE distributions and versions	Can deploy using Comply?
		OpenJDK JRE version 8 with the HotSpot JVM	Yes [3]
	IBM AIX 7.2	IBM JRE version 8	Yes [2]
		OpenJDK JRE version 8 with the HotSpot JVM	Yes [3]
Solaris [4]	Oracle Solaris 10u11 SPARC	Oracle JRE 8	Yes [4]
	Oracle Solaris 10u11 x86 [1]	Oracle JRE 8	Yes [4]
	Oracle Solaris 11 SPARC	Oracle JRE 8	Yes [4]
	Oracle Solaris 11 x86 [1]	Oracle JRE 8	Yes [4]

[1] 64-bit only.

[2] Only IBM JRE 8 64-bit is supported for deployment through Comply. You must repackage the JRE before it can be deployed through Comply. For more information, see Repackage the IBM JRE for deployment to AIX endpoints on page 362 .

[3] Only version 8 is supported for deployment through Comply. Check the OpenJDK release site for supported service pack levels for a particular OpenJDK JRE release: AdoptOpenJDK: Latest release .

[4] Only version 8 is supported for deployment through Comply. Upload Java version 8 distributions provided by Oracle. See Import JREs on page 94 . This footnote applies to the legacy Tanium Scan Engine. Tanium Scan Engine 7.0 vulnerability scans on Solaris do not require a JRE.

[5] The JRE provided with Comply may not work with older versions of Linux. Refer to the support information provided in Amazon Corretto FAQs . Upload your own version of Java 8 if you have older versions of Linux.

©2026 Tanium Inc. All Rights Reserved

Reference: Remote authenticated scanning

Guidance for configuring privileges, platforms, and security controls so Comply can perform remote authenticated scans (RAS) effectively while minimizing errors and reducing credential exposure risk.

General best practices

Important: Remote Authenticated Assessment (RAS) support for Windows, Linux, MacOS, AIX, and Solaris devices will be removed in a future release. If you are currently using RAS to scan endpoints running these operating systems, you should move to client-based assessments.

The following sections provide recommendations for setting privileges for the Tanium Scan Engine (TSE) so Comply can perform remote authenticated scans with optimal results and minimal errors.

Note: Comply provides standards for scanning unmanaged endpoints using a remote authenticated scan. For more information, see Unmanaged Endpoints on page 34.

Background: The Tanium Scan Engine

The Tanium Scan Engine (TSE) is designed to collect all the information required to evaluate SCAP rules and OVAL definitions. When the TSE encounters an issue that prevents it from collecting required information, for example an access control issue or other error, that issue will be reflected in the results. This can mean "unknown" or "error" results for rules in some cases. In other cases, these errors may not impact the evaluation of a specific rule at all. The result always depends on a combination of the state of the machine being scanned and the construction of the rule logic.

©2026 Tanium Inc. All Rights Reserved

Background: Privileges

When planning privilege levels, the principle of "least privilege" directs you to only grant the exact rights required to perform a designated task. But in the context of vulnerability and configuration compliance scanning, the "least" privilege required to collect every conceivable piece of configuration data is total access to everything. This means unrestricted root-level access on Unix, and Administrator-level access on Windows. The practical reasons for this general conclusion are discussed later for each supported operating system.

You are free to use more restricted accounts for scanning with the TSE, but in doing so you must accept that this can (and in most cases will) result in at least some of the aforementioned unknown and error rule results. Therefore, a best practice for avoiding unknown and error results is for the TSE to be run using the highest privilege level available.

Microsoft Windows

On Windows, remote authenticated assessments should be configured using an account that is a member of the target machine's built-in Administrators group (S-1-5-32-544). For remote access questions, see Troubleshooting remote login issues on Windows on page 344.

While it is theoretically possible to create Windows accounts with very fine-grained access controls and with only the exact permissions the scan engine requires without being a member of the Administrators group, this has never been accomplished in the field despite many attempts by Tanium, the engine vendor (Joval), and OEM customers. Therefore, the TSE now checks for the presence of the Administrator role in the runtime user principal to determine whether the scanner has the necessary privileges to attempt certain actions, such as mounting user registry files or reading runtime environment data from running processes.

Unix/Linux/macOS

On Unix-type operating systems, the super-user (root) account has access to all resources on the machine. This is the account that should be used to invoke remote authenticated scans. For remote scanning purposes, the TSE can use either sudo or the su command to gain root access since the root account is not typically permitted to have login rights via SSH. The selection of sudo or su is chosen when creating the credential.

©2026 Tanium Inc. All Rights Reserved

It is possible to use a sudoers file on Linux to control which commands certain users are permitted to employ when using sudo. Tanium recommends not attempting to use this mechanism to restrict the commands available to the TSE for scanning purposes. The TSE dynamically constructs complex commands based on a combination of the SCAP content and detected configuration data on the system itself at scan-time. It wraps them inside invocations of '/bin/sh -c' (for a number of reasons), which would render such an allow list meaningless.

Note: If you are using the legacy Tanium Scan Engine with Joval on Ubuntu 26.x, RAS does not work with sudo escalation. This is because Rust-based sudo does not support the `"-E"` option that the Tanium Scan Engines uses. To use RAS with Ubuntu 26.x, change the machine back to the default non-Rust based version as follows:

```
update-alternatives --set sudo /usr/bin/sudo.ws
sudo --version | head -1      # expect: Sudo version 1.9.17p2
```

Although the TSE only reads configuration data (and only ever writes to temporary files), it must invoke certain commands that can be used to either get or set configurations. Even though Unix filesystem extended permissions could theoretically make it possible to create a user with execute permissions only in the Tanium Scan Engine's command vocabulary, at a practical level, the architecture of the Unix operating system makes creating such a user highly impractical.

Cisco

Cisco operating systems feature configurable levels of access control up to "level 15," which is the highest level of access control. Administrators can configure the OS to allow different commands and sub-commands at different privilege levels. When a command is invoked that is configured for a privilege level higher than the current login context, the Cisco operating system behaves as if the command does not exist.

There is no way of knowing why a command does not run as expected on Cisco operating systems. It could be because of a privilege level issue. It could also be because the command does not exist on the version of the OS or because some feature is not enabled. Cisco commands do not even have exit codes.

For this reason, the TSE cannot obtain definitive findings on an arbitrarily configured Cisco device unless it has level 15 access privileges. Comply is not able to make representations about the accuracy of rule results when run with lower privilege levels.

©2026 Tanium Inc. All Rights Reserved

Technically, it should be possible to create a privilege level that has permissions to run all the show commands that the TSE requires, in addition to the pwd and terminal commands, and such an account could be used for the purpose of scanning with the Tanium Scan Engine. However, such an account would need to enter this privilege level by default because its elevation implementation is currently written to only request level 15 privileges.

VMware and ESXi

For ESXi endpoints, when you configure the assessment, you target the IP address of VMware vCenter managing the ESXi hosts. You cannot connect directly to an ESXi host. After the scan completes, Endpoint Statistics displays the ESXi endpoints. Comply does not know about those ESXi endpoints until the scan is run. For best results, it is recommended that the account being used for the scan have the Administrator role to ensure that all rules/checks can evaluate as expected.

Troubleshooting remote login issues on Windows

There are several possible reasons a remote authenticated assessment may fail on a Windows target:

1. You have provided an incorrect password.

2. You are attempting to log in as a user who is not a member of the “Administrators” or “Remote Management Users” groups. In most cases, only members of these groups are able to log in via WS-Management.

3. The target machine is configured to disallow the “Negotiate” authentication method. To view permitted authentication methods on the target, run the command: winrm get winrm/config/Client/Auth

4. Due to User Account Control (UAC), the remote account must be a domain account and a member of the remote computer Administrators group. If the remote account is a local computer member of the Administrators group, then UAC will not allow access to the WinRM service. This problem has been observed after upgrading from Windows Management Framework 1.0 to 2.0; for example, on a Windows 2008 (non-R2) Server machine.

   To access a remote WinRM service in a workgroup, you must disable UAC filtering for local accounts by creating the following **DWORD** registry and setting its value to **1**:

©2026 Tanium Inc. All Rights Reserved

- LocalAccountTokenFilterPolicy registry value: Key Path: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Value Name: **LocalAccountTokenFilterPolicy**
- Type: **DWORD**
- Value: **1**

5. Ensure the necessary firewall rules are in place to allow the satellite to connect to the remote target using WinRM on TCP port 5985. WinRM must be enabled on the remote target.
6. Review the Host and network security requirements on page 36 for unmanaged endpoints.

Security best practices

While performing remote authenticated scans (RAS), it is necessary for IT and security organizations to maintain the necessary level of visibility and control as these scans carry more risk than local scans.

Note: When a new, unmanaged endpoint is detected on a network, there is currently no way for a program to determine whether this endpoint is legitimate or belongs to an attacker. If a tool attempts to perform an authenticated scan against an attacker-controlled endpoint, the attacker could potentially learn credentials that are valid on other endpoints and use them to pivot from a network-based position to gain unauthorized access to endpoints targeted by the scanner. See https://www.atredis.com/blog/2020/1/26/flamingo-captures-credentials for information on how IT/Security products spray credentials.

Tanium has implemented several mitigating controls within Comply to enable customers to use this feature while limiting the risk they are exposed to. The following section documents the security best practices when using remote authenticated scans and how users may configure RAS to best mitigate risk.

1. First and foremost, Tanium recommends that customers prefer local scans over remote scans. If an endpoint can be managed by the Tanium Client, installing the Tanium Client on this endpoint is the preferred and most secure way.
2. When setting up credentials for RAS assessments, it is recommended you select **SSH Key** as

©2026 Tanium Inc. All Rights Reserved

opposed to **Password** when possible. The risk associated with a malicious actor stealing a public key is negligible compared to stealing a password. Currently, SSH authentication is only available for non-Windows endpoints.

3. When using SSH Keys and password credentials (non-Windows) for RAS assessments, it is recommended you also use fingerprint comparison enabled using the **Trust on First Use** checkbox on the assessment page. With this feature, Comply trusts an endpoint on the first connection and collects the SSH fingerprint. The endpoint must then present the same SSH fingerprint on every future connection or Comply will log an error that the fingerprint has changed and the endpoint may be compromised. Endpoints with fingerprint mismatch errors are not scanned.

4. You should regularly rotate passwords used for remote authenticated scans, but do not reuse those credentials for endpoints that are not targeted by RAS to limit the extent of horizontal pivot.

5. Avoid attempting a large number of authentications against individual endpoints (the kitchen sink approach). If there is one malicious endpoint on your network, and you have an assessment that contains 100 password credentials, the scan could potentially try all those credentials against the malicious endpoint and then all 100 of those credentials are compromised. This approach could also have performance implications. Instead, plan your assessments in a logical, purposeful way that uses a targeted, limited number of credentials for each scan. For example, you could group routers together in one assessment, configure one credential list for the group, and not use this list for other assessments.

6. Avoid usage of the **Include newly discovered endpoints on recurring scans** option when feasible. By default, if scans are recurring, Comply only scans endpoints that were reachable during the initial scan. If new endpoints come online, they are not scanned unless you change the assessment's targeting or select to automatically include new endpoints. This means that even if an attacker gains unauthorized network access, Comply scans will not automatically send credentials to the attacker controlled endpoint unless a Tanium user instructs it to do so. While this option has the benefit of not having to change the configuration if a new endpoint comes online, it introduces a significant risk as you are going to authenticate against an attacker’s endpoint and compromise your credentials.

©2026 Tanium Inc. All Rights Reserved

Reference: Common errors in Comply

Review common Comply error messages, their causes, and recommended solutions.

Review common Comply error messages and possible solutions. For information about general errors in Comply, see Troubleshooting Comply on page 310.

COMPLY_STATUS_COULD_NOT_FIND_ENGINE

Error type: Health check - `Could not find matching engine configured for scan.`

Cause

This occurs when the engine (Legacy Tanium Scan Engine, Tanium Scan Engine 7.0, CIS-CAT, or SCC) targeted for an endpoint cannot be found or is not configured.

Solution

Check your targeting. Engines must be targeted for the correct endpoints.

COMPLY_STATUS_DB_CORRUPTED

Error type: Health check - `Database may be corrupted. Not performing any scans.`

Cause

This may occur if the database is being connected to manually while Comply is writing to it.

Solution

The database is automatically deleted and reset when the client is restarted. To prevent database corruption, do not manually interact with the database outside of Tanium.

©2026 Tanium Inc. All Rights Reserved

COMPLY_STATUS_ENGINE_SETUP_FAILURE_JRE

Error type: Health check - `Engine setup failure: Could not setup JRE.`

Cause

This can occur if a bad JRE zip file was deployed, if there was an issue with encryption for the JRE, or if there is a problem with security exclusions or antimalware software. This message may appear if the JAVA_TOOL_OPTIONS environment variable is defined. For more information, see Java tool options when executing java on page 317.

Solution

Check for a Security exclusions on page 37 issue, an antimalware software issue, or any other software trying to catch script executions.

COMPLY_STATUS_FAILED_STOP_ENGINE_TIMEOUT

Error type: Health check - `Failed to stop one or more engines, engine in scanning state.`

Cause

This may occur if a current scan needs to be stopped. For instance, if the same scan is set to run in debug mode, the current scan will be stopped.

Solution

Redeploy the scan.

COMPLY_STATUS_INSTALL_FAILURE

Error type: Health check - `Installation failure for ECF category.`

Cause

This type of failure could be due to insufficient disk space or an issue with security exclusions.

©2026 Tanium Inc. All Rights Reserved

Solution

If this occurs, check Security exclusions on page 37 and make sure disk space requirements are met.

COMPLY_STATUS_INVALID_JAVA

Error type: Health check - `The java executable in the package is invalid for this system.`

Cause

This may occur if the wrong executable was targeted for an endpoint. For example, if a Windows JRE is targeted to a Linux endpoint.

Solution

Check your targeting.

COMPLY_STATUS_JRE_INSUFFICIENT_MEMORY_FOR_HEAP

Error type: Health check - `Insufficient memory to run the engine.`

Cause

This only occurs on Windows and Linux endpoints. Comply checks the heap size defined in the profile configuration or custom configuration, and if there's more heap size defined than what is available on the system, this message may appear. In some circumstances, with virtual systems that dynamically allocate memory, the system may not yet have allocated the necessary amount of memory at start up. If so, this message may appear.

Solution

Allocate sufficient memory or scans will not run.

©2026 Tanium Inc. All Rights Reserved

Legacy Tanium Scan Engine [compliance or vulnerability] scan failure

Error type: Health check for ComplyCX 1.5

This legacy Tanium Scan Engine scan failure message may appear if the JAVA_TOOL_OPTIONS environment variable is defined. For more information, see Java tool options when executing java on page 317. If debug is enabled or low resources mode is configured, error could appears as follows: Joval [debug] [low resource] [compliance or vulnerability] scan failure: <error string>

Error string could be one of the following:

- Scan failure - See scan output logs for more details
- Low resource scan failure - See scan output logs for more details
- Configuration file was not found
- Schema validation error in an input intel XML
- Not enough memory was allocated to run scan



Note: If you encounter this error, you can try increasing the Java heap size memory allocation using Comply Custom Settings. For more information, see Custom settings on page 103

Nmap network scan failure

Error type: Health check for network unauthenticated scans

When an nmap scan fails, (where debug is enabled) the following error may appear as follows: `Nmap [debug] network scan failure: <error string>`

Error string could be one of the following:

- Generic error - An unspecified error reported by the nmap provider (in Extras CX) or other internal error.
- Timeout error - A scan timeout, as reported by the nmap provider.

©2026 Tanium Inc. All Rights Reserved

- Executable error <exit code> [(overflow!)] - A non-zero, signed 32-bit exit code from the nmap binary, as reported by the nmap provider. Some large magnitude exit codes cannot be represented. For these, the (overflow!) warning will be appended.
- Results write error - The scan completed successfully with results, but there was an error producing the results output.

Could not add scan – bad configuration?

Error type: Health check for scans

Cause

An attempt was made to add a scan with a bad configuration, such as missing required fields, this scan already exists, or other various reasons. This generally indicates an internal error between the Comply service and Comply CX.

Solution

This error is not user actionable.

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.

COMPLY-ENGINETIMEOUT

Cause

The Legacy Tanium Scan Engine is stuck on a particular task that exceeds the engine timeout threshold and sends this error to Comply CX. This is a catch-all message for several engine timeout issues. For example, this error may occur if a vulnerability scan with a find command is searching a large file system and the engine hits a timeout before the search can complete.

Solution

Check the following log files (the highest numbered files) from the endpoint for further information, *-LOCALHOST.log, *-_scan.log, *-stdout.txt. For more information, see Locate log files on page 312.

©2026 Tanium Inc. All Rights Reserved

COMPLY-EXCEPTION

Error type: Sensor, assessment status

Cause

This may be due to an OS problem, such as Windows file locking.

Solution

Look for health check issues and get log files from the endpoint. For more information, see Locate log files on page 312.

COMPLY-INVALID-ERROR-ENUM

Error type: Sensor, assessment status

Cause

The assessment status provided an invalid error number. The number may be invalid due to having been retired. This can occur for endpoints that have recently upgraded from an older version of the comply-cx endpoint tool and have not performed the associated scan with the upgraded software.

Solution

Re-run the scan with the upgraded software.

COMPLY-JVMEXCEPTION

Error type: Sensor, assessment status

Cause

The Java-based scan engine encountered a runtime exception. This can occur due to a defect in the underlying scan engine, external factors like resource exhaustion, or misconfigured custom Java runtime settings (debug libraries).

©2026 Tanium Inc. All Rights Reserved

Solution

Try re-running the scan. If the cause is external factors, they may be transient. You could also try splitting the scan by severity to see if that helps with a possible resource exhaustion issue.

COMPLY-NO-CHECKS-EVALUATE

Error type: Sensor, assessment status

Cause

The assessment was not able to evaluate any of the specified checks on the endpoint. This usually means the targeting is incorrect. The content you targeted for that endpoint does not apply to the endpoint.

Solution

Check the targeting. For example, make sure Windows vulnerabilities aren't targeted for a Red Hat Linux machine.

COMPLY-NOCISCAT

Error type: Sensor, assessment status

Cause

The assessment is configured to use the CIS-CAT scan engine, but it was not found on the endpoint

Solution

Go to your configuration and deploy CIS-CAT to the endpoint before redeploying the assessment. For more information, see Download and import the CIS-CAT engine on page 88.

COMPLY-NOINTEL

Error type: Sensor, assessment status

©2026 Tanium Inc. All Rights Reserved

Cause

Something went wrong assembling the intel for the scan on the endpoint.

Solution

Try deleting and re-creating the assessment, or uninstalling and re-installing Comply CX on the endpoint.

COMPLY-NOJRE

Error type: Sensor, assessment status

Cause

The assessment was supposed to use a scan engine that requires a JRE and none were found on the endpoint. This message could also indicate the wrong JRE is on the endpoint.

Solution

Make sure you targeted a JRE at the endpoint, and if so, that the one you targeted is correct. For more information, see Upload a Java Runtime Environment (JRE) package on page 93.

COMPLY-NORESULTS

Error type: Sensor, assessment status

Cause

The assessment did not generate a result on the endpoint. This can happen when the assessment runs, but the engine encounters an issue due to bad content, such as benchmark rules or oval definitions.

Solution

Look at logs on the endpoint for a more specific reason for this message. For more information, see Locate log files on page 312.

©2026 Tanium Inc. All Rights Reserved

COMPLY-NOSCC

Error type: Sensor, assessment status

Cause

The assessment is configured to use the SCC scan engine, but none were found on the endpoint.

Solution

Go to your configuration and deploy SCC to the endpoint before redeploying the assessment. For more information, see Download and import the SCC scan engine on page 91.

COMPLY-SCANTIMEOUT

Error type: Sensor, assessment status

Cause

The scan took longer than six hours.

Solution

It may need more time or you may need to scan fewer CVE's or use larger intel chunks and/or a larger heap size. Alternatively, in the assessment page, under **Scan Timeout**, you can change the default of 6 hours to allow for scans that may take more time. For more information, see Creating compliance assessments on page 121 and Creating vulnerability assessments on page 146.

COMPLY-UNKNOWN

Error type: Sensor, assessment status

Cause

There was a unknown error when the assessment attempted to run on the endpoint. This is a catch-all message for several issues.

©2026 Tanium Inc. All Rights Reserved

Solution

Likely there were health check messages that were ignored before the fatal message appeared. Look for health check issues and get log files from the endpoint. For more information, see Locate log files on page 312.

Failed_Auth

Error type: Sensor, assessment status

Cause

The assessment failed to login to an unmanaged endpoint to evaluate the assessment on that endpoint. In a RAS scan, the provided credentials did not work for the targeted endpoint.

Solution

Check that the provided credentials are correct for the endpoint.

©2026 Tanium Inc. All Rights Reserved

Reference: Deprecated sensors

Lists deprecated Comply sensors and, where available, their recommended replacements.

Deprecated Comply sensors Download as CSV

Name	Content	Category	Description
Comply - All Engine Versions	Comply - Has Engine Versions	Comply Deployment	[DEPRECATED] Returns true/false based on endpoint containing all specified deployment values.
Comply - CIS-CAT Results	Comply Reporting	Compliance	[DEPRECATED] Returns the configuration compliance results for the given report hash.
Comply - CIS-CAT Results - Full	Comply Reporting	Compliance	[DEPRECATED] Returns the full configuration compliance results for the given report hash.
Comply - CIS-CAT Vulnerabilities	Comply Reporting	Compliance	[DEPRECATED] Returns found vulnerabilities for the given report hash.
Comply - CIS-CAT Vulnerabilities - Full	Comply Reporting	Compliance	[DEPRECATED] Returns found vulnerabilities for the given report hash.
Comply - Has Engine Versions	Comply Deployment	Compliance	[DEPRECATED] Returns true/false based on endpoint containing all specified deployment values.
Comply - JovalCM Results	Comply Reporting	Compliance	[DEPRECATED] Returns the configuration compliance results for the given report hash.
Comply - JovalCM	Comply Reporting	Compliance	[DEPRECATED] Returns the full configuration compliance results for the given report hash.

©2026 Tanium Inc. All Rights Reserved

Name	Content	Category	Description
Results - Full			
Comply - JovalCM Vulnerabilities	Comply Reporting	Compliance	[DEPRECATED] Returns found vulnerabilities for the given report hash.
Comply - JovalCM Vulnerabilities - Full	Comply Reporting	Compliance	[DEPRECATED] Returns found vulnerabilities for the given report hash.
Comply - Metrics Engines Deployed	Comply Deployment	Compliance	[DEPRECATED] Returns 'SCC', 'CIS-CAT', 'Tanium Scan Engine', 'No Engine Installed'.
Comply - Metrics Tools Deployed	Comply Deployment	Compliance	[DEPRECATED] Returns 'Deployed' if Comply tools are deployed. 'Not Deployed' otherwise.
Comply - Metrics Tools Outdated	Comply Deployment	Compliance	[DEPRECATED] Returns 'Current' if Comply tools are up to date. 'Outdated' if Comply tools are deployed but old. 'not installed' otherwise.
Comply - Tools Version	Comply Deployment	Compliance	[DEPRECATED] Returns Comply tools version number.
Comply - Open Ports Full	Comply Reporting	Compliance	[DEPRECATED] Identifies the listening TCP ports, including the process listening to the port, the display name of the process (if available), and the listening IP Address and port. The sensor definition can be modified to exclude process and IP range.
Comply - SCC Results	Comply Deployment	Compliance	[DEPRECATED] Returns the configuration compliance results for the given report hash.
Comply - SCC Results - Full	Comply Deployment	Compliance	[DEPRECATED] Returns the full configuration compliance results for the given report hash.

©2026 Tanium Inc. All Rights Reserved

Name	Content	Category	Description
Comply - SCC Vulnerabilities	Comply Deployment	Compliance	[DEPRECATED] Returns found vulnerabilities for the given report hash.
Comply - SCC Vulnerabilities - Full	Comply Deployment	Compliance	[DEPRECATED] Returns found vulnerabilities for the given report hash.
Comply - Has High Vulnerabilities	Comply Reporting	Compliance	[DEPRECATED] Returns "Vulnerabilities Found" if endpoint has high vulnerabilities. "No Vulnerabilities Found" otherwise.
Comply - Vulnerability Findings Aggregate	Comply Reporting	Compliance	[DEPRECATED] Returns the most severe Vulnerability level reported (High, Medium, Low, Unscored, No Vulnerabilities).
Comply - Vulnerability Aggregates	Comply Reporting	Compliance	[DEPRECATED] Aggregates vulnerability result data from scans.
Comply - Hygiene - Outdated High Severity Vulnerabilities	Default	Comply	[DEPRECATED] Parses vulnerability results on targeted endpoints and returns the normalized operating system of the targeted endpoint if discovered vulnerability scan results have a severity score of 7.0 (High Severity under CVSSv2) or higher _and_ those vulnerability results originate from calendar year 2019 or earlier. Parameter input must be either blank to target all available reports on the targeted endpoint, or be a comma-separated list of at least one Tanium Comply report hash (e.g. b31337c1 or 6c750c51,b31337c1).
Comply - Hygiene - Product Vulnerability Results	Default	Comply	[DEPRECATED] Pulls back the discovered CVEs, Release Year, Severities, and Titles for detected vulnerabilities on an endpoint based on the report hashes targeted and the product strings provided. To target vulnerabilities for Adobe, for example, use parameters (Adobe,adobe). Must be either blank to target all available reports on targeted endpoint, or comma-separated list of at least one Tanium Comply report hash (e.g. b31337c1 or 6c750c51,b31337c1).
Comply - Hygiene -	Default	Comply	[DEPRECATED] Pulls back the discovered CVEs, Release Year, Severities, and Titles for detected vulnerabilities on an endpoint based on the report hashes or max

©2026 Tanium Inc. All Rights Reserved

Name	Content	Category	Description
Vulnerability Results			report age targeted. Must be either blank to target all available reports on targeted endpoint, or comma-separated list of at least one Tanium Comply report hash (e.g. b31337c1 or 6c750c51,b31337c1).
Comply - Max Vulnerability Score	Comply Reporting	Compliance	[DEPRECATED] Returns the highest CVSS score of any vulnerability found on an endpoint.
Comply - Metrics Vulnerability Counts	Comply Reporting	Compliance	[DEPRECATED] Counts the number of vulnerabilities by level.
Comply - Compliance Results Joined	Comply Reporting	Compliance	[DEPRECATED] Returns the configuration compliance results for the given report hash joined into a single field.
Comply - Vulnerability CVE Search	Comply Reporting	Vulnerability	[DEPRECATED] Searches vulnerability results for CVE.
Comply - Compliance Findings	Comply Reporting	Compliance	[DEPRECATED] Returns the unique compliance findings present on an endpoint. Use **Comply - Compliance Status** instead.
Comply - CVE Findings	Comply Reporting	Vulnerability	[DEPRECATED] Returns the unique vulnerability findings (CVEs) present on an endpoint. Use **Comply - Vulnerability Status** instead.
Comply - Compliance Findings - First Found	Comply Reporting	Compliance	[DEPRECATED] This returns the first found date for all the unique compliance findings present on an endpoint. If the compliance finding state changes (from Pass to Fail, for example), this date is reset to the new discovery date. Use **Comply - Compliance Status** instead.
Comply - Compliance Findings -	Comply Reporting	Compliance	[DEPRECATED] This returns the last scan date for all the unique compliance findings present on an endpoint. Use **Comply - Compliance Status** instead.

©2026 Tanium Inc. All Rights Reserved

Name	Content	Category	Description
Last Scan			
Comply - CVE Findings - First Found	Comply Reporting	Vulnerability	[DEPRECATED] Returns the first time a vulnerability is identified in an environment. Note that if a vulnerability is found and remediated and then found again, the first found date is set to the date of the most recent first finding. Use **Comply - Vulnerability Status** instead.
Comply - CVE Findings - Last Found	Comply Reporting	Vulnerability	[DEPRECATED] Returns the last found date for all observed vulnerabilities that the endpoint is currently vulnerable to. Use **Comply - Vulnerability Status** instead.
Comply - CVE Findings - Absolute First Found	Comply Reporting	Vulnerability	[DEPRECATED] Returns the very first time a vulnerability is found on an endpoint. This date is not reset if the vulnerability is remediated. Use **Comply - Vulnerability Status** instead.
Comply - CVE Findings - Last Scan	Comply Reporting	Vulnerability	[DEPRECATED] Returns the last scan date for all observed vulnerabilities that the endpoint is currently vulnerable to. Use **Comply - Vulnerability Status** instead.

©2026 Tanium Inc. All Rights Reserved

Reference: Repackage the IBM JRE for deployment to AIX endpoints

Repackage IBM Java SE Version 8 (64-bit) on AIX so that the JRE can be deployed through Comply to AIX 6.1 and later endpoints.

Before you begin

You can deploy supported versions of OpenJDK JRE version 8 through Comply to endpoints running AIX 7.1 TL1SP10 and later or AIX 7.2. Check the OpenJDK release site for supported service pack levels for a particular OpenJDK JRE release: AdoptOpenJDK: Latest release.

The OpenJDK JRE version 8 does not support AIX 6.1; therefore, you must use the IBM JRE on AIX 6.1 endpoints.

If needed, you can deploy IBM Java SE Version 8 (64-bit) to AIX endpoints through Comply, but you must repackage it first to a format that is compatible with Comply.

Note: The IBM JRE is usually already installed on AIX endpoints and supported versions can be used with Comply 2.10 and earlier.

Repackage the JRE

Important: You must complete these steps on an AIX machine.

1. Download IBM Java SE Version 8 (64-bit).
2. Complete the following steps from a command line on an AIX machine:
    a. Move the downloaded JRE file to the directory where you want to extract the files.

©2026 Tanium Inc. All Rights Reserved

b. Change directory to the directory where you moved the file.

c. Run the following commands, which use these variables:

- `<downloaded file name>`: the file that you downloaded from the IBM website. For example, Java8_64.jre.8.0.0.610.tar.gz.
- `<extracted file name>`: the extracted file. For example, Java8_64.jre.
- `<extracted file path>`: the directory to which the file was extracted. For example, Java8_64.
- <file name for resulting file>: Name that you specify for the resulting file. This name must reflect the exact JRE version. For example, Java8_64.jre.8.0.0.605.tar.gz.

Important: You must name the file so that it reflects the exact IBM JRE version. For example, Java8_64.jre.8.0.0.605.tar.gz. In most cases, the file name will match the file name of the original JRE that you downloaded.

Important: For AIX Open JDK JRE, the format of the file name must include the following regex jre_ppc64_aix.*_(8u\d+).*\.tar\.gz

```
gzip -dc <downloaded file name> | tar -xof -
                                restore -qxvdf <extracted file name> .
                                cp -R usr/lpp/<extracted file name>/inst_root/
etc/<extracted file path>/jre/lib/* usr/<extracted file path>/jre/lib/
                                cd usr/<extracted file path>/
tar -cvf /tmp/<file name for resulting file>.tar jre
                                cd /tmp
                                //If you downloaded the original file to /tmp,
you must delete that file using the following command
// before you can create the resulting .tar file since the two files have the
same name.
                                //If you downloaded the file to a location
other than /tmp, skip to the last command
                                rm -rf <downloaded file name>
                                gzip <file name for resulting file>.tar
```

©2026 Tanium Inc. All Rights Reserved

The subsequent example shows the commands with actual filenames and paths.

Example

The following example shows the commands to generate the file that can be deployed through Comply.

This example uses these inputs:

- The version of the downloaded JRE is 8.0.0.605
- The file name for the downloaded JRE is Java8_64.jre.8.0.0.605.tar.gz
- The directory for file extraction is /tmp/jre_extract
- The resulting JRE file is Java8_64.jre.8.0.0.605.tar.gz (the same as the original downloaded JRE file)

```
cd /tmp/jre_extract
                        gzip -dc Java8_64.jre.8.0.0.605.tar.gz | tar -xof -
                        restore -qxvdf Java8_64.jre .
                        cp -R usr/lpp/Java8_64.jre/inst_root/etc/java8_64/jre/lib/* usr/
java8_64/jre/lib/
                        cd usr/java8_64/
                        tar -cvf /tmp/Java8_64.jre.8.0.0.605.tar jre
                        cd /tmp
                        gzip Java8_64.jre.8.0.0.605.tar
```

These commands produce a file, Java8_64.jre.8.0.0.605.tar.gz, that can be deployed to AIX endpoints through Comply.

©2026 Tanium Inc. All Rights Reserved

Reference: Gateway examples for Comply

Tanium Gateway GraphQL examples that show how to query endpoints for Comply compliance and vulnerability findings, including filtered result sets.

Tanium Gateway provides a GraphQL API integration point for Tanium solutions, including Comply. Comply queries retrieve endpoints and associated compliance or vulnerability findings.

For additional Gateway example syntax, see Tanium Gateway User Guide: Reference: Filter syntax and Tanium Gateway User Guide: Reference: Gateway examples.

Comply query filter syntax

Endpoint queries that request Comply-related information using `complianceFindings` or `cveFindings` support the `path` and `value` filter fields. Comply 2.16.97 or later is required to submit a request that filters specific System Vulnerability and System Compliance risk vector fields.

For more information on syntax, see `FieldFilter` in the **Documentation Explorer** pane of the query explorer.

Single column

You can filter on field values. Define a filter object using one of the following syntaxes:

```
complianceFindings(filter:
  {
    path: "field-path",
    op: "operator-value",
    value: "field-value"
  }
)
```

```
cveFindings(filter:
  {
    path: "field-path",
    op: "operator-value",
    value: "field-value"
  }
)
```

©2026 Tanium Inc. All Rights Reserved

Use dot notation for sub-fields not at the root level. You can filter the endpoints returned and filter the endpoints based on Comply information in a single request.

For example, the following query retrieves the first endpoint with a compliance findings `category` of `Error` and returns that endpoint's associated compliance findings:

```
query exampleFilterComplianceFindings($first: Int) {
  endpoints(first: $first) {
    edges {
      node {
        name
        ipAddress
        compliance {
          complianceFindings(filter: {
            path: "category"
            value: "Error"
          }) {
            category
            id
            profile
            profileVersion
            rule
            ruleId
            standard
            standardVersion
            state
          }
        }
      }
    }
    pageInfo {
      startCursor
      endCursor
      hasPreviousPage
      hasNextPage
    }
  }
}
```

Include the cursor variable in the **Variables** panel or in your variables dictionary:

```
{
  "first": 1
}
```

Multiple columns

You can filter on multiple Comply-related columns. Define a filter object using one of the following syntaxes:

```
complianceFindings(filter:
  {any: boolean,
    filters: [
      {path: "field-path-1", op: "operator-1", value: "filter-value-1"},
      {path: "field-path-2", op: "operator-2", value: "filter-value-2"},
      {path: "field-path-n", op: "operator-n", value: "filter-value-n"}
```

©2026 Tanium Inc. All Rights Reserved

```
    ]
  }
)
```

```
cveFindings(filter:
  {any: boolean,
    filters: [
      {path: "field-path-1", op: "operator-1", value: "filter-value-1"},
      {path: "field-path-2", op: "operator-2", value: "filter-value-2"},
      {path: "field-path-n", op: "operator-n", value: "filter-value-n"}
    ]
  }
)
```

Use dot notation for sub-fields not at the root level. You can filter the endpoints returned and filter the endpoints based on Comply information in a single request.

For example, the following query retrieves the first endpoint that is a member of the All Mac computer group, with a vulnerability findings `cveYear` of `2020` and `cvssScore` value of `5`, and returns that endpoint's associated vulnerability findings:

```
query exampleFilterMacOSEndpointVulnerability($first: Int!) {
  endpoints(first: $first, filter: {memberOf: {name: "All Mac"}}) {
    edges {
      node {
        name
        ipAddress
        compliance {
          cveFindings(
            filter: {any: false, filters: [{path: "cveYear", value: "2020"}, {path:
"cvssScore", value: "5"}]}
          ) {
            cveId
            cveYear
            cvssScoreV3
            firstFound
            lastFound
            severityV3
            summary
          }
        }
      }
    }
    pageInfo {
      startCursor
      endCursor
      hasPreviousPage
      hasNextPage
    }
  }
}
```

Include the cursor variable in the **Variables** panel or in your variables dictionary:

```
{
  "first": 1
}
```

©2026 Tanium Inc. All Rights Reserved

Get endpoints with compliance findings information

`query.endpoints.edges.node.compliance.complianceFindings`

Get endpoint compliance findings information

The following query retrieves the first endpoint and associated compliance findings.

```
query exampleEndpointComplianceFindings($first: Int!) {
  endpoints(first: $first) {
    edges {
      node {
        name
        ipAddress
        compliance {
          complianceFindings {
            category
            excepted
            firstFoundDate
            id
            lastScanDate
            profile
            profileVersion
            rule
            ruleId
            standard
            standardVersion
            state
          }
        }
      }
    }
    pageInfo {
      startCursor
      endCursor
      hasPreviousPage
      hasNextPage
    }
  }
}
```

Include the cursor variable in the **Variables** panel or in your variables dictionary:

```
{
  "first": 1
}
```

Example response:

```
{
  "data": {
    "endpoints": {
      "edges": [
```

©2026 Tanium Inc. All Rights Reserved

```
        {
          "node": {
            "name": "comply-findings",
            "ipAddress": "192.0.2.10",
            "compliance": {
              "complianceFindings": [
                {
                  "category": "Fail",
                  "excepted": false,
                  "firstFoundDate": "2023-01-01",
                  "id": "CIS Microsoft Windows 10 Enterprise Release 20H2 Benchmark;1.10.1;MB
Custom
Win10;xccdf_com.tanium.comply_tailoring_1639024882628;xccdf_org.cisecurity.benchmarks_rule_18
.9.4.1_L2_Ensure_Allow_a_Windows_app_to_share_application_data_between_users_is_set_to_Disabl
ed",
                  "lastScanDate": "2023-02-02",
                  "profile": "MB Custom Win10",
                  "profileVersion": "xccdf_com.tanium.comply_tailoring_1639024882628",
                  "rule": "(L2) Ensure 'Allow a Windows app to share application data between
users' is set to 'Disabled'",
                  "ruleId":
"xccdf_org.cisecurity.benchmarks_rule_18.9.4.1_L2_Ensure_Allow_a_Windows_app_to_share_applica
tion_data_between_users_is_set_to_Disabled",
                  "standard": "CIS Microsoft Windows 10 Enterprise Release 20H2 Benchmark",
                  "standardVersion": "1.10.1",
                  "state": "fail"
                }
              ]
            }
          }
        }
      ],
      "pageInfo": {
        "startCursor": "NTc2NTM4MDow",
        "endCursor": "NTc2NTM4MDoxOQ==",
        "hasPreviousPage": false,
        "hasNextPage": true
      }
    }
  }
}
```

Get filtered endpoint compliance findings information

The following query requires Comply 2.16.97 or later and retrieves the first endpoint with a compliance finding `category` of `Error` and `FirstFoundDate` greater than or equal to `2025-07-10` and then returns the associated compliance findings for that endpoint with a `category` of `Error`.

```
query exampleFilterComplianceFindings($first: Int) {
  endpoints(first: $first) {
    edges {
      node {
        name
        ipAddress
        compliance {
          complianceFindings(
```

```
            filter: {any: false, filters: [{path: "category", value: "Error"}, {path:
"firstFoundDate", op: GTE, value: "2025-07-10"}]}
          ) {
            category
            firstFoundDate
            id
            lastScanDate
            profile
            profileVersion
            rule
            ruleId
            standard
            standardVersion
            state
          }
        }
      }
    }
    pageInfo {
      startCursor
      endCursor
      hasPreviousPage
      hasNextPage
    }
  }
}
```

Include the pagination variable in the **Variables** panel or in your variables dictionary:

```
{
  "first": 1
}
```

Example response:

```
{
  "data": {
    "endpoints": {
      "edges": [
        {
          "node": {
            "name": "IsolatedVM-Pdejesus",
            "ipAddress": "192.10.1.102",
            "compliance": {
              "complianceFindings": [
                {
                  "category": "Error",
                  "firstFoundDate": "2025-07-12",
                  "id": "Microsoft Windows 11 STIG SCAP Benchmark;002.001;I - Mission
Critical Public;1;xccdf_mil.disa.stig_rule_SV-253275r958478_rule",
                  "lastScanDate": "2025-07-12",
                  "profile": "I - Mission Critical Public",
                  "profileVersion": "1",
                  "rule": "Internet Information System (IIS) or its subcomponents must not be
installed on a workstation.",
                  "ruleId": "xccdf_mil.disa.stig_rule_SV-253275r958478_rule",
                  "standard": "Microsoft Windows 11 STIG SCAP Benchmark",
                  "standardVersion": "002.001",
                  "state": "error"
                },
                {
```

©2026 Tanium Inc. All Rights Reserved

```
                  "category": "Error",
                  "firstFoundDate": "2025-07-12",
                  "id": "Microsoft Windows 11 STIG SCAP Benchmark;002.001;I - Mission
Critical Public;1;xccdf_mil.disa.stig_rule_SV-253278r958480_rule",
                  "lastScanDate": "2025-07-12",
                  "profile": "I - Mission Critical Public",
                  "profileVersion": "1",
                  "rule": "The Telnet Client must not be installed on the system.",
                  "ruleId": "xccdf_mil.disa.stig_rule_SV-253278r958480_rule",
                  "standard": "Microsoft Windows 11 STIG SCAP Benchmark",
                  "standardVersion": "002.001",
                  "state": "error"
                },
                {
                  "category": "Error",
                  "firstFoundDate": "2025-07-12",
                  "id": "Microsoft Windows 11 STIG SCAP Benchmark;002.001;I - Mission
Critical Public;1;xccdf_mil.disa.stig_rule_SV-253287r958478_rule",
                  "lastScanDate": "2025-07-12",
                  "profile": "I - Mission Critical Public",
                  "profileVersion": "1",
                  "rule": "The Server Message Block (SMB) v1 protocol must be disabled on the
SMB server.",
                  "ruleId": "xccdf_mil.disa.stig_rule_SV-253287r958478_rule",
                  "standard": "Microsoft Windows 11 STIG SCAP Benchmark",
                  "standardVersion": "002.001",
                  "state": "error"
                },
                {
                  "category": "Error",
                  "firstFoundDate": "2025-07-12",
                  "id": "Microsoft Windows 11 STIG SCAP Benchmark;002.001;I - Mission
Critical Public;1;xccdf_mil.disa.stig_rule_SV-253279r958480_rule",
                  "lastScanDate": "2025-07-12",
                  "profile": "I - Mission Critical Public",
                  "profileVersion": "1",
                  "rule": "The TFTP Client must not be installed on the system.",
                  "ruleId": "xccdf_mil.disa.stig_rule_SV-253279r958480_rule",
                  "standard": "Microsoft Windows 11 STIG SCAP Benchmark",
                  "standardVersion": "002.001",
                  "state": "error"
                },
                {
                  "category": "Error",
                  "firstFoundDate": "2025-07-12",
                  "id": "Microsoft Windows 11 STIG SCAP Benchmark;002.001;I - Mission
Critical Public;1;xccdf_mil.disa.stig_rule_SV-253285r958478_rule",
                  "lastScanDate": "2025-07-12",
                  "profile": "I - Mission Critical Public",
                  "profileVersion": "1",
                  "rule": "The Windows PowerShell 2.0 feature must be disabled on the
system.",
                  "ruleId": "xccdf_mil.disa.stig_rule_SV-253285r958478_rule",
                  "standard": "Microsoft Windows 11 STIG SCAP Benchmark",
                  "standardVersion": "002.001",
                  "state": "error"
                },
                {
                  "category": "Error",
                  "firstFoundDate": "2025-07-12",
                  "id": "Microsoft Windows 11 STIG SCAP Benchmark;002.001;I - Mission
Critical Public;1;xccdf_mil.disa.stig_rule_SV-253286r958478_rule",
                  "lastScanDate": "2025-07-12",
                  "profile": "I - Mission Critical Public",
```


©2026 Tanium Inc. All Rights Reserved

```
                  "profileVersion": "1",
                  "rule": "The Server Message Block (SMB) v1 protocol must be disabled on the
system.",
                  "ruleId": "xccdf_mil.disa.stig_rule_SV-253286r958478_rule",
                  "standard": "Microsoft Windows 11 STIG SCAP Benchmark",
                  "standardVersion": "002.001",
                  "state": "error"
                },
                {
                  "category": "Error",
                  "firstFoundDate": "2025-07-12",
                  "id": "Microsoft Windows 11 STIG SCAP Benchmark;002.001;I - Mission
Critical Public;1;xccdf_mil.disa.stig_rule_SV-253288r958478_rule",
                  "lastScanDate": "2025-07-12",
                  "profile": "I - Mission Critical Public",
                  "profileVersion": "1",
                  "rule": "The Server Message Block (SMB) v1 protocol must be disabled on the
SMB client.",
                  "ruleId": "xccdf_mil.disa.stig_rule_SV-253288r958478_rule",
                  "standard": "Microsoft Windows 11 STIG SCAP Benchmark",
                  "standardVersion": "002.001",
                  "state": "error"
                },
                {
                  "category": "Error",
                  "firstFoundDate": "2025-07-12",
                  "id": "Microsoft Windows 11 STIG SCAP Benchmark;002.001;I - Mission
Critical Public;1;xccdf_mil.disa.stig_rule_SV-256893r958552_rule",
                  "lastScanDate": "2025-07-12",
                  "profile": "I - Mission Critical Public",
                  "profileVersion": "1",
                  "rule": "Internet Explorer must be disabled for Windows 11.",
                  "ruleId": "xccdf_mil.disa.stig_rule_SV-256893r958552_rule",
                  "standard": "Microsoft Windows 11 STIG SCAP Benchmark",
                  "standardVersion": "002.001",
                  "state": "error"
                }
              ]
            }
          }
        }
      ],
      "pageInfo": {
        "startCursor": "MTQ2MDIwMzQ3OjA=",
        "endCursor": "MTQ2MDIwMzQ3OjA=",
        "hasPreviousPage": false,
        "hasNextPage": true
      }
    }
  }
}
```


Get filtered endpoint compliance findings information from filtered set of endpoints

The following query requires Comply 2.16.97 or later and retrieves the first endpoint that is a member of the All Windows computer group, with a compliance findings `category` of `Error` and `standardVersion` value of `1.1.1`, and returns that endpoint's associated compliance findings

©2026 Tanium Inc. All Rights Reserved

with a `category` of `Error` and `standardVersion` value of `1.1.1`.

```
query exampleFilterWindowsComplianceFindings($first: Int!) {
  endpoints(first: $first, filter: {memberOf: {name: "All Windows"}}) {
    edges {
      node {
        name
        ipAddress
        compliance {
          complianceFindings(
            filter: {any: false, filters: [{path: "category", value: "Error"}, {path:
"standardVersion", value: "1.1.1"}]}
          ) {
            category
            firstFoundDate
            id
            lastScanDate
            profile
            profileVersion
            rule
            ruleId
            standard
            standardVersion
            state
          }
        }
      }
    }
    pageInfo {
      startCursor
      endCursor
      hasPreviousPage
      hasNextPage
    }
  }
}
```

Include the cursor variable in the **Variables** panel or in your variables dictionary:

```
{
  "first": 1
}
```

Example response:

```
{
  "data": {
    "endpoints": {
      "edges": [
        {
          "node": {
            "name": "example-host-2",
            "ipAddress": "192.0.2.20",
            "compliance": {
              "complianceFindings": [
                {
                  "category": "Error",
                  "firstFoundDate": "2023-01-01",
                  "id": "CIS Microsoft IIS 10 Benchmark;1.1.1;Level 1 - IIS
10;1;xccdf_org.cisecurity.benchmarks_rule_4.6_L1_Ensure_HTTP_Trace_Method_is_disabled",
```

©2026 Tanium Inc. All Rights Reserved

```
                  "lastScanDate": "2023-02-02",
                  "profile": "Level 1 - IIS 10",
                  "profileVersion": "1",
                  "rule": "(L1) Ensure 'HTTP Trace Method' is disabled",
                  "ruleId":
"xccdf_org.cisecurity.benchmarks_rule_4.6_L1_Ensure_HTTP_Trace_Method_is_disabled",
                  "standard": "CIS Microsoft IIS 10 Benchmark",
                  "standardVersion": "1.1.1",
                  "state": "error"
                },
                {
                  "category": "Error",
                  "firstFoundDate": "2023-01-01",
                  "id": "CIS Microsoft IIS 10 Benchmark;1.1.1;Level 1 - IIS
10;1;xccdf_org.cisecurity.benchmarks_rule_3.4_L1_Ensure_IIS_HTTP_detailed_errors_are_hidden_f
rom_displaying_remotely",
                  "lastScanDate": "2023-02-02",
                  "profile": "Level 1 - IIS 10",
                  "profileVersion": "1",
                  "rule": "(L1) Ensure IIS HTTP detailed errors are hidden from displaying
remotely",
                  "ruleId":
"xccdf_org.cisecurity.benchmarks_rule_3.4_L1_Ensure_IIS_HTTP_detailed_errors_are_hidden_from_
displaying_remotely",
                  "standard": "CIS Microsoft IIS 10 Benchmark",
                  "standardVersion": "1.1.1",
                  "state": "error"
                }
              ]
            }
          }
        }
      ],
      "pageInfo": {
        "startCursor": "NjA5ODg0MDow",
        "endCursor": "NjA5ODg0MDow",
        "hasPreviousPage": false,
        "hasNextPage": true
      }
    }
  }
}
```

Get endpoints with vulnerability findings information

`query.endpoints.edges.node.compliance.cveFindings`

Get endpoint vulnerability findings information (CVSS v2)

The following query retrieves the first endpoint and associated vulnerability findings, including CVSS v2 score and severity, and related CISA KEV information.

```
query exampleEndpointVulnerabilityCVSSv2($first: Int!) {
  endpoints(first: $first) {
```

©2026 Tanium Inc. All Rights Reserved

```
    edges {
      node {
        name
        ipAddress
        compliance {
          cveFindings {
            absoluteFirstFoundDate
            affectedProducts
            cisaDateAdded
            cisaDueDate
            cisaNotes
            cisaProduct
            cisaRequiredAction
            cisaShortDescription
            cisaVendor
            cisaVulnerabilityName
            cpes
            cveId
            cveYear
            cvssScore
            detectedProducts
            detectedCPEs
            excepted
            firstFound
            isCisaKev
            lastFound
            scanType
            severity
            summary
          }
        }
      }
    }
    pageInfo {
      startCursor
      endCursor
      hasPreviousPage
      hasNextPage
    }
  }
}
```

Include the pagination variable in the **Variables** panel or in your variables dictionary:

```
{
  "first": 1
}
```

Example response:

```
{
  "data": {
    "endpoints": {
      "edges": [
        {
          "node": {
            "name": "example-host-one",
            "ipAddress": "192.10.80.10",
            "compliance": {
              "cveFindings": [
                {
```

```
                  "absoluteFirstFoundDate": "2024-07-03",
                  "affectedProducts": [
                    ""
                  ],
                  "cisaDateAdded": null,
                  "cisaDueDate": null,
                  "cisaNotes": "",
                  "cisaProduct": "",
                  "cisaRequiredAction": "",
                  "cisaShortDescription": "",
                  "cisaVendor": "",
                  "cisaVulnerabilityName": "",
                  "cpes": [
                    ""
                  ],
                  "cveId": "CVE-2022-1966",
                  "cveYear": "2022",
                  "cvssScore": null,
                  "detectedProducts": [
                    "kernel",
                    "kernel-core",
                    "kernel-modules",
                    "oraclelinux-release"
                  ],
                  "detectedCPEs": [
                    ""
                  ],
                  "excepted": false,
                  "firstFound": "2024-07-03",
                  "isCisaKev": false,
                  "lastFound": "2025-07-11",
                  "scanType": "oval",
                  "severity": "Unscored",
                  "summary": "A description for this vulnerability has not yet been
provided."
                }
              ]
            }
          }
        }
      ],
      "pageInfo": {
        "startCursor": "MTQ2NTkwMjQzOjA=",
        "endCursor": "MTQ2NTkwMjQzOjA=",
        "hasPreviousPage": false,
        "hasNextPage": true
      }
    }
  }
}
```


Get endpoint vulnerability findings information (CVSS v3)

The following query retrieves the first endpoint and associated vulnerability findings, including CVSS v3 score and severity, and related CISA KEV information.

```
query exampleEndpointVulnerabilityCVSSv3($first: Int!) {
  endpoints(first: $first) {
```

©2026 Tanium Inc. All Rights Reserved

```
    edges {
      node {
        name
        ipAddress
        compliance {
          cveFindings {
            absoluteFirstFoundDate
            affectedProducts
            cisaDateAdded
            cisaDueDate
            cisaNotes
            cisaProduct
            cisaRequiredAction
            cisaShortDescription
            cisaVendor
            cisaVulnerabilityName
            cpes
            cveId
            cveYear
            cvssScoreV3
            cvssTemporalScoreV3
            detectedProducts
            detectedCPEs
            excepted
            firstFound
            isCisaKev
            lastFound
            scanType
            severityV3
            summary
          }
        }
      }
    }
    pageInfo {
      startCursor
      endCursor
      hasPreviousPage
      hasNextPage
    }
  }
}
```

Include the pagination variable in the **Variables** panel or in your variables dictionary:

```
{
  "first": 1
}
```

Example response:

```
{
  "data": {
    "endpoints": {
      "edges": [
        {
          "node": {
            "name": "example.host.two",
            "ipAddress": "1.2.3.4",
            "compliance": {
              "cveFindings": [
```

©2026 Tanium Inc. All Rights Reserved

```
                {
                  "absoluteFirstFoundDate": "2025-10-30",
                  "affectedProducts": [
                    "Microsoft .NET Framework",
                    "Microsoft .NET Framework 4.7.2"
                  ],
                  "cisaDateAdded": "2025-10-14",
                  "cisaDueDate": "2025-11-04",
                  "cisaNotes": "https://msrc.microsoft.com/update-guide/en-US/vulnerability/
CVE-2025-24990 ; https://nvd.nist.gov/vuln/detail/CVE-2025-24990",
                  "cisaProduct": "Windows",
                  "cisaRequiredAction": "Apply mitigations per vendor instructions, follow
applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if
mitigations are unavailable.",
                  "cisaShortDescription": "Microsoft Windows Agere Modem Driver contains an
untrusted pointer dereference vulnerability that allows for privilege escalation. An attacker
who successfully exploited this vulnerability could gain administrator privileges.",
                  "cisaVendor": "Microsoft",
                  "cisaVulnerabilityName": "Microsoft Windows Untrusted Pointer Dereference
Vulnerability",
                  "cpes": [
                    "cpe:/o:microsoft:windows_10_1507:::~~~~x64~",
                    "cpe:/o:microsoft:windows_10_1607:::~~~~x64~",
                    "cpe:/o:microsoft:windows_10_1809:::~~~~x64~",
                    "cpe:/o:microsoft:windows_10_21h2:::~~~~x64~",
                    "cpe:/o:microsoft:windows_10_22h2:::~~~~x64~",
                    "cpe:/o:microsoft:windows_11_22h2:::~~~~x64~",
                    "cpe:/o:microsoft:windows_11_23h2:::~~~~x64~",
                    "cpe:/o:microsoft:windows_11_24h2:::~~~~x64~",
                    "cpe:/o:microsoft:windows_11_25h2:::~~~~x64~",
                    "cpe:/o:microsoft:windows_server_2008:-:sp2:~~~~x64~",
                    "cpe:/o:microsoft:windows_server_2008:r2:sp1:~~~~x64~",
                    "cpe:/o:microsoft:windows_server_2012:-",
                    "cpe:/o:microsoft:windows_server_2012:r2",
                    "cpe:/o:microsoft:windows_server_2016",
                    "cpe:/o:microsoft:windows_server_2019",
                    "cpe:/o:microsoft:windows_server_2022",
                    "cpe:/o:microsoft:windows_server_2022_23h2",
                    "cpe:/o:microsoft:windows_server_2025"
                  ],
                  "cveId": "CVE-2025-24990",
                  "cveYear": "2025",
                  "cvssScoreV3": 7.8,
                  "cvssTemporalScoreV3": 7.8,
                  "detectedProducts": [
                    "Operating System"
                  ],
                  "detectedCPEs": [
                    "cpe:/o:microsoft:windows_11:23h2::x64"
                  ],
                  "excepted": false,
                  "firstFound": "2025-10-30",
                  "isCisaKev": true,
                  "lastFound": "2025-12-03",
                  "scanType": "oval",
                  "severityV3": "High",
                  "summary": "Microsoft is aware of vulnerabilities in the third party Agere
Modem driver that ships natively with supported Windows operating systems.  This is an
announcement of the upcoming removal of ltmdm64.sys driver.  The driver has been removed in
the October cumulative update.\nFax modem hardware dependent on this specific driver will no
longer work on Windows.\nMicrosoft recommends removing any existing dependencies on this
hardware."
                }
              ]
```


©2026 Tanium Inc. All Rights Reserved

```
            }
          }
        }
      ],
      "pageInfo": {
        "startCursor": "ODU5Nzk2MDow",
        "endCursor": "ODU5Nzk2MDow",
        "hasPreviousPage": false,
        "hasNextPage": true
      }
    }
  }
}
```

Get filtered endpoint vulnerability findings information

The following query requires Comply 2.16.97 or later and retrieves the first endpoint with a vulnerability findings `cveYear` of `2020` and `firstFound` greater than or equal to `2025-07-10` and then returns the associated vulnerability findings for that endpoint with a finding `cveYear` of `2020`.

```
query exampleFilterEndpointVulnerability($first: Int!) {
  endpoints(first: $first) {
    edges {
      node {
        name
        ipAddress
        compliance {
          cveFindings(
            filter: {any: false, filters: [{path: "cveYear", value: "2020"}, {path:
"firstFound", op: GTE, value: "2025-07-10"}]}
          ) {
            absoluteFirstFoundDate
            cveId
            cveYear
            cvssScore
            detectedProducts
            detectedCPEs
            firstFound
            lastFound
            severity
            summary
          }
        }
      }
    }
    pageInfo {
      startCursor
      endCursor
      hasPreviousPage
      hasNextPage
    }
  }
}
```

Include the cursor variable in the **Variables** panel or in your variables dictionary:

©2026 Tanium Inc. All Rights Reserved

```
{
  "first": 1
}
```

Example response:

```
{
  "data": {
    "endpoints": {
      "edges": [
        {
          "node": {
            "name": "example-host-1",
            "ipAddress": "192.30.80.203",
            "compliance": {
              "cveFindings": [
                {
                  "absoluteFirstFoundDate": "2025-07-14",
                  "cveId": "CVE-2020-0817",
                  "cveYear": "2020",
                  "cvssScore": null,
                  "detectedProducts": [
                    "Operating System"
                  ],
                  "detectedCPEs": [
                    "cpe:/o:microsoft:windows_10:1507::x64"
                  ],
                  "firstFound": "2025-07-14",
                  "lastFound": "2025-07-14",
                  "severity": "Unscored",
                  "summary": "A remote code execution vulnerability exists in the Windows
Remote Desktop Client when a user connects to a malicious server. An attacker who
successfully exploited this vulnerability could execute arbitrary code on the computer of the
connecting client. An attacker could then install programs; view, change, or delete data; or
create new accounts with full user rights. NOTE: This vulnerability is currently awaiting
analysis."
                },
                {
                  "absoluteFirstFoundDate": "2025-07-14",
                  "cveId": "CVE-2020-0818",
                  "cveYear": "2020",
                  "cvssScore": null,
                  "detectedProducts": [
                    "Operating System"
                  ],
                  "detectedCPEs": [
                    "cpe:/o:microsoft:windows_10:1507::x64"
                  ],
                  "firstFound": "2025-07-14",
                  "lastFound": "2025-07-14",
                  "severity": "Unscored",
                  "summary": "An elevation of privilege vulnerability exists in the way that
the sysmain.dll handles objects in memory. An attacker who successfully exploited the
vulnerability could execute code with elevated permissions. NOTE: This vulnerability is
currently awaiting analysis."
                }
              ]
            }
          }
        }
      ],
      "pageInfo": {
```

```
        "startCursor": "MTQ2NTkxODE5OjA=",
        "endCursor": "MTQ2NTkxODE5OjA=",
        "hasPreviousPage": false,
        "hasNextPage": true
      }
    }
  }
}
```

Get filtered endpoint vulnerability findings information from filtered set of endpoints

The following query requires Comply 2.17.167 or later and retrieves the first endpoint that is a member of the All Windows computer group, with a vulnerability findings `cveYear` of `2020` and `cvssScore` value of `5`, and returns that endpoint's associated vulnerability findings with a `cveYear` of `2020` and `cvssScore` value of `5`.

```
query exampleFilterWindowsEndpointVulnerability($first: Int!) {
  endpoints(first: $first, filter: {memberOf: {name: "All Windows"}}) {
    edges {
      node {
        name
        ipAddress
        compliance {
          cveFindings(
            filter: {any: false, filters: [{path: "cveYear", value: "2020"}, {path:
"cvssScore", value: "5"}]}
          ) {
            absoluteFirstFoundDate
            cveId
            cveYear
            cvssScoreV3
            detectedProducts
            detectedCPEs
            firstFound
            lastFound
            severityV3
            summary
          }
        }
      }
    }
    pageInfo {
      startCursor
      endCursor
      hasPreviousPage
      hasNextPage
    }
  }
}
```

Include the cursor variable in the **Variables** panel or in your variables dictionary:

```
{
  "first": 1
}
```

©2026 Tanium Inc. All Rights Reserved

Example response:


```
{
  "data": {
    "endpoints": {
      "edges": [
        {
          "node": {
            "name": "example-host-3",
            "ipAddress": "10.30.0.100",
            "compliance": {
              "cveFindings": [
                {
                  "absoluteFirstFoundDate": "2024-02-08",
                  "cveId": "CVE-2020-0645",
                  "cveYear": "2020",
                  "cvssScoreV3": 7.5,
                  "detectedProducts": [
                    "Operating System"
                  ],
                  "detectedCPEs": [
                    "cpe:/o:microsoft:windows_server_2016:::x64"
                  ],
                  "firstFound": "2024-02-08",
                  "lastFound": "2025-07-10",
                  "severityV3": "High",
                  "summary": "A tampering vulnerability exists when Microsoft IIS Server
improperly handles malformed request headers, aka 'Microsoft IIS Server Tampering
Vulnerability'."
                },
                {
                  "absoluteFirstFoundDate": "2024-02-08",
                  "cveId": "CVE-2020-0660",
                  "cveYear": "2020",
                  "cvssScoreV3": 7.5,
                  "detectedProducts": [
                    "Operating System"
                  ],
                  "detectedCPEs": [
                    "cpe:/o:microsoft:windows_server_2016:::x64"
                  ],
                  "firstFound": "2024-02-08",
                  "lastFound": "2025-07-10",
                  "severityV3": "High",
                  "summary": "A denial of service vulnerability exists in Remote Desktop
Protocol (RDP) when an attacker connects to the target system using RDP and sends specially
crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service
Vulnerability'."
                }
              ]
            }
          }
        }
      ],
      "pageInfo": {
        "startCursor": "MTQ2NTkyOTI5OjA=",
        "endCursor": "MTQ2NTkyOTI5OjA=",
        "hasPreviousPage": false,
        "hasNextPage": true
      }
    }
  }
}
```


©2026 Tanium Inc. All Rights Reserved