Tanium Endpoint Configuration User Guide

2026H2 Semiannual Release

Version 2.14

November 19, 2026



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

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

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

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

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

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

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

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

©2026 Tanium Inc. All Rights Reserved

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

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

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

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

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

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

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

© 2026 Tanium Inc. All rights reserved.

Table of contents

Overview 8
- Endpoint tools 8
- Client upgrades 8
- Change management 8
- Configurations 9
- Targeting 9
- Approvals 13
- Interoperability with other Tanium products 13
  - Other Tanium solutions 14
    - Content-only Tanium Solutions 15

Requirements 16
- Core platform dependencies 16
- Computer group dependencies 16
- Solution dependencies 17
  - Tanium recommended installation 17
  - Import specific solutions 18
  - Required dependencies 18
  - Feature-specific dependencies 18
- Client extensions and endpoint tools 18
- Tanium™ Module Server 19
- Endpoints 19
  - Supported operating systems 19
- Host and network security requirements 20
  - Ports 20
    - Endpoint Configuration ports 20
  - Security exclusions 21
    - Endpoint Configuration server exclusions 21
- User role requirements 22

©2026 Tanium Inc. All Rights Reserved

Installing 27
Before you begin 27
Import Endpoint Configuration 27
Default settings for Endpoint Configuration 28
Manage solution dependencies 28
Upgrade Endpoint Configuration 28
Upgrade to version 2.2 or later 28
Verify Endpoint Configuration version 29
Troubleshoot problems 29

Configuring 30
Configure the Endpoint Configuration action group 30
Set up Endpoint Configuration users 30
Configure update rings for endpoint change management 32

Managing configurations 33
View configurations 34
Remove configurations for uninstalled solutions 35

Managing approvals 37
Enable configuration approvals 37
Approve or reject configuration changes 37

Managing Tanium Client and endpoint tool upgrade rollouts 40
Before you begin 43
Plan the upgrade stages 43
(Optional) Determine excluded endpoints 44
Configure computer groups 44
Disable action locks or configure Endpoint Configuration to ignore action locks 45
(macOS) Prepare endpoints for Tanium Client upgrades 45
Configure upgrade rings 46
(Optional) Exclude certain endpoints from automatic upgrades 51
Configure excluded endpoints 52
Upgrade excluded endpoints 52
Manage and promote toolset versions in the upgrade rings 52
Review upgrade status 55
Manually promote a toolset version 57

©2026 Tanium Inc. All Rights Reserved

Pause a promotion 57
Review a disqualified toolset version 58
Apply a hotfix 58

Managing installed endpoint tools 60
View deployed endpoint tools 61
Automatic tool removal 61
How automatic tool removal works 62
Offline endpoints 62
Remove unused endpoint tools 63
Block or unblock tools from installing on an endpoint 64
Review tool installations that are scheduled for a retry 65
Manage Client extension shared process mode 66
Determine whether shared process mode is enabled on endpoints 67
Enable or disable shared process mode 67

View and manage content-only solutions 69
View the status of content-only solutions 69
Configure action groups for content-only solutions 70

Reviewing and exporting the audit log 73
Reviewing the audit log 73
Exporting an audit log 73
Before you begin 73
Create a connection 74
Test a connection and review data 75

Maintaining 76
Review and remediate tools deployment 76
Verify whether endpoints have the latest manifest 76
Update the manifest 77

Troubleshooting 79
Collect logs 79
Identify and resolve issues with endpoint tools or Client extensions 79
Manage Client extension shared process mode 84
Determine whether shared process mode is enabled on endpoints 85

©2026 Tanium Inc. All Rights Reserved

Enable or disable shared process mode 85
Verify and manually update the Endpoint Configuration manifest 86
Check the manifest version on endpoints 86
Manually update the manifest on endpoints 87
Review the Extensions log for an endpoint 87
Restart installed Client extensions 88
Disable and enable Client extensions 89
Toggle specific Client extensions 89
Disable or re-enable all Client extensions 89
Uninstall tools installed by Endpoint Configuration 90
Reinstall tools installed by Endpoint Configuration 92
Uninstall Endpoint Configuration 93
Contact Tanium Support 93

Reference: Settings 94

©2026 Tanium Inc. All Rights Reserved

Endpoint Configuration overview

Use Endpoint Configuration to deliver configuration information to endpoints managed using Tanium™ Client, consistently for all Tanium solutions that are available in an environment. 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 Configuration adds solution-specific configurations to a configuration manifest and uses one consistent action to distribute it to all endpoints managed using Tanium Client. All the configuration data that reaches the endpoint is then sensitive to changes that affect the endpoint. For example, the configuration is not applied to an endpoint if the endpoint is no longer a member of the relevant targeting group.

Endpoint tools

In addition to the Tanium Client binary, Tanium installs Tanium™ Client Extensions and other tools on endpoints managed using Tanium Client to perform tasks that are common to certain Tanium™ solutions. Endpoint Configuration installs these tools as they are needed by those solutions. You can review installed endpoint tools on page 60 in Endpoint Configuration, and you can use the packages provided by Endpoint Configuration to restart, uninstall, reinstall, block, or unblock endpoint tools as necessary.

Client upgrades

Though you use Tanium Client Management to initially deploy the Tanium Client, you can enable Endpoint Configuration to install upgrades to Tanium Client along with upgrades to endpoint tools. Use the change management feature on page 40 to manage these upgrades across endpoints. For information about initial deployment of the Tanium Client, see Tanium Client Management User Guide: Deploying the Tanium Client.

Change management

©2026 Tanium Inc. All Rights Reserved

About this task

You can use the change management feature on page 40 to perform staged rollouts of endpoint tools and the Tanium Client. Configure upgrade rings. This feature lets you configure upgrade rings that accommodate the software upgrade and testing strategy for your organization. Each toolset version is promoted through each ring, and you determine the endpoints that receive the upgrade in each ring.

Configurations

Configurations combine solution-specific data and targeting information—for example, a computer group or the results of a sensor. Examples of configurations could be a change to a Tanium™ Threat Response profile that targets one or more computer groups, or an updated Tanium™ Patch scan configuration that targets one or more endpoints that match the results of a sensor. If configuration approval is enabled in Endpoint Configuration, the configuration change appears in Endpoint Configuration for approval for deployment to endpoints that the configuration targets when configuration changes are made in a Tanium solution.

Solution administrators can evaluate and configure the priority for configuration items to address specific scenarios. For example, consider a patching scenario where all Windows endpoints must receive all patches but Windows servers must receive only security related patches. Since a Windows Server target is more specific than a Windows Endpoint target, a solution administrator can configure that setting as having higher priority.



Note: Because a service account that is managed by the System User service distributes the configuration changes, these changes automatically bypass action approval at the Tanium Platform level if it is enabled. To require approval for these changes, use Managing approvals on page 37.

Targeting

The set of endpoints that receive certain endpoint tools and configuration changes depends on multiple targeting factors:

- Solution action group: The action group for the solution that initiates each configuration change or endpoint tool deployment determines the set of endpoints that can receive any endpoint tools or configuration changes from that solution. For more information, see the

©2026 Tanium Inc. All Rights Reserved

user guide for the applicable module or shared service.

- Configuration item or endpoint tool targeting from the solution: The solution that initiates each configuration change or endpoint tool deployment defines the targeting for that configuration change or endpoint tool, such as the targeting defined in a Threat Response profile. In some cases, a solution targets endpoint tools to all endpoints included in the action group for that solution; in other cases, endpoint tool distribution is associated with certain configuration changes. For more information, see the user guide for the applicable module or shared service.

- User computer group assignments: The computer group assignments for the user who initiates a configuration change in a solution limit the final targeting for the configuration change and any associated endpoint tool deployments. For more information, see Tanium Console User Guide: Managing users.

- Change management upgrade ring (endpoint tools only): If you use the change management feature to promote endpoint tools through upgrade rings, the upgrade ring to which an endpoint is assigned is an additional factor in endpoint tool targeting. For more information, see Managing Tanium Client and endpoint tool upgrade rollouts on page 40.

Figure 1. Configuration change targeting

©2026 Tanium Inc. All Rights Reserved

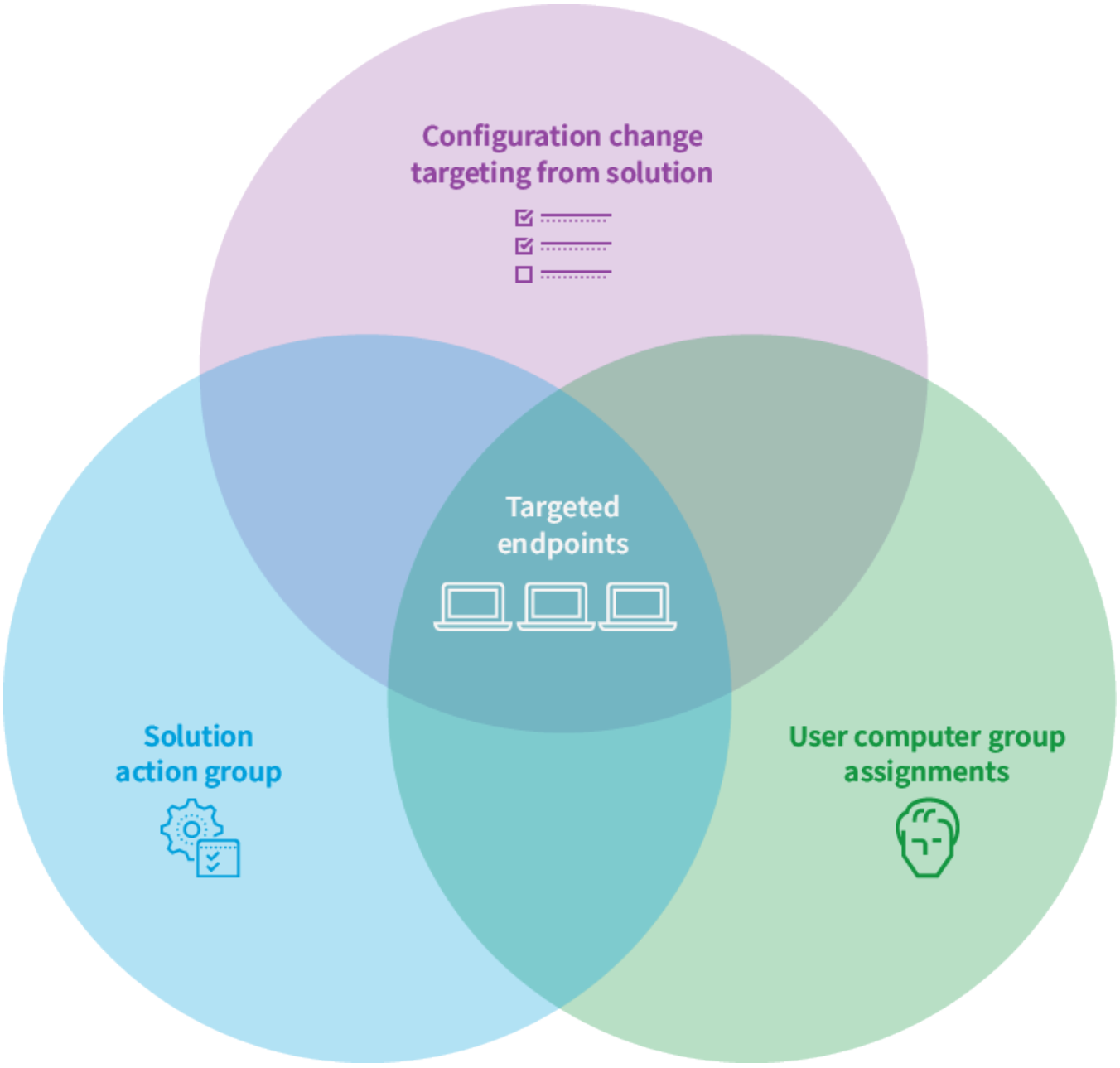
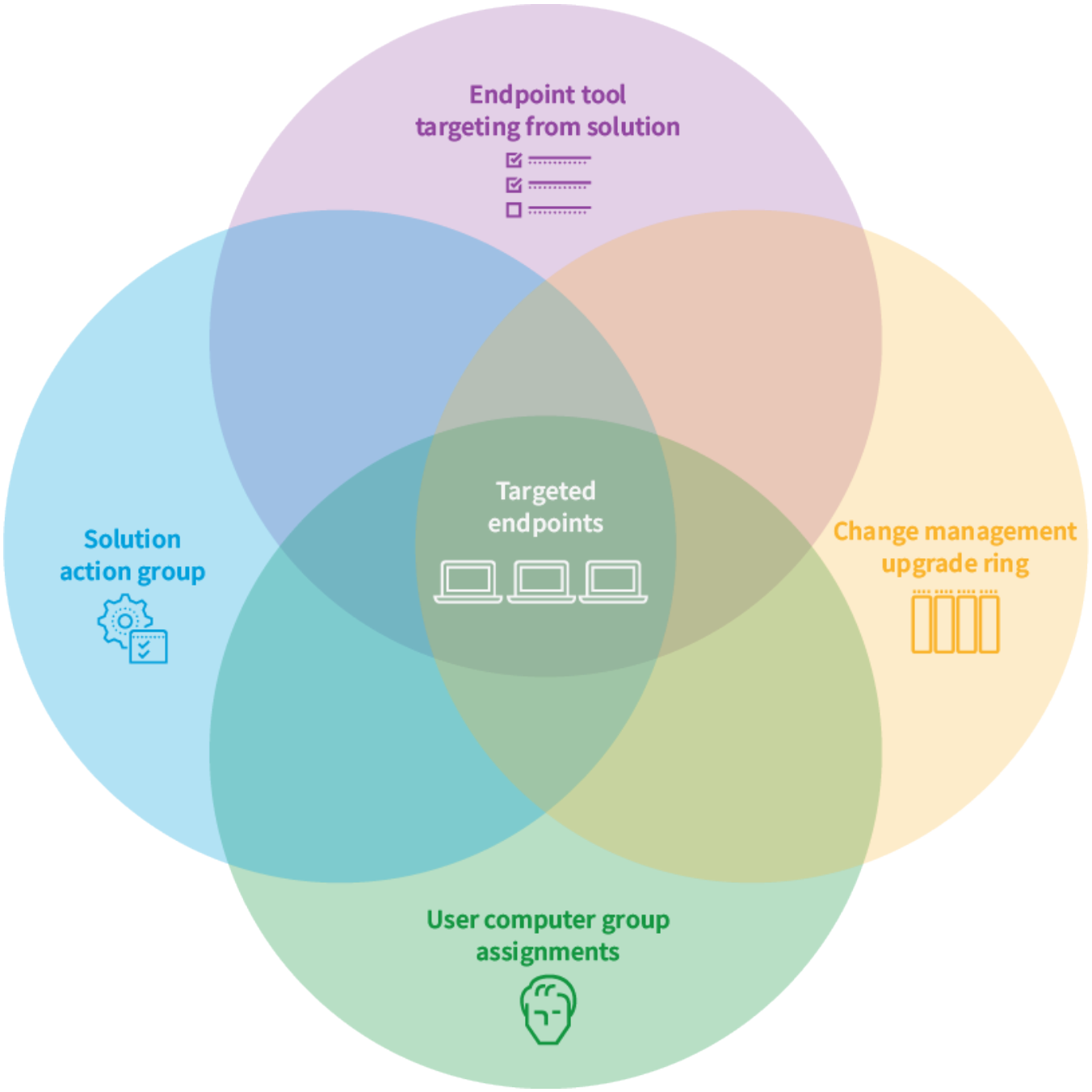


Figure 2. Endpoint tool targeting

©2026 Tanium Inc. All Rights Reserved



Note: The Endpoint Configuration action group also determines the set of endpoints that can receive *any* endpoint tools or configuration changes. It is a best practice to keep the Endpoint Configuration action group assigned to the `All Computers` computer group. For more information, see Configure the Endpoint Configuration action group on page 30.

©2026 Tanium Inc. All Rights Reserved

Note: Endpoint Configuration does not deploy tools to container-based endpoints; containers are not traditional endpoints that run packages or tooling, and they support only basic monitoring. For more information, see the Tanium Cloud Workloads User Guide.

Reevaluation of targeting

Changes in configuration item or endpoint tool targeting from a solution typically trigger new configuration changes with new targeting. However, other changes can affect whether an endpoint is targeted, such as changes to the properties of an endpoint that change its membership in a computer group that was used for targeting.

In general, each endpoint reevaluates its targeting every five minutes. This interval might be longer for a specific configuration item or endpoint tool if a sensor in a question that defines the targeting for that configuration item or endpoint tool has a max sensor age longer than five minutes.

When the reevaluation occurs, if a change in computer group membership that affects the targeting of a prior configuration change or endpoint tool deployment has occurred, Endpoint Configuration makes the appropriate changes on the endpoint.

If a new configuration change or a Client reset occurs before the next reevaluation interval, changes to the endpoint occur at that time (depending on the distribute over time settings; see Reference: Endpoint Configuration settings on page 94) rather than waiting on the next reevaluation.

Approvals

When configuration approval on page 37 is enabled, Endpoint Configuration creates an *approval* for each configuration that is a candidate for deployment to targeted endpoints. When an approval appears in Endpoint Configuration, a configuration approver with appropriate credentials can approve or reject the approval. Each approval displays the domain (the Tanium solution to which it applies), a category for that domain, and a description of the configuration change that would be deployed to the targeted endpoints if approved. To show the effect that deploying the configuration change to the targeted endpoints would have, each approval also displays a before-and-after comparison of the configuration change that would be made.

Interoperability with other Tanium products

©2026 Tanium Inc. All Rights Reserved

Tanium™ Connect

You can use Endpoint Configuration audit logs as a connection source. For more information, see Reviewing and exporting the audit log on page 73.

Other Tanium solutions

The following table lists solutions for which Endpoint Configuration manages configuration changes, approvals, and tool deployment.

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.

Tanium Solution	Configuration Changes and Approvals	Tool Deployment
Tanium™ Asset	✓	✓
Tanium™ Benchmark	✓	✓
Tanium™ Comply	✓	✓
Tanium™ Deploy	✓	✓
Tanium™ Direct Connect	✓	✓
Tanium™ Discover	✓	✓
Tanium™ End-User Notifications	✓	✓
Tanium™ Enforce	✓	✓

©2026 Tanium Inc. All Rights Reserved

Tanium Solution	Configuration Changes and Approvals	Tool Deployment
Tanium™ Engage	✓	✓
Tanium™ Impact	✓	✓
Tanium™ Integrity Monitor	✓	✓
Tanium™ Investigate		✓
Tanium™ Patch	✓	✓
Tanium™ Performance	✓	✓
Tanium™ Provision	✓	✓
Tanium™ Reveal	✓	✓
Tanium™ Threat Response	✓	✓

CONTENT-ONLY TANIUM SOLUTIONS

Additionally, Endpoint Configuration manages tool deployment for content-only solutions that provide content but do not have a service or workbench. For more information, see View and manage content-only solutions on page 69.

©2026 Tanium Inc. All Rights Reserved

Endpoint Configuration requirements

Review the requirements before you install and use Endpoint Configuration.

> **Note:** Older versions of Endpoint Configuration were installed as part of Tanium™ Client Management. For more information about Client Management, see Tanium Client Management User Guide.

Core platform dependencies

- Tanium license that includes Endpoint Configuration. For more information about how to get Endpoint Configuration, see Tanium Solutions & Bundles.
- Tanium Core Platform servers
- Any supported version of Tanium Client. For more information, see Client version and host system requirements. If you use a Client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed Client versions.

  > **Note:** Some Tanium solutions that manage the deployment of configuration changes with Tanium Endpoint Configuration might require a higher Client version.

Computer group dependencies

Endpoint Configuration requires only the `All Computers` computer group.

©2026 Tanium Inc. All Rights Reserved

Best Practice: If you import Endpoint Configuration with restricted targeting disabled, leave the Endpoint Configuration action group set to the default of `All Computers`. If you use restricted targeting to set the Endpoint Configuration action group to target the **No Computers** filter group, then before using any modules, set the Endpoint Configuration action group to target the `All Computers` computer group.

Optionally, you can set the Endpoint Configuration action group to target the **No Computers** filter group by enabling restricted targeting before importing Endpoint Configuration. This option prevents Endpoint Configuration from automatically deploying tools to endpoints. 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 deployment.

Important: If you use restricted targeting to set the Endpoint Configuration action groups to target the **No Computers** filter group, then make sure that before using any modules, you set it to target the appropriate endpoints (typically `All Computers`). For more information, see Configure the Endpoint Configuration action group on page 30. Modules cannot deploy configurations or tools to endpoints that are not targeted by the Endpoint Configuration action group. Use the appropriate targeting groups within modules to control targeted deployment of configurations or tools. If you have endpoints with operating systems that are not supported by Endpoint Configuration, Contact Tanium Support on page 93.

Solution dependencies

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

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

Tanium recommended installation

©2026 Tanium Inc. All Rights Reserved

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

Import specific solutions

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

Required dependencies

Endpoint Configuration has the following required dependencies:

- Tanium™ Endpoint Configuration Toolset Solution
- Tanium™ RDB

Feature-specific dependencies

Endpoint Configuration has the following feature-specific dependency:

- Tanium Connect is required to use Endpoint Configuration audit logs as a connection source.

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.

©2026 Tanium Inc. All Rights Reserved

Tanium™ Module Server

Endpoint Configuration is installed and runs as a service on the Module Server host computer. The impact on the Module Server is minimal and depends on usage.

For more information, see Tanium Core Platform Installation Guide: Host system sizing guidelines.

Endpoints

Supported operating systems

The following endpoint operating systems are supported with Endpoint Configuration.

Endpoint operating systems supported by Endpoint Configuration

Operating System	Version	Notes
Windows	A minimum of Windows 7 SP1 or Windows Server 2008 R2 SP1 is required.	
macOS	Same as Tanium Client support. For more information, see Tanium Client Management User Guide: Client version and host system requirements.	
Linux	Same as Tanium Client support. For more information, see Tanium Client Management User Guide: Client version and host system requirements.	
AIX	A minimum of AIX 7.1.4 is required.	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: Deploy the Tanium Client to AIX endpoints using a package file.

©2026 Tanium Inc. All Rights Reserved

Operating System	Version	Notes
Solaris	Same as Tanium Client support. For more information, see Tanium Client Management User Guide: Client version and host system requirements .	

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

Some modules that work with Endpoint Configuration have more specific requirements for endpoints. For more information, see the User Guide for each module.

Note: Endpoint Configuration does not deploy tools to container-based endpoints; containers are not traditional endpoints that run packages or tooling, and they support only basic monitoring. For more information, see the Tanium Cloud Workloads User Guide.

Host and network security requirements

Specific ports and processes are needed to run Endpoint Configuration.

Ports

The following ports are required for Endpoint Configuration communication.

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

ENDPOINT CONFIGURATION PORTS

©2026 Tanium Inc. All Rights Reserved

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17499	TCP	Used for internal communication for Endpoint Configuration **Note:** This port is used with the loopback interface and usually does not require a firewall rule.

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.

ENDPOINT CONFIGURATION SERVER EXCLUSIONS

Endpoint Configuration security exclusions for Tanium Core Platform Servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe

©2026 Tanium Inc. All Rights Reserved

User role requirements

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

- solution permissions on page 23
- administration and platform content permissions on page 25: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Endpoint Configuration users on page 30.

Important: Each Tanium Solution features a role such as **<*Solution Name*> Configuration Approver** that grants a **<solution name> endpoint configuration approve** permission. This permission is required for a user to make approvals in Endpoint Configuration. For the exact names of solution-specific roles and permissions, see the for the specific Tanium solution.

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

Some Endpoint Configuration 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 Endpoint Configuration. If you create custom roles for Endpoint Configuration users, be sure to assign all the solution permissions and content set permissions that are required for Endpoint Configuration 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

©2026 Tanium Inc. All Rights Reserved

Endpoint Configuration solution permissions

Permission	Endpoint Configuration Administrator	Endpoint Configuration Approver	Endpoint Configuration Auditor	Endpoint Configuration Read Only User
Endpoint Configuration View the Endpoint Configuration workbench, and access and manage configuration changes	✓ SHOW READ WRITE	✓ APPROVE [1] DISMISS [1] REJECT SHOW READ	✓ SHOW READ	✓ SHOW READ
Endpoint Configuration Administrator Provides write privileges for actions and read privileges for sensors and packages in Endpoint Configuration	✓ ADMINISTER	✗	✗	✗
Endpoint Configuration API Perform Endpoint Configuration operations using the API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE
Endpoint Configuration Audit Review Endpoint Configuration audit logs	✓ READ WRITE	✗	✓ READ	✗
Endpoint Configuration Change Management [2] Manage upgrade rings and endpoint tool upgrade rollouts	✓ READ WRITE	✗	✓ READ	✓ READ
Endpoint Configuration Content Only Access and manage content-only solution information in Endpoint Configuration	✓ READ WRITE	✗	✓ READ	✓ READ
Endpoint Configuration Module Register or use the Endpoint Configuration module	✓ USE	✗	✗	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Endpoint Configuration Administrator	Endpoint Configuration Approver	Endpoint Configuration Auditor	Endpoint Configuration Read Only User
Endpoint Configuration Read Only Provides read privileges for sensors, packages and actions in Endpoint Configuration	✗	✗	✗	✓ USER
Endpoint Configuration Service Account Provides the service account with the necessary permissions	✓ READ WRITE EXECUTE	✗	✗	✗
Endpoint Configuration Settings Access Endpoint Configuration settings	✓ READ WRITE	✗	✓ READ	✓ READ
Endpoint Configuration Support Bundle Access the support bundle for Endpoint Configuration	✓ READ	✗	✓ READ	✗
Endpoint Configuration Bypass [3] You can apply this permission to module service account roles, and based on the content set, it bypasses approval for solution-generated configuration items, for example tools or intel deployment. You can apply this permission to a user account, and based on the content set, it bypasses approval for user-generated configuration items.	✗	✗	✗	✗

[1] This permission is provided to a solution-specific role for managing configuration approvals.

[2] To manage promotions, a user must have the Endpoint Configuration Change Management WRITE permission and have all computer groups assigned. To edit change management rings, a user must have the Endpoint Configuration Change Management

©2026 Tanium Inc. All Rights Reserved

Permission	Endpoint Configuration Administrator	Endpoint Configuration Approver	Endpoint Configuration Auditor	Endpoint Configuration Read Only User
WRITE permission, have the Endpoint Configuration Settings READ permission, and have all computer groups assigned. A user who has the required permissions but does not have all computer groups assigned can view upgrade rings but cannot edit the rings or manage promotions.				
[3] This permission is not provided by default to any roles.				

Endpoint Configuration administration and platform content permissions

Permission	Role Type	Endpoint Configuration Administrator	Endpoint Configuration Approver	Endpoint Configuration Auditor	Endpoint Configuration Read Only User
Action	Platform Content	READ WRITE			READ
Computer Group	Administration	READ		READ	READ
Endpoint Configuration	Platform Content	READ WRITE	SPECIAL READ	READ	READ
Endpoint Configuration Module	Platform Content	SPECIAL			
Filter Group	Platform Content	READ WRITE		READ	READ
Own Action	Platform				

©2026 Tanium Inc. All Rights Reserved

Permission	Role Type	Endpoint Configuration Administrator	Endpoint Configuration Approver	Endpoint Configuration Auditor	Endpoint Configuration Read Only User
	Content	READ			READ
Package	Platform Content	✓ READ	✗	✗	✓ READ
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ	✓ READ EXECUTE
Sensor	Platform Content	✓ READ	✗	✗	✓ READ
Show Endpoint	Platform Content	✗	✓ SPECIAL	✗	✗

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

©2026 Tanium Inc. All Rights Reserved

Installing Endpoint Configuration

About this task

Use the Tanium Console **Solutions** page to install Endpoint Configuration.

> **Note:** Choosing automatic or manual configuration does not have an effect on Endpoint Configuration.

Before you begin

- Read the .
- Review the Endpoint Configuration requirements on page 16.
- Assign the correct roles to users for Endpoint Configuration. Review the User role requirements on page 22.
    - To import the Endpoint Configuration solution, you must be assigned the Administrator reserved role.
    - To configure the Endpoint Configuration action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Action Group** write permission.

Import Endpoint Configuration

About this task

Optionally, you can set the Endpoint Configuration action group to target the **No Computers** filter group by enabling restricted targeting before importing Endpoint Configuration. This option prevents Endpoint Configuration from automatically deploying tools to endpoints. 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 deployment.

©2026 Tanium Inc. All Rights Reserved

Default settings for Endpoint Configuration

When you import Endpoint Configuration (regardless of whether you use automatic configuration), the following default setting is configured:

Setting	Default Value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group **Important:** If you use restricted targeting to set the Endpoint Configuration action groups to target the **No Computers** filter group, then make sure that before using any modules, you set it to target the appropriate endpoints (typically `All Computers`). Modules cannot deploy configurations or tools to endpoints that are not targeted by the Endpoint Configuration action group. Use the appropriate targeting groups within modules to control targeted deployment of configurations or tools. **Best Practice:** If you import Endpoint Configuration with restricted targeting disabled, leave the Endpoint Configuration action group set to the default of `All Computers`. If you use restricted targeting to set the Endpoint Configuration action group to target the **No Computers** filter group, then before using any modules, set the Endpoint Configuration action group to target the `All Computers` computer group.

Manage solution dependencies

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

Upgrade Endpoint Configuration

For information about upgrading Endpoint Configuration, see Tanium Console User Guide: Manage Tanium solutions. After the upgrade, verify that the correct version is installed: see Verify Endpoint Configuration version on page 29.

Upgrade to version 2.2 or later

Endpoint Configuration 2.2 and later includes the change management feature, which enables you to perform staged rollouts of endpoint tools and, optionally, the Tanium Client. By default, a single ring is configured, with the **All Computers** computer group assigned, and Tanium Client upgrades are disabled within the change management feature. With this configuration, tools are deployed directly

©2026 Tanium Inc. All Rights Reserved

to all endpoints as soon as the tools are available instead of performing staged rollouts, and you continue to manage Tanium Client upgrades in Tanium Client Management or another tool. Configure the change management feature to manage the upgrade schedule and optionally enable Tanium Client upgrades as part of that schedule. For more information, see Managing Tanium Client and endpoint tool upgrade rollouts on page 40.

Verify Endpoint Configuration version

About this task

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

1. Refresh your browser.
2. From the Main menu, go to **Shared Services** > **Endpoint Configuration** to open the **Endpoint Configuration Overview** page.
3. To display version information, click Info .

Troubleshoot problems

About this task

If you experience problems with configuring Endpoint Configuration, see Troubleshooting Endpoint Configuration on page 79.

©2026 Tanium Inc. All Rights Reserved

Configuring Endpoint Configuration

About this task

After you import Endpoint Configuration, you can reconfigure the default settings.

Configure the Endpoint Configuration action group

About this task

Importing the Endpoint Configuration 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 Endpoint Configuration, the action group targets **No Computers**.

If you used automatic configuration and restricted targeting was disabled when you imported Endpoint Configuration, configuring the Endpoint Configuration action group is optional.

Select the computer groups to include in the Endpoint Configuration action group.



Best Practice: If you import Endpoint Configuration with restricted targeting disabled, leave the Endpoint Configuration action group set to the default of `All Computers`. If you use restricted targeting to set the Endpoint Configuration action group to target the **No Computers** filter group, then before using any modules, set the Endpoint Configuration action group to target the `All Computers` computer group.

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

Set up Endpoint Configuration users

©2026 Tanium Inc. All Rights Reserved

About this task

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

To review specific permissions for each role, see User role requirements on page 22.

Important: On installation, Endpoint Configuration creates an Endpoint Configuration user to automatically manage the Endpoint Configuration service account. Do not edit or delete the Endpoint Configuration user.

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

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

Endpoint Configuration Administrator

Assign the **Endpoint Configuration Administrator** role to users who manage the configuration and deployment of Endpoint Configuration functionality to endpoints.

This role can configure Endpoint Configuration service settings.

Endpoint Configuration Approver

Assign the **Endpoint Configuration Approver** role to a user who approves or rejects configuration changes and tool deployments that are initiated by Endpoint Configuration itself.

Endpoint Configuration Auditor

Assign the **Endpoint Configuration Auditor** role to users who can audit activity and review audit logs in Endpoint Configuration.

Endpoint Configuration Read Only User

Assign the **Endpoint Configuration Read Only User** role to users who can review settings and

©2026 Tanium Inc. All Rights Reserved

configuration items in Endpoint Configuration.

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

Configure update rings for endpoint change management

About this task

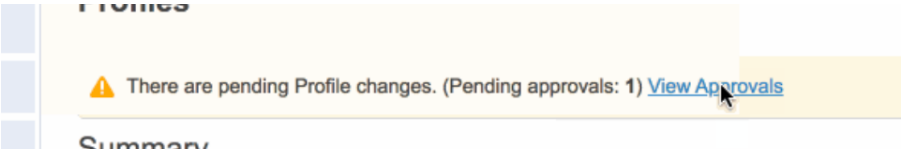
If you want to perform staged rollouts of endpoint tools to accommodate a software upgrade and testing strategy for your organization, configure update rings for the change management feature. For more information, see Managing Tanium Client and endpoint tool upgrade rollouts on page 40.

©2026 Tanium Inc. All Rights Reserved

Managing configurations

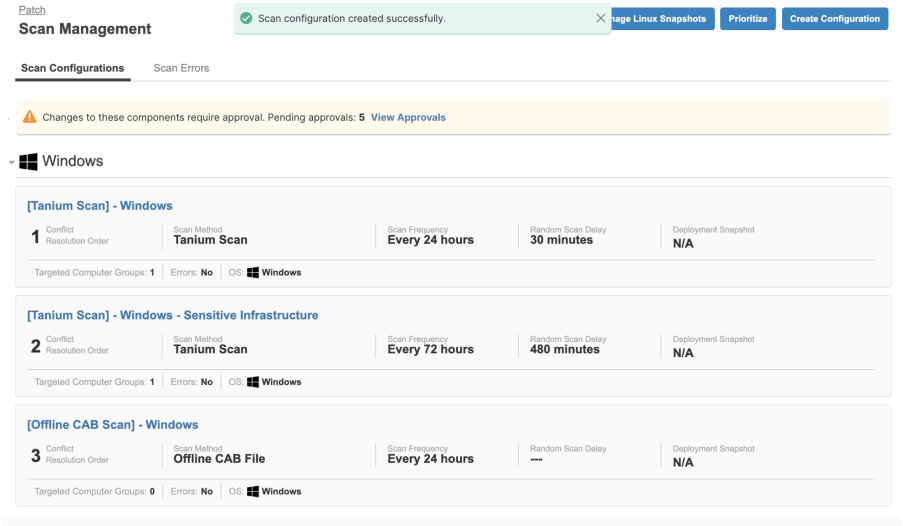
About this task

Each Tanium solution defines configurations. If you enable configuration approval, a banner appears in the solution to alert that configuration changes are pending approval in Endpoint Configuration when a user creates or changes a configuration. For example, if a Threat Response profile changes, a banner appears to alert that a configuration change has been made and requires approval in Endpoint Configuration before you can deploy it to endpoints.



When you create or change a configuration, the configuration appears in Endpoint Configuration in the **Proposed** state. After a configuration approver approves the pending configuration, the configuration is deployed to the targeted endpoints.

For example, if a Tanium Patch Administrator makes or updates scan configurations in Patch, the new and changed scan configurations appear in Endpoint Configuration as **Proposed**. The data in these configurations is not deployed to the targeted endpoints until they have been approved.



©2026 Tanium Inc. All Rights Reserved

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.

Note: The set of endpoints targeted by a configuration change depends on multiple factors. For more information, see Targeting on page 9.

View configurations

About this task

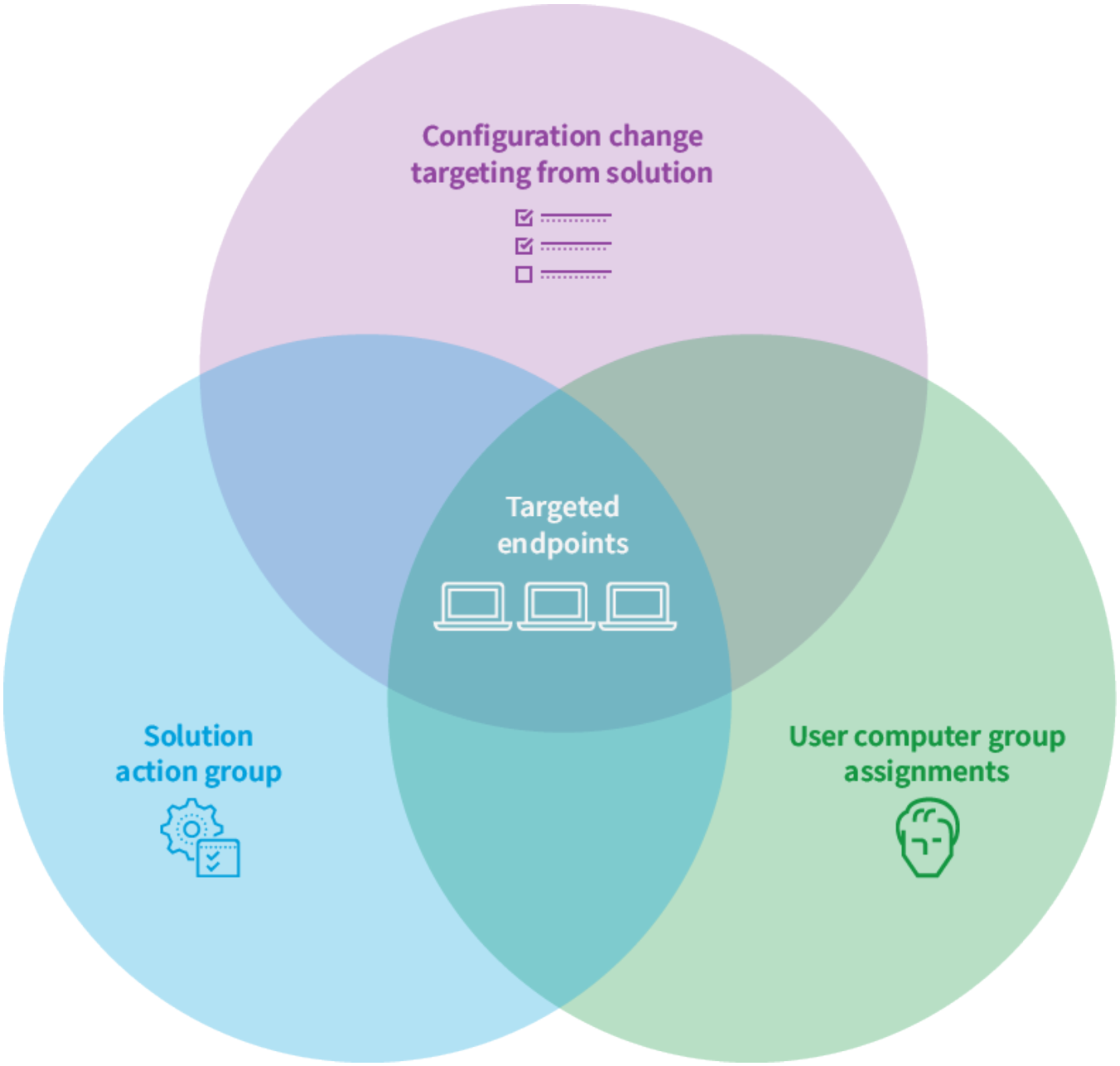
To view configurations, click **Configurations** from the Endpoint Configuration menu.

The **Configurations** page lists the configurations for all installed solutions. The **Pending Changes** column displays Pending Changes for a configuration if there are changes that have not yet been approved. For more information about approvals, see Managing approvals on page 37.

Expand a configuration item to view additional details, including a **Targeting Criteria** section that shows the effective targeting for the configuration. The targeting reflects the combined effect of the solution action group, the targeting defined in the configuration, and the computer group assignments for the user viewing the configuration, including any management rights group that applies. To open the targeted endpoints as a question result in Interact, click **Preview in Interact**.

Figure 3. Configuration change targeting

©2026 Tanium Inc. All Rights Reserved



Remove configurations for uninstalled solutions

About this task

Some configurations remain installed even after the associated solution is no longer installed. If the solution that is associated with a configuration is no longer installed, the **Installed Module** column displays **No** for that configuration.

Manually uninstall a configuration that you no longer need when the associated solution is currently not installed.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Shared Services >** Endpoint Configuration.
2. Go to **Configurations**.
3. Select a configuration and click **Delete**.

©2026 Tanium Inc. All Rights Reserved

Managing approvals

About this task

Enable configuration approvals

About this task

To use Endpoint Configuration to manage approvals, you must enable configuration approvals.

1. From the Main menu, go to **Shared Services** > **Endpoint Configuration**.
2. Click Settings and then click the **Global** tab.
3. Select **Enable Configuration Approvals**, and click **Save**.

Result

If you do not enable configuration approvals, solution-specific configuration changes are made through individual Tanium solutions.

Note: You can bypass configuration approvals for solution or user-generated configuration changes by applying the **Endpoint Configuration Bypass Approval** permission to a service or user role that is associated with one or more content sets to limit the scope of approvals.

Approve or reject configuration changes

About this task

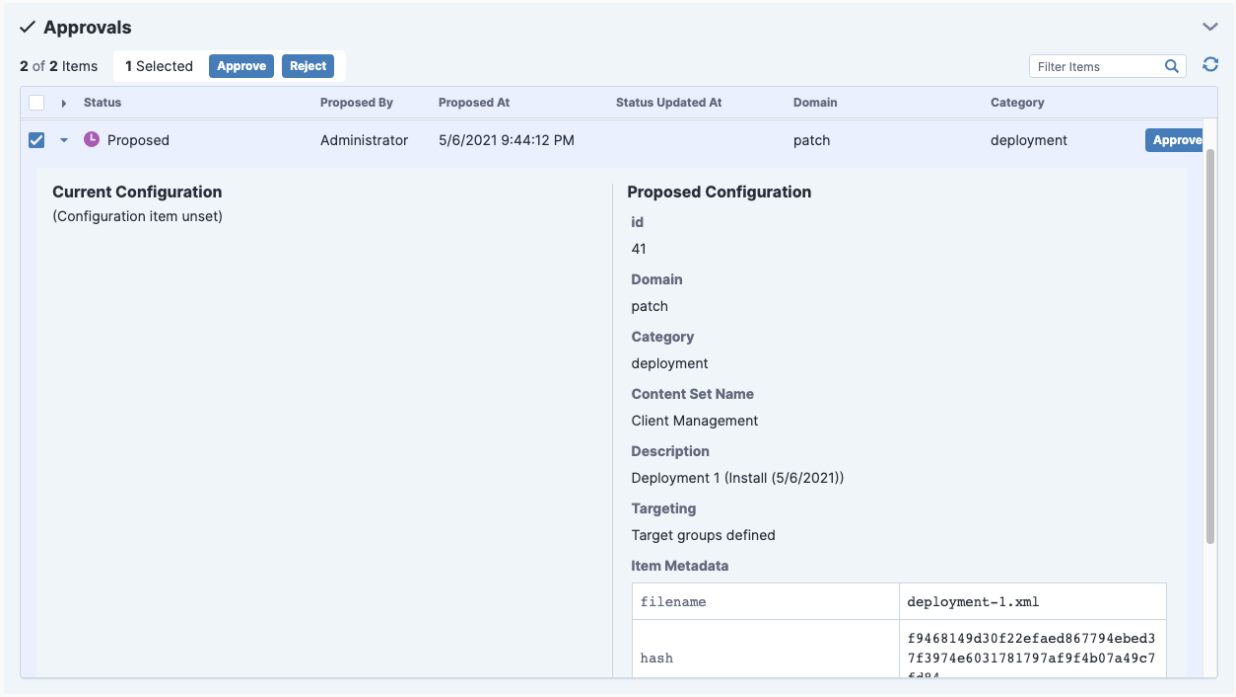
When configuration approvals are enabled, and a configuration change is created or made in a supported Tanium solution, an approval appears in the Approvals page of Endpoint Configuration for a configuration approver to approve or reject. If approved, the configuration change is deployed to the targeted endpoints.

©2026 Tanium Inc. All Rights Reserved

Note: To approve a configuration change, you must have both Endpoint Configuration permissions and appropriate solution permissions. The approver cannot be the same user who made a configuration change. The **Requires other approver** status displays If a user who made a configuration change attempts to approve them.

1. From the Main menu, go to **Shared Services >** Endpoint Configuration.
2. Go to **Overview**.

   Figure 4. Approvals overview



3. Review configurations that are awaiting approval or rejection, which display a status of **Proposed**. Select one or more configurations. View the description of the configurations to understand the domain (Tanium solution) with which the approvals are associated, the functional area of the domain, and a description of the configuration change.

   Note: By default, you can only see configurations for modules for which you have credentials to view.

   Additionally, a comparison of the configuration change is provided for an at-a-glance understanding of the impacts that the change has on the targeted endpoints.

4. (Optional) Click **Download data describing the domain endpoint configurations** to view the content of the configuration.

©2026 Tanium Inc. All Rights Reserved

5. Click **Approve** or **Reject**. Confirm that you want to Approve or Reject the pending approvals.
6. If an approval is in the **Approved** or **Rejected** state, click **Dismiss** to remove the approval from the Approvals page.

Result

After a configuration is approved, it is immediately deployed to endpoints. Rejected approvals are automatically dismissed after 30 days by default. You can configure the **Config Rejected Item Retention Days** setting to adjust the time for automatic dismissal. For more information, see Global Endpoint Configuration settings on page 95.

©2026 Tanium Inc. All Rights Reserved

Managing Tanium Client and endpoint tool upgrade rollouts

About this task

When you upgrade a solution or install a new Tanium solution, Endpoint Configuration must deploy the associated Client extensions and any other needed tools to endpoints to provide the functionality included in the upgrade or the new solution. Tools are bundled together in a versioned toolset that contains a specific version of each tool and any upgrades to the Tanium Client. 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.

The endpoint change management feature lets you perform a staged rollout of each toolset that accommodates the software upgrade strategy for your organization. You can configure upgrade rings through which each toolset version will be promoted, and you assign computer groups to each ring to determine the endpoints that receive the upgrade after each promotion. The toolset is automatically promoted after a configurable number of days, and you can manually promote a toolset after testing is complete in a ring.

For information about viewing and managing installed tools across all endpoints, see Managing installed endpoint tools on page 60.

©2026 Tanium Inc. All Rights Reserved

Important:

- Each version of the endpoint toolset includes a specific version of the Tanium Client, which Tanium recommends that you install with the toolset. It is a best practice to upgrade the Tanium Client on endpoints using the change management feature. To do so, you must enable Tanium Client upgrades in the upgrade ring configuration. For more information, see Configure upgrade rings on page 46. If you do not enable this setting, or if you need to upgrade the Tanium Client in upgrade rings for which Client upgrades are not yet enabled, you can upgrade to the required version of the Tanium Client on endpoints using Client Management or other means. For more information, see Tanium Client Management User Guide: Upgrading Tanium Clients.

- 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.

- The change management feature cannot upgrade endpoints from Tanium Client 7.2. If you need to upgrade endpoints that have version 7.2 installed, you must either perform a reinstallation of the Tanium Client that includes wiping Client data, or manually perform an intermediate upgrade to version 7.4, after which you can upgrade to the latest version. Perform this upgrade before upgrading Tanium Core Platform to the 2025H1 semiannual release. For more information, see Tanium Client Management User Guide: Deploy Clients or Tanium Client Management User Guide: Upgrading Tanium Clients.

©2026 Tanium Inc. All Rights Reserved

Note:

- The endpoint change management feature requires Tanium Core Platform 7.6.2.1204 or later.
- Additional factors affect the set of endpoints that is targeted by endpoint tools. For more information, see Targeting on page 9.
- You cannot manually edit or assign a specific toolset version in an upgrade ring. All toolset versions must be promoted through each upgrade ring starting with the first ring.
- Tanium recommends the universal binary on all Mac computers running macOS 11 or later, and replacing the x86-64 binary if it is already installed. The universal binary is supported and runs natively on both Intel-based Mac computers running macOS 11 or later and Apple "M" series-based Mac computers. However, the change management upgrade process (or any other type of direct Client upgrade) does not upgrade an existing installation of the x86-64 version of the Tanium Client directly to the Universal version. You must first uninstall the existing Tanium Client or perform a reinstallation that includes wiping data with Tanium Client Management. For more information, see Tanium Client Management User Guide: Uninstall the Tanium Client on macOS and Tanium Client Management User Guide: Manage Client deployments. The change management process installs a newer version of the x86-64 Client for existing x86-64 Clients.
- When you receive an upgrade to the toolset, the change management feature allows you to perform a staged rollout of the endpoint tools associated with the new version of the solution. The solution 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 solution upgrade 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 Threat Response and 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

©2026 Tanium Inc. All Rights Reserved

affect the Index-related functionality of Reveal on the upgraded endpoints.

Tip: By default, a single ring is configured, with the **All Computers** computer group assigned. Keep this configuration if you want to deploy endpoint tools directly to all endpoints as soon as the tools are available instead of performing staged rollouts.

Before you begin

Plan the stages of endpoint tool upgrade rollouts and the endpoints that will receive the upgrades in each stage.

Plan the upgrade stages

Plan upgrade stages that fit the software upgrade strategy for your organization.

For example, you might have the following stages:

1. Deployment to a small group of lab endpoints for initial testing by administrators
2. Deployment to a closely monitored group of endpoints for canary testing
3. Deployment to a larger group of endpoints for acceptance testing
4. Deployment to all endpoints

You can configure up to 15 upgrade rings that correspond to each stage of the rollout. The last ring must always deploy upgrades to all endpoints in your environment.

Note: Configuring more than five rings requires that 90% or more of your endpoints are running cx-config 2.0 or later, which was first included in toolset version 2.22.72. If fewer than 90% of endpoints meet this requirement, the maximum is five rings.

©2026 Tanium Inc. All Rights Reserved

Tip: To check how many endpoints in your environment are running cx-config 2.0 or later, use the `Endpoint Configuration - Tools Status` sensor and filter by **Tool Name** containing `cx-config`. Review the **Installed Version** column to assess progress toward the 90% threshold. For example: `Get Endpoint Configuration - Tools Status from all machines having Endpoint Configuration - Tools Status:Tool Name contains cx-config`. For more information, see Manage and promote toolset versions in the upgrade rings on page 52.

Best Practice:

- Use the first ring to test the upgrade in a lab environment that resembles the production environment as closely as possible. For example, use a lab environment that has all endpoint operating systems (OSs) and deployed Tanium module tools in use.
- Use subsequent early rings to test the upgrade on non-critical endpoints.

(Optional) Determine excluded endpoints

About this task

Determine whether your organization has specific endpoints that should not be automatically upgraded, such as high-priority servers. You can assign specific computer groups to be excluded entirely from the upgrade rings. Any endpoint in an excluded computer group is never automatically upgraded with ring promotions, even if it also belongs to a computer group that you have assigned to a particular upgrade ring.

Important: If you choose to exclude endpoints from the upgrade rings, it might result in keeping endpoint tool versions installed that Tanium no longer supports. Tanium does not provide support for issues with endpoints that have unsupported versions of endpoint tools installed.

Configure computer groups

About this task

©2026 Tanium Inc. All Rights Reserved

Determine and configure the computer groups where Endpoint Configuration should deploy endpoint tools in each stage. In the preceding example, you might configure **Lab**, **Canary**, and **Acceptance Testing** computer groups. If you have endpoints that you intend to exclude from the upgrade rings, assign these endpoints to a separate computer group. For more information, see Tanium Console User Guide: Managing computer groups.

Note: Create computer groups with membership based on filters. You cannot assign manual computer groups to upgrade rings.

Disable action locks or configure Endpoint Configuration to ignore action locks

About this task

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**. As a best practice, do not turn on action locks. For more information about action locks, see Tanium Console User Guide: Managing action locks.

Important:

Endpoint Configuration cannot upgrade the Tanium Client on endpoints with action locks turned on, even if you enable the **Manifest Package Ignore Action Lock** and **Deploy Client Configuration and Support Package Ignore Action Lock** settings. As a best practice, do not turn on action locks.

(macOS) Prepare endpoints for Tanium Client upgrades

About this task

If you plan to enable Tanium Client upgrades using the change management feature, perform the following actions as necessary for macOS endpoints:

- If you deploy upgrades to endpoints that have a firewall enabled on macOS 10.14 (Mojave) or

©2026 Tanium Inc. All Rights Reserved

later, perform the steps under Tanium Client Management User Guide: Manage pop-ups for Tanium Client upgrades.

- **macOS:** If you previously created a Privacy Preferences Policy Control (PPPC) custom payload for a version of the Tanium Client earlier than 7.2.314.3608 and you are upgrading to a new version of Tanium Client, you must update the code signing requirement. For more information about creating a PPPC custom payload, see Tanium Client Management User Guide: Prepare for deployment to Linux, macOS, or UNIX endpoints (for deployment with Endpoint Configuration) or Tanium Client Management User Guide: Deploy the Tanium Client to macOS endpoints using the installer.

Configure upgrade rings

About this task

You can configure up to 15 upgrade rings that match the upgrade strategy in your organization, and you can configure the time for automatic promotion for each ring. The last ring always has the **All Computers** computer group assigned.



Note: Configuring more than five rings requires that 90% or more of your endpoints are running cx-config 2.0 or later, which was first included in toolset version 2.22.72. If fewer than 90% of endpoints meet this requirement, the maximum is five rings.

Tip: To check how many endpoints in your environment are running cx-config 2.0 or later, use the `Endpoint Configuration - Tools Status` sensor and filter by **Tool Name** containing `cx-config`. Review the **Installed Version** column to assess progress toward the 90% threshold. For example: `Get Endpoint Configuration - Tools Status from all machines having Endpoint Configuration - Tools Status:Tool Name contains cx-config`. For more information, see Manage and promote toolset versions in the upgrade rings on page 52.

©2026 Tanium Inc. All Rights Reserved

Tip: By default, a single ring is configured, with the **All Computers** computer group assigned. Use this configuration if you want to deploy endpoint tools directly to all endpoints as soon as the tools are available instead of performing staged rollouts.

For the example in the preceding section, you might configure four rings, named **Lab**, **Canary**, **Acceptance Testing**, and **All Endpoints**, with the associated computer groups assigned.

1. Click **Change Management** from the **Endpoint Configuration** menu.
2. Click **Edit Rings**.
3. Configure the upgrade rings as needed:
   - **Insert a ring:** Click Add new ring where you want to insert a ring. The new ring initially receives the same toolset version as the ring that follows it.
   - Remove a ring: Click Remove ring.

     Note: If you remove a ring, the toolset version that was in the ring remains installed on the endpoints that were assigned to the ring before it was removed. When the next promotion occurs from the ring that preceded the removed ring, the next ring in the new configuration receives the promoted toolset.
   - **Edit the name of a ring:** Enter a **Name** that describes the purpose of the upgrade ring.
   - Select computer groups targeted by a ring: Click **Select Computer Groups**. The endpoints in the selected computer groups receive the upgrade when a toolset is promoted to the ring.

     To remove an existing computer group from a ring, you can clear the selection for that computer group while editing groups in the **Target Computer Groups** dialog, or you can click Remove beside the computer group in the **Target** section of the ring.

©2026 Tanium Inc. All Rights Reserved

Note:

- You cannot assign manual computer groups to upgrade rings.
- When you assign multiple computer groups that contain the same endpoint to different upgrade rings, the endpoint receives the upgrade with the earliest of the upgrade rings to which it is assigned. However, excluding an endpoint from automatic upgrades takes precedence; if an endpoint is also assigned to a computer group that is excluded from automatic upgrades, it is never upgraded with ring promotions. For more information about such exclusions, see (Optional) Exclude certain endpoints from automatic upgrades on page 51.
- You cannot change the computer groups assigned to the last ring. The last ring always has the **All Computers** computer group assigned.

Tip: To allow review of toolset upgrades before they are deployed to *any* endpoints, you can assign the **No Computers** computer group to the first upgrade ring.

- Configure the distribution time for tools promoted to the ring: Edit the **Distribute Over Time** setting to configure the time over which to randomize distribution of the endpoint tools distributed when the ring receives a newly promoted toolset. The default is **0**, which distributes tools to all endpoints as soon as possible after the promotion, but randomizing the tool distribution over a period of time can help balance resource use.

Note: If a value greater than zero is configured for this setting, you can override the setting to immediately install a specific tool by using the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package: see Reinstall tools installed by Endpoint Configuration on page 92.

Best Practice: Do not set this value higher than 24 hours.

©2026 Tanium Inc. All Rights Reserved

- Configure promotion timing: Edit the **Minimum Wait Time**, and optionally configure a window for the promotion to take place by selecting **Specify Day and Time for Promotion** and editing the **Day of Week**, **Promotion Window Start Time**, **Time Zone**, and **Promotion Window Duration** as necessary. By default, **Day of Week** is set to **Any Day**, which allows the promotion to occur on any day of the week.

  > **Note:** When you select a time zone where daylight saving time is observed, the promotion window start time is automatically adjusted for DST.

  Promotions occur as follows, depending on whether you configure a promotion window:

  - If you do not configure a promotion window, the promotion occurs as soon as the **Minimum Wait Time** has elapsed.
  - If you configure a promotion window, the promotion occurs at the next **Promotion Window Start Time** after the **Minimum Wait Time** has elapsed, or as soon as the **Minimum Wait Time** has elapsed if that occurs during the configured promotion window.

  For example, consider a ring with **Minimum Wait Time** set to 3 days, **Promotion Window Start Time** set to Tuesday at 1:00 PM, and **Promotion Window Duration** set to 2 hours, so the window is open 1:00 PM–3:00 PM every Tuesday:

  - If a toolset entered the ring on a Monday at 12:25 PM, the wait period ends on Thursday at 12:25 PM. That time falls outside the configured promotion window, so promotion to the following ring occurs when the next promotion window opens on the following Tuesday at 1:00 PM.
  - If a toolset entered the ring on a Saturday at 2:25 PM, the wait period ends on Tuesday at 2:25 PM. Because that time falls within the configured promotion window, promotion to the following ring occurs immediately.

  > **Tip:** Promotion of the toolset to the next ring is instantaneous when the promotion conditions are met. Deployment of the toolset to endpoints in the ring begins at the time of promotion and proceeds according to the availability of endpoints and the **Distribute Over Time** setting.

©2026 Tanium Inc. All Rights Reserved

Note:

The promotion timer is always based on the time that the toolset version entered the ring. If you reduce the **Minimum Wait Time** setting for a non-paused ring to less time than the current toolset version has been in the ring, the ring immediately promotes the upgrade when you save the new ring configuration, or if **Specify Day and Time for Promotion** is enabled and the current time does not fall within the promotion window, the promotion occurs during the next promotion window.

Best Practice:

- Set the **Minimum Wait Time** for each ring to 30 days or less.
- Set the **Minimum Wait Time** for each subsequent ring to the same or shorter than the setting for the prior ring, and consider whether a configured promotion window might delay promotions for longer than the promotion time from the previous ring. A longer promotion time for a later ring or a delayed promotion window can impede the rollout process by preventing automatic promotions in subsequent rings. For example, consider a configuration with **ring A**, followed by **ring B**, and then **ring C**. If **ring B** has a longer promotion time than **ring A** or the promotion window configured for **ring B** regularly delays promotions for longer than the promotion time from **ring A**, then promotions from **ring A** repeatedly overwrite the toolset version in **ring B**, which resets the timer in **ring B** each time. Thus, **ring B** might never automatically promote toolset versions to **ring C**.

4. (Optional) Select **Enable Tanium Client upgrades** to upgrade the Tanium Client on endpoints together with a toolset version as you promote it through the rings.

Best Practice: Enable this setting to streamline Client upgrades and to more easily maintain a supported configuration.

©2026 Tanium Inc. All Rights Reserved

Important:

- When you enable this setting after it was previously disabled, Endpoint Configuration creates Client upgrade deployments for each new toolset, starting with the next toolset that enters ring 1, as well as any new hotfixes introduced to any rings. The Client will not be upgraded with toolsets that are already in upgrade rings or for promotions of these existing toolsets. To maintain support, you must continue to upgrade the Client on these endpoints using Client Management or other means until the next toolset begins moving through the rings or a hotfix is introduced to a ring. For more information, see Tanium Client Management User Guide: Upgrading Tanium Clients.

- If you do not enable this setting, or if you need to upgrade the Tanium Client in upgrade rings for which Client upgrades are not yet enabled, you must upgrade the Tanium Client on endpoints using Client Management or other means. For more information, see Client Management User Guide: Deploying the Tanium Client using Client Management.

- Endpoint Configuration cannot upgrade the Tanium Client on endpoints with action locks turned on, even if you enable the **Manifest Package Ignore Action Lock** and **Deploy Client Configuration and Support Package Ignore Action Lock** settings. As a best practice, do not turn on action locks.

5. (Optional) To enable excluding endpoints from the upgrade rings, **Exclude certain endpoints from automatic upgrades**. For more information, see (Optional) Exclude certain endpoints from automatic upgrades on page 51.

6. Click **Save** to apply the new ring configuration.

(Optional) Exclude certain endpoints from automatic upgrades

About this task

Configure excluded computer groups that contain endpoints that should not be automatically upgraded, such as high-priority servers. Any endpoint in an excluded computer group is never automatically upgraded with ring promotions, even if it also belongs to a computer group that you have assigned to a particular upgrade ring.

©2026 Tanium Inc. All Rights Reserved

Important: If you choose to exclude endpoints from the upgrade rings, it might result in keeping endpoint tool versions installed that Tanium no longer supports. Tanium does not provide support for issues with endpoints that have unsupported versions of endpoint tools installed.

Configure excluded endpoints

1. Enable excluding endpoints from the upgrade rings:
    a. Click **Change Management** from the **Endpoint Configuration** menu.
    b. Click **Edit Rings**.
    c. Select **Exclude certain endpoints from automatic upgrades** and then click **Save**.
2. In the **Endpoints to Exclude** section, click **Select Computer Groups**. The endpoints in the selected computer groups are excluded from automatic upgrades, even the final ring that has the **All Computers** computer groups assigned.
3. Click **Save**.

Upgrade excluded endpoints

On the **Change Management** page, the **Applied Toolset Version** indicates the toolset version that will remain installed on the endpoints in the excluded computer groups until you manually upgrade. You can manually upgrade these endpoints to the toolset version that is assigned to the final upgrade ring at any time.

When you are ready to manually upgrade the excluded computer groups, click **Upgrade** under **Applied Toolset Version** to upgrade them to the toolset version that is currently assigned to the final upgrade ring.

Note: If you have enabled the **Enable Tanium Client upgrades** setting in your upgrade ring configuration, and the toolset version that is currently assigned to the final upgrade ring includes a Tanium Client upgrade, then upgrading the toolset version on the excluded endpoints also upgrades the Tanium Client on those endpoints.

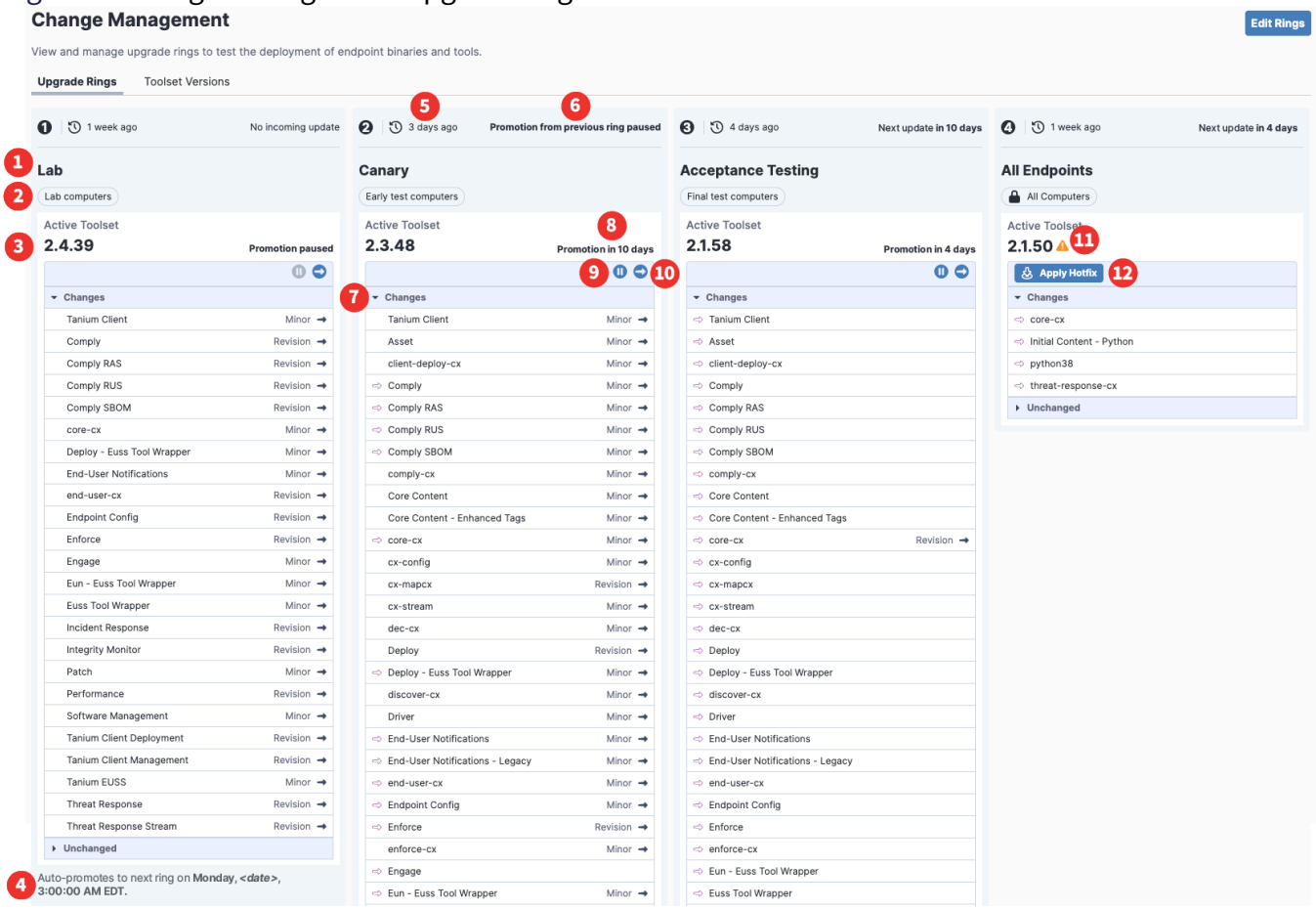
Manage and promote toolset versions in the upgrade rings

About this task

©2026 Tanium Inc. All Rights Reserved

The **Change Management** page displays the rings you have configured, with information about the toolset version in each ring and controls to manage promotions.

Figure 5. Change management upgrade rings



1	The name of the upgrade ring. Configure this name in the upgrade ring configuration on page 46 .
2	Computer groups that are assigned to the upgrade ring. Configure these groups in the upgrade ring configuration on page 46 .
3	The version of the toolset in the ring
4	The time at which the upgrade ring will promote its toolset version to the next ring
5	The time since the upgrade ring received its current toolset version

©2026 Tanium Inc. All Rights Reserved

6	The time until the version of the toolset in the ring is promoted until the next ring, or an indicator that automatic promotion is paused on page 57
7	Expand the **Changes** list to view the individual endpoint tools that a promotion from the previous ring will upgrade in the current ring, or that a promotion from this ring will upgrade in the following ring. Changes are indicated as follows: • Inbound updates pending on the left side of the column indicates that the tool will be upgraded on endpoints assigned to this ring when the toolset from the previous upgrade ring is promoted. • Promotable to the next ring on the right side of the column indicates that the tool will be upgraded on endpoints assigned to the following ring when the toolset version is promoted from this ring. The level of change appears beside the icon. **Tip:** You can view the specific version number for each tool in each version of the toolset that is assigned to an upgrade ring on the **Toolset Versions** tab. These version numbers are typically needed only for troubleshooting purposes. Endpoint tools in the **Unchanged** list are at the same version in the previous and following rings; they will neither be upgraded in the current ring when the toolset version is promoted from the previous ring, nor in the following ring when the toolset is promoted from the current ring.
8	The time left until the toolset version in the ring will automatically be promoted to the following ring
9	Click Pause Promotion to withhold the toolset version from automatic promotion on page 57 .
10	Click Promote Now to immediately promote the toolset to the following ring on page 57 .
11	Issues have been reported beside a toolset version number indicates that Tanium is aware of issues in the current toolset version. Typically, a hotfix on page 58 will become available to resolve such issues.
12	**Apply Hotfix** appears when a hotfix on page 58 is available for the toolset version in the ring. Click the button to apply the hotfix.

When a toolset upgrade is prompted by a solution upgrade or installation or a Tanium Client upgrade, the new version automatically appears in the first upgrade ring, and Endpoint Configuration automatically deploys the toolset to all endpoints in the computer groups assigned to the ring. (If you have assigned the **No Computers** computer group to the first ring, the toolset simply appears in

©2026 Tanium Inc. All Rights Reserved

the ring for review.) Endpoint Configuration automatically promotes the toolset from each ring according to the automatic promotion schedule configured for that ring.

Because the first ring receives all incoming toolset upgrades, multiple toolset versions can queue in the first ring. As soon as a new toolset becomes available, Endpoint Configuration automatically deploys it to the computer groups assigned to the first ring. Any other toolsets remain queued, and Endpoint Configuration continues to promote each queued toolset to the next ring according to when it became available and the automatic promotion schedule configured for the first ring.

Tip: An upgrade to a new semiannual release always queues a new toolset version in the first ring, which is stacked with the toolset version that was there before the upgrade.

In other rings, if a toolset version is promoted into the ring before the current toolset version is promoted, the incoming toolset version overwrites the current toolset version in the ring, and the promotion timer restarts for the ring.



Important:

For each toolset that enters ring 1, review the release notes for the included version of Tanium Client read the release notes and to understand the enhancements, bug fixes, and known issues that those versions include.

In addition to automatic promotions, you can take the following actions during the upgrade rollout process.

Review upgrade status

To determine the status of endpoints, ask a question using the following sensors as needed:

Endpoint Configuration sensors for monitoring tool upgrade status

Sensor	Description
`Endpoint Configuration`	Returns the installation status for all tools collectively across endpoints:

©2026 Tanium Inc. All Rights Reserved

Sensor	Description
`- Tools Status Summary`	• `Ok`: Any Tanium Client upgrades and all targeted endpoint tools have been installed. • `In progress`: The Tanium Client or some targeted endpoint tools have yet to be installed. • `Error`: An error has occurred in at least one tool installation. • `Other`: Another status applies, such as a later version of a tool is already installed, which can occur after you move an endpoint to a later upgrade ring.[1]
`Endpoint Configuration - Tools Status Summary Per Tool`	Returns the targeted version and the installation status for each tool across endpoints: • `Ok`: Any Tanium Client upgrades and all targeted endpoint tools have been installed. • `In progress`: The Tanium Client or some targeted endpoint tools have yet to be installed. • `Error`: An error has occurred in at least one tool installation. • `Other`: Another status applies, such as a later version of a tool is already installed, which can occur after you move an endpoint to a later upgrade ring.[1]
`Endpoint Configuration - Tools Status Details`	For each tool, returns the installed version, the targeted version, installation status, and other details related to failures blocks in place across endpoints. You can filter by **Tool Name** to investigate installation of a specific tool. **Tip:** The installed version of a tool might be later than the targeted version if you move an endpoint to an earlier upgrade ring. [1] For example: `Get Endpoint Configuration - Tools Status Details having Endpoint Configuration - Tools Status Details:Tool Name contains cx-config from all machines`
`Endpoint Configuration - Change Management Status`	Returns the upgrade ring and toolset manifest version that applies across endpoints. You can filter a question using the **Upgrade Ring** field to investigate installation status in a specific ring. For example: `Get Endpoint Configuration - Tools Status Summary from all machines with Endpoint Configuration - Change Management`

©2026 Tanium Inc. All Rights Reserved

Sensor	Description
	`Status:Upgrade Ring contains 4`
`Endpoint Configuration - Tools Status`	For each endpoint tool on each endpoint, returns the tool name, installed version, targeted version, installation status, failure step, failing dependencies, and whether the tool is blocked from installing or upgrading. Filter by **Tool Name** to check the status of a specific tool. For example: `Get Endpoint Configuration - Tools Status from all machines having Endpoint Configuration - Tools Status:Tool Name contains cx-config`

[1] After you begin using the change management feature, the `Other` status might apply to many endpoints, and the installed version of the toolset might be later than the targeted version on these endpoints. This mismatch can occur because the endpoints already had the later toolset version installed before you assigned them to an upgrade ring where you have not yet promoted the later version. This condition resolves itself over time as new toolset versions move through the upgrade rings.

Manually promote a toolset version

If testing is complete before the toolset version in a ring reaches the configured time for automatic promotion, click Promote Now. This action immediately promotes the toolset version to the next ring, and Endpoint Configuration deploys the upgrade to the computer groups assigned that ring.

Pause a promotion

About this task

If you encounter a reason that you do not want to have a toolset automatically promoted at the configured time, such as more time needed for testing or a concern that arises with a toolset during testing, click Pause Promotion, and select the **Reason for Pausing Auto-Promotion** in the dialog that appears. The ring pauses promotion, and the toolset version will not be promoted until you manually promote it.

©2026 Tanium Inc. All Rights Reserved

Note: If a new toolset version is promoted into a paused ring, the promoted toolset version overwrites the current toolset version. Because a new toolset version is in the ring, the ring is no longer paused, and the promotion timer restarts.

Review a disqualified toolset version

In certain cases in which an issue is discovered in a toolset version, Tanium might disqualify that version. This disqualification automatically pauses automatic promotion from the ring that contains the toolset version and disables manual promotion, so the disqualified toolset version cannot be promoted from the ring at all. The message **Disqualified toolset** appears for the toolset version.

Depending on the resolution to the issue, Tanium might provide a hotfix version, or the toolset version might remain disqualified until the following minor version is promoted into the ring to overwrite it.

Apply a hotfix

About this task

Tanium sometimes provides a hotfix version of the toolset to fix specific issues in one or more tools. This level of upgrade increments the third octet of the toolset version number—for example, *x*.1.0 to *x*.1.1. You can promote a hotfix version through the rings as usual. However, you can also choose to directly apply the upgrade to any ring that contains a toolset with the same minor version, without requiring promotion of a later version of the toolset through the preceding rings.

For example, suppose that toolsets have been promoted as follows:

- Ring 1: Toolset *x*.2.0
- Ring 2: Toolset *x*.1.1
- Ring 3: Toolset *x*.1.0

If hotfix version *x*.1.2 is provided to fix an issue, you can optionally apply the hotfix in both Ring 2 and Ring 3. Doing so immediately updates the endpoints assigned to those rings to version *x*.1.2, instead of waiting to promote it through the rings or promoting version *x*.2.0.

When a hotfix version is provided, the **Apply Hotfix** button appears in each ring that contains a toolset version to which the hotfix can be applied.

©2026 Tanium Inc. All Rights Reserved

1. To review information about the hotfix, click **Apply Hotfix**.
2. When you are ready to apply the hotfix, click **Confirm** in the **Apply Hotfix** dialog.
   The hotfix version updates in the ring, and Endpoint Configuration deploys the updated endpoint tools to the computer groups assigned to the ring. If promotion from the ring was paused, applying the hotfix unpauses it.

©2026 Tanium Inc. All Rights Reserved

Managing installed endpoint tools

About this task

In addition to the Tanium Client binary, Tanium installs Client extensions and other tools on endpoints to perform tasks that are common to certain Tanium solutions. Endpoint Configuration installs these tools as they are needed by those solutions. You can review installed endpoint tools in Endpoint Configuration, and you can use the packages provided by Endpoint Configuration to manage these tools.

Tip: To manage general installation of endpoint tools, including configuring staged rollouts, see Managing Tanium Client and endpoint tool upgrade rollouts on page 40.

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.

Note:

- You cannot manage tools using the packages listed in the following sections on endpoints with action locks turned on. For more information about action locks, see Tanium Console User Guide: Managing action locks.
- The set of endpoints targeted by endpoint tools depends on multiple factors. For more information, see Targeting on page 9.

©2026 Tanium Inc. All Rights Reserved

Tip: For a list of Client extensions and endpoint tools used for each solution, see Tanium Client Management User Guide: Reference: Client extensions and endpoint tools used for Tanium solutions.

View deployed endpoint tools

About this task

View deployed endpoint tools on the **Tools** page.

1. From the Main menu, go to **Shared Services >** Endpoint Configuration.
2. Click **Tools** from the Endpoint Configuration menu.
3. Expand a tool to view the status of that tool across all endpoints.
4. (Optional) Click a status category to open question results that contain all endpoints in that category for the tool, or click View question results in Interact to view the installation status for a tool across all endpoints where the tool is targeted.

   Note: The **Tools** page displays cached data that is provided by Tanium Data Service, and this data includes offline endpoints. If you view the question results for a tool, Interact retrieves real-time data from only online endpoints.

Automatic tool removal

To reduce operational overhead and prevent orphaned tools from accumulating on endpoints over time, Endpoint Configuration automatically removes endpoint tools that are no longer targeted by any module after a configurable period (45 days by default). Endpoint Configuration also deletes all files and databases associated with a removed tool.

Automatic tool removal is enabled by default. For more information about configuring the number of days before removal, see Global Endpoint Configuration settings on page 95.

©2026 Tanium Inc. All Rights Reserved

Important:

The following tools are always excluded from automatic removal:

- **config-cx** and **cx-core**: These are foundational Client extensions that are always required on endpoints. Removal requires reinstallation of the Tanium Client.
- **Npcap**: Removal of Npcap can cause stability issues on some endpoint configurations.

How automatic tool removal works

A tool can become untargeted on an endpoint if the endpoint is removed from targeting in all modules that use the tool, or if a module is uninstalled. If multiple modules use a tool, that tool is considered untargeted on an endpoint only if none of those modules target that endpoint.

When a tool becomes untargeted, Endpoint Configuration tracks it through two stages before removal:

- Safe to Remove: The tool is installed but is no longer targeted by any module. Endpoint Configuration marks it as **Safe to Remove** on the **Tools** page and starts the removal countdown. For information about removing tools manually during this stage, see Remove unused endpoint tools on page 63.
- Pending Automatic Uninstall: When the remaining time drops to 50% of the configured period, the tool advances to **Pending Automatic Uninstall** status. For example, with a 30-day setting, the tool enters this status when 15 days remain. During this stage, the **Endpoint Configuration - Automatic Uninstall Status** sensor reports the number of days remaining until removal. When the configured time has elapsed and the endpoint confirms it is communicating with the Tanium Server, Endpoint Configuration removes the tool and any associated files or databases.

If a tool is re-targeted at any point before the configured time has elapsed, the timer resets, and the tool returns to a normal installed status.

Offline endpoints

Endpoint Configuration does not automatically remove endpoint tools from endpoints while they are offline. When an endpoint comes back online after the configured time has elapsed, Endpoint

©2026 Tanium Inc. All Rights Reserved

Configuration waits at least 60 minutes before checking whether removal should proceed, giving the endpoint time to receive the current manifest. If a tool is re-targeted during that window, removal is canceled. If the endpoint has not yet communicated with the Tanium Server when the check runs, the check is postponed another 60 minutes.

Remove unused endpoint tools

About this task

Some tools remain installed on an endpoint even after the associated solution no longer targets that endpoint or after the associated solution is no longer installed. Endpoints that have an endpoint tool installed under these conditions are in the **Safe to Remove** category for that tool.

To manually remove an endpoint tool from endpoints where it is no longer needed, deploy the appropriate action to those endpoints.

1. From the Main menu, go to **Shared Services >** Endpoint Configuration.
2. Click **Tools** from the Endpoint Configuration menu.
3. Click the **Safe to Remove** category.

   Tip: This category shows tools that are safe to remove on some endpoints, but the total installations displayed for each tool still include all installations of the tool.
4. Expand the line for the tool that you want to remove and click the **Safe to Remove** item in the chart legend.
5. In the question results, select the rows for installed versions that you want to remove, and click **Drill Down**.
6. Click **Create a Question**, and ask one of the following questions to target an appropriate group of endpoints.
   - Windows endpoints: `Get Is Windows equals true from all machines`
   - Non-Windows endpoints: `Get Is Windows equals false from all machines`
7. Select the row from the drill-down question results, and click **Deploy Action**.
8. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or

©2026 Tanium Inc. All Rights Reserved

Endpoint Configuration - Uninstall Tool [Non-Windows], depending on the endpoints you are targeting.

9. For **Tool Name**, select the name of the tool you are uninstalling.

   > **Note:** In some cases, such as when the solution associated with a tool has been removed from the Tanium environment, the tool might not appear in the **Tool Name** list. In such a case, enter the tool name in the **Manually specified tool name** box, exactly as it appears in the **Tools** list in Endpoint Configuration.

10. (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**.
11. (Optional) Select **Soft uninstall** to only remove the tool and preserve databases and logs that might be useful for troubleshooting on the endpoint. To remove all databases and logs for the tool from the endpoints, clear the selection.
12. (Optional) To remove any tools that were dependencies of the tools you are installing but are not dependencies for other solutions, select **Remove unreferenced dependencies**.
13. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

    > **Best Practice:** If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

14. Click **Show preview to continue**.
15. A results grid appears at the bottom of the page showing you the targeted endpoints for the action. If you are satisfied with the results, click **Deploy Action**.

Block or unblock tools from installing on an endpoint

About this task

Blocking a tool prevents the tool from installing on an endpoint if it is not already installed, or upgrading if it is installed.

> **Note:** Blocking a tool does not prevent the tool from running if it is already installed.

©2026 Tanium Inc. All Rights Reserved

1. In Interact, ask a question that targets the endpoints on which you want to block or unblock the installation of a tool.
2. Select the results for the endpoints you want to target, and click **Deploy Action**.
3. For the **Deployment Package**, select one of the following packages:
    - To block installation, select **Endpoint Configuration - Block Tool [Windows]** or **Endpoint Configuration - Block Tool [Non-Windows]**, depending on the endpoints you are targeting.
    - To unblock installation, select **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]**, depending on the endpoints you are targeting.
4. For **Tool Name**, select the tool to block or unblock, or to block or unblock all tools, select **All Module Tools**.

    Note: If you select **All Module Tools**, the package blocks or unblocks all endpoint tools except for core-cx and cx-config.
5. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

    Best Practice: If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.
6. Click **Show preview to continue**.
7. 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**.

Review tool installations that are scheduled for a retry

Ask a question using the `Endpoint Configuration - Tools Retry Status` sensor to view tool installations that previously failed and that Endpoint Configuration will retry. For example, ask the question: `Get Computer Name and IP Address and Endpoint Configuration - Tools Retry Status from all machines with all Endpoint Configuration - Tools Retry Status not matches "(No Tools Pending Retry|^N\/A.*$)"`.

The sensor returns the following columns:

©2026 Tanium Inc. All Rights Reserved

- Tool Name: The tool for which Endpoint Configuration will retry installation
- Targeted Version: The version of the tool that Endpoint Configuration is attempting to install
- Retry Backoff Seconds: The current delay between the failed installation and retrying the installation. This value increases each time the installation fails.
- Retry Count: The number of times the installation has been retried, within a range
- Next Retry: The approximate time until the next retry

Manage Client extension shared process mode

You can enable or disable *client extension shared process mode* to control whether Client extensions run in separate processes or in a single combined process:

- Shared process mode disabled: Each Client extension runs in its own isolated instance of TaniumCX.exe (Windows) or TaniumCX (non-Windows), associated with the dynamic library for that Client extension. For example, on a Windows endpoint, ConfigCX runs with the following command:

```
"C:\Program Files (x86)\Tanium\Tanium Client\TaniumCX.exe" run --purpose
TaniumConfig.dll
```

- Shared process mode enabled: All Client extensions run together in a single instance of TaniumCX.exe (Windows) or TaniumCX (non-Windows). For example, on a Windows endpoint, all Client extensions run under the following command:

```
"C:\Program Files (x86)\Tanium\Tanium Client\TaniumCX.exe" run-framework
```



Important:

- If you use Tanium Patch, you must have Patch 3.15.148 or later installed to use shared process mode.
- If you use Tanium Deploy, you must have Deploy 2.21.150 or later installed to use shared process mode.

©2026 Tanium Inc. All Rights Reserved

Note:

- With shared process mode enabled, other processes, such as Tanium Client processes and endpoint tools other than Client extensions, continue to run separately.
- Enabling shared process mode reduces the number of Tanium processes running on endpoints. However, you cannot determine the CPU or memory usage of individual Client extensions within the combined process. While troubleshooting an issue where it is necessary to identify a specific extension causing the issue, such as excessive CPU usage, disable shared process mode. For more information about troubleshooting Client extensions, see Identify and resolve issues with endpoint tools or Client extensions on page 79.

Determine whether shared process mode is enabled on endpoints

About this task

To view the status of shared process mode on endpoints, ask a question using the `Tanium Client Explicit Setting[DisableExtensionIsolation]` sensor. Endpoints that return a value of `1` for this sensor have shared process mode enabled.

Enable or disable shared process mode

1. In Interact, ask a question that targets the endpoints on which you want to enable or disable shared process mode.
2. Select the results for the endpoints you want to target, and click **Deploy Action**.
3. For the **Deployment Package**, select the appropriate package to enable or disable shared process mode on the endpoints your are targeting:
   - Enable shared process mode: Select **Endpoint Configuration - Enable Shared Process Mode [Windows]** or **Endpoint Configuration - Enable Shared Process Mode [Non-Windows]**.
   - Disable shared process mode: Select **Endpoint Configuration - Disable Shared Process Mode [Windows]** or **Endpoint Configuration - Disable Shared Process Mode [Non-Windows]**.

©2026 Tanium Inc. All Rights Reserved

4. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   Best Practice: If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

5. Click **Show preview to continue**.

6. 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**.

©2026 Tanium Inc. All Rights Reserved

View and manage content-only solutions

About this task

Endpoint Configuration manages tool deployment for content-only solutions that provide content but do not have a service or workbench, such as **Tanium™ Core Content**. Some predefined scheduled actions distribute tools from these content-only solutions that endpoints need to perform functions for certain core sensors and packages. For example, the action **Distribute Application Management Tools** deploys a package that includes scripts for starting and stopping services.

Endpoint Configuration creates an action group for each content-only solution. By default, each of these action groups includes only the **No Computers** computer group, and so associated tools do not deploy to endpoints until you select another computer group for the action group.

For more information about the required configuration for specific content-only solutions, see Tanium Community article: Configure Delivery of Endpoint Tools and Content.

View the status of content-only solutions

About this task

You can review the status of content-only solutions in Endpoint Configuration, including the configured action groups, and applicable content sets, and deployment status. Click **Content-Only Solutions** from the Endpoint Configuration menu.

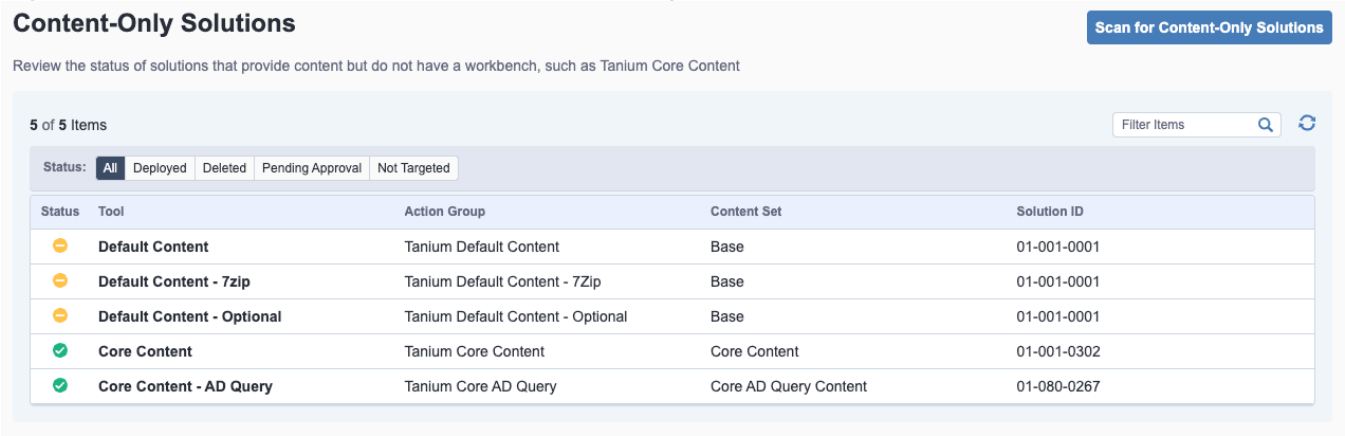
Solutions that are targeted for deployment have a status of Deployed. The status Not Targeted indicates that the action group for a solution targets **No Computers**, and associated tools are not deployed for the solution until you update the targeting for the listed action group. Follow the steps in Configure action groups for content-only solutions on page 70 to deploy a tool.

By default, Endpoint Configuration scans the environment for changes to content-only solutions every 15 minutes. To initiate a scan immediately, click **Scan for Content-Only Solutions**. You can configure the **Content-Only Solution Job Frequency** setting to adjust the time between scans. For more information, see Global Endpoint Configuration settings on page 95.

©2026 Tanium Inc. All Rights Reserved

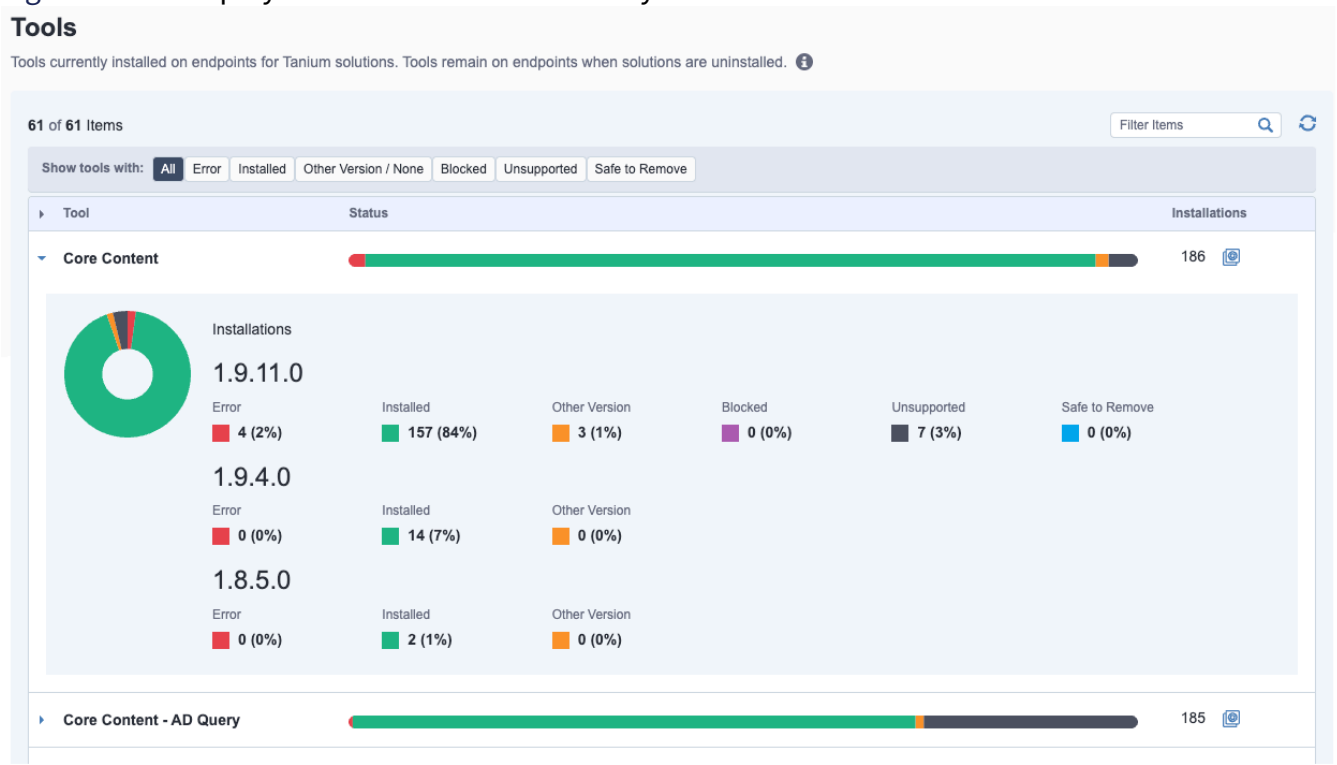
In the following example, the action groups for **Core Content** and **Core Content - AD Query** have been configured to target endpoints. The action groups for the **Default Content**, **Default Content - 7zip**, and **Default Content - Optional** solutions target **No Computers**, and the tools associated with each of those solutions are not deployed to endpoints.

Figure 6. Content-only solutions in Endpoint Configuration



The tools for deployed solutions appear on the **Tools** page with the detailed deployment status. For more information, see Managing installed endpoint tools on page 60.

Figure 7. Tool deployment status for content-only solutions



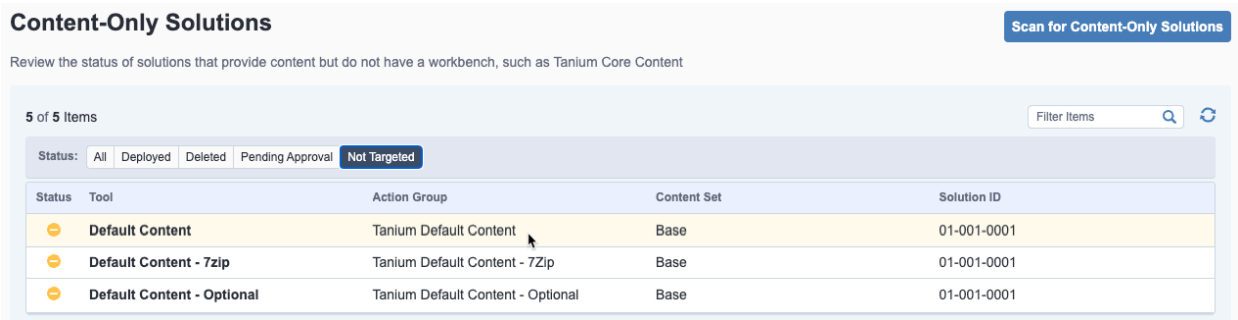
Configure action groups for content-only solutions

©2026 Tanium Inc. All Rights Reserved

About this task

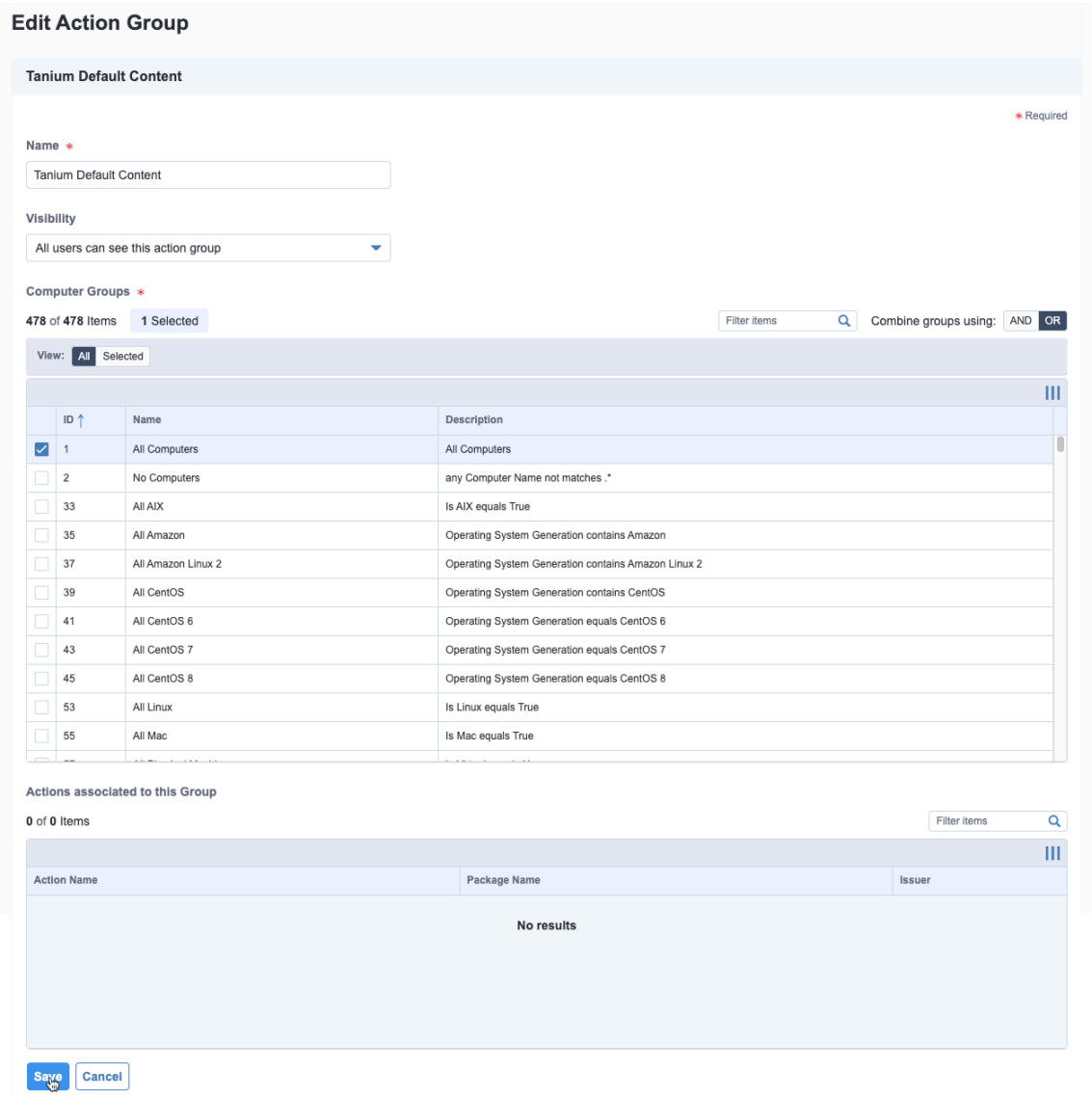
To enable Endpoint Configuration to deploy tools for a content-only solution to the appropriate endpoints, configure the associated action group.

1. From the Main menu, go to **Shared Services >** Endpoint Configuration.
2. Go to **Content-Only Solutions**.
3. Click **Not Targeted** to view the tools that target **No Computers**.
4. For each listed tool, note the associated **Action Group**, and configure that action group to target the appropriate endpoints:
   Figure 8. Action group name



   a. From the Main menu, go to **Administration** > **Actions** > **Action Groups**.
   b. Click the action group name.
   c. Select the **Computer Groups** that the action group should target and then click **Save**.
      Figure 9. Default content action group

©2026 Tanium Inc. All Rights Reserved



Best Practice: Select the **All Computers** computer group for these action groups.

For more information about action groups, see Tanium Console User Guide: Managing action groups.

©2026 Tanium Inc. All Rights Reserved

Reviewing and exporting the audit log

Reviewing the audit log

About this task

To review the Endpoint Configuration audit log, click **Audit Log** from the Endpoint Configuration menu. By default, the log shows the last 30 days.

To adjust the time range or to filter the log by action, expand the **Filters** section.

Exporting an audit log

About this task

Create a connection in Tanium Connect to export an Endpoint Configuration audit log to Connect destinations, such as Email, File, HTTP, Socket Receiver, Splunk, or SQL Server. The audit log includes the following information:

- Additions, deletions, and updates of configuration items
- Approval, rejection, and dismissal actions
- Manifest actions
- Bootstrap package updates, such as updates to the Client Configuration and Support package when a toolset version is promoted

Note: The audit log is also included in the support package for Endpoint Configuration. For information about downloading the support package, see Collect logs on page 79.

Before you begin

You must have access to Connect with the Connect User role.

©2026 Tanium Inc. All Rights Reserved

Create a connection

1. From the Connect menu, 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. For **Source**, select **Tanium Endpoint Configuration**.
    b. For **History Retrieval (Days)**, enter the number of days of history that the exported audit log contains.
    c. Configure the connection destination.
    Select a connection destination from the **Destination** list. Provide the configuration information for the destination you select. For more information about configuring destinations, see the Tanium Connect User Guide: Connection destinations.
5. Configure the **Format** for the data. For more information about configuring the format, see the section on the destination type that you selected in the Tanium Connect User Guide.
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 about the types of filters you can configure, see Tanium Connect User Guide.
7. (Optional) Customize columns for the exported data. In the **Columns** section, select the available **Source** items and configure the **Value Type** and **Customization**, see Tanium Connect User Guide: Format data for emails.
8. (Optional) Select **Enable Schedule** and configure a schedule for the connection. For more information about how to run connections on a schedule, see Tanium Connect User Guide: Schedule connections. If the schedule is not enabled, the connection only runs when you manually run it.
9. Click **Save** or **Save and Run**.

©2026 Tanium Inc. All Rights Reserved

Test a connection and review data

1. From the Connect menu, click **Connections**.
2. Click the connection that you created for the Endpoint Configuration audit log.
3. Click **Run Now**. Confirm that you want to run the connection.
4. View the summary of the run.
5. View the audit log in the destination that you configured for the connection.

©2026 Tanium Inc. All Rights Reserved

Maintaining Endpoint Configuration

About this task

Perform monthly maintenance tasks to ensure that Endpoint Configuration successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Endpoint Configuration is not performing as expected, you might need to troubleshoot issues or change settings. For related procedures, see Troubleshooting Endpoint Configuration on page 79.

Review and remediate tools deployment

1. From the Main menu, go to **Shared Services** > **Endpoint Configuration**.
2. Review the deployment status of tools:
    a. Go to **Tools**. For more information, see Tanium™ Endpoint Configuration User Guide: View deployed endpoint tools.
    b. Go to **Content-Only Solutions**. For more information, see Tanium Endpoint Configuration User Guide: View the status of content-only solutions.
3. To troubleshoot deployment issues for tools, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or Client extensions.

Verify whether endpoints have the latest manifest

About this task

Verify that endpoints have the latest Endpoint Configuration *manifest*, which is a file that determines the versions of solution tools to install on endpoints. If endpoints do not have the latest manifest because of action locks or some other issue, the endpoints do not install the latest tools versions.

1. From the Main menu, go to **Shared Services** > **Endpoint Configuration**.
2. On the Endpoint Configuration **Overview** page, note the **Manifest Revision** (version) in the **Summary** section.
3. Go to the Tanium **Home** page and ask the following question:

©2026 Tanium Inc. All Rights Reserved

`Get Endpoint Configuration - Manifest Metadata?maxAge=60 and Action Lock Status from all machines`

> **Best Practice:** The manifest changes whenever a configuration or tool change occurs. Therefore, use the `maxage=60` option for the **Manifest Metadata** sensor to ensure that you retrieve the latest data from endpoints.

> **Tip:** Sort the **Question Results** grid by **Revision** to list the versions in descending numerical order, which makes it easier to identify endpoints with an earlier manifest version.

4. If the **Question Results** indicate **Action Lock Status** is on for some endpoints that do not have the latest manifest:
    a. Consult whoever turned on the action locks to verify that it is now safe to run actions on those endpoints.
    b. Perform one of the following tasks:
        - Disable action locks on the endpoints that require an updated manifest. For more information, see Tanium Console User Guide: Turn off action locks.
        - Configure Endpoint Configuration to ignore action locks for all endpoints. For more information, see Tanium Endpoint Configuration User Guide: Global Endpoint Configuration settings.
5. Update the manifest on page 77 on any endpoints that require an updated version.

Update the manifest

About this task

Windows and non-Windows endpoints require separate packages to update the manifest. Therefore, perform the following steps for each type of endpoint:

1. Go to the Tanium **Home** page and ask the following question:
   `Get Endpoint Configuration - Manifest Metadata?maxAge=60 from all machines`
2. Select the endpoints that have an outdated manifest and click **Deploy Action**.

©2026 Tanium Inc. All Rights Reserved

3. Select the **Deployment Package** that matches the target endpoints:
    - Windows endpoints: **Endpoint Configuration - Manifest [Windows] (v. <latest_manifest_version>)**
    - Non-windows endpoints: **Endpoint Configuration - Manifest [Non-Windows] (v. <latest_manifest_version>)**
4. Configure the remaining action settings and deploy the action. For more information, see Tanium Console User Guide: Deploying actions.
   If the manifest update fails, investigate environmental factors, such as security exclusions, file locks, CPU usage, RAM usage, and disk failures. Contact Tanium Support for additional help.

©2026 Tanium Inc. All Rights Reserved

Troubleshooting Endpoint Configuration

Collect logs

About this task

The information is saved as ZIP files that you can download with your browser.

To download logs:

1. From the Main menu, go to **Shared Services >** Endpoint Configuration.
2. From the **Endpoint ConfigurationOverview** page, click Help ?.
3. From the **Troubleshooting** tab, select the solutions for which to gather troubleshooting packages and click **Create Packages**. By default, all solutions are selected.
4. When the packages are ready, click **Download Support Bundle**. ZIP files of all the selected packages download to the local download directory.

   Tip: Some browsers might block multiple downloads by default. Make sure to configure your browser to permit multiple downloads from Tanium Console.
5. Contact Tanium Support on page 93 to determine the best option to send the ZIP files.

Identify and resolve issues with endpoint tools or Client extensions

About this task

You might become aware of issues with endpoint tools or Client extensions through solution-specific errors or through Overview pages for modules or shared services that indicate endpoints that need attention.

©2026 Tanium Inc. All Rights Reserved

Tools are bundled together in a versioned toolset that 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.

Use the following steps to troubleshoot issues with endpoint tools or Client extensions. During troubleshooting, consider environmental factors such as security exclusions, file locks, CPU usage, RAM usage, and disk failures.

1. If endpoints have Client extension shared process mode enabled and you need to troubleshoot resource usage or crashes in the combined TaniumCX.exe or TaniumCX process, disable shared process mode on the affected endpoints, and then reproduce the issue if possible. For more information, see Manage Client extension shared process mode on page 84.

2. To actively review the health of endpoint tools and Client extensions or to start an investigation into an existing error, ask a question using any of the following sensors as appropriate.
    - To determine the toolset version that should be installed and installation status of tools in that toolset, use the following sensor:

        - `Endpoint Configuration - Change Management Status`: Retrieves the upgrade ring to which endpoints are assigned (for the change management feature on page 40) and the associated toolset manifest version.

        Tip:

        - You can determine the versions of specific tools that are included in any of the toolset versions assigned to upgrade rings in Endpoint Configuration. From the Main menu, go to **Shared Services >** Endpoint Configuration. Go to **Change Management**, and then click the **Toolset Versions** tab.

        - For more information about the results from these, sensors, see Review upgrade status on page 55.

    - To get detailed tool information, use the `Endpoint Configuration - Tools Status Details` sensor. For each tool, this sensor returns the installed version,

©2026 Tanium Inc. All Rights Reserved

the targeted version, installation status, and other details related to failures blocks in place across endpoints. You can filter by **Tool Name** to investigate installation of a specific tool. (For more information about the results from this sensor, see step 4. If reinstalling the tool in the next step does not resolve the issue, you will use this sensor to perform further troubleshooting.)

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. 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 Uninstall tools installed by Endpoint Configuration on page 90.



CAUTION: When you perform a hard uninstallation of some tools, such as Recorder or Index, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data, such as recorded events (in the case of Recorder) or file indexes (in the case of Index). If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool. To help determine what data a tool stores on endpoints, review the User Guide for the tool or for the Tanium solution that installed it, and contact Tanium Support on page 93 for additional help.

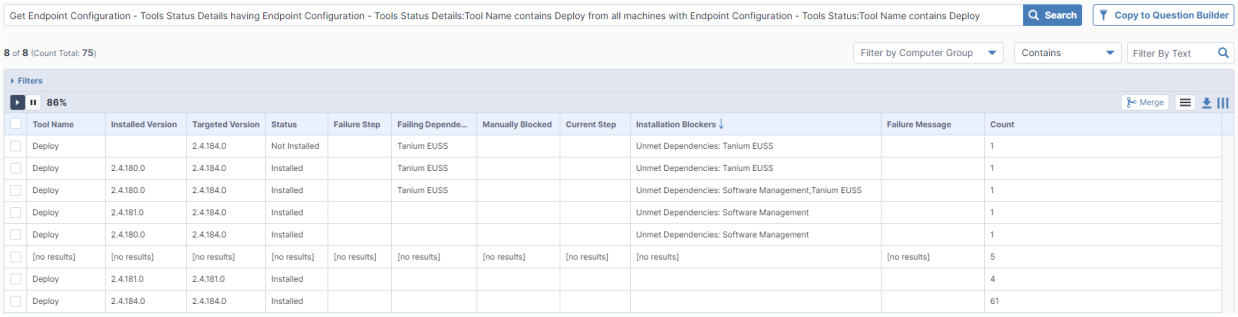
Wait for automatic reinstallation of the tool. If the reinstallation does not resolve the issue, continue to the next step.

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
Deploy from all machines with Endpoint Configuration - Tools
Status:Tool Name contains Deploy
```

Figure 10. Example question results

©2026 Tanium Inc. All Rights Reserved



Review the columns in the results for specific information about errors. The following table provides guidance for some common error conditions:

Common endpoint tool error conditions and resolutions in Endpoint Configuration

Error Condition	Possible Resolution
No error appears, but an available new version has not been installed	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 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 Verify and manually update the Endpoint Configuration manifest on page 86. • Action lock is enabled on the endpoint. Follow the steps in Verify and manually update the Endpoint Configuration manifest on page 86 to identify endpoints with action lock turned on. • The solution that installs the tool is no longer installed, or it is no longer targeting the endpoint. In some cases, a solution might stop targeting an endpoint because it no longer needs the endpoint for a particular workload. For example, if an endpoint is being used in a level 4 distributed scan in Discover, and peer endpoints appear with adjacent IP addresses, Discover no longer needs the original endpoint for the level 4 scan and no longer targets it. Consider whether the solution that installs the tool should still target the endpoint: • If it is expected or intentional that the solution no longer targets the endpoint, you can optionally uninstall the tool. For more information, see Uninstall tools installed by Endpoint Configuration on page 90. • If the solution should still target the endpoint, make sure that the action group for the solution that installs the tool includes the endpoint, and make sure the solution targets the endpoint in any expected configurations or profiles. Then, either wait for

©2026 Tanium Inc. All Rights Reserved

Error Condition	Possible Resolution
	the manifest to update and then review the results again, or follow the steps in Verify and manually update the Endpoint Configuration manifest on page 86.
No error appears, but the installed version is later than the targeted version	The endpoint was moved from an earlier upgrade ring, or you have just begun using the change management feature and the endpoint already had the later toolset version installed before you assigned it to an upgrade ring where you have not yet promoted the later version. No action is necessary, and this condition resolves itself over time as new toolset versions move through the upgrade rings.
No error appears, but tools are not installed on a container-based endpoint, nor does the endpoint appear in tool status results	This is expected behavior. Endpoint Configuration does not deploy tools to container-based endpoints; containers are not traditional endpoints that run packages or tooling, and they support only basic monitoring. No client-side log entry is generated for container endpoints. For more information, see the Tanium Cloud Workloads User Guide .
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 tool installation. For more information, see Review tool installations that are scheduled for a retry on page 65 .
Manually Blocked: `blocked`	The tool was previously blocked, either manually or during a previous uninstallation. Unblock the tool. For more information, see Uninstall tools installed by Endpoint Configuration on page 90 .

©2026 Tanium Inc. All Rights Reserved

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 87. For additional help, Collect logs on page 79, and Contact Tanium Support on page 93.

Manage Client extension shared process mode

You can enable or disable *client extension shared process mode* to control whether Client extensions run in separate processes or in a single combined process:

- Shared process mode disabled: Each Client extension runs in its own isolated instance of TaniumCX.exe (Windows) or TaniumCX (non-Windows), associated with the dynamic library for that Client extension. For example, on a Windows endpoint, ConfigCX runs with the following command:

```
"C:\Program Files (x86)\Tanium\Tanium Client\TaniumCX.exe" run --purpose
TaniumConfig.dll
```

- Shared process mode enabled: All Client extensions run together in a single instance of TaniumCX.exe (Windows) or TaniumCX (non-Windows). For example, on a Windows endpoint, all Client extensions run under the following command:

```
"C:\Program Files (x86)\Tanium\Tanium Client\TaniumCX.exe" run-framework
```



Important:

- If you use Tanium Patch, you must have Patch 3.15.148 or later installed to use shared process mode.
- If you use Tanium Deploy, you must have Deploy 2.21.150 or later installed to use shared process mode.

©2026 Tanium Inc. All Rights Reserved

Note:

- With shared process mode enabled, other processes, such as Tanium Client processes and endpoint tools other than Client extensions, continue to run separately.
- Enabling shared process mode reduces the number of Tanium processes running on endpoints. However, you cannot determine the CPU or memory usage of individual Client extensions within the combined process. While troubleshooting an issue where it is necessary to identify a specific extension causing the issue, such as excessive CPU usage, disable shared process mode. For more information about troubleshooting Client extensions, see Identify and resolve issues with endpoint tools or Client extensions on page 79.

Determine whether shared process mode is enabled on endpoints

About this task

To view the status of shared process mode on endpoints, ask a question using the `Tanium Client Explicit Setting[DisableExtensionIsolation]` sensor. Endpoints that return a value of `1` for this sensor have shared process mode enabled.

Enable or disable shared process mode

1. In Interact, ask a question that targets the endpoints on which you want to enable or disable shared process mode.
2. Select the results for the endpoints you want to target, and click **Deploy Action**.
3. For the **Deployment Package**, select the appropriate package to enable or disable shared process mode on the endpoints your are targeting:
   - Enable shared process mode: Select **Endpoint Configuration - Enable Shared Process Mode [Windows]** or **Endpoint Configuration - Enable Shared Process Mode [Non-Windows]**.
   - Disable shared process mode: Select **Endpoint Configuration - Disable Shared Process Mode [Windows]** or **Endpoint Configuration - Disable Shared Process Mode [Non-Windows]**.

©2026 Tanium Inc. All Rights Reserved

4. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   Best Practice: If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

5. Click **Show preview to continue**.

6. 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**.

Verify and manually update the Endpoint Configuration manifest

Check the manifest version on endpoints

1. From the Main menu, go to **Shared Services >** Endpoint Configuration.

2. On the Endpoint Configuration **Overview** page, note the **Manifest Revision** (version) in the **Summary** section.

3. Go to the Tanium **Home** page and ask the following question:
   `Get Endpoint Configuration - Manifest Metadata?maxAge=60 and Action Lock Status from all machines`

   Best Practice: The manifest changes whenever a configuration or tool change occurs. Therefore, use the `maxage=60` option for the **Manifest Metadata** sensor to ensure that you retrieve the latest data from endpoints.

   Tip: Sort the **Question Results** grid by **Revision** to list the versions in descending numerical order, which makes it easier to identify endpoints with an earlier manifest version.

4. If the **Question Results** indicate **Action Lock Status** is on for some endpoints that do not have the latest manifest:
   a. Consult whoever turned on the action locks to verify that it is now safe to run actions on those endpoints.
   b. Perform one of the following tasks:
      - Disable action locks on the endpoints that require an updated manifest. For

©2026 Tanium Inc. All Rights Reserved

more information, see Tanium Console User Guide: Turn off action locks.

- Configure Endpoint Configuration to ignore action locks for all endpoints. For more information, see Global Endpoint Configuration settings on page 95.

5. Manually update the manifest on endpoints on page 87 on any endpoints that require an updated version.

Manually update the manifest on endpoints

About this task

Windows and non-Windows endpoints require separate packages to update the manifest. Therefore, perform the following steps for each type of endpoint:

1. Go to the Tanium **Home** page and ask the following question:
   `Get Endpoint Configuration - Manifest Metadata?maxAge=60 from all machines`
2. Select the endpoints that have an outdated manifest and click **Deploy Action**.
3. Select the **Deployment Package** that matches the target endpoints:
   - Windows endpoints: **Endpoint Configuration - Manifest [Windows] (v. <latest_manifest_version>)**
   - Non-windows endpoints: **Endpoint Configuration - Manifest [Non-Windows] (v. <latest_manifest_version>)**
4. Configure the remaining action settings and deploy the action. For more information, see Tanium Console User Guide: Deploying actions.
   If the manifest update fails, investigate environmental factors, such as security exclusions, file locks, CPU usage, RAM usage, and disk failures. Contact Tanium Support on page 93 for additional help.

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**.

©2026 Tanium Inc. All Rights Reserved

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 logs on page 79, and Contact Tanium Support on page 93.

Restart installed Client extensions

About this task

Some changes to Client extension settings might require restarting Client extensions.

1. In Interact, target the endpoints on which you want to restart Client extensions. For example, ask a question that targets a specific operating system: `Get Endpoint Configuration - Tools Status from all machines with Is <OS> equals true`
2. In the results, select the appropriate rows, drill down as necessary, and select the targets on which you want to restart Client extensions. For more information, see Tanium Interact User Guide: Drill Down.
3. Click **Deploy Action**.
4. For the **Deployment Package**, select **Endpoint Configuration - Restart Client Extensions [Windows]** or **Endpoint Configuration - Restart Client Extensions [Non-Windows]**, depending on the endpoints you are targeting.
5. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   Best Practice: If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.
6. Click **Show preview to continue**.
7. A results grid appears at the bottom of the page showing you the targeted endpoints for your

©2026 Tanium Inc. All Rights Reserved

action. If you are satisfied with the results, click **Deploy Action**.

Disable and enable Client extensions

About this task

You can temporarily disable Client extensions on endpoints by toggling specific Client extensions individually, or by disabling all installed Client extensions at once.



Important: Disable Client extensions only at the direction of Tanium Support.

Toggle specific Client extensions

About this task

To disable or enable individual Client extensions, use the **Endpoint Configuration - Toggle Client Extension [Windows]** or **Endpoint Configuration - Toggle Client Extension [Non-Windows]** package. Configure the following parameters:

- Extension Names: A comma-separated list of extension names to toggle. Use the domain values returned by the `Client Extensions - Status` sensor. For example: `dec,threatresponse,index`.
- Action: Select **Enable** or **Disable**.
- Restart Client Extensions: Select this option to restart Client extensions immediately after applying the change. A restart is required for the change to take effect.



Note: The `core` (core-cx), `client` (internal Tanium Client extension functionality), and `config` (cx-config) Client extensions cannot be disabled. These extensions are required for core Tanium functionality.

Disable or re-enable all Client extensions

About this task

©2026 Tanium Inc. All Rights Reserved

To disable all installed Client extensions on an endpoint, use the **Endpoint Configuration - Disable Client Extensions [Windows]** or **Endpoint Configuration - Disable Client Extensions [Non-Windows]** package. Re-enable all Client extensions using the **Endpoint Configuration - Enable Client Extensions [Windows]** or **Endpoint Configuration - Enable Client Extensions [Non-Windows]** package.

Uninstall tools installed by Endpoint Configuration

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 <OS> equals true`

2. In the results, select the row for the tool you want to uninstall, drill down as necessary, and select the targets from which you want to remove Endpoint Configuration 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 the tool to uninstall, or to uninstall all tools, select **All Module Tools**.

   > **Note:**
   >
   > - If you select **All Module Tools**, the package uninstalls all endpoint tools except for core-cx and cx-config.
   > - In some cases, such as when the solution associated with a tool has been removed from the Tanium environment, the tool might not appear in the **Tool Name** list. In such a case, enter the tool name in the **Manually specified tool name** box, exactly as it appears in the **Tools** list in Endpoint Configuration.

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 was blocked manually or during a previous uninstallation, you must unblock it manually:

- To allow Endpoint Configuration 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 Endpoint Configuration databases and logs from the endpoints, clear the selection for **Soft uninstall**.

CAUTION: When you perform a hard uninstallation of some tools, such as Recorder or Index, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data, such as recorded events (in the case of Recorder) or file indexes (in the case of Index). If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool. To help determine what data a tool stores on endpoints, review the User Guide for the tool or for the Tanium solution that installed it, and contact Tanium Support on page 93 for additional help.

8. (Optional) To also remove any tools that were dependencies of the Endpoint Configuration 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.

Best Practice: 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**.

©2026 Tanium Inc. All Rights Reserved

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**.

Reinstall tools installed by Endpoint Configuration

1. In Interact, ask a question that targets the endpoints on which you want to reinstall a tool.
2. Select the results for the endpoints you want to target, and click **Deploy Action**.
3. For the **Deployment Package**, select **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
4. For **Tool Name**, select the tool to reinstall, or to reinstall all tools, select **All Module Tools**.

   Note:

   If you select **All Module Tools**:

   - The package reinstalls all endpoint tools except for core-cx and cx-config.
   - Reinstallation of all tools honors the Distribute Over Time tools installation setting: see Tools installation settings on page 94.
5. (Optional) To reinstall any dependencies of the tool being installed, select **Reinstall Dependencies**.
6. If reinstallation of the tool was previously blocked, select **Unblock Tool**.
7. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   Best Practice: If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.
8. Click **Show preview to continue**
9. 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**.

©2026 Tanium Inc. All Rights Reserved

Important:

- If you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package to reinstall a specific tool, it overrides the **Distribute Over Time** setting for tools installation: see Tools installation settings on page 94.
- Each Tanium solution includes one or more **Endpoint Tooling Cache - Tool name [#]** packages. Do not manually deploy these packages to endpoints.

Uninstall Endpoint Configuration

CAUTION: Uninstalling Endpoint Configuration disables functionality for all Tanium solutions. Contact Tanium support before you uninstall Endpoint Configuration.

1. From the Main menu, click **Administration** > **Configuration** > **Solutions**.
2. In the **Content** section, select the **Endpoint Configuration** row.
3. Click Delete Selected. Click **Uninstall** to complete the process.

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: Endpoint Configuration settings

To access Endpoint Configuration settings from the Endpoint Configuration **Overview** page, click Settings.

Important: Contact Tanium Support on page 93 before you edit any setting in Endpoint Configuration that is not listed here.

Tools installation settings

Endpoint Configuration tools installation settings

Setting	Default value	Description
Distribute Over Time	0 seconds	The time over which to randomize distribution of the endpoint tools that each endpoint requires, based on the modules that are in use with that endpoint. Randomizing this distribution over a period of time helps balance resource use. **Important:** This global setting has been superseded by the **Distribute Over Time** setting on each change management upgrade ring. This setting applies only to endpoints with a toolset version earlier than 2.22. For more information about configuring this setting on upgrade rings, see Configure upgrade rings on page 46 . **Best Practice:** Do not set this value higher than 24 hours.

©2026 Tanium Inc. All Rights Reserved

Global Endpoint Configuration settings

Global Endpoint Configuration settings

Setting	Default value	Description
Enable Configuration Approvals	Unselected	Determines whether to require approvals for configuration changes. For more information, see Managing approvals on page 37 .
Config Rejected Item Retention Days	30 days	The time after which a rejected configuration item is automatically dismissed if it has not been manually dismissed. For more information, see Managing approvals on page 37 .
Manifest Action Distribute Over Time	1 minute	The time over which to randomize distribution of the manifest that contains updated endpoint configuration information to endpoints. Randomizing this distribution over a period of time helps balance resource use. The duration that you specify for this setting must be shorter than the duration that you specify for the **Manifest action duration seconds** setting.
Manifest Action Duration	1 hour	The time after which the action that is used to deliver the manifest expires and is reissued. The duration that you specify for this setting must be longer than the duration that you specify for the **Manifest action distribute seconds** setting.
Manifest Package Ignore Action Lock	Unselected	Determines whether the action that is used to deliver the manifest ignores an action lock in place on an endpoint. If this setting is disabled, the manifest is not distributed to an endpoint that has an action lock, and that endpoint does not evaluate needed configuration changes. For more information, see Tanium Console User Guide: Managing action locks .
Deploy Client Configuration and Support Action Distribute Over Time	1 minute	The time over which to randomize distribution of the Client Extensions bootstrap installer for endpoint tools. Randomizing this distribution over a period of time helps balance resource use. The duration that you specify for this setting must be shorter than the duration that you specify for the **Deploy Client configuration and support action duration** setting.
Deploy Client Configuration and Support	1 hour	The time after which the action that is used to distribute the Client Extensions bootstrap installer for endpoint tools expires and is reissued. The duration that you specify for this setting must be longer than the duration that is specified for the **Deploy Client Configuration and Support**

©2026 Tanium Inc. All Rights Reserved

Setting	Default value	Description
Action Duration		**Action Distribute Over Time** setting.  **Important:** Do not change the **Deploy Client Configuration and Support Action Distribute Over Time** setting except at the direction of Tanium Support.
Deploy Client Configuration and Support Package Ignore Action Lock	Unselected	Determines whether the action that is used to distribute the Client Extensions bootstrap installer for endpoint tools ignores an action lock in place on an endpoint. If this setting is disabled, the bootstrap installer is not distributed to an endpoint that has an action lock, and that endpoint does not install tools. For more information, see Tanium Console User Guide: Managing action locks .
Time Before Auto-Uninstall	45 days	The number of days an untargeted tool remains on an endpoint before Endpoint Configuration automatically removes it. You can configure between 30 and 90 days. For more information, see Automatic tool removal on page 61 .
Content-Only Solution Job Frequency	15 minutes	The interval at which Endpoint Configuration scans for changes in content-only solutions. For more information, see View and manage content-only solutions on page 69 .

©2026 Tanium Inc. All Rights Reserved