Tanium™ Endpoint Configuration User Guide

Version 1.7.151

November 10, 2022

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://docs.tanium.com for the most current Tanium product documentation.

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

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

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years and has most recently completed certification against the WCAG 2.1 / VPAT 2.3 standards for all major product modules in summer 2021. In the recent testing the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.1 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 best efforts to address any gaps quickly, as is feasible, given the severity of the issue and scope of the changes. These objectives are factored into the ongoing delivery schedule of features and releases with our existing resources.

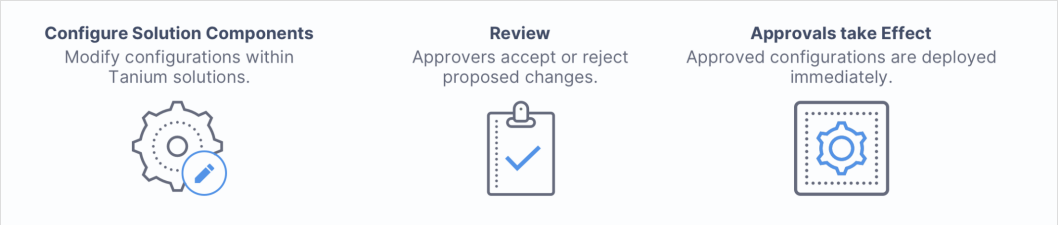
Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, email Tanium Support at support@tanium.com, or email accessibility@tanium.com to make further inquiries.

Table of contents

Endpoint Configuration overview

Use Endpoint Configuration to deliver configuration information to endpoints 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. 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

Other Tanium solutions use Endpoint Configuration to install client extensions and any other needed tools on endpoints. You can review installed endpoint tools in Endpoint Configuration, and you can use the packages provided by Endpoint Configuration to restart, uninstall, reinstall, block, or unblock endpoint tools as necessary.

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 Endpoint Configuration approvals.

Approvals

When configuration approval 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.

Integration with other Tanium products

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 32.

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 Tanium Console User Guide: Managing action locks.

Tanium Solution	Configuration Changes and Approvals	Tool Deployment
Tanium™ Asset	✓	✓
Tanium™ Comply	✓	✓
Tanium™ Deploy	✓	✓
Tanium™ Direct Connect	✓	✓
Tanium™ Discover	✓	✓
Tanium™ Enforce	✓	✓
Tanium™ Impact	✓	✓
Tanium™ Integrity Monitor	✓	✓

Tanium Solution	Configuration Changes and Approvals	Tool Deployment
Tanium™ Map	✓	✓
Tanium™ Patch	✓	✓
Tanium™ Performance	✓	✓
Tanium™ Reveal	✓	✓
Tanium™ Risk	✓	✓
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 30.

Getting started with Endpoint Configuration

Step 1: Install Tanium Client Management and configure Endpoint Configuration

Endpoint Configuration is installed as part of Tanium™ Client Management. Use the **Solutions** page to install Client Management and choose either automatic or manual configuration. After installing Client Management, you can reconfigure the Endpoint Configuration service account if necessary.

For more information, see Tanium Client Management User Guide: Installing Client Management and Verifying installation of Endpoint Configuration on page 16.

Step 2: Manage configurations

Configurations are defined in a Tanium solution. When a configuration is created or changed, the configuration is displayed in Endpoint Configuration in the **Proposed** state if configuration approval is enabled.

See Managing configurations.

Step 3: Manage approvals

If configuration approval is enabled, when a configuration change is made in a supported Tanium solution, an approval is displayed in the Approvals page of Endpoint Configuration.

See Managing approvals.

Endpoint Configuration requirements

Endpoint Configuration is installed as part of Tanium Client Management. Review the requirements before you install Client Management and use Endpoint Configuration.

For more information about Client Management, see Tanium Client Management User Guide.

Core platform dependencies

Make sure that your environment meets the following requirements:

- **Tanium™ Core Platform servers**: 7.4.3.1204 or later
- **Tanium™ Client**: Any supported version of Tanium Client. For the Tanium Client versions supported for each OS, see Tanium Client Management User Guide: Client version and host system requirements.

  If you use a client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed client versions.

  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.

If you import Client Management 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 Client Management and Endpoint Configuration action group to target the **No Computers** filter group, then before using any modules, first set the Client Management action group to target the `All Computers` computer group, and then set the Endpoint Configuration action group to target the `All Computers` computer group. If you have endpoints with operating systems that are not supported by Endpoint Configuration, contact Tanium Support.

(Tanium Core Platform 7.4.5 or later only) Optionally, you can set the Endpoint Configuration action group to target the **No Computers** filter group by enabling restricted targeting before importing Client Management. 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: Dependencies, default settings, and tools deployment.

If you use restricted targeting to set the Client Management and Endpoint Configuration action groups to target the **No Computers** filter group, then make sure that before using any modules, you first set the Client Management action group to target the appropriate endpoints (typically `All Computers`), and then set the Endpoint Configuration action group to target the same endpoint. For more information, see Tanium Client Management User Guide: Configure the Endpoint Configuration action group and Configure the Endpoint Configuration action group

on page 18 in this guide. 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.

Solution dependencies

Other Tanium solutions are required for specific Endpoint Configuration features to work. 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 by clicking the links in the lists of Required dependencies on page 10 and Feature-specific dependencies on page 11. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Endpoint Configuration requires.

IMPORTANT

- Make sure you upgrade each module that uses Endpoint Configuration to a version from after support for Endpoint Configuration was introduced (follow links for Tanium Dependencies from Tanium Client Management User Guide: Module- and service-specific requirements for the Tanium Client and endpoints and see the release notes for each module).
- After Endpoint Configuration is installed, do not use the **Initial Content - Python** solution to deploy Python to endpoints that support Endpoint Configuration (see Endpoints on page 11).

Tanium recommended installation

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

Import specific solutions

If you select only Endpoint Configuration to import and are using Tanium Core Platform 7.5.2.3531 or later with Tanium Console 3.0.72 or later, 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.

If you select only Endpoint Configuration to import and you are using Tanium Core Platform 7.5.2.3503 or earlier with Tanium Console 3.0.64 or earlier, you must manually import or update required dependencies. See Tanium Console User Guide: Import, re-import, or update specific solutions.

Required dependencies

Endpoint Configuration has the following required dependencies at the specified minimum versions:

- Tanium™ RDB 1.2.11 or later
- Tanium™ System User service 1.0.77 or later

Feature-specific dependencies

Endpoint Configuration has the following feature-specific dependencies at the specified minimum versions:

- Tanium Connect 5.9 or later is required to use Endpoint Configuration audit logs as a connection source.

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.

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. See Tanium Client Management User Guide: Client version and host system requirements.	
Linux	Same as Tanium Client support. 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.

Operating System	Version	Notes
Solaris	Same as Tanium Client support. 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.

Host and network security requirements

Ports

The following ports are required for Endpoint Configuration communication.

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.

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

Security exclusions

If security software is in use in the environment to monitor and block unknown host system processes, Tanium recommends that a security administrator create exclusions to allow the Tanium processes to run without interference. The configuration of these exclusions varies depending on AV software. For a list of all security exclusions to define across Tanium, see Tanium Core Platform Deployment Reference Guide: Host system security exclusions.

Endpoint Configuration security exclusions

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

User role requirements

The following tables list the role permissions required to use Endpoint Configuration. To review a summary of the predefined roles, see Set up Endpoint Configuration users on page 18.

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 user guide 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.

For more information about role permissions and associated content sets, see Tanium Core Platform User Guide: Managing RBAC.

Endpoint Configuration user role 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 user role permissions (continued)

Permission	Endpoint Configuration Administrator	Endpoint Configuration Approver	Endpoint Configuration Auditor	Endpoint Configuration Read Only User
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	✗	✗	✗
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[2] 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] This permission is not provided by default to any roles.

Provided 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
Endpoint Configuration	Platform Content	✓ READ WRITE	✓ SPECIAL READ	✓ READ	✓ READ
Endpoint Configuration Module	Platform Content	✓ SPECIAL	✗	✗	✗
Own Action	Platform 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 which content set permissions are granted to a role, see Tanium Console User Guide: View effective role permissions.

Verifying installation of Endpoint Configuration

Endpoint Configuration is installed as part of Tanium Client Management. When you install Client Management the Endpoint Configuration workbench becomes available from the Tanium Console. For more information, see Tanium Client Management User Guide: Installing Client Management.

(Tanium Core Platform 7.4.5 or later only) Optionally, you can set the Endpoint Configuration action group to target the **No Computers** filter group by enabling restricted targeting before importing Client Management. 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: Dependencies, default settings, and tools deployment.

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

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 Client Management and Endpoint Configuration action groups to target the **No Computers** filter group, then make sure that before using any modules, you first set the Client Management action group to target the appropriate endpoints (typically `All Computers`), and then set the Endpoint Configuration action group to target the same endpoint. For more information, see Tanium Client Management User Guide: Configure the Endpoint Configuration action group and Configure the Endpoint Configuration action group on page 18 in this guide. 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 Client Management 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 Client Management and Endpoint Configuration action group to target the **No Computers** filter group, then before using any modules, first set the Client Management action group to target the `All Computers` computer group, and then set the Endpoint Configuration action group to target the `All Computers` computer group. If you have endpoints with operating systems that are not supported by Endpoint Configuration, contact Tanium Support.

Verify Endpoint Configuration version

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

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

Troubleshoot problems

If you experience problems with configuring Endpoint Configuration, see Troubleshooting Endpoint Configuration on page 34.

Configuring Endpoint Configuration

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

Configure the Endpoint Configuration action group

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.

If you import Client Management 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 Client Management and Endpoint Configuration action group to target the **No Computers** filter group, then before using any modules, first set the Client Management action group to target the `All Computers` computer group, and then set the Endpoint Configuration action group to target the `All Computers` computer group. If you have endpoints with operating systems that are not supported by Endpoint Configuration, contact Tanium Support.

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

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 13.

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 Core Platform User Guide: Manage role assignments for a user.

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.

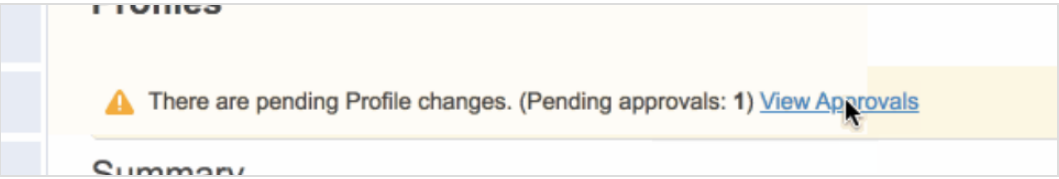
Endpoint Configuration Read Only User

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

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.

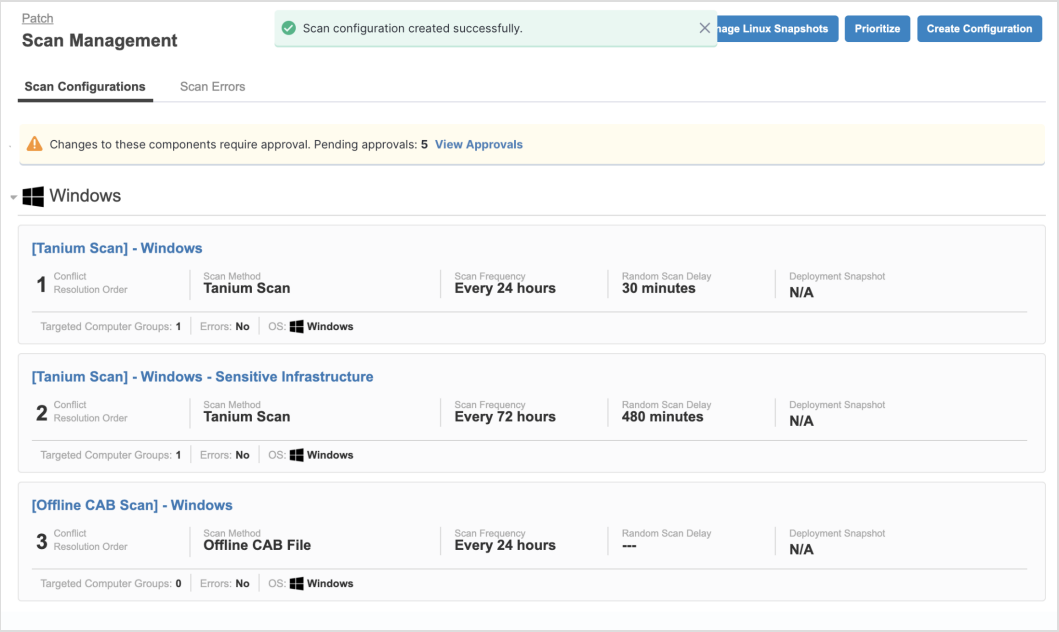
Managing configurations

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 deployed 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.



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 Tanium Console User Guide: Managing action locks.

View configurations

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 22.

Remove configurations for uninstalled solutions

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.

1. From the Endpoint Configuration menu, click **Configurations**.
2. Select a configuration and click **Delete**.

Managing approvals

Enable configuration approvals

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

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

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.

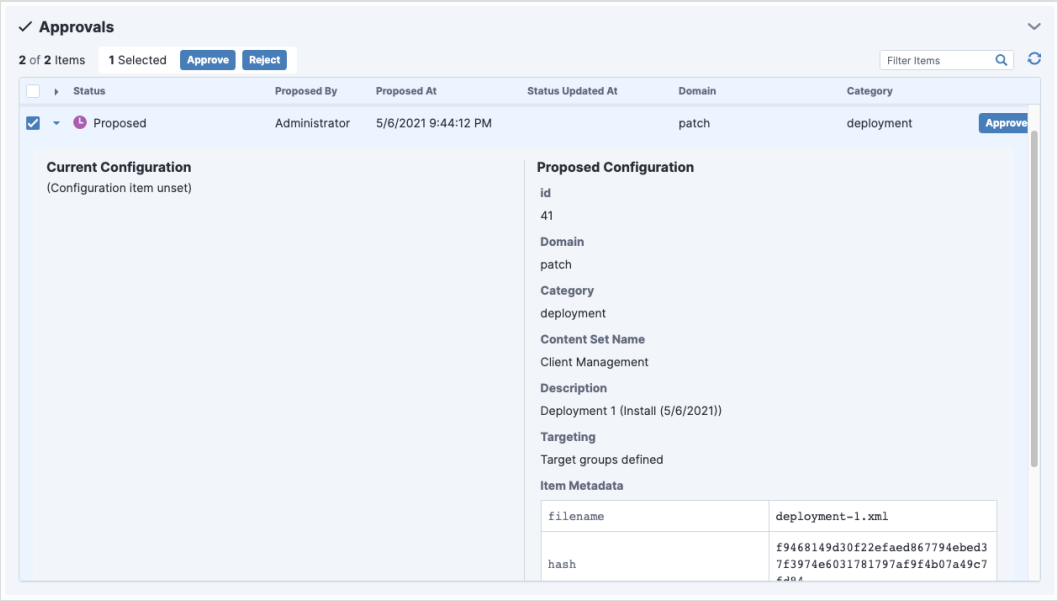
Approve or reject configuration changes

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.

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 Endpoint Configuration menu, click **Overview**.



2. 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.

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

4. Click **Approve** or **Reject**. Confirm that you want to Approve or Reject the pending approvals.

5. If an approval is in the **Approved** or **Rejected** state, click **Dismiss** to remove the approval from the Approvals page.

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. See Global Endpoint Configuration settings on page 39.

Managing endpoint tools

Other Tanium solutions use Endpoint Configuration to install client extensions and any other needed tools on endpoints. You can review installed endpoint tools in Endpoint Configuration, and you can use the packages provided by Endpoint Configuration to manage these tools.

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 Tanium Console User Guide: 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.

View deployed endpoint tools

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

1. Click **Tools** from the Endpoint Configuration menu.
2. Expand a tool to view the status of that tool across all endpoints.
3. (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 all endpoints that have the tool installed.

NOTE The **Tools** page displays cached data that is provided by the 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.

Remove unused endpoint tools

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

1. Click **Tools** from the Endpoint Configuration menu.
2. Click the **Safe to Remove** category.
3. Beside the tool that you want to remove, click View question results in Interact.

4. In the question results, select the rows for installed versions that you want to remove, and click **Drill Down**.
5. 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`
6. Select the row from the drill-down question results, and click **Deploy Action**.
7. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
8. For **Tool Name**, select the name of the tool you are uninstalling.
9. (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**.
10. (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.
11. (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**.
12. (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.
13. Click **Show preview to continue**.
14. 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**.

Restart installed client extensions

Some changes to client extension settings 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 action. If you are satisfied with the results, click **Deploy Action**.

Block or unblock tools from installing on an endpoint

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.

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**.

Disable all installed client extensions

You can temporarily disable all client extensions that are installed on an endpoint using the **Endpoint Configuration - Disable Client Extensions [Windows]** or **Endpoint Configuration - Disable Client Extensions [Non-Windows]** package.

IMPORTANT

Disable client extensions only at the direction of Tanium Support.

Re-enable client extensions using the **Endpoint Configuration - Enable Client Extensions [Windows]** or **Endpoint Configuration - Enable Client Extensions [Non-Windows]** package.

NOTE

Some components have packages to disable only specific client extensions, such as the **Index - Disable Extension [Windows]** package, which disables only the Index client extension.

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.
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.

   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, go to https://docs.tanium.com/ and review the documentation for the tool or for the Tanium solution that installed it, and contact Tanium Support 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**.

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 39.

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**.

IMPORTANT

- If you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package, it overrides the **Distribute Over Time** setting for tools installation: see Tools installation settings on page 39.
- Each Tanium solution includes one or more **Endpoint Tooling Cache - *Tool name* [#]** packages. Do not manually deploy these packages to endpoints.

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:

- **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

View and manage content-only solutions

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.

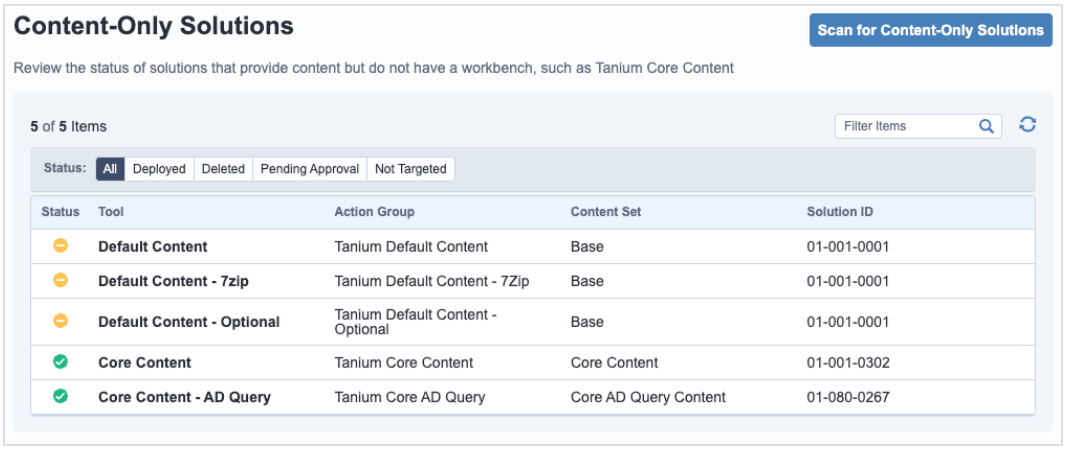
Endpoint Configuration creates an action group for each content-only solution. By default, each of these action groups includes only the **No Computers** computer group, and so associated tools do not deploy to endpoints until you select another computer group for the action group.

View the status of content-only solutions

You can review the status of the tools that Endpoint Configuration has deployed for these solutions, including the configured action groups and applicable content sets. To view the tools for content-only solutions, Click **Content-Only Solutions** from the Endpoint Configuration menu.

Successfully deployed tools have a status of Deployed. The status Not Targeted indicates that the action group for a tool targets **No Computers**. Follow the steps in Configure action groups for content-only solutions on page 30 to deploy the 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. See Global Endpoint Configuration settings on page 39.



Configure action groups for content-only solutions

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

1. From the Endpoint Configuration menu, click **Content-Only Solutions**.
2. Click **Not Targeted** to view the tools that target **No Computers**.
3. For each listed tool, note the associated **Action Group**, and configure that action group to target the appropriate endpoints:
    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**.

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

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

Reviewing and exporting the audit log

Reviewing the audit log

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

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

The audit log is also included in the support package for Endpoint Configuration. For the steps to download the support package, see Collect logs on page 34.

Before you begin

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

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 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**.

Test a connection and review data

1. From the Connect menu, click **Connections**.
2. Click the connection that you created for the Direct Connect 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.

Troubleshooting Endpoint Configuration

Collect logs

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

To download logs:

1. From the Endpoint Configuration**Overview** page, click Help .
2. From the **Troubleshooting** tab, select the solutions for which to gather troubleshooting packages and click **Create Packages**. By default, all solutions are selected.
3. 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 the Tanium Console.

4. Contact Tanium Support to determine the best option to send the ZIP files. For information, see Contact Tanium Support on page 38.

Tanium Endpoint Configuration maintains logging information in the `Endpoint Configuration.log` file in the `\Program Files\Tanium\Tanium Module Server\services\Endpoint Configuration` directory.

Endpoint Configuration maintains logging information in the `tanium-config.log` file in the `<Module Server>/services/endpoint-configuration-files` directory.

Identify and resolve issues with endpoint tools or client extensions

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.

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. To actively review the health of endpoint tools and client extensions or to start an investigation into an existing error, ask a question using the `Endpoint Configuration - Tools Status`, `Client Extensions - Status`, or *`[Module] - Tools Version`* sensor.
   The results of these questions help to identify endpoints with errors and provide a starting point to deploy actions that might help correct the issue. 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.

2. Target one or more endpoints with errors, and uninstall tools that report errors without blocking reinstallation: see Troubleshooting Endpoint Configuration on page 34.

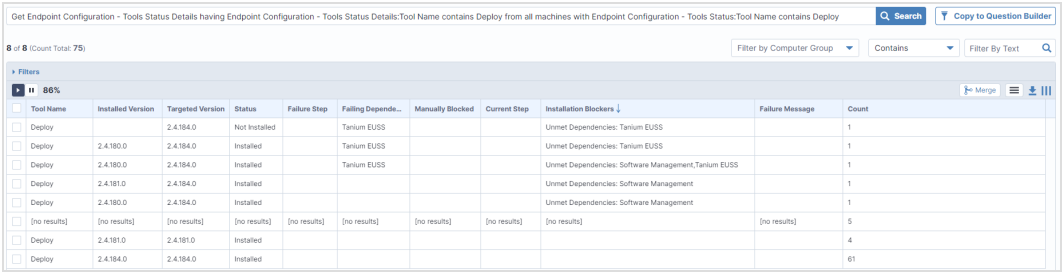
   CAUTION

   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, go to https://docs.tanium.com/ and review the documentation for the tool or for the Tanium solution that installed it, and contact Tanium Support for additional help.

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

3. 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`



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

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 37. • 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: see Troubleshooting Endpoint Configuration on page 34. ◦ 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 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 37.
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 29.
Manually Blocked: `blocked`	The tool was previously blocked, either manually or during a previous uninstallation. Unblock the tool: see Troubleshooting Endpoint Configuration on page 34.

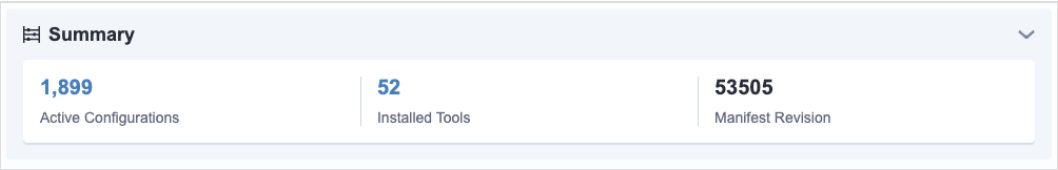
4. Review the Extensions logs on the endpoint. Take note of entries that include `fail` or `error`: see Review the Extensions log for an endpoint on page 37.

For additional help, collect all logs for Tanium Endpoint Configuration, and contact Tanium Support.

Verify and manually update the Endpoint Configuration manifest

Check the manifest revision on the Tanium Server

1. From the Endpoint Configuration menu, go to **Overview**.
2. The **Manifest Revision** appears in the **Summary** section of the Overview page.



Check the manifest version on endpoints

1. In Interact, ask the question: `Get Endpoint Configuration - Manifest Metadata?maxAge=60 from all machines`
   Optionally add filters to the question to check the manifest revision on specific endpoints.

   BEST PRACTICE

   Use the `maxAge=60` option for this question to return the latest results that are available.
2. Review the **Revision** column and note versions that are different from the manifest on the server. Drill down as necessary.

Manually update the manifest on endpoints

1. Ask a question to target endpoints that require a manifest update, or start from the results that the steps in Check the manifest version on endpoints on page 37 returned.
2. Select the results for the endpoints you want to target, and click **Deploy Action**.
3. For the **Deployment Package**, select **Endpoint Configuration - Manifest [Windows]** or **Endpoint Configuration - Manifest [Non-Windows]**, depending on the endpoints you are targeting.
4. Click **Show preview to continue**
5. 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**.

If the manifest update fails, investigate environmental factors, such as security exclusions, file locks, CPU usage, RAM usage, and disk failures. For additional help, contact Tanium Support.

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 **Administration > Shared Services > Client Management**.
2. From the Client Management menu, click **Client Health**.
3. In the **Direct Connect** search box, enter all or part of an IP address or a computer name.
   Matching results are displayed after the search completes.
4. From the search results, click the computer name to connect to the endpoint.
5. Click the **Logs** tab, and select an **extensions*[#]*.log** file.
6. (Optional) To download the log, click **Download**.

For additional help, collect all logs for Tanium Endpoint Configuration, and contact Tanium Support.

Uninstall Endpoint Configuration

Uninstalling Endpoint Configuration affects all Tanium solutions. Contact Tanium support before you uninstall Endpoint Configuration.

Endpoint Configuration is uninstalled with Client Management. For more information, see Uninstall Client Management.

Contact Tanium Support

To contact Tanium Support for help, send an email to support@tanium.com.

Reference: Endpoint Configuration settings

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

IMPORTANT

Contact Tanium Support before you edit any setting in Endpoint Configuration that is not listed here.

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. 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 Troubleshooting Endpoint Configuration on page 34.

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 22.
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.

Setting	Default value	Description
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 Action Duration	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 you specify for the **Deploy client configuration and support action distribute seconds** setting.
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 22.
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 30.
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 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.