Tanium™ Endpoint Configuration User Guide

Version 1.5.258

March 21, 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.

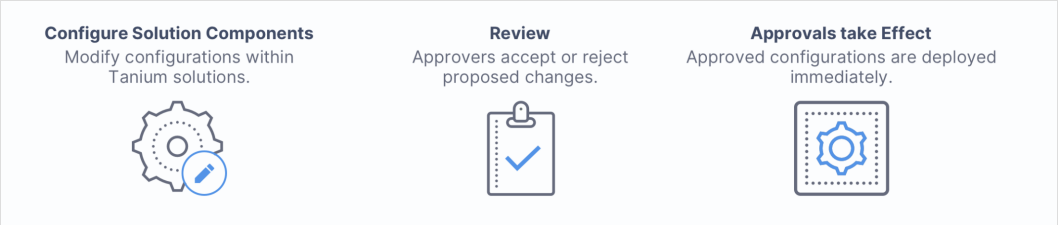
Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are committed to prioritizing these compliance efforts as part of our overall product roadmap. 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.



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.

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 Exporting an audit log on page 25.

Other Tanium solutions

Endpoint Configuration manages configuration changes, approvals, and tool deployment for the following solutions:

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™ Map	✓	✓
Tanium™ Patch	✓	✓
Tanium™ Performance	✓	✓
Tanium™ Reveal	✓	✓
Tanium™ Risk	✓	
Tanium™ Threat Response	✓	✓

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 15.

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**: 7.3.314.4250 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 Endpoint Configuration action group to target the **No Computers** filter group, set the action group to target the `All Computers` computer group before using any modules. 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 Endpoint Configuration action group to target the **No Computers** filter group, make sure you set the action group to target the appropriate endpoints (typically `All Computers`) before using any modules: see Configure the Endpoint Configuration action group on page 17. 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 Endpoint Configuration requirements on page 8 and Feature-specific dependencies on page 9. 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 10).

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, you must manually import dependencies. See Tanium Console User Guide: Import, re-import, or update specific solutions.

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.
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.

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

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.

Endpoint Configuration user role permissions

Permission	Endpoint Configuration Administrator	Endpoint Configuration Approver	Endpoint Configuration Read Only User	Endpoint Configuration Service Account	Endpoint Configuration Service Account Read All Sensors
Endpoint Configuration View the Endpoint Configuration workbench, and access and manage configuration changes	✓ SHOW WRITE	✓ APPROVE[1] DISMISS[1]	✓ SHOW READ	✓ READ WRITE[1]	✗
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	✗
Endpoint Configuration Module Register or use the Endpoint Configuration module	✓ USE	✗	✗	✓ REGISTER USE	✗
Endpoint Configuration Read Only Provides read privileges for sensors, packages and actions in Endpoint Configuration	✗	✗	✓ USER	✗	✗
Endpoint Configuration Service Account Access the service account settings for Endpoint Configuration, and provide the service account with the necessary permissions	✓ READ WRITE	✗	✗	✓ EXECUTE	✗

Endpoint Configuration user role permissions (continued)

Permission	Endpoint Configuration Administrator	Endpoint Configuration Approver	Endpoint Configuration Read Only User	Endpoint Configuration Service Account	Endpoint Configuration Service Account Read All Sensors
Endpoint Configuration Settings Access Endpoint Configuration settings	✓ READ WRITE	✗	✓ SHOW READ	✗	✗
Endpoint Configuration Support Bundle Access the support bundle for Endpoint Configuration	✓ READ	✗	✗	✗	✗
Endpoint Configuration Bypass[2] You can apply this permission to module service accounts, 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 Configurationadministration and platform content permissions

Permission	Role Type	Endpoint Configuration Administrator	Endpoint Configuration Approver	Endpoint Configuration Read Only User	Endpoint Configuration Service Account	Endpoint Configuration Service Account Read All Sensors
Action Group	Administration	✗	✗	✗	✓ READ	✗
Allowed URLs	Administration	✗	✗	✗	✓ READ WRITE	✗
Computer Group	Administration	✗	✗	✗	✓ READ	✗
Persona	Administration	✗	✗	✗	✓ READ	✗
User	Administration	✗	✗	✗	✓ READ	✗
Action	Platform Content	✗	✗	✓ READ	✓ READ WRITE	✗
Bypass Action Approval	Platform Content	✗	✗	✗	✓ SPECIAL	✗
Own Action	Platform Content	✗	✗	✓ READ	✓ READ	✗
Package	Platform Content	✗	✗	✓ READ	✓ READ WRITE	✗
Plugin	Platform Content	✗	✗	✓ READ	✓ READ EXECUTE	✗
Sensor	Platform Content	✗	✗	✓ READ	✓ READ	✓ READ

You can view which content sets are granted to any role in the Tanium Console.

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.

BEST PRACTICE When you import Client Management, sign in to the Tanium Console with the account that will be used as the Client Management and Endpoint Configuration service account. The Endpoint Configuration service account is set to the account that you used to import the Client Management service, regardless of whether you use automatic configuration when you import 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 settings are 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 Endpoint Configuration action group to target the **No Computers** filter group, make sure you set the action group to target the appropriate endpoints (typically `All Computers`) before using any modules: see Configure the Endpoint Configuration action group on page 17. 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 Endpoint Configuration action group to target the **No Computers** filter group, set the action group to target the `All Computers` computer group before using any modules. If you have endpoints with operating systems that are not supported by Endpoint Configuration, contact Tanium Support.

Setting	Default Value
Service account	The service account is set to the account that you used to import the Client Management service. Configuring a unique service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization. See Configure the service account on page 17.

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 27.

Configuring Endpoint Configuration

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

Configure the service account

The service account is a user that runs several background processes for Endpoint Configuration. This user requires one of the following combinations of roles:

- **Tanium Administrator**
- **Endpoint Configuration Service Account** and **Endpoint Configuration Service Account Read All Sensors**

IMPORTANT If action approval is enabled for Tanium Core Platform, you must either use the **Endpoint Configuration Service Account** and **Endpoint Configuration Service Account Read All Sensors** roles for the service account, or, if you are using the **Tanium Administrator** role, grant the **Bypass Action Approval** permission to the Endpoint Configuration service account. For more information, see Tanium Console User Guide: Managing action approval.

For more information about Endpoint Configuration permissions, see User role requirements on page 11.

NOTE If you imported Client Management with default settings, the service account is set to the account that you used to perform the import. Configuring a unique service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization.

1. From the Main menu, click **Endpoint Configuration** to open the Endpoint Configuration **Overview** page.
2. Click Settings and open the **Service Account** tab.
3. Update the service account settings and click **Save**.

Configure the Endpoint Configuration action group

Importing the Client Management module automatically creates an Endpoint Configuration action group to target specific endpoints. Select the computer groups to include in the Endpoint Configuration action group.

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 Endpoint Configuration action group to target the **No Computers** filter group, set the action group to target the `All Computers` computer group before using any modules. 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 11.

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 Users who can review settings and configuration items in Endpoint Configuration.

Endpoint Configuration Service Account

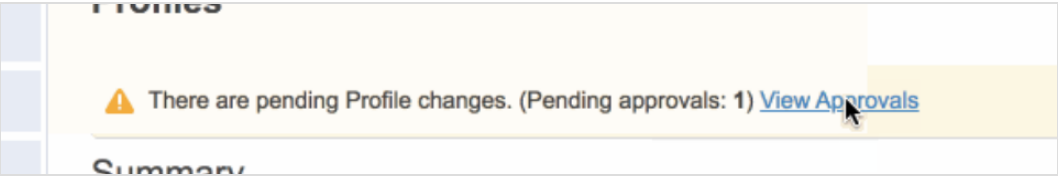
Assign the **Endpoint Configuration Service Account** role to the account that performs background processes for Endpoint Configuration. You must also assign the **Endpoint Configuration Service Account Read All Sensors** role to this account. For more information, see Configure the service account on page 17.

Endpoint Configuration Service Account Read All Sensors

Assign the **Endpoint Configuration Service Account Read All Sensors** role to the account that performs background processes for Endpoint Configuration. You must also assign the **Endpoint Configuration Service Account** role to this account. For more information, see Configure the service account on page 17.

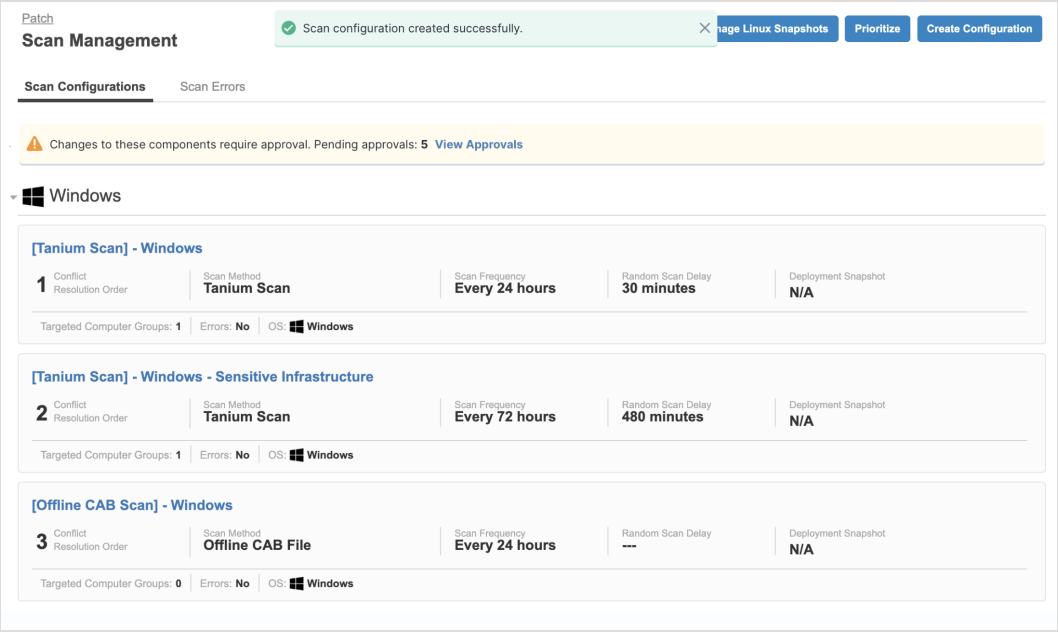
Managing configurations

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.



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 21.

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 Home page, 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.

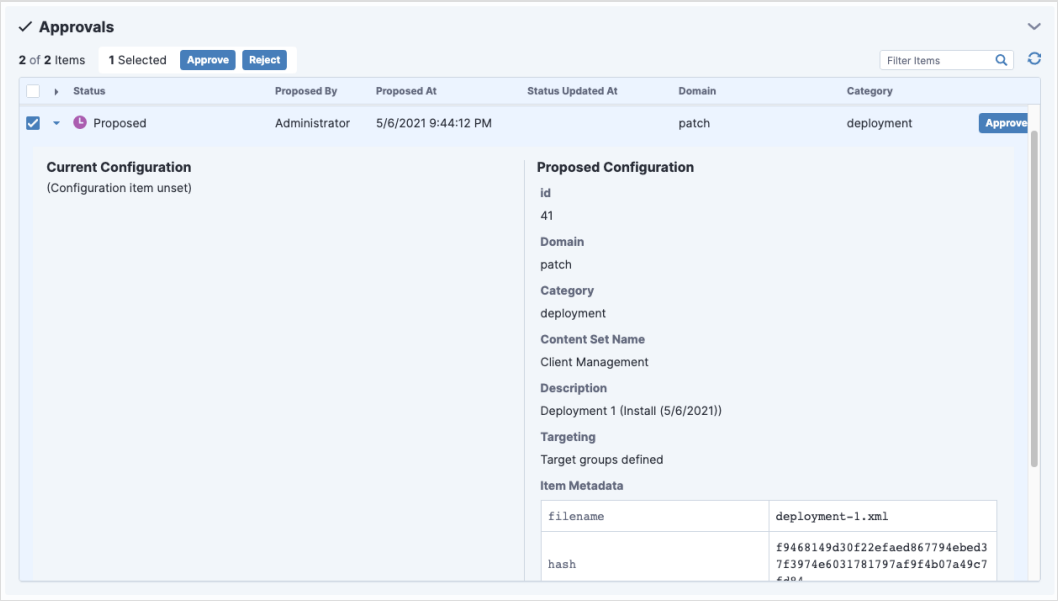
Approve or reject configuration changes

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.

Managing endpoint tools

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

View deployed endpoint tools

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 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. From the **Tools** page, expand a tool that has endpoints in the **Safe to Remove** category.
2. Click the **Safe to Remove** category.
3. In the question results, select the row for the tool, and click **Drill Down**.
4. 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`
5. Select the row from the drill-down question results, and click **Deploy Action**.
6. On the **Deploy Action** page, enter `Endpoint Configuration - Uninstall` in **Enter package name here**, and select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
7. For **Tool Name**, select the name of the tool you are uninstalling.
8. (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**.

9. (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.
10. (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**.
11. Click **Show preview to continue**.
12. 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**.

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 27.

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

To collect and send information to Tanium for troubleshooting, and other relevant information.

Collect logs

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

1. From the Endpoint Configuration home page, click Help, then the **Troubleshooting** tab.
2. Click **Download Support Package**.
   A `tanium-endpoint-configuration-support-[timestamp].zip` file downloads to the local download directory.
3. Attach the ZIP file to your Tanium Support case form or contact Tanium Support.

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

Block or unblock tools from installing on an endpoint

To block or unblock the installation of one or more tools on an endpoint that is included in an Endpoint Configuration manifest, distribute the **Endpoint Configuration - Block Tool** or **Endpoint Configuration - Unblock Tool** package.

Block the installation of a tool

1. Target the endpoints on which you want to block tool installation.
2. Click **Deploy Action**.
3. (Windows) Select the **Endpoint Configuration - Block Tool [Windows]** package.
4. (Non-Windows) Select the **Endpoint Configuration - Block Tool [Non-Windows]** package.
5. Choose a tool from the dropdown, or provide a manual tool name.

Unblock the installation a tool

1. Target the endpoints on which you want to unblock tool installation.
2. Click **Deploy Action**.
3. (Windows) Select the **Endpoint Configuration - Unblock Tool [Windows]** package.
4. (Non-Windows) Select the **Endpoint Configuration - Unblock Tool [Non-Windows]** package.
5. Choose a tool from the dropdown, or provide a manual tool name.

Uninstall one or more tools installed by Endpoint Configuration

To uninstall one or more tools on an endpoint that was installed by Endpoint Configuration, distribute the **Endpoint Configuration - Uninstall Tool** package.

1. Target the endpoints on which you want to uninstall a tool.
2. Click **Deploy Action**.
3. (Windows) Select the **Endpoint Configuration - Uninstall Tool [Windows]** package.
4. (Non-Windows) Select the **Endpoint Configuration - Uninstall Tool [Non-Windows]** package.
5. Select **Block reinstallation** to block the reinstallation of the tool. If unset, the tool will be installed on the endpoint the next time the Endpoint Configuration tools installation is performed.
6. Select **Soft uninstall** to perform a soft uninstall, leaving some content in place; for example, logs and data. Clear the selection to perform a hard uninstall, removing everything tracked by the tool.
7. Select **Remove unreferenced dependencies** to remove any additional unreferenced tools that were a dependency of the tool being removed.

Reinstall one or more tools installed by Endpoint Configuration

To reinstall one or more tools on an endpoint that was installed by Endpoint Configuration, distribute the **Endpoint Configuration - Reinstall Tool** package. The most recent version of the targeted tooling is installed.

1. Target the endpoints on which you want to reinstall a tool.
2. Click **Deploy Action**.
3. (Windows) Select the **Endpoint Configuration - Reinstall Tool [Windows]** package.
4. (Non-Windows) Select the **Endpoint Configuration - Reinstall Tool [Non-Windows]** package.
5. Choose a tool from the dropdown, or provide a manual tool name.
6. Select **Reinstall Dependencies** to reinstall any dependencies of the tool being installed.
7. Select **Unblock Tool** to unblock reinstallation if it was previously blocked.

Each Tanium solution features a **ToolName -- Tools Cache [1]** package. These packages define how all the files that an endpoint downloads are loaded into the Tanium Server cache. These packages should never be manually deployed to endpoints.

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.

Global Endpoint Configuration settings

Setting	Default value	Description
Enable configuration approval	Unselected	Determines whether to require approvals for configuration changes. For more information, see Managing approvals on page 21.
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.
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.
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.

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.