



Tanium™ Endpoint Configuration User Guide

Version 1.3.276

December 22, 2020

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 to make interaction with Tanium software more intuitive and to accelerate the time to success. To ensure high accessibility standards, Tanium complies with the U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. We have conducted third-party accessibility assessments over the course of product development for many years, and most recently a comprehensive audit against the WCAG 2.1 / VPAT 2.3 standards for all major product modules was completed in September 2019. 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.

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

© 2020 Tanium Inc. All rights reserved.

Table of contents

- Endpoint Configuration overview 6**
 - Configurations 6
 - Approvals 7
- Getting started with Endpoint Configuration 7**
 - Step 1: Install and configure Endpoint Configuration 7
 - Step 2: Manage configurations 7
 - Step 3: Manage approvals 7
- Endpoint Configuration requirements 8**
 - Tanium dependencies 8
 - Tanium™ Module Server 8
 - Endpoints 9
 - Supported operating systems 9
 - Host and network security requirements 10
 - Security exclusions 10
 - User role requirements 10
- Installing Endpoint Configuration 15**
 - Before you begin 15
 - Import and configure Endpoint Configuration with default settings 15
 - Import and configure Endpoint Configuration with custom settings 16
 - Configure service account 16
 - Configure Endpoint Configuration action group 16
 - Verify Endpoint Configuration version 17
 - Troubleshoot problems 17

Managing configurations	18
Managing approvals	19
Enable configuration approvals	19
Approve or reject configuration changes	19
Troubleshooting Endpoint Configuration	21
Collect logs	21
Block or unblock tools from installing on an endpoint	21
Block the installation of a tool	21
Unblock the installation a tool	21
Uninstall one or more tools installed by Endpoint Configuration.	22
Reinstall one or more tools installed by Endpoint Configuration.	22
Uninstall Endpoint Configuration	23
Contact Tanium Support	23
Reference: Endpoint Configuration settings	24
Global Endpoint Configuration settings	24
Tools install settings	25

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.

Configure Solution Components
Modify configurations within Tanium solutions.



Review
Approvers accept or reject proposed changes.



Approvals take Effect
Approved configurations are deployed immediately.



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.

Getting started with Endpoint Configuration

Step 1: Install and configure Endpoint Configuration

Endpoint Configuration is installed as part of Tanium™ Client Management. Use the **Tanium Solutions** page to install Client Management and choose either automatic or manual configuration.

For more information, see [Installing Endpoint Configuration](#).

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 pending 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

Review the requirements before you install and use Endpoint Configuration.

Tanium dependencies

In addition to a license for Endpoint Configuration, make sure that your environment meets the following requirements.

Component	Requirement
Tanium™ Core Platform	7.3.314.4250 or later
Tanium™ Client	<p>Any supported version of Tanium Client. For the Tanium Client versions supported for each OS, see Tanium Client User Guide: Client version and host system requirements.</p> <p>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.</p> <p>Some Tanium solutions that manage the deployment of configuration changes with Tanium Endpoint Configuration might require a higher client version.</p>
Tanium products	<p>If you selected Install with Recommended Configurations when you installed Client Management, the Tanium Server automatically installed all your licensed modules at the same time. Otherwise, you must manually install the modules with which you are using Endpoint Configuration, as described under Tanium Console User Guide: Manage Tanium modules.</p>
Computer groups	<p>When you first log into the Tanium Console after a fresh installation of Tanium Server 7.4.2 or later, the server automatically imports the computer groups that Endpoint Configuration requires.</p> <p>For earlier versions of the Tanium Server, or after upgrading from an earlier version, you must manually create the computer groups: see Create computer groups.</p>

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 User Guide: Host system requirements .	
Linux	Same as Tanium Client support. See Tanium Client User Guide: Host system requirements .	
AIX	A minimum of AIX 7.1.4 is required.	The IBM XL C++ runtime libraries file set (<code>xlc.rte</code>), version 16.1.0.0 or later, and the IBM LLVM runtime libraries file set (<code>libc++.rte</code>) must be installed. For installation instructions, see Tanium Client User Guide: Deploying the Tanium Client to AIX endpoints .
Solaris	Same as Tanium Client support. See Tanium Client User Guide: Host system requirements .	

For Tanium Client operating system support, see [Tanium Client User Guide: 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

Security exclusions

If security software is in use in the environment to monitor and block unknown host system processes, your security administrator must create exclusions to allow the Tanium processes to run without interference. For a list of all security exclusions to define across Tanium, see [Tanium Core Platform Deployment Reference Guide: Host system security exclusions](#).

Table 1: Endpoint Configuration security exclusions

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

User role requirements

The following tables list the role permissions required to use Endpoint Configuration. 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.

Table 2: Endpoint Configuration user role permissions

Permission	Endpoint Configuration Administrator	Endpoint Configuration Service Account
Show Endpoint Configuration Allows the user to see the Endpoint Configuration workbench	✓	✗
Show Endpointconfiguration Allows the user to see the Endpoint Configuration workbench	✓	✗
Endpoint Configuration Service Account Write Allows users to write the service account for Endpoint Configuration	✓	✗
Endpoint Configuration Module Use	✓	✗
Endpoint Configuration Read Allows users to read endpoint configurations	✓	✗
Endpoint Configuration Service Account Read Allows users to write the service account for Endpoint Configuration	✓	✗
Endpoint Configuration Use API Perform Endpoint Configuration operations using the API	✓	✗

Permission	Endpoint Configuration Administrator	Endpoint Configuration Service Account
<p>Endpoint Configuration Module Register</p> <p>Provides the Endpoint Configuration service account permission to register Tanium solutions with Endpoint Configuration</p>	✘	✔
<p>Endpoint Configuration Service Account</p> <p>Allows service account credentials to the user</p>	✘	✔
<p>Endpoint Configuration Reject</p> <p>Allows the user to reject configuration changes in Endpoint Configuration</p>	1	1
<p>Endpoint Configuration Dismiss</p> <p>Allows the user to dismiss configuration changes in Endpoint Configuration</p>	1	1
<p>Endpoint Configuration Write</p> <p>Allows the user to write configuration changes in Endpoint Configuration</p>	1	1
<p>Endpoint Configuration Approve</p> <p>Allows the user to approve configuration changes in Endpoint Configuration</p>	1	1

Permission	Endpoint Configuration Administrator	Endpoint Configuration Service Account
<p>Endpoint Configuration Bypass Approval</p> <p>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.</p> <p>You can apply this permission to a user account, and based on the content set, it bypasses approval for user-generated configuration items.</p>	2	2
<p>¹ This permission is provided to a solution specific role for managing configuration approvals.</p> <p>² This permission is not provided by default to any roles.</p>		

Table 3: Provided Endpoint Configuration Micro Admin and Advanced user role permissions

Permission	Role Type	Content Set for Permission	Endpoint Configuration Administrator	Endpoint Configuration Service Account
Read Computer Group	Micro Admin		✘	✔
Read Filter Group	Micro Admin		✘	✔
Read Action Group	Micro Admin		✘	✔
Read Action	Advanced	Endpoint Configuration	✘	✔
Execute Plugin	Advanced	Endpoint Configuration	✔	✔

Permission	Role Type	Content Set for Permission	Endpoint Configuration Administrator	Endpoint Configuration Service Account
Read Plugin	Advanced	Endpoint Configuration	✓	✓
Write Action	Advanced	Endpoint Configuration	✗	✓
Write Package	Advanced	Endpoint Configuration	✗	✓
Read Own Action	Advanced	Endpoint Configuration	✗	✓
Read Package	Advanced	Endpoint Configuration	✗	✓
Show Preview	Advanced	Endpoint Configuration	✗	✓
Read Plugin	Advanced	Endpoint Configuration	✗	✓

Installing 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](#).

Use the **Tanium Solutions** page to install Endpoint Configuration and choose either automatic or manual configuration:

- **Automatic configuration with default settings** (Tanium Core Platform 7.4.2 or later only): Endpoint Configuration is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information about the automatic configuration for Endpoint Configuration, see [Import and configure Endpoint Configuration with default settings on page 15](#).
- **Manual configuration with custom settings:** After installing Endpoint Configuration, you must manually configure required settings. Select this option only if Endpoint Configuration requires settings that differ from the recommended default settings. For more information, see [Import and configure Endpoint Configuration with custom settings on page 16](#).

Before you begin

- Read the [release notes](#).
- Review the [Endpoint Configuration requirements on page 8](#).
- Assign the correct roles to users for Endpoint Configuration. Review the [User role requirements on page 10](#).
 - To import the Endpoint Configuration solution, you must be assigned the Administrator reserved role.
 - To configure the ProductName action group, you must be assigned the Content Administrator reserved role.

Import and configure Endpoint Configuration with default settings

To import Endpoint Configuration and configure default settings, be sure to select the **Apply Tanium recommended configurations** check box while performing the steps in

[Tanium Console User Guide: Manage Tanium modules](#). After the import, verify that the correct version is installed: see [Verify Endpoint Configuration version on page 17](#).

Import and configure Endpoint Configuration with custom settings

To import Endpoint Configuration without automatically configuring default settings, be sure to clear the **Apply Tanium recommended configurations** check box while performing the steps in [Tanium Console User Guide: Manage Tanium modules](#). After the import, verify that the correct version is installed: see [Verify Endpoint Configuration version on page 17](#).


Configure service account

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

- **Tanium Administrator** or **Endpoint Configuration Service Account** role

IMPORTANT: If action approval is enabled for Tanium Core Platform, you must either use the **Endpoint Configuration Service Account** role 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 10](#).


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 Endpoint Configuration action group

1. From the Main menu, click **Administration > Actions > Scheduled Actions**.
2. From the list of action groups, click **Endpoint Configuration**.
3. Click **Edit**, select computer groups to include in the action group, and click **Save**.

Verify Endpoint Configuration version

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

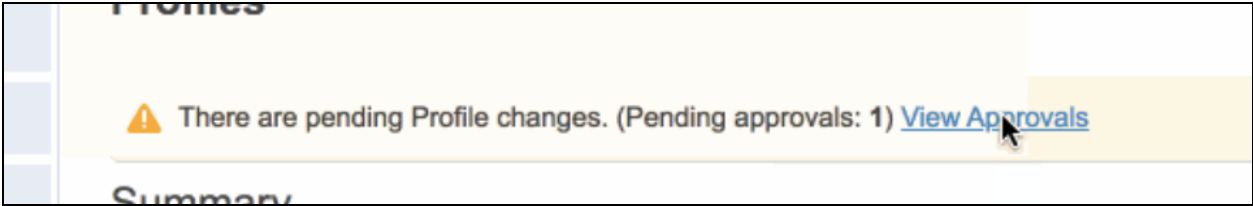
1. Refresh your browser.
2. From the Main menu, go to **Administration > Shared Services > Endpoint Configuration** to open the Endpoint Configuration **Overview** page.
3. To display version information, click Info .

Troubleshoot problems

If you experience problems with installing Endpoint Configuration, see [Troubleshooting Endpoint Configuration on page 21](#).

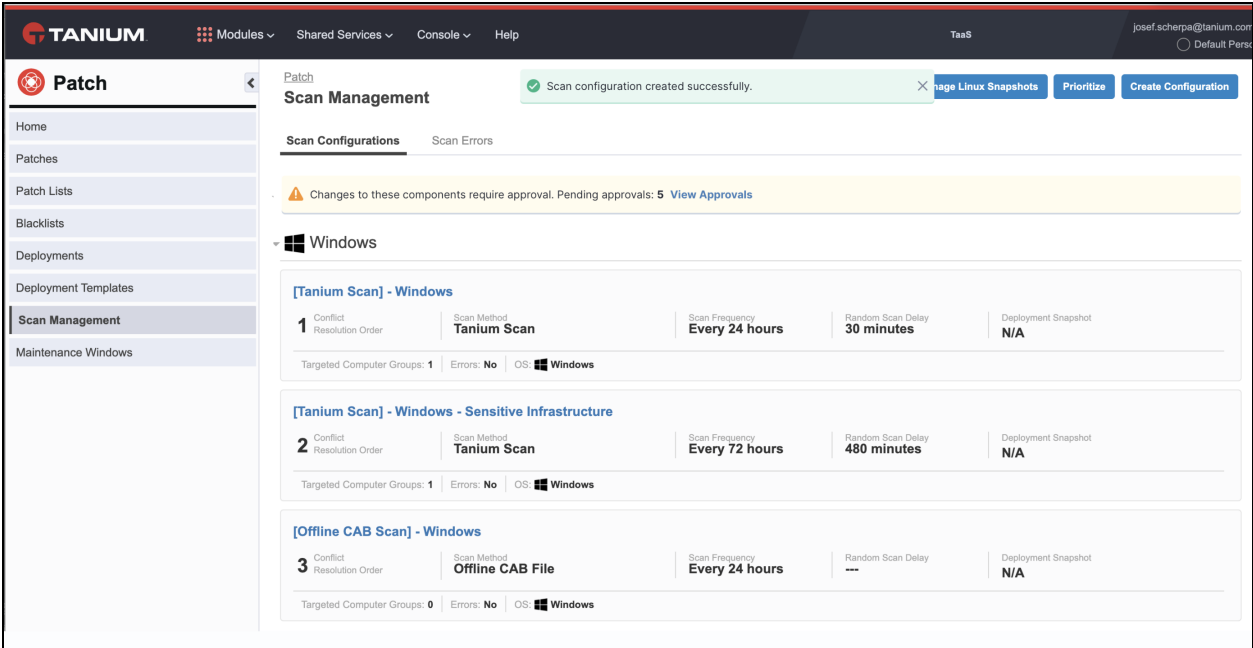
Managing configurations

Configurations are defined in each Tanium solution. If configuration approval is enabled, a banner appears in the solution to alert the user that configuration changes are pending approval in Endpoint Configuration when a user creates or changes a configuration. For example, if a Threat Response profile is changed, a banner appears to alert the user that a configuration change has been made and requires approval in Endpoint Configuration before it can be deployed to endpoints.



When you create or change a configuration, the configuration appears in Endpoint Configuration in the pending 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 **Pending**. The data in these configurations is not deployed to the targeted endpoints until they have been approved.



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.

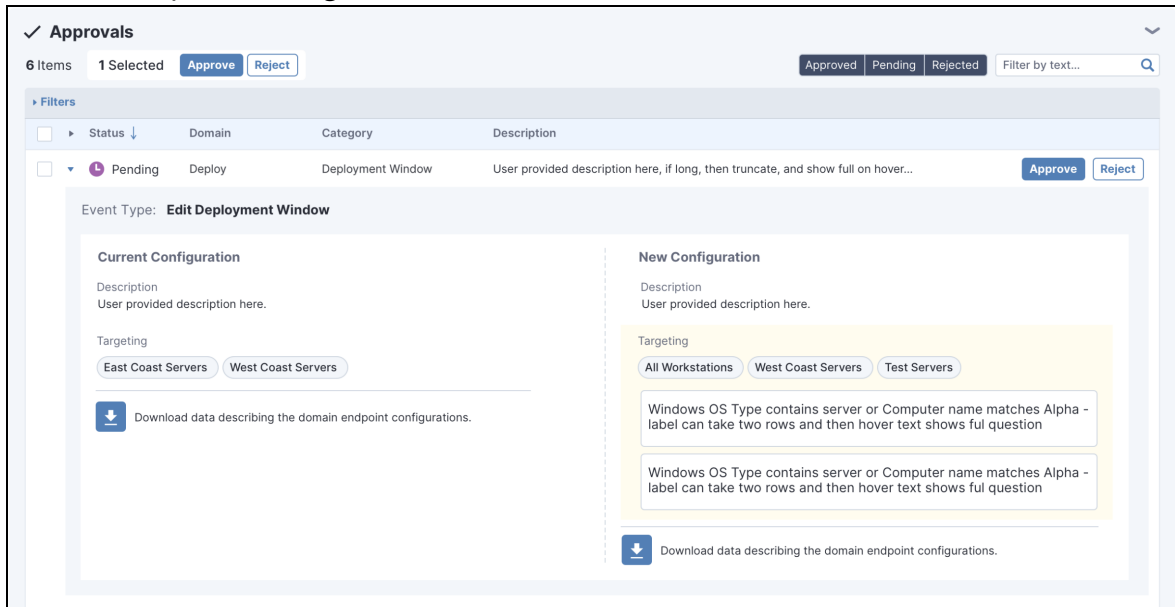
Note: You can bypass configuration approvals for solution or user-generated configuration changes by applying the **Endpoint Configuration Bypass Approval** permission to a service or user role that is associated with one or more content sets to limit the scope of approvals.

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 **Approvals**.



2. Review configurations that are awaiting approval or rejection, which display a status of **Pending**. 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.

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 Client Management home page, click Help , then the **Troubleshooting** tab.
2. Click **Download Debug Package**.
A `tanium-client-management-support.zip` file downloads to the local download directory.
3. Attach the ZIP file to your Tanium Support case form or send it to your Technical Account Manager (TAM).

Tanium Client Management maintains logging information in the `client-management.log` file in the `\Program Files\Tanium\Tanium Module Server\services\client-management-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 block 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. Set the **Block reinstallation** parameter 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. Set the **Soft uninstall** parameter to perform a soft uninstall, leaving some content in place; for example, logs and data. Uncheck to perform a hard uninstall, removing everything tracked by the tool.
7. Set the **Remove unreferenced dependencies** parameter 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.

Note: Before you attempt to reinstall a tool, ensure that the tool is not blocked on the endpoint.

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. Set Reinstall Dependencies to reinstall any dependencies of the tool being installed.

Note: 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


IMPORTANT: Uninstalling Endpoint Configuration impacts all Tanium solutions. Contact Tanium support before you uninstall Endpoint Configuration.

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

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, go to Settings  and click **Settings**.

IMPORTANT: Consult with your Technical Account Manager (TAM) before you edit any settings in Endpoint Configuration.

Global Endpoint Configuration settings

Setting	Default value	Description
Enable configuration approval	Unselected	Toggles configuration approval with Endpoint Configuration.
Manifest job quiet period seconds	30 seconds	The amount of time to wait (in seconds) to run the manifest job after receiving a configuration update.
Manifest job retry seconds	60 seconds	The amount of time to wait (in seconds) to retry a failed manifest job.
Manifest action distribute seconds	60 seconds	The time (in seconds) over which to distribute the manifest distribution action.
Manifest action duration seconds	3600 seconds	The duration of time (in seconds) that the manifest action that configures both expiration and issue can run.
Manifest action weight package sections	600 seconds	The duration of time to wait for the manifest package to cache files before deploying the action.
Tools package job seconds	60 seconds	The frequency (in intervals of seconds) of the tools package manager job.
Deploy client configuration and support action distribute seconds	60 seconds	The distribute over time value for the client configuration and support distribution action.
Auditing retention days	90 days	The number of days to retain audit logs.
Auditing cleanup interval minutes	240 minutes	The number of minutes between checks to clean up audit logs.

Tools install settings

Setting	Default value	Description
Distribute over time (seconds)	0 seconds	Endpoint Configuration randomizes tools deployments over an interval to prevent excessive resource consumption. Changing the value of distribute over time changes the length of that window.