

Tanium™ Jump Gate User Guide

Autonomous IT. Unstoppable Business.

2026H1 Semiannual Release

Version 1.8

June 08, 2026

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

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

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

This documentation may provide access to or information about content, products (including hardware and software), and 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. We certify against the WCAG 2.2 / VPAT 2.5 standards for all major product modules. Tanium performs ongoing reassessments as appropriate, given the scope and type of changes to the UI and product features from release to release. In the most recent testing, the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.2 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

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

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

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

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

© 2026 Tanium Inc. All Rights Reserved

© 2026 Tanium Inc. All rights reserved.

Table of contents

Jump Gate overview **7**

Secure, just-in-time access 7

Monitoring and auditing of user activity 7

Interoperability with other Tanium products 7

Tanium™ Guide 7

Tanium™ Integrations Gallery 7

Tanium™ Reporting 7

Jump Gate requirements **9**

Core platform dependencies 9

Solution dependencies 9

Tanium recommended installation 9

Import specific solutions 9

Required dependencies 9

Tanium™ Module Server 10

Endpoints 10

Supported Internet protocols 10

Supported operating systems 10

Host and network security requirements 11

Ports 11

Security exclusions 11

Third-party internet URLs 11

User role requirements 11

Configuring Jump Gate **14**

Install and configure Tanium Endpoint Configuration 14

Manage solution configurations with Tanium Endpoint Configuration 14

Configure computer groups and users for Jump Gate 15

Configure the Jump Gate action group 15

© 2026 Tanium Inc. All Rights Reserved

Organize computer groups ... 15
Set up Jump Gate users ... 15
(Optional) Configure third-party integrations for Jump Gate notifications ... 17
Configure Jump Gate module settings and access policies ... 17
Configure Jump Gate module settings ... 17
Configure access policies ... 18
Prioritize access policies ... 20
Jumping to endpoints ... **21**
Make a jump request for an endpoint ... 21
View your own requests ... 22
Jump to an endpoint ... 22
Run a command on an endpoint ... 23
View the command history with command outputs ... 23
Stop a running command ... 24
Manage favorite endpoints ... 24
Add a favorite endpoint ... 24
Remove a favorite endpoint ... 25
Approving jump requests and viewing activity ... **26**
View, approve, and close jump requests ... 26
View pending jump requests ... 26
View details and activity for approved jump requests ... 27
Close approved jump requests ... 27
View and export jump activity ... 27
Export jump activity ... 27
View the details of a jump request and jumps initiated ... 28
View all Jump Gate activity ... 28
Audit record fields ... 28
Audit event types ... 28
Maintaining Jump Gate ... **30**
Perform quarterly maintenance ... 30

© 2026 Tanium Inc. All Rights Reserved

Review access policies 30
Review timeout and data retention policies 30
Troubleshooting Jump Gate **32**
Collect logs 32
Verify endpoint tools 32
Troubleshooting automatically rejected jump requests 32
Troubleshooting disconnected jump sessions 32
Uninstall Jump Gate 33
Contact Tanium Support 33

© 2026 Tanium Inc. All Rights Reserved

Jump Gate overview

With Jump Gate, you can provide secure, controlled just-in-time access to critical systems and data in your environment. Incorporating zero-trust principles, Jump Gate eliminates standing access, enforces least-privilege controls, and provides real-time visibility into user activity in controlled infrastructure.

Secure, just-in-time access

You can grant temporary role-based access to controlled infrastructure endpoints managed by Tanium Client, only when needed. A Jump Gate operator defines the access policies that determine endpoints that users can access, the users who can access those endpoints, and the required approvals. Users can then request to jump to target endpoints. Depending on the access policy that applies, Jump Gate can automatically approve or reject these requests, or a designated user can approve or reject them.

Approved users can access a PowerShell session on a controlled Windows endpoint or a Bash session on a controlled macOS or Linux endpoint. Traffic between the user and the controlled server is encrypted and uses the Tanium™ Protocol.

For more information, see Configure access policies on page 18, Jumping to endpoints on page 21, and View, approve, and close jump requests on page 26.

Monitoring and auditing of user activity

Jump Gate maintains a record of all jump activity, as well as configuration activity. Operators and auditors can review this information, as well as export jump activity for long-term record keeping.

For more information, see View and export jump activity on page 27 and View all Jump Gate activity on page 28.

Interoperability with other Tanium products

Tanium™ Guide

Tanium Guide can generate notifications for Jump Gate users to alert them when there are jump requests to approve or when requests they submitted change in status.

Tanium™ Integrations Gallery

Tanium Integrations Gallery enables you to configure notifications for third-party applications, such as Slack and Microsoft Teams.

Tanium™ Reporting

The Jump Gate **Activity** page uses a chart to visualize data that Tanium Reporting provides through a report. For more information, see Tanium Reporting User Guide: Working with reports.

Jump Gate metrics are based on data that Reporting provides through reports. For more information, see Tanium Reporting User Guide: Working with reports.

© 2026 Tanium Inc. All Rights Reserved

Jump Gate provides access to the Endpoint Details page in Reporting, where you can view comprehensive information about a single endpoint and manage the endpoint. To access the page, see View, approve, and close jump requests on page 26. For more information about endpoint details, see Tanium Reporting User Guide: Working with a single endpoint.

© 2026 Tanium Inc. All Rights Reserved

Jump Gate requirements

Review the requirements before you install and use Jump Gate.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Jump Gate. For more information about how to get Jump Gate, see Tanium Solutions & Bundles.
- Tanium™ Core Platform servers
- Tanium™ Client 7.7.3 or later

Solution dependencies

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

NOTE

Some Jump Gate dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 9 and Jump Gate requirements on page 9. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Jump Gate requires.

Tanium recommended installation

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

Import specific solutions

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

Required dependencies

Jump Gate has the following required dependencies:

© 2026 Tanium Inc. All Rights Reserved

- Tanium™ Automation Engine
- Tanium™ Blob
- Tanium™ Data Service
- Tanium™ Direct Connect
- Tanium™ Guide
- Tanium™ Integrations Gallery
- Tanium™ Interact
- Tanium™ RDB
- Tanium™ Reporting

Tanium™ Module Server

Jump Gate 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.

Endpoints

Supported Internet protocols

Jump Gate supports IPv4 and IPv6 addresses.

Supported operating systems

The following endpoint operating systems are supported with Jump Gate.

Supported operating systems for Tanium Jump Gate

Operating System	Version

Windows	• Windows Server:
	  ◦ Windows Server 2025
	  ◦ Windows Server 2022
	  ◦ Windows Server 2019
	• Windows (workstation):
	  ◦ Windows 11
	  ◦ Windows 10, version 1809 or later

© 2026 Tanium Inc. All Rights Reserved

Supported operating systems for Tanium Jump Gate (continued)

Operating System	Version
macOS	Same as Tanium Client support. For more information, see Tanium Client Management User Guide: Client version and operating system requirements.
Linux	Same as Tanium Client support. For more information, see Tanium Client Management User Guide: Client version and operating system requirements.

Host and network security requirements

Specific processes are needed to run Jump Gate.

Ports

Ports for Tanium Jump Gate communication

Source	Destination	Port	Protocol	Purpose
Module Server	Zone Server[1]	17472	TCP	Module Server communication with Zone Servers for Jump Gate sessions.
[1] This port is required only when you use a Zone Server.				

Security exclusions

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

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`"<Module Server>\services\jump-gate-service\TaniumJumpGateService.exe`

No additional security exclusions are required.

Third-party internet URLs

Jump Gate does not require access to third-party URLs directly. However, you must allow certain URLs when you configure notifications for third-party applications, such as Slack or Microsoft Teams. For more information, see the Tanium Integrations Gallery User Guide.

User role requirements

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

© 2026 Tanium Inc. All Rights Reserved

- Jump Gate solution permissions on page 12
- Jump Gate administration and platform content permissions on page 13: The solution permissions automatically provide some of these permissions.

To review a summary of the predefined roles, see Set up Jump Gate users on page 15.

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

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

Jump Gate solution permissions

Permission	Jump Gate Operator[1,2]	Jump Gate User[1,2]	Jump Gate Auditor[1]
Jump Gate View the Jump Gate workbench	✓ SHOW	✓ SHOW	✓ SHOW
Jump Gate Audits Read Jump Gate audits	✓ READ	✓ READ[3]	✓ READ
Jump Gate My Requests Read your own requests in the Jump Gate module	✓ READ	✓ READ	✗
Jump Gate Policies Access Jump Gate access policies	✓ READ WRITE	✗	✓ READ

© 2026 Tanium Inc. All Rights Reserved

Jump Gate solution permissions (continued)

Permission	Jump Gate Operator[1,2]	Jump Gate User[1,2]	Jump Gate Auditor[1]
Jump Gate Requests Manage jump requests in Jump Gate	✓ READ APPROVE CLOSE	✓ WRITE APPROVE	✓ READ
Jump Gate Settings Access Jump Gate settings	✓ READ WRITE	✓ READ	✓ READ

[1] To view the content sets to which the platform content permissions apply, see Tanium Console User Guide: View effective role permissions.

[2] The permissions for these roles provide solution permissions for other solutions. To view the provided permissions, see Tanium Console User Guide: View effective role permissions.

[3] For the **Jump Gate User** role, the **Jump Gate Audits** permission provides the ability to read only that user's audits.

Jump Gate administration and platform content permissions

Permission	Permission Type	Jump Gate Operator	Jump Gate User	Jump Gate Auditor
Action Group	Administration	✓ READ	✗	✓ READ
User	Administration	✓ READ	✓ READ	✓ READ
User Group	Administration	✓ READ	✗	✓ READ
Filter Group	Platform Content	✓ READ	✗	✓ READ
Plugin	Platform Content	✓ READ	✓ READ	✓ READ
Sensor	Platform Content	✓ READ	✓ READ	✓ READ

To view the content sets to which the platform content permissions apply, see Tanium Console User Guide: View effective role permissions.

© 2026 Tanium Inc. All Rights Reserved

Configuring Jump Gate

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

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

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

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

IMPORTANT

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

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

NOTE

For information about how to install Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Installing Endpoint Configuration.

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Jump Gate, see User role requirements on page 11. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

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

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

Configure computer groups and users for Jump Gate

Configure the Jump Gate action group

Importing the Jump Gate module automatically creates an action group, which targets **All Computers** by default. If you did not use automatic configuration or you enabled restricted targeting when you imported Jump Gate, the action group targets **No Computers**.

If you used automatic configuration and restricted targeting was disabled when you imported Jump Gate, configuring the Jump Gate action group if you want to limit the endpoints that are available to Jump Gate.

Select the computer groups to include in the Jump Gate action group.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Click **Tanium Jump Gate**.
3. Select the computer groups that you want 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.

Organize computer groups

One way to define Jump Gate access policies is by computer group. Create relevant computer groups to organize your endpoints. Some options include:

- Endpoint type, such as servers or employee workstations
- Endpoint location, such as by country or time zone
- Endpoint priority, such as business-critical machines
- Endpoint configuration needs, such as VDI machines

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

Set up Jump Gate users

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

To review specific permissions for each role, see User role requirements on page 11.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

On installation, Jump Gate creates a **Jump Gate** user to automatically manage the Jump Gate service account. Do not edit or delete the **Jump Gate** user.

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

Jump Gate Operator

Assign the **Jump Gate Operator** role to users who manage the configuration of Jump Gate.
This role can perform the following tasks:

- Configure Jump Gate module settings.
- View and modify Jump Gate configurations.
- Dismiss or reject approvals for Jump Gate tasks in Tanium Endpoint Configuration.
- Review and approve jump requests for which the user is a designated approver.
- View live and historical jump sessions.
- View all user and group activity.
- Close any jump request and associated sessions.

Jump Gate User

Assign the **Jump Gate User** role to users who jump to endpoints and approve jump requests for which they are designated approvers.
This role can perform the following tasks:

- Search for endpoints to which they can initiate a jump request.
- Submit jump requests.
- Jump to endpoints when approved.
- View the user's own session history.
- Review and approve jump requests for which the user is a designated approver.

Jump Gate Auditor

Assign the **Jump Gate Auditor** role to users who audit user activity in Jump Gate.
This role can perform the following tasks:

- View session logs and audit data.

NOTE

Do not assign the **Jump Gate Service Account** role to users. This role is for internal purposes only.

© 2026 Tanium Inc. All Rights Reserved

(Optional) Configure third-party integrations for Jump Gate notifications

You can configure third-party integrations for notifications, such as Slack or Microsoft Teams, for which you can later enable notifications in access policies. You configure these integrations in Tanium Integrations Gallery. For more information, see the Tanium Integrations Gallery User Guide.

The initial configuration of Jump Gate provides a shortcut to Integrations Gallery to configure these integrations.

Configure Jump Gate module settings and access policies

Configure Jump Gate module settings

You can configure request timeouts, session timeouts, and the data retention period.

1. From the Main menu, go to **Modules > Jump Gate**.
2. Click Settings.
3. Configure the Jump Gate module settings:

Jump Gate General settings

Setting	Description
Jump Request Expiration	Configure the amount of time after which a jump request expires. The time begins when a user submits a request and includes the time before the request is approved. After a request is approved, the requester can initiate unlimited new jump sessions before the approved request expires. After the request expires, the requester must submit a new request and receive new approval as applicable to open new session.
Maximum Request Scheduling Time	Configure the maximum amount of time in the future that a user can schedule a request.
Session Inactivity	Configure the amount of time after which a user is disconnected from a jump session when the user has not performed any actions.

© 2026 Tanium Inc. All Rights Reserved

Jump Gate General settings (continued)

Setting	Description
Maximum Session Time	Configure the amount of time after which a user is disconnected from a jump session even if the user is active. NOTE • Jump sessions can be interrupted by Tanium Client resets, which typically occur every two to six hours and might occur before the configured maximum session time. For more information, see Troubleshooting disconnected jump sessions on page 32. • If the associated jump request expires during an active jump session, that session disconnects, even if it has not reached the maximum session time.
Maximum Command Time	Configure the amount of time that an asynchronous command issued by a user can run on an endpoint before it terminates.
Data Retention	Configure the amount of time to maintain records of Jump Gate activity.

4. Click **Save**.

Configure access policies

Configure access policies to determine which users can make jump requests for certain endpoints. Access policies also determine whether jump requests require approval and who can approve requests.

TIP

Jump Gate includes a preconfigured access policy to help you get started quickly. The default configuration of this policy depends on whether you had restricted targeting enabled when you imported Jump Gate:

- **Restricted targeting disabled (default):** The initial configuration of Jump Gate includes the **Jump Gate Default Policy: Automatically approve all requests** policy. By default, this policy automatically approves all jump requests, made by all users, to all endpoints. You can modify this policy to restrict endpoints or users, or to add approvers.
- **Restricted targeting enabled:** The initial configuration of Jump Gate includes the **Jump Gate Sample Policy: Automatically approve requests (no targeted endpoints)** policy. This policy is structured to automatically approve all jump requests made by all users, but with no targeted endpoints because restricted targeting is enabled. You can modify this policy to include endpoints, to restrict users, or to add approvers. This policy does not approve jump requests until you modify it to target endpoints.

For more information about restricted targeting, see Tanium Console User Guide: Tools deployment.

© 2026 Tanium Inc. All Rights Reserved

IMPORTANT

You must have access policies for all valid jump requests. Jump Gate automatically rejects any jump requests where the user and targeted endpoint do not match an existing access policy.

NOTE

The computer management groups assigned to a user or an alternative persona can restrict the endpoints available to a user who is designated in an access policy. For example, consider an access policy that applies to all users and includes all endpoints, and a user who is using an alternative persona that restricts that user to a computer group that does not include "Endpoint A." While using that persona, the user cannot see "Endpoint A" or create a jump request for that endpoint, even though the access policy includes that endpoint. For more information about assigning computer management groups, see Tanium Console User Guide: Manage computer group assignments for a user. For more information about personas, see Tanium Console User Guide: Managing personas.

1. From the Main menu, go to **Modules > Jump Gate > Access Policies**, and do one of the following:
   a. Click **Add Policy** to create a new policy.
   b. Click Duplicate Policy beside an existing policy to create a new policy starting with the same settings as the existing policy.
   c. Click Edit Policy beside an existing policy to modify that policy.
2. Enter a **Name** and **Description** and click **Next**.
3. Select users and user groups to which the policy applies:
   - To add individual users to the policy, click **User**, select the users, and click **Select**.
   - To add user groups to the policy, click **User Group**, select the user groups, and click **Select**.

   TIP

   If you want to automatically approve all jump requests for certain endpoints, you must create a user group that contains all Jump Gate users and prioritize that policy before any other policies that apply to the same endpoints. For more information, see Prioritize access policies on page 20.
4. Click **Next**.
5. Enter Tanium question filters to determine the endpoints to be governed by the policy. For example, to target endpoints in the `192.168.1.0/24` subnet, you can type `Tanium Client IP Address starts with 192.168.1` in the **Filter Bar** or use the **Filter Builder** to select the **Tanium Client IP Address** sensor, and then apply the same filter.

   TIP

   You can copy the criteria from a filter used for a computer group using the **Filter Builder** tab. Click **Add Row**, select **Computer Group** and then select a computer group name.
6. Click **Next**.

© 2026 Tanium Inc. All Rights Reserved

7. If you want to require approval when one of the specified requesters makes a jump request to one of the targeted endpoints, enable **Require Approval** and select approvers:
    - To add individual users to the policy, click **User**, select the users, and click **Select**.
    - To add user groups to the policy, click **User Group**, select the user groups, and click **Select**.

    NOTE

    - Only one of the selected approvers is required to approve each jump request.
    - Even if a user is configured as both a requester and an approver by the applicable access policy, a user cannot approve that user's own request. In cases where a user does not require approval from another individual for access, you can configure an access policy with **Require Approval** disabled. Jump Gate automatically approves requests where such a policy applies.

8. (Optional) To enable external notifications for Jump Gate to send to each user or user group for a jump request., select **Enabled** in the **External Notifications** section, and select a configured external notification type.

    TIP

    - To configure notification types for third-party applications, such as Slack or Microsoft Teams, see the Tanium Integrations Gallery User Guide.
    - Tanium Guide always provides Jump Gate notifications regardless of the configuration here.

9. Click **Next**, review the policy criteria, and click **Create**.

Prioritize access policies

Jump Gate applies access policies in the order that they appear in the list. If the requester and endpoint in a jump request match more than one configured access policy, the matching policy that appears first in the list determines whether the request requires approval and who can approve the request.

1. From the Main menu, go to **Modules > Jump Gate > Access Policies** and click **Prioritize**.
2. Drag policies into the order you want to prioritize them, or click Move to Position in the row for a policy you want to reorder, enter the new position, and click **Move**. After you reorder the policies, click **Save**.

TIP

If you want to automatically approve jump requests from certain users to certain endpoints, prioritize the policy before any other policies that apply to the same users and endpoints.

© 2026 Tanium Inc. All Rights Reserved

Jumping to endpoints

You can jump to an endpoint to access a PowerShell session on a Windows endpoint or a Bash session on a macOS or Linux endpoint, or you can run a PowerShell or Bash command on the endpoint asynchronously without opening a jump session. Before you initiate a jump or run a command on an endpoint, you must make a jump request for that endpoint. After a designated user approves the request or Jump Gate automatically approves the request, and, if the request is scheduled, you have reached the start time for the request, you can open a jump session or run a command. You can open multiple jump sessions and run multiple commands for the approved request within the time window specified by the Jump Request Expiration that is configured for Jump Gate.

Make a jump request for an endpoint

Before you open a jump session or run a command on an endpoint, you must create a request, which can be approved or rejected. Depending on the access policy that applies, a user might be required to approve the request, or Jump Gate might automatically approve or reject the request. If no one approves a request that requires approval, the request expires after the expiration time configured by an operator. For more information, see Configure access policies on page 18.

1. From the Main menu, go to **Modules > Jump Gate**.
2. Use one of the following methods to select an endpoint:
   - To select a favorite endpoints, go to **My Endpoints** and click a tile for an endpoint.
   - To select any available endpoint:
     a. Go to **Overview** and in the **Search for Endpoints** box, enter all or part of the name of an endpoint to which you want to jump.
     b. In the results that appear, click the name of the endpoint.

   You can also search for endpoints and initiate a jump request from the Quick Search bar in the Tanium Console header or on the Home page.
3. Enter a **Justification** for the request.
4. (Optional) To schedule the request for a future time, enable **Scheduling** and configure a **Request Start Time**.
   If you schedule the request, an approver can approve it any time after you submit it, but you cannot open jump sessions or run commands until the scheduled time. If the request is approved before the start time, it will be active starting at the scheduled time and ending after the time specified by the Jump Request Expiration that is configured for Jump Gate has elapsed since the start time.
5. Click **Submit**.
   The **Request Details** page appears, which includes the approval status. For an approved request, you can initiate a jump or run a command from this page.

© 2026 Tanium Inc. All Rights Reserved

View your own requests

The **My Requests** page displays your requests, with tabs available for each phase of the request.

1. From the Main menu, go to **Modules > Jump Gate > My Requests**.
2. Select a tab to view **Open**, **Scheduled**, or **Closed** requests:
    - The **Open** tab displays non-scheduled requests and scheduled requests for which the scheduled start time has occurred. A request on this tab can have a **Status** of **Pending** if it has not yet been approved or **Approved** if it has been approved and is available to initiate jump sessions and run commands.
    - The **Scheduled** tab displays scheduled requests for which the scheduled start time has not yet occurred. A request on this tab can have a **Status** of **Pending** if it has not yet been approved, or **Approved** if it has been approved and will be available to initiate jump sessions and run commands at the scheduled start time. A request moves to the **Open** tab at its scheduled start time.
    - The **Closed** tab displays closed requests. A request on this tab can have a status of **Rejected** if an approver rejected it, or **Closed** if it reached its expiration time or an approver closed it before the expiration.

- Tanium Guide provides notifications when the status of your request changes. Depending on the access policy that applies, you might also receive notifications in a third-party application, such as Slack or Microsoft Teams.
- You can re-create a closed request to quickly request access to the same endpoint. On the request details page for the closed request, click **Recreate Request**. Enter a **Justification** and optionally configure **Scheduling** just as when creating a new request.



Even if you are designated as an approver by the applicable access policy, you cannot approve your own request.

Jump to an endpoint

After a designated user approves the request and, if scheduled, the request is active, you can initiate a jump to an endpoint.

1. From the Main menu, go to **Modules > Jump Gate > My Requests**.
2. If necessary, go to the **Open** tab.
3. Click the name of the endpoint of a request to open the request details and click **Jump**.
   The window for the jump session appears on the **Request Details** page.

© 2026 Tanium Inc. All Rights Reserved

TIP

- Click the endpoint name in the **Target Details** section of the **Request Details** page to access the Endpoint Details page in Tanium Reporting, where you can view comprehensive information about the endpoint and manage the endpoint.
- Tanium Guide provides a notification when a user approves a jump request. You can also click **View request** directly in this notification to open the **Request Details** page.

BEST PRACTICE

Use a method or program to detach any long-running processes from the terminal, such as the `START /B` command on Windows or the `tmux` program for Linux and macOS, so that those processes do not terminate if the session ends unexpectedly. For more information about troubleshooting disconnected sessions, see Troubleshooting disconnected jump sessions on page 32.

Run a command on an endpoint

After a designated user approves the request and, if scheduled, the request is active, you can run a PowerShell command on a Windows endpoint or a Bash command on a macOS or Linux endpoint.

1. From the Main menu, go to **Modules > Jump Gate > My Requests**.
2. Click the name of the endpoint of a request to open the request details and click **Run Command**.
3. Type the command you want to run on the endpoint, and click **Confirm**.

TIP

- Click the endpoint name in the **Target Details** section of the **Request Details** page to access the Endpoint Details page in Tanium Reporting, where you can view comprehensive information about the endpoint and manage the endpoint.
- Tanium Guide provides a notification when a user approves a jump request. You can also click **View request** directly in this notification to open the **Request Details** page.

NOTE

A command can run only for the time configured for the **Maximum Command Time** setting before it terminates. For more information about configuring this setting, see Configure Jump Gate module settings on page 17.

View the command history with command outputs

You can view the history of commands you have run on an endpoint, including the output from each command in the **Command History** section of a request details page.

© 2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules > Jump Gate > My Requests**.
2. Click the name of the endpoint of a request to open the request details.
3. Expand the **Command History** section.
4. (Optional) Expand a command to view its output.

Stop a running command

A command can finish on its own, or it terminates if the time configured for the **Maximum Command Time** setting elapses, but you can manually stop a command in some cases.

1. From the Main menu, go to **Modules > Jump Gate > My Requests**.
2. Click the name of the endpoint of a request to open the request details.
3. Expand the **Command History** section.
4. In the entry for the running command you want to stop, click **Stop Command**.
   Jump Gate attempts to stop the command.



In certain cases, Jump Gate might not be able to interrupt a command, and the command might continue to run after you attempt to stop it.



Stopping a command does not undo work that the command has already completed.

Manage favorite endpoints

You can add endpoints that you frequently access to your favorites on the **My Endpoints** page.

You can also add or remove the endpoint targeted by a request to your favorites by clicking Favorite Endpoint or Unfavorite Endpoint beside the endpoint name in the heading of the **Request Details** page.

Add a favorite endpoint

1. From the Main menu, go to **Modules > Jump Gate > My Endpoints**.
2. In the **Add Target** box, enter all or part of the name of an endpoint that you want to add to your favorite endpointss.
3. In the results that appear, click the name of the endpoint to add it to your favorites.

© 2026 Tanium Inc. All Rights Reserved

Remove a favorite endpoint

1. From the Main menu, go to **Modules > Jump Gate > My Endpoints**.
2. In the entry you want to remove, click **More > Unfavorite**.

© 2026 Tanium Inc. All Rights Reserved

Approving jump requests and viewing activity

You can view jump requests that are pending approval and approve or reject jump requests for which the applicable access policy designates you as an approver. You can also view records of jump session activity, and other Jump Gate activity, such as changes to access policies.

Tanium Guide provides notifications for pending jump requests. Additionally, you can configure notifications for third-party applications, such as Slack or Microsoft Teams, in an access policy. For more information, see Configure access policies on page 18.

View, approve, and close jump requests

You can view jump requests and approve or reject pending jump requests for which the applicable access policy designates you as an approver. A user with the **Jump Request Close** privilege can also close any open jump requests, which also ends any sessions associated with that request.

View pending jump requests

1. From the Main menu, go to **Modules > Jump Gate > My Approvals**.

   TIP

   You can also access a jump request directly from a Tanium Guide notification or, if configured in the applicable access policy, a notification in a third-party application, such as Slack or Microsoft Teams. To view a jump request from a Guide notification:

   a. In the Console header, click Guide to open the Guide panel and click Approvals.

   b. In a notification for a jump request, click Expand to view the notification details.

   c. Click **View Request** to view the details of a request.

2. View details for the request, or approve or reject the request:

   - Click the endpoint name to view the details of a request.

     TIP

     Click the endpoint name in the **Target Details** section of the **Request Details** page to access the Endpoint Details page in Tanium Reporting, where you can view comprehensive information about the endpoint and manage the endpoint.

   - Click **Approve** to approve the request.
   - Click **Reject** to reject the request, and enter a reason for the rejection.

© 2026 Tanium Inc. All Rights Reserved

TIP To approve or reject multiple requests at one time, select the requests from the list, and click **Approve Selected** or **Reject Selected**.

NOTE Even if you are designated as an approver by the applicable access policy, you cannot approve your own request.

View details and activity for approved jump requests

1. From the Main menu, go to **Modules > Jump Gate > My Approvals**.
2. Click the endpoint name to view the details of an approved request.
   You can view the information from the original request, as well as view and export **Terminal Recording** logs for jump sessions and **Command History**, which includes all the asynchronous commands run on the endpoint from jump requests.

Close approved jump requests

1. From the Main menu, go to **Modules > Jump Gate > My Approvals**.
2. Click the endpoint name to view the details of an approved request.
3. To close the request and end any jump sessions associated with the request, click **Close Request**.

TIP To close multiple requests at one time, select the requests from the list on the **My Approvals** page, and click **Close selected open requests**.

View and export jump activity

You can view the number of jump requests over the past seven days, and the details of each jump request from the time specified for the data retention period in the Jump Gate settings.

TIP For information about viewing logs from individual requests, including jump session recordings and asynchronous commands, see View details and activity for approved jump requests on page 27.

From the Main menu, go to **Modules > Jump Gate > Activity**. You can filter requests by **Status** and **Access Type**.

Export jump activity

To export jump activity, click **Export > Export to CSV** or **Export > Copy to clipboard**.

© 2026 Tanium Inc. All Rights Reserved

View the details of a jump request and jumps initiated

1. Click the computer name in the entry for the request.
2. If necessary, click Expand  in the **Status** section of the request to see the detailed status and the jumps initiated from the request.

View all Jump Gate activity

You can view a detailed record of all activity in Jump Gate from the time specified for the data retention period in the Jump Gate settings. This activity includes events related to access policies, jump requests, favorite endpoints, jump sessions, and commands run on endpoints.

From the Main menu, go to **Modules > Jump Gate > Audit**.

To filter the events, expand the **Filters** section, and select an **Event** or **Date Range** by which to filter. You can filter by a specific event name to find all records of that type, or by an entity ID to see all audit activity associated with a particular request, session, or other object.

Audit record fields

Each audit record contains the following fields.

Field	Description
id	Unique ID of the audit record.
created_at	Timestamp of when the event occurred.
created_by	The user who triggered the event. Contains a `user_name` sub-field.
entity_id	The ID of the primary object affected, such as a session, command, request, or policy.
parent_id	The ID of the parent resource, if applicable. For sessions, commands, and approvals, this is the associated request ID.
operation	The category of change: create, update, or delete. For a list of operations, see Audit event types on page 28.
event_name	The specific event that occurred. For a list of event names, see Audit event types on page 28.
new_value	The JSON state of the object after the operation. The structure varies by event type.

Audit event types

Each audit record contains an **Operation** field that categorizes the type of change, and an **Event** field that identifies the specific action. The following tables describe the possible values for each field.

Operations

Operation	Description
create	A new object was created or an action was initiated.
update	An existing object was modified.
delete	An object was removed.

© 2026 Tanium Inc. All Rights Reserved

Event names

Event name	Operation	Description
Favorite targets		
CreateFavoriteTarget	create	A user saved a new favorite target.
DeleteFavoriteTarget	delete	A user removed a saved favorite target.
Policies		
CreatePolicy	create	An operator created an access policy.
UpdatePolicy	update	An operator modified an existing access policy.
DeletePolicy	delete	An operator deleted an access policy.
PrioritizePolicies	update	The policy priority order changed. The `new_value` field contains the full re-ordered policy list.
Requests		
CreateRequest	create	A user submitted a jump request.
UpdateRequest	update	A request state changed, for example after an approval action.
CloseRequest	update	A request was closed manually or expired.
Approvals		
CreateApproval	create	An approver acted on a request (approved or rejected). The `parent_id` field contains the request ID.
Sessions		
CreateSession	create	A jump session started (SSH, RDP, AWS credentials, or AWS console URL).
CloseSession	update	A jump session was closed. The `parent_id` field contains the request ID.
Commands		
CreateCommand	create	A command was dispatched to a target. The `parent_id` field contains the request ID.
CompleteCommand	update	A command finished (success or failure). The `parent_id` field contains the request ID.
StopCommand	create	A user explicitly canceled an in-progress command. The `parent_id` field contains the request ID.
TerminateCommand	update	A command was force-terminated during request teardown. The `parent_id` field contains the request ID.
Settings		
UpdateSetting	create, update, or delete	A Jump Gate configuration setting was created, changed, or deleted. The **Operation** field indicates which action occurred.

© 2026 Tanium Inc. All Rights Reserved

Maintaining Jump Gate

Perform regular maintenance tasks to ensure that you maintain the necessary records for jump activity and that the appropriate restrictions are in place for making jumps. If Jump Gate is not performing as expected, you might need to troubleshoot issues or change settings. For related procedures, see Troubleshooting Jump Gate on page 32

Perform quarterly maintenance

Review access policies

Regularly review the access policies that are in place to determine the available endpoints for jump requests, the users who can jump to those endpoints, and the approvals that are required:

1. From the Main menu, go to **Modules > Jump Gate > Access Policies**.
2. Click Expand  for each policy to view the details as necessary, or click Expand All  in the list header to expand all policies. For information about managing policies, see Configure access policies on page 18.
3. Make sure that policies are arranged in the appropriate priority order. For information about prioritizing policies, see Prioritize access policies on page 20.

Review timeout and data retention policies

Regularly review the timeout and data retention settings that are configured to make sure they align with your organizational guidelines and policies:

1. From the Main menu, go to **Modules > Jump Gate**.
2. Click Settings .
3. Review each setting to make sure it aligns with your organizational guidelines and policies, and make any necessary adjustments:

Jump Gate General settings

Setting	Description
Jump Request Expiration	Configure the amount of time after which a jump request expires. The time begins when a user submits a request and includes the time before the request is approved. After a request is approved, the requester can initiate unlimited new jump sessions before the approved request expires. After the request expires, the requester must submit a new request and receive new approval as applicable to open new session.
Maximum Request Scheduling Time	Configure the maximum amount of time in the future that a user can schedule a request.

© 2026 Tanium Inc. All Rights Reserved

Jump Gate General settings (continued)

Setting	Description
Session Inactivity	Configure the amount of time after which a user is disconnected from a jump session when the user has not performed any actions.
Maximum Session Time	Configure the amount of time after which a user is disconnected from a jump session even if the user is active. NOTE • Jump sessions can be interrupted by Tanium Client resets, which typically occur every two to six hours and might occur before the configured maximum session time. For more information, see Troubleshooting disconnected jump sessions on page 32. • If the associated jump request expires during an active jump session, that session disconnects, even if it has not reached the maximum session time.
Maximum Command Time	Configure the amount of time that an asynchronous command issued by a user can run on an endpoint before it terminates.
Data Retention	Configure the amount of time to maintain records of Jump Gate activity.

4. Click **Save**.

© 2026 Tanium Inc. All Rights Reserved

Troubleshooting Jump Gate

If Jump Gate is not performing as expected, you might need to troubleshoot issues or change settings.

Collect logs

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

1. From the Main menu, go to **Modules > Jump Gate** to open the Jump Gate **Overview** page.
2. Click Help  and then click the **Troubleshooting** tab if needed.
3. Click **Collect**.
   A `productname-support.[timestamp].zip` file downloads to the local download directory.
4. Contact Tanium Support to determine the best option to send the ZIP file. For more information, see Contact Tanium Support on page 33.

Verify endpoint tools

If you are experiencing issues such as a feature not working on an endpoint or seeing incorrect data in the workbench, confirm that your endpoints have the latest toolset version. For more information, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or Client Extensions.

Troubleshooting automatically rejected jump requests

If Jump Gate immediately rejects a jump request without intervention from an approver, the reason is often that a Jump Gate operator has not configured an access policy that designates you as a requester for the endpoint. When this occurs, the **Finding Policy** step in the **Status** section of the **Request Details** page indicates `Not Found`.

To jump to the targeted endpoint, you must have a Jump Gate operator create an access policy that includes you as a requester and the requested endpoint as a target. For more information, see Configure access policies on page 18.

Troubleshooting disconnected jump sessions

If a jump session unexpectedly disconnects, it might be for one of the following reasons:

- **The session reached the maximum time allowed:** If you reach the maximum session time configured for Jump Gate, the jump session ends. You can start a new jump session as long as the associated jump request has not expired.
- **The associated jump request expired, or an operator closed it:** If the associated jump request expires or an operator closes the request during an active jump session, that session ends, even if it has not reached the maximum session time. You cannot start a new jump session until you submit a new request and it receives any necessary approvals.

© 2026 Tanium Inc. All Rights Reserved

- **The endpoint is offline or the connection was interrupted:** If the endpoint shuts down or otherwise disconnects from the network, your jump session ends. You can initiate a new jump session when the endpoint is back online, as long as the associated jump request has not expired.
- **The Tanium Client reset on the endpoint:** The Tanium Client must reset to re-initialize registration with the Tanium Server at a randomized interval, which is typically two to six hours. This reset ends an active jump session, but you can initiate a new jump session immediately after the reset is complete, as long as the associated jump request has not expired. For more information about Client registration and resets, see Tanium Client Management User Guide: Registration.

Until the applicable request expires, you can initiate unlimited new sessions with an available endpoint without additional approval. When you initiate a new session, the timer restarts for the maximum session time allowed. For more information about configuring jump request expiration and maximum session time, see Configure Jump Gate module settings on page 17.



Use a method or program to detach any long-running processes from the terminal, such as the `START /B` command on Windows or the `tmux` program for Linux and macOS, so that those processes do not terminate if the session ends unexpectedly.

Uninstall Jump Gate



Consult with Tanium Support before you uninstall or reinstall Jump Gate.

1. Sign in to Tanium Console as a user with the Administrator role.
2. From the Main menu, go to **Administration > Configuration > Solutions**.
3. Under **Jump Gate**, click **Uninstall**.
4. Review the summary and click **Uninstall**.
5. When prompted to confirm, enter your password.

Contact Tanium Support

To contact Tanium Support for help, sign in to the Tanium Customer Community.

For more information about how to submit a support case, see Case Submission Form.

© 2026 Tanium Inc. All Rights Reserved