Tanium Jump Gate User Guide

2026H2 Semiannual Release

Version 1.28

November 19, 2026



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

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

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

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

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

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

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

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

©2026 Tanium Inc. All Rights Reserved

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

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

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

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

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

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

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

© 2026 Tanium Inc. All rights reserved.

Table of contents

Overview 7
- Secure, just-in-time access 7
- Monitoring and auditing of user activity 7
- Tanium Autonomous IT Platform in Jump Gate 8
- Interoperability with other Tanium products 8

Requirements 9
- Core platform dependencies 9
- Solution dependencies 9
  - Tanium recommended installation 9
  - Import specific solutions 10
  - Required dependencies 10
- Tanium™ Module Server 10
- Endpoints 11
  - Supported Internet protocols 11
  - Supported operating systems 11
- Host and network security requirements 12
  - Ports 12
    - Ports for Jump Gate communication 12
  - Security exclusions 12
    - Jump Gate server exclusions 12
  - Third-party internet URLs 13
- User role requirements 13

Configuring 16
- Install and configure Tanium Endpoint Configuration 16
  - Manage solution configurations with Tanium Endpoint Configuration 16
- Configure computer groups and users for Jump Gate 18
  - Configure the Jump Gate action group 18
  - Organize computer groups 18

©2026 Tanium Inc. All Rights Reserved

Set up Jump Gate users 19
(Optional) Configure third-party integrations for Jump Gate notifications 20
Configure Jump Gate module settings and access policies 21
Configure Jump Gate module settings 21
(Optional) End idle Windows sessions on endpoints 24
Configure access policies 25
Prioritize access policies 31
Content set scoping for access policies and activity 31
Enable and configure Remote Desktop on endpoints where you will use RDP-based jump sessions 32
Select a language 33
Select a language 33

Jumping to endpoints 35
Make a jump request for an endpoint 35
View your own requests 36
Jump to an endpoint 37
Start an RDP session (Windows endpoints only) 38
Start a CLI session 40
Run a command on an endpoint 41
View the command history with command outputs 42
Stop a running command 42
Jump Gate CLI 43
Manage favorite endpoints 43
Add a favorite endpoint 44
Remove a favorite endpoint 44

Approving jump requests and viewing activity 45
View, approve, and close jump requests 45
View pending jump requests 45
View details and activity for approved jump requests 46
View session recordings and command history 46
View request history 47
Close approved jump requests 48
View and export jump activity 48
Export jump activity 49

©2026 Tanium Inc. All Rights Reserved

View the details of a jump request and jumps initiated 49
View all Jump Gate activity 49
Audit record fields 49
Audit event types 50

Maintaining 53
Perform quarterly maintenance 53
Review access policies 53
Review timeout and data retention policies 53

Troubleshooting 56
Collect logs 56
Verify endpoint tools 56
Troubleshooting automatically rejected jump requests 56
Troubleshooting RDP sessions that close because RDP is not enabled 57
Troubleshooting disconnected jump sessions 57
Uninstall Jump Gate 58
Contact Tanium Support 59

©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 or RDP session on a controlled Windows endpoint, or a Bash session on a controlled macOS or Linux endpoint. An operator controls which authentication methods each session can use, so that a session can connect with full superuser privileges, with a temporary account that Jump Gate creates and removes for the request, or with credentials that the user supplies. Traffic between the user and the controlled server is encrypted and uses the Tanium™ Protocol.

For more information about the available authentication methods, see Configure Jump Gate module settings on page 21.

> **Note:** RDP sessions are supported only where the Tanium environment runs on TanOS. RDP sessions are not supported if the Tanium environment is installed on Windows-based servers.

For more information, see Configure access policies on page 25, Jumping to endpoints on page 35, and View, approve, and close jump requests on page 45.

Monitoring and auditing of user activity

©2026 Tanium Inc. All Rights Reserved

About this task

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 48 and View all Jump Gate activity on page 49.

Tanium Autonomous IT Platform in Jump Gate

Tanium Autonomous IT Platform comprises a set of interrelated features across multiple Tanium solutions that collect real-time intelligence about conditions in your environment. Tanium Jump Gate provides the following Autonomous IT Platform feature:

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.

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 45. 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

> **Note:** RDP sessions are supported only where the Tanium environment runs on TanOS. RDP sessions are not supported if the Tanium environment is installed on Windows-based servers.

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 in the lists of required and feature-specific dependencies below. Where a dependency links to its own user guide, that link opens the guide for the latest version of the solution, not necessarily the minimum version that Jump Gate requires.

Tanium recommended installation

©2026 Tanium Inc. All Rights Reserved

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:

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

Note: Some Jump Gate dependencies have their own dependencies, which you can see by clicking the links in the list of Required dependencies. 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™ Module Server

©2026 Tanium Inc. All Rights Reserved

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
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 .

©2026 Tanium Inc. All Rights Reserved

Host and network security requirements

Specific ports and processes are needed to run Jump Gate.

Ports

PORTS FOR JUMP GATE COMMUNICATION

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

If antivirus (AV) or other security software is in use in the environment to monitor and block unknown host system processes, Tanium requires that a security administrator create exclusions to allow the Tanium processes to run without interference. This software can include security applications that are included with an endpoint operating system, such as fapolicyd on some Linux distributions, or Microsoft Defender on Windows. The configuration of these exclusions varies depending on the security software.

For more information about security exclusions to define across Tanium, see Reference: Endpoint security exclusions. For Windows-based Tanium Core Platform deployments, see Tanium Core Platform Server security exclusions.

Note: If the required exclusions are not configured, or if Tanium suspects interference from AV or security software, Tanium might require you to remove or disable the AV or security software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.

JUMP GATE SERVER EXCLUSIONS

©2026 Tanium Inc. All Rights Reserved

Jump Gate 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

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:

- solution permissions on page 14
- administration and platform content permissions on page 15: 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 19.

Jump Gate Policies, Jump Gate Requests, and Jump Gate Audits permissions can be scoped to Tanium RBAC content sets. For more information, see Content set scoping for access policies and activity on page 31.

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

©2026 Tanium Inc. All Rights Reserved

- 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
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 View effective role permissions .

[2] The permissions for these roles provide solution permissions for other solutions. To view the provided permissions, see 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.

©2026 Tanium Inc. All Rights Reserved

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 View effective role permissions .

©2026 Tanium Inc. All Rights Reserved

Configuring Jump Gate

About this task

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.

©2026 Tanium Inc. All Rights Reserved

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 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. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Managing approvals.

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

©2026 Tanium Inc. All Rights Reserved

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

About this task

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

About this task

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

©2026 Tanium Inc. All Rights Reserved

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 13.

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 Console User Guide: Manage role assignments for a user.

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

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.

©2026 Tanium Inc. All Rights Reserved

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.

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

About this task

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.

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

©2026 Tanium Inc. All Rights Reserved

Configure Jump Gate module settings and access policies

Configure Jump Gate module settings

About this task

The Jump Gate settings are organized into three tabs: **General** for request timeouts, session timeouts, and the data retention period; **Guide Notification Priority** for the priority of Tanium Guide notifications; and **Access Methods** for the ways that users can authenticate to endpoints.

1. From the Main menu, go to **Modules** > **Jump Gate** to open the **Overview** page.
2. Click Settings .
3. On the **General** tab, 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.
Maximum Concurrent GUI Sessions	Configure the maximum number of GUI-based jump sessions, such as RDP sessions, that can run at the same time in Jump Gate .
Session Inactivity Timeout	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.

©2026 Tanium Inc. All Rights Reserved

Setting	Description
	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 57. • 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. (Optional) On the **Guide Notification Priority** tab, select the priority that Tanium Guide applies to each type of Jump Gate notification. Options are **Low**, **Medium**, and **High**.

Jump Gate Guide notification priority settings

Setting	Description
Awareness Messages	Set the priority of notifications that inform users about Jump Gate activity, such as a jump request that is waiting for approval.
Approval Status Messages	Set the priority of notifications that inform a requester when the approval status of the requester's jump request changes.

Tip: For more information about Guide notifications, see the Tanium Guide User Guide: Viewing and managing notifications.

5. In the table on the **Access Methods** tab, use the switches to toggle whether each access method is **Allowed** or **Not allowed** for each operating system.

©2026 Tanium Inc. All Rights Reserved

Jump Gate access methods

Access method	Description	Supported operating systems
Terminal > Root	Connect to a PowerShell or Bash session as the account that runs the Tanium Client, which has full superuser privileges on the endpoint.	Linux, Windows, macOS
Terminal > Ephemeral user	Connect to a Bash session as a temporary local account that Jump Gate creates for the request and removes when the request closes.	Linux, macOS
GUI > Ephemeral user	Connect to a GUI-based session as a temporary local administrator account that Jump Gate creates for the request and removes when the request closes.	Windows
GUI > Existing credentials	Connect to an RDP session with the user name and password of an account that already exists on the endpoint.	Windows
GUI > OS sign-in screen	Skip the sign-in prompt from Jump Gate and sign in directly to the operating system. Use this access method for endpoints that require multifactor authentication. This access method is available only when Network Level Authentication (NLA) is not required on the endpoint.	Windows

Note: If you disallow every access method for a type of session, the corresponding option remains in the **Jump** menu, but the option is disabled and a message indicates that the access method is disabled by policy or settings. For more information, see Jump to an endpoint on page 37.

6. (Optional) On the **Access Methods** tab, configure the following additional settings:

Jump Gate access method settings

Setting	Description
RDP user groups	Select the local Windows groups to which you want Jump Gate to add the ephemeral user for the duration of an RDP session. You can select from **Administrators**, **Users**, and **Power Users**. The default is **Administrators**.

©2026 Tanium Inc. All Rights Reserved

Setting	Description
	Note: • Jump Gate always adds the ephemeral user to the **Remote Desktop Users** group, regardless of this setting. • For endpoints where you plan to use RDP-based jump sessions, ensure that members of the groups configured in the **RDP user groups** setting can sign in to those endpoints through Remote Desktop Services. For more information, see Enable and configure Remote Desktop on endpoints where you will use RDP-based jump sessions on page 32.
macOS user groups	Add the local macOS groups (for example, `admin` or `staff`) to which you want Jump Gate to add the ephemeral user when a terminal session starts. Type the group name and then click **Add group** or press Enter. **Note:** • The group must already exist on the endpoint. If a group does not exist, Jump Gate starts the session without adding the ephemeral user to that group.
Linux user groups	Add the local Linux groups (for example, `sudo`, `wheel`, or `adm`) to which you want Jump Gate to add the ephemeral user when a terminal session starts. Type the group name and then click **Add group** or press Enter. **Note:** The group must already exist on the endpoint. If a group does not exist, Jump Gate starts the session without adding the ephemeral user to that group.
Enable clipboard copy	Allow users to copy content from RDP sessions to their local computer. When cleared, users cannot copy content out of RDP sessions. Changes to this setting do not affect active sessions.

7. Click **Save**.

(Optional) End idle Windows sessions on endpoints

The **Session Inactivity** setting disconnects a user from a jump session. It does not sign the user out

©2026 Tanium Inc. All Rights Reserved

of Windows on the endpoint. If a user disconnects from an RDP jump session without signing out, the Windows session can remain active on the endpoint until the jump request expires or an operator closes it.

To end Windows sessions that are idle or disconnected before the jump request closes, use the following Remote Desktop Services session time limit settings in Windows:

- **Set time limit for active but idle Remote Desktop Services sessions**: Specify how long a session can be idle before Windows disconnects it.
- **End session when time limits are reached**: Enable this setting so that Windows signs the user out instead of only disconnecting the session when a time limit is reached.
- **Set time limit for disconnected sessions**: Specify how long a disconnected session remains on the endpoint before Windows deletes it.

For more information about these settings, see Microsoft: Policy CSP - ADMX_TerminalServer.

Configure access policies

About this task

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. If your environment uses Tanium RBAC content sets to separate access between departments or teams, you can also assign a policy to a content set to scope its visibility and management to users with access to that content set.

©2026 Tanium Inc. All Rights Reserved

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.

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.

©2026 Tanium Inc. All Rights Reserved

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 a **Content Set** to determine which users can see and manage this policy. The list shows only the content sets for which your role grants **Jump Gate Policies write** permission.

    Tip: If you do not select a content set, Jump Gate assigns the policy to the **Jump Gate** content set. Any user with **Jump Gate Policies read** permission can see the policy.
4. 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 31.

©2026 Tanium Inc. All Rights Reserved

> **Note:** If the policy is assigned to a content set other than the default **Jump Gate** content set, the policy matches only requesting users or groups that also have access to that content set. This applies even when the policy is configured to match all users.

5. Click **Next**.
6. 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.

7. Click **Next**.
8. 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.

   > **Important:** Designated approvers must also have **Jump Gate Requests approve** permission for the policy's content set. Jump Gate rejects an approval action from an approver who lacks access to the policy's content set.

©2026 Tanium Inc. All Rights Reserved

9. (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.

10. Click **Next**.

11. (Optional) On the **Access Method Settings** step, override the global access method settings for this access policy.
    Every cell in the matrix is locked to the global value. Click Unlock in a cell to override the global value, and then click the cell to switch between **Allowed** and **Not allowed**. Click Lock to remove the override and return the cell to the global value.

    Note:

    - Each cell is an independent setting. Unlocking one cell does not override the other operating systems in the same row.
    - For more information about the access methods and the global settings that these settings override, see Configure Jump Gate module settings on page 21.

12. Click **Next**.

13. (Optional) On the **Request Settings** step, override the Jump Gate module settings for this access policy. Click Unlock beside a setting to override the global value, and then configure the setting. Click Lock to remove the override and return the setting to the global value.

    ### Jump Gate request settings

Setting	Description
Jump	Configure the amount of time after which a jump request expires. The time begins when a user submits a

©2026 Tanium Inc. All Rights Reserved

Setting	Description
Request Expiration	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.
Session Inactivity Timeout	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 57. • 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.
RDP user groups	Override the global setting to select the local Windows groups to which Jump Gate adds users for RDP sessions under this policy.
macOS user groups	Override the global setting to select the local macOS groups to which Jump Gate adds the ephemeral user for terminal sessions under this policy.
Linux user groups	Override the global setting to select the local Linux groups to which Jump Gate adds the ephemeral user for terminal sessions under this policy.
Enable clipboard copy	Override the global setting to control whether users can copy content from RDP sessions to their local computer under this policy.

©2026 Tanium Inc. All Rights Reserved

> **Tip:** For more information about configuring the module settings that these settings override, see Configure Jump Gate module settings on page 21.

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

Prioritize access policies

About this task

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.

> **Note:** Policy priority order is global across all content sets. If a policy is assigned to a content set you cannot access, the policy does not appear in your prioritized list. The policy retains its position in the overall priority order.

Content set scoping for access policies and activity

Every access policy belongs to a Tanium RBAC content set, which limits visibility and management of the policy, and the requests, sessions, commands, and audit records associated with the policy, to users with access to that content set. You can change the content set a policy belongs to when you create or edit the policy.

- Users can create or edit an access policy only in a content set for which their role grants

©2026 Tanium Inc. All Rights Reserved

Jump Gate Policies write permission.

- Users can view an access policy on the **Access Policies** page only if their role grants **Jump Gate Policies read** permission for the policy's content set.
- Jump Gate matches a jump request only against access policies in the content sets the requesting user can access, before evaluating the requesting users and groups configured on each policy. If the user submits the request while using an alternative persona, Jump Gate matches the request only against access policies in the content sets the persona can access.
- A jump request inherits the content set of the access policy it matches. To view and approve a request, a designated approver must have **Jump Gate Requests approve** permission for that content set.
- On the **Activity** and **Audit** pages, users see only the jump requests, sessions, commands, and audit records associated with access policies in their accessible content sets. Counts and totals on these pages reflect only this scoped result set.

By default, an access policy belongs to the **Jump Gate** content set, and the predefined Jump Gate roles are scoped to that content set. Jump requests that do not match any access policy belong to a separate **Jump Gate Unmatched Requests** content set. The predefined Jump Gate roles are also scoped to that content set. To grant a custom role visibility into unmatched requests, assign that role **Jump Gate Requests read** or **Jump Gate Audits read** permission for the **Jump Gate Unmatched Requests** content set.



Important: Reassigning an access policy to a different content set immediately changes the content set scope of all jump requests, sessions, commands, and audit records associated with that policy. This includes historical records and open requests. For example, if an approver can currently view and approve open requests matched to a policy, and that policy is reassigned to a different content set, the approver immediately loses access to those requests unless their role also grants access to the new content set.

You manage content sets and role assignments in the Tanium console. For more information, see Tanium Console User Guide: Managing content sets.

Enable and configure Remote Desktop on endpoints where you will use RDP-based jump sessions

©2026 Tanium Inc. All Rights Reserved

About this task

Note: RDP sessions are supported only where the Tanium environment runs on TanOS. RDP sessions are not supported if the Tanium Module Server runs on a Windows-based server.

On Windows endpoints where you plan to use RDP-based jump sessions, you must enable Remote Desktop through a group policy, in Windows settings, or through other means.

Tip: Because Jump Gate encrypts and redirects Remote Desktop traffic for RDP sessions using the Tanium Protocol, it is not necessary to open TCP port 3389 or any other Remote Desktop port configured in your firewall or network for Jump Gate RDP sessions.

Note:

- For endpoints where you plan to use RDP-based jump sessions, ensure that members of the Windows local groups configured in the **RDP user groups** setting can sign in to those endpoints through Remote Desktop Services. Jump Gate adds users to those groups when an RDP session starts. For more information, see Configure Jump Gate module settings and access policies on page 21.
- Any Remote Desktop policy settings for Windows endpoints in your environment apply to RDP-based jump sessions. Review your Remote Desktop policy settings to ensure that they are appropriate for RDP-based jump sessions.
- Domain controllers do not support ephemeral RDP sessions. If endpoints governed by an access policy include domain controllers, ensure that the global settings and the access policy allow the **GUI > Existing credentials** access method for Windows.

Select a language

Select a language

©2026 Tanium Inc. All Rights Reserved

Select one of the supported languages for the Jump Gate workbench and Jump Gate user guide, as described in Tanium Console User Guide: Reference: Language support.

©2026 Tanium Inc. All Rights Reserved

Jumping to endpoints

About this task

You can jump to an endpoint to access a PowerShell or RDP session on a Windows endpoint, 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 on page 21 that is configured for Jump Gate.

Make a jump request for an endpoint

About this task

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 25.

1. From the Main menu, go to **Modules** > **Jump Gate** to open the **Overview** page.
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.

©2026 Tanium Inc. All Rights Reserved

> **Tip:** 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 on page 21 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.

View your own requests

About this task

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

©2026 Tanium Inc. All Rights Reserved

Rejected if an approver rejected it, or **Closed** if it reached its expiration time or an approver closed it before the expiration. The request details page shows the reason for the rejection or closure.

Tip:

- 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.

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

Jump to an endpoint

About this task

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

Note: The **Jump** menu lists every access type that the targeted endpoint supports. If the applicable global settings or access policy disables every access method for an access type, that option remains in the menu, but the option is disabled and a message indicates that the access type is disabled by policy or settings. Contact a Jump Gate operator if you expect an access type to be available. For more information, see Configure Jump Gate module settings on page 21.

Tip: 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.

©2026 Tanium Inc. All Rights Reserved

Start an RDP session (Windows endpoints only)

About this task

> **Note:** RDP sessions are supported only where the Tanium environment runs on TanOS. RDP sessions are not supported if the Tanium Module Server runs on a Windows-based server.

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 to open the request details, then click **Jump** > **RDP**.
4. If this is your first session, the **Recording Acknowledgment** dialog appears. Click **Acknowledge** to proceed. Jump Gate remembers your acknowledgment and does not show this dialog again for your user account on the same browser.
5. In the **RDP Authentication** dialog, select an authentication method and click **Connect**:
   - **Use ephemeral account**: Jump Gate creates a temporary local user account on the endpoint for the session in the groups configured by the **RDP user groups** setting. The account is removed when the request closes.
   - **Enter credentials**: Enter the username and password of an existing account on the endpoint.
   - **Windows logon screen**: Connect without pre-authenticating. Windows presents its native login screen. This option is available only when Network Level Authentication (NLA) is not required on the endpoint.

©2026 Tanium Inc. All Rights Reserved

Note:

- An authentication method that the applicable settings, access policy, or endpoint do not permit appears in the dialog, but the method is disabled and a message indicates why. If no authentication method is available, **Connect** is also disabled.
- If Remote Desktop is disabled on the endpoint, the dialog shows the warning `RDP appears to be disabled on this endpoint. Your connection may fail.` You can still attempt to connect, because the endpoint data behind the warning might be out of date. For more information, see Troubleshooting RDP sessions that close because RDP is not enabled on page 57.

6. The RDP session opens in a separate browser window.

Note:

- When you use the ephemeral account for the first RDP session on an endpoint, it takes up to a few minutes for Windows to set up the new user, and onboarding dialogs might appear after Jump Gate signs you in. Jump Gate reuses the same temporary account for subsequent RDP sessions to the same endpoint within the same request, so setup does not repeat until you start the first RDP session for a new request.
- Windows-based session limitations apply for RDP sessions in Jump Gate. For example, desktop versions of Windows typically allow only a single session, and Windows Server session limits depend on Windows licensing and group policies. All other Remote Desktop policy settings and behaviors apply to RDP-based jump sessions as well.
- If your browser blocks the popup, the session opens inline on the **Request Details** page instead.
- Domain controllers do not support the **Use ephemeral account** option for RDP sessions. If you select this option on a domain controller, Jump Gate displays an error. Use the **Enter credentials** option instead.

©2026 Tanium Inc. All Rights Reserved

Tip: RDP sessions support clipboard redirection. You can copy text on your computer and paste it into the RDP session. Copying content from the RDP session to your local computer is enabled by default and can be controlled by an operator using the **Enable clipboard copy** setting. For more information, see Configure Jump Gate module settings on page 21.

Start a CLI session

About this task

A CLI session opens a PowerShell session on a Windows endpoint, or a Bash session on a macOS or Linux 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**.
4. For a Bash session on a Linux or macOS endpoint, select an authentication method in the **Terminal Authentication** dialog and click **Connect**:
   - **Root user**: Connect as the account that runs the Tanium Client, which has full superuser privileges on the endpoint.
   - **Ephemeral user**: Jump Gate creates a temporary local user account on the endpoint for the session in the groups configured by the **Linux user groups** setting for a Linux endpoint, or the **macOS user groups** setting for a macOS endpoint. The account is removed when the request closes.

Note:

- The dialog lists only the authentication methods that the applicable global settings and access policy permit. For more information, see Configure Jump Gate module settings on page 21.
- PowerShell sessions on Windows endpoints always connect as the root user and do not show this dialog.

Result

©2026 Tanium Inc. All Rights Reserved

The window for the jump session appears on the **Request Details** page.

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 57.

Run a command on an endpoint

About this task

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.

Commands run as the root user on the endpoint. On a Linux or macOS endpoint where the applicable global settings or access policy disallows the **Terminal > Root** access method, commands run as the ephemeral user instead. If neither access method is allowed for the endpoint, Jump Gate rejects the command and does not record it in the command history.

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**.

©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.

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 21.

View the command history with command outputs

About this task

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.

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

About this task

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**.

©2026 Tanium Inc. All Rights Reserved

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**.

Result

Jump Gate attempts to stop the command.

Note: 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.

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

Jump Gate CLI

You can interact with Jump Gate from the command line on your computer using the Jump Gate CLI. You can use the CLI to, for example, create access requests, initiate jump sessions, run commands on endpoints, and approve or reject requests from scripts or automated workflows. You can download the CLI and access the full CLI documentation directly from the Jump Gate interface.

1. From the Main menu, go to **Modules** > **Jump Gate**.
2. Click Help ?, and then click the **Jump Gate CLI** tab.
3. Click **Download CLI** and follow the instructions on the page to install and use the CLI.

Tip: The Jump Gate CLI Documentation page provides references for **macOS / Linux** and **Windows** on separate tabs. The tab for the operating system you are using to access Tanium Console is selected by default.

Manage favorite endpoints

About this task

©2026 Tanium Inc. All Rights Reserved

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

Tip: You can also add or remove the endpoint targeted by a request to your favorites by clicking Favorite Endpoint  or Remove from Favorites  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 endpoints.
3. In the results that appear, click the name of the endpoint to add it to your favorites.

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** > **Remove from favorites**.

©2026 Tanium Inc. All Rights Reserved

Approving jump requests and viewing activity

About this task

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 25.

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.

©2026 Tanium Inc. All Rights Reserved

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. The request details page shows this reason, or the reason the request was otherwise closed, such as reaching its expiration time.

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 review session recordings, command history, and request activity.

VIEW SESSION RECORDINGS AND COMMAND HISTORY

You can view session recordings and command history in the **Session Monitoring** section.

©2026 Tanium Inc. All Rights Reserved

Note: The **Session Monitoring** section appears only if you created the request or have **Jump Gate Requests read** permission for the request's content set. Having only the **Jump Gate Requests approve** or **Jump Gate Requests close** permission does not grant access to session recordings and command history.

- **Terminal Recordings**: View recordings of PowerShell and Bash jump sessions. Expand a session card to view an AI-generated summary of the session activity and a table of the commands that were run. Click **Export Session Data** to download a session log as a .txt file.

  Note:

  - Jump Gate sends the transcript to an AI model to generate a summary. The transcript and summary then remain in your environment and are not retained by Tanium.
  - Session transcripts can contain sensitive data such as passwords, tokens, or credentials entered during a session. AI-generated summaries do not surface any sensitive data beyond what is already in the transcript. A user who has read access to a session recording also has read access to the session summary.
  - Terminal session summaries require the **Tanium AI Features** setting to be enabled in platform settings. If your organization has disabled this setting, session summaries are not generated. For more information, see Tanium Console User Guide: Optimizing and automating workflows through the Autonomous IT Platform.

- **GUI Recordings**: View recordings of GUI-based jump sessions, such as RDP. Click **Export Session Data** to download a session recording as an .m4v file. This tab appears only for endpoints that support GUI-based jump sessions.
- **Command History**: View all asynchronous commands run on the endpoint from jump requests.

VIEW REQUEST HISTORY

©2026 Tanium Inc. All Rights Reserved

You can view a chronological list of all activity associated with the request in the **Request History** section. Each entry shows the event type, the user or service that performed the action, and the timestamp. Expand an entry to view details of the change: an update shows the before-and-after state of the affected object, while a create or delete shows the object's state at that point.

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

About this task

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 46.

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

Note: If access policies in your environment are assigned to different content sets, the Activity page is scoped to your accessible content sets. Counts and totals on this page reflect only this scoped result set. For more information, see Content set scoping for access policies and activity on page 31.

©2026 Tanium Inc. All Rights Reserved

Export jump activity

About this task

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

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

About this task

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**.

> **Note:** If access policies in your environment are assigned to different content sets, the audit records shown on this page are scoped to your accessible content sets. For more information, see Content set scoping for access policies and activity on page 31.

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.

©2026 Tanium Inc. All Rights Reserved

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 50 .
event_name	The specific event that occurred. For a list of event names, see Audit event types on page 50 .
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.

Event names

Event name	Operation	Description
Favorite targets		
CreateFavoriteTarget	create	A user saved a new favorite target.

©2026 Tanium Inc. All Rights Reserved

Event name	Operation	Description
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.
Users		
CreateEphemeralUser	create	A temporary local account was created on the endpoint for an RDP, macOS, or Linux ephemeral session. The `new_value` field contains the `request_users` row, including the groups the account was granted on the endpoint. The `parent_id` field contains the request ID.
DeleteEphemeralUser	delete	The temporary local account was removed from the endpoint after the request closed. The `parent_id` field contains the request ID.
DeleteEphemeralUserFailed	delete	An attempt to remove the temporary local account from the endpoint failed, and the account might still be present. Jump Gate retries automatically every six hours until cleanup succeeds; this event can recur for the same account if retries continue to fail. The `parent_id` field contains the request ID.

©2026 Tanium Inc. All Rights Reserved

Event name	Operation	Description
AddExistingUserToGroups	create	An existing endpoint user supplied for an RDP session (BYO credentials) was added to local groups. The `new_value` field contains the `request_users` row, including the groups actually granted. The `parent_id` field contains the request ID.
RemoveExistingUserFromGroups	delete	The supplied user was removed from those groups after the request closed. The `parent_id` field contains the request ID.
RemoveExistingUserFromGroupsFailed	delete	An attempt to remove the supplied user from those groups failed, and the user might still hold them. Jump Gate retries automatically every six hours until cleanup succeeds; this event can recur for the same user if retries continue to fail. 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

About this task

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 56

Perform quarterly maintenance

Review access policies

About this task

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 Tanium Jump Gate User Guide: Configure access policies.
3. Make sure that policies are arranged in the appropriate priority order. For information about prioritizing policies, see Tanium Jump Gate User Guide: Prioritize access policies.

Review timeout and data retention policies

About this task

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 ⚙.

©2026 Tanium Inc. All Rights Reserved

3. On the **General** tab, 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.
Maximum Concurrent GUI Sessions	Configure the maximum number of GUI-based jump sessions, such as RDP sessions, that can run at the same time in Jump Gate .
Session Inactivity Timeout	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 57. • 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.

©2026 Tanium Inc. All Rights Reserved

Setting	Description
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

About this task

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

Collect logs

About this task

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 **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 59.

Result

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 and Reference: Client extensions and endpoint tools used for Tanium solutions.

Troubleshooting automatically rejected jump requests

©2026 Tanium Inc. All Rights Reserved

About this task

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 25.

Troubleshooting RDP sessions that close because RDP is not enabled

About this task

If an RDP jump session closes with the message `Jump to <endpoint> closed: RDP is not enabled on the endpoint`, Remote Desktop is disabled on the endpoint at the operating system level, either in Windows settings or through a group policy.

To use RDP-based jump sessions with the endpoint, enable Remote Desktop on the endpoint. For more information, see Enable and configure Remote Desktop on endpoints where you will use RDP-based jump sessions on page 32.

Tip: Jump Gate determines whether Remote Desktop is enabled on an endpoint from the **Jump Gate RDP Security Posture** sensor. When that sensor reports that Remote Desktop is disabled, the **RDP Authentication** dialog also warns you before you connect. For more information, see Start an RDP session (Windows endpoints only) on page 38.

Troubleshooting disconnected jump sessions

About this task

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

©2026 Tanium Inc. All Rights Reserved

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.
- **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 21.



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.

Uninstall Jump Gate



Important: Consult with Tanium Support on page 59 before you uninstall or reinstall Jump Gate.

1. Sign in to Tanium Console as a user with the Administrator role.

©2026 Tanium Inc. All Rights Reserved

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 submitting a support case, see Case Submission Form.

©2026 Tanium Inc. All Rights Reserved