Tanium Atlas MCP Server User Guide

2026H2 Semiannual Release

Version 1.6.12

November 18, 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 6
- Example use cases 6
- Model Context Protocol 6
- MCP tools, tool catalog, and toolsets 7
- Tanium skills 8

Requirements 9
- Core platform dependencies 9
- Recommended AI models 9
- Solution dependencies 10
  - Tanium recommended installation 10
  - Import specific solutions 10
  - Required dependencies 10
  - Feature-specific dependencies 11
- Tanium™ Module Server 11
- MCP clients 11
- Endpoints 12
- Host and network security requirements 12
- User role requirements 12

Installing 15
- Before you begin 15
- Import Atlas MCP Server with default settings 15
- Import Atlas MCP Server with custom settings 16
- Troubleshoot issues 16

Configuring 17
- Set up Tanium Atlas MCP Server users 17
  - Assign predefined Atlas MCP Server roles 17
  - Assign additional roles for Atlas MCP Server functionality 17

©2026 Tanium Inc. All Rights Reserved

Enable MCP clients to access the Tanium Server 18
Authenticate with OAuth 19
Connect Claude Desktop to Tanium Atlas MCP Server 20
Connect Claude Desktop through an organization-wide custom connector 20
Connect Claude Desktop through a personal custom connector 22
Connect other MCP clients to Tanium Atlas MCP Server 23
Filter tools 23
Add filters through headers in the MCP client configuration 24
Add filters through the MCP endpoint URL 24

Troubleshooting 26
Export MCP tool-call audit data 26
Connection errors 27
403 RBACInsufficientPrivilege 27
Tool catalog is missing an expected tool 27
OAuth and authentication errors 28
Tanium consent page shows "No role overlap for any persona" 28
Refresh token rejected 28
Claude Desktop connection errors 28
Contact Tanium Support 29

Reference: Tool availability 30
Tool availability based on RBAC 30
Tool availability based on installed solutions 30
Tool availability based on filters 31

Reference: Core tools, toolsets, and resources 32
Core tools 32
Core resources 32
Toolsets and reference resources 33

©2026 Tanium Inc. All Rights Reserved

Tanium Atlas MCP Server overview

Tanium Atlas MCP Server is a service that exposes a catalog of Tanium tools to an external MCP client through Model Context Protocol (MCP). Users can access the functionality of Tanium solutions directly from MCP clients without switching to a Tanium UI. Agentic pipelines in an AI orchestration platform can also use the tools to run automated tasks.

For example, a user can enter a chat prompt in an MCP client for a list of operating system (OS) patches that are missing on Tanium endpoints. The MCP client runs the required tool, which collects patch information from endpoints. The MCP client then shows the list to the user.

Example use cases

The following use cases describe how different roles in your organization might use Tanium Atlas MCP Server.

Security analyst working in a human-interactive MCP client

Security analysts work within an interactive MCP client to access Tanium functionality through Tanium Atlas MCP Server. The analysts enter chat prompts in the MCP client to query Tanium endpoints for data during threat investigations. Analysts can then review the query results within the client interface.

IT operations engineer designing agentic pipelines in an AI orchestration platform

An IT operations engineer connects Tanium Atlas MCP Server to an AI orchestration platform to automate remediation pipelines from threat detection to action deployment. Examples of an orchestration platform include an internal chatbot, a custom Microsoft Copilot agent, or an agentic workflow framework. Engineers build pipelines that call read-only Tanium tools automatically. For example, a read-only tool might generate a report about threats in your environment.

Model Context Protocol

MCP is an open standard that defines how MCP clients discover and call server-side tools. Tanium

©2026 Tanium Inc. All Rights Reserved

Atlas MCP Server implements the Streamable HTTP transport variant of this standard. Tanium Atlas MCP Server does not support the stdio transport.

MCP tools, tool catalog, and toolsets

MCP tools are discrete operations that an MCP client can invoke. A tool catalog is the set of MCP tools that are available in a particular environment. An MCP client acquires the Tanium tool catalog during its initial connection to Tanium Atlas MCP Server. Each Tanium solution provides its toolset for the catalog.

A toolset is a capability domain: the named group of Tanium operations for one capability. Each toolset surfaces one entry-point tool with the naming convention tanium_<domain>_tools. The entry-point tool accelerates tool selection when an MCP client user requests a tool. A domain-specific request matches the tool directly and searches within the toolset instead of searching the global catalog.

For example, a user might enter a chat prompt in an MCP client for a list of OS patches that are missing on Tanium endpoints. The client matches the prompt through the entry-point tool tanium_patch_tools to find a specific tool in the Tanium™ Patch toolset. The client runs the tool to collect patch information from endpoints and then shows the list to the user.

For more information, see Reference: Core tools, toolsets, and resources on page 32.



Note:

Even if a tool is in the catalog, the MCP client can find the tool only if the user has the RBAC permissions to access the tool. For more information, see Tool availability based on RBAC on page 30.

Disabling an entry-point tool in your MCP client (for example on the **Connectors** page in Anthropic Claude) removes only the shortcut to the tool; the corresponding toolset operations remain discoverable and callable through the tanium_search_tools tool and the global call tools. To restrict which toolsets a client can use, apply MCP client-side toolset filtering. For more information, see Filter tools on page 23.

The MCP client might match the prompt to a skill, which can result in multiple tool requests. For more information, see Tanium skills on page 8.

©2026 Tanium Inc. All Rights Reserved

Tanium skills

A skill is a predefined agentic workflow that combines one or more MCP tools into a repeatable, single-prompt operation. Tanium provides predefined skills that make common security and IT operations tasks available as single-call operations in an MCP client. For example, a skill might combine all the tools that are needed to review patch compliance and remediate non-compliant endpoints.

In an MCP client, a user can enter a prompt that invokes the skill by name or description. In other cases, the client might automatically match the prompt with a skill even if the user does not know that skill exists. When the client runs the skill, it automatically performs all the tool calls, sequencing, and error handling for its workflow. This automation enables users to perform complex workflows without authoring custom orchestration logic.

©2026 Tanium Inc. All Rights Reserved

Tanium Atlas MCP Server requirements

Review the requirements before you install and use Tanium Atlas MCP Server.

Core platform dependencies

Make sure that your environment meets the following requirements:

- The Atlas MCP Server solution is installed and its service is running. To install the solution, see Tanium Console User Guide: Managing Tanium solutions. To check the service status and restart the service, see:
    - Tanium Appliance User Guide: Reference: TanOS management commands
    - Tanium Core Platform User Guide for Windows Deployments: Manage Windows services for core platform servers (the steps work for solution services also)
- Any supported version of Tanium Client. For more information, see Client version and host system requirements. If you use a Client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed Client versions.

Recommended AI models

The following are the recommended minimum AI models and reasoning effort to use in your MCP client:

Recommended models

Vendor	Model	Reasoning effort
Anthropic	Claude Haiku 5.5	High
OpenAI	GPT-5.6 Luna	High

©2026 Tanium Inc. All Rights Reserved

Vendor	Model	Reasoning effort
Google	Gemini 4 Argon	Medium
xAI	Grok 4.7	Low

Solution dependencies

Other Tanium solutions are required for Atlas MCP Server to function (required dependencies) or for specific Atlas MCP Server 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 Atlas MCP Server 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 Atlas MCP Server requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Atlas MCP Server, 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 Atlas MCP Server 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 Atlas MCP Server, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Atlas MCP Server has the following required dependencies:

©2026 Tanium Inc. All Rights Reserved

- Tanium™ Console
- Tanium™ RDB Service

Feature-specific dependencies

If you select only Tanium Atlas MCP Server to import, you must manually import or update its feature-specific dependencies regardless of Tanium Console or Tanium Core Platform versions. Atlas MCP Server has the following feature-specific dependencies:

- Tanium™ Data Service (TDS): Required to cache question results. Without TDS, questions can return only live results from online endpoints.
- Tanium™ Gateway: Required to use GraphQL-based tools (the tanium_gateway_tools toolset).
- Tanium™ Interact: Required to issue questions to managed endpoints.
- Any additional Tanium solutions that provide the toolsets that MCP users expect to use. For example, if users must access the Asset toolset, import Tanium™ Asset. For more information, see Tool availability based on installed solutions on page 30.

Tanium™ Module Server

Atlas MCP Server is installed and runs as a service on the Module Server host computer. Atlas MCP Server requires the following resources on the Module Server:

- CPU: 0.5 cores
- Memory: 150-200 MB

For more information about Module Server sizing in a Windows deployment, see Tanium Core Platform User Guide for Windows Deployments: Host system sizing guidelines.

MCP clients

Tanium Atlas MCP Server works with MCP-enabled clients such as:

- ChatGPT

©2026 Tanium Inc. All Rights Reserved

- Claude Code
- Claude Desktop
- Codex
- Cursor
- Microsoft Copilot Studio
- VS Code Copilot

For recommended models to use with Tanium Atlas MCP Server, see Recommended AI models on page 9.

Endpoints

MCP client users who access Tanium functionality through Tanium MCP can view and manage all the endpoints that the Tanium Core Platform supports. For more information, see Tanium Console User Guide: Endpoints.

Tanium Atlas MCP Server does not deploy packages to endpoints but the tools that it runs might. For example, the Tanium Deploy solution provides tools for running software packages. For more information about the endpoint requirements for a solution, see the user guide for that solution in the Tanium Resource Center.

Host and network security requirements

Host and network security requirements for the Tanium Core Platform and all supported Tanium solutions apply to Tanium MCP. For more information about security exclusions to define across Tanium, see:

- Tanium Core Platform User Guide for Windows Deployments: Tanium Core Platform Server security exclusions
- Tanium Client Management Guide: Reference: Endpoint security exclusions

User role requirements

©2026 Tanium Inc. All Rights Reserved

Predefined roles grant the following permissions, which are required to use Tanium Atlas MCP Server functionality:

- Atlas MCP Server solution permissions on page 13
- Table 3. Atlas MCP Server platform content permissions on page 14: The solution permissions automatically provide some of these permissions.

If you create custom roles for Atlas MCP Server users, be sure to assign all the solution permissions and content set permissions that are required for Atlas MCP Server functionality. If you are not sure which permissions are required for a custom role, view the permissions of the predefined role. 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

Important: The predefined roles for Atlas MCP Server do not grant all the permissions that are required to issue questions to endpoints. For more information, see Assign additional roles for Atlas MCP Server functionality on page 17.

Tanium Atlas MCP Server solution permissions

Permission	MCP User	MCP Read Only User
Mcp Use Read Only View and run tools that retrieve information from your Tanium environment. For example, the information can be data from endpoints (such as threat alerts), data that Tanium solutions generate (such as the Tanium Risk Score), or Tanium™ Jump Gate requests.	✗	✓ API
Mcp Api In the current release, this permission enables the same functionality as the **Mcp Use Read Only** permission.	✓ EXECUTE	✗

©2026 Tanium Inc. All Rights Reserved

Permission	MCP User	MCP Read Only User
Mcp Read audit Read the MCP tool usage data of all users.	✗	✗

The permissions for these roles provide solution permissions for other solutions. To view the provided permissions, see View effective role permissions .

Atlas MCP Server platform content permissions

Permission	Permission Type	MCP User	MCP Read Only User
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE

To view the content sets to which the platform content permissions apply, see View effective role permissions .

©2026 Tanium Inc. All Rights Reserved

Installing Atlas MCP Server

About this task

Use Tanium Console **Solutions** page to install Atlas MCP Server and choose either automatic or manual configuration:

- Automatic configuration with default settings: Atlas MCP Server is installed with any required dependencies and other selected products. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information about the automatic configuration for Atlas MCP Server, see Import Atlas MCP Server with default settings on page 15.
- Manual configuration with custom settings: After installing Atlas MCP Server, you must manually configure required settings. Select this option only if Atlas MCP Server requires settings that differ from the recommended default settings. For more information, see Import Atlas MCP Server with custom settings on page 16.

Before you begin

- Read the release notes.
- Review the Tanium Atlas MCP Server requirements on page 9.
- Assign the correct roles to users for Atlas MCP Server. Review the User role requirements on page 12.

> **Note:** To import the Atlas MCP Server solution, you must be assigned the **Administrator** reserved role.

Import Atlas MCP Server with default settings

About this task

To import Atlas MCP Server and configure default settings, see Tanium Console User Guide: Import all

©2026 Tanium Inc. All Rights Reserved

modules and services.

Import Atlas MCP Server with custom settings

About this task

To import Atlas MCP Server without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** option while performing the steps in Tanium Console User Guide: Import or update specific solutions. On the **Solutions** page, the **Content** grid lists Atlas MCP Server as **MCP**.

Troubleshoot issues

About this task

If you experience issues with installing Atlas MCP Server, see Troubleshooting Tanium Atlas MCP Server on page 26.

©2026 Tanium Inc. All Rights Reserved

Configuring Tanium Atlas MCP Server

Set up Tanium Atlas MCP Server users

About this task

Atlas MCP Server provides predefined user roles that enable users to access Tanium tools through MCP clients. Additional roles are required for users to access certain features.

Atlas MCP Server enforces RBAC whenever a user or AI agent requests a tool through an MCP client. For more information, see Tool availability based on RBAC on page 30.

To assign user roles, see Tanium Console User Guide: Manage role assignments for a user.

Assign predefined Atlas MCP Server roles

About this task

You can use the following set of predefined user roles to set up Atlas MCP Server users.

For more information about permissions for each role, see User role requirements on page 12.

MCP User

Assign the **MCP User** role to users who view information from your Tanium environment. For example, the information can be data from endpoints (such as threat alerts), data that Tanium solutions generate (such as the Tanium Risk Score), or Tanium™ Jump Gate requests.

MCP Read Only User

In the current release, the **MCP Read Only User** role provides access to the same functionality as the **MCP User** role.

Assign additional roles for Atlas MCP Server functionality

About this task

©2026 Tanium Inc. All Rights Reserved

The predefined roles for Atlas MCP Server do not grant all the permissions that are required to issue questions to managed endpoints. You must assign a predefined Tanium Interact role to all Atlas MCP Server users. The **Interact Power User** role provides the broadest set of Interact permissions, including the permission to issue questions. For more information, see Tanium Interact User Guide: Interact permissions.

Additional RBAC assignments control which specific tools and managed endpoints users can access:

- Tanium solution permissions control which tools an MCP client can invoke on behalf of users.
- Computer group assignments control which endpoints the tools can access.

Enable MCP clients to access the Tanium Server

About this task

On each Tanium Server, you must configure a platform setting and replace the self-signed certificate if any of the following conditions apply in your environment:

- The Tanium Server connects through a load balancer, reverse proxy server, or DNS alias. The DNS alias condition applies only if the Tanium Server row in the servers table uses the machine name instead of the alias.
- MCP clients connect through a DNS Canonical Name (CNAME) that differs from the registered Tanium Server name.
- The Tanium Server, or a server through which it connects, uses a non-standard external port. For example, a proxy server might expose port 8443.
- The servers table uses an IP address or short hostname of the Tanium Server but MCP clients use an FQDN, or vice versa.

You might see the following errors if the preceding conditions exist:

- Browser error 404 on the well-known OAuth metadata URLs
- 401 challenges in HTTP or API responses that are missing `resource_metadata`

Perform the following tasks to enable MCP clients to communicate with the Tanium Server in the preceding conditions.

©2026 Tanium Inc. All Rights Reserved

Note: These tasks are not necessary if MCP clients connect directly from your internal network to a Tanium Server and the systems that host the clients have the trusted certificate of that server.

1. On each Tanium Server, replace the self-signed certificate with one that a certificate authority (CA) has signed. For the steps, see Tanium Console User Guide: Securing Console and API access through certificates.
2. Configure the setting **oauth_authority_override** with the FQDN or IP address of the Tanium Server. If the Tanium Server, or a server in front of it (such as a proxy server), uses a non-standard port, specify the port also. For the steps, see Tanium Console User Guide: Edit advanced settings.

Authenticate with OAuth

About this task

Tanium Atlas MCP Server uses the OAuth 2.1 or 2.0 Authorization Code Flow as its authentication method. Your The Tanium Server acts as the Authorization Server (AS) and your MCP client is the OAuth client. Perform the following tasks to set up OAuth authentication:

1. Register an OAuth client.
   You must register an OAuth client before it can authenticate to Tanium Atlas MCP Server for tool requests. During registration, you assign the roles that the client is permitted to use on behalf of users.

   For the steps, see Tanium Console User Guide: Register an OAuth client.

2. Connect an MCP client to Tanium Atlas MCP Server:
   - Connect Claude Desktop to Tanium Atlas MCP Server on page 20
   - Connect other MCP clients to Tanium Atlas MCP Server on page 23

3. Complete the OAuth consent flow.
   After each user first connects an MCP client to Tanium Atlas MCP Server, the user must perform the OAuth consent flow. The flow generates an access token that authorizes the client to request tools through Tanium Atlas MCP Server. For the steps, see Tanium Console User Guide: Authorize access. For more information about how token RBAC permissions determine which tools are available, see Tool availability based on RBAC on page 30.

©2026 Tanium Inc. All Rights Reserved

Connect Claude Desktop to Tanium Atlas MCP Server

About this task

After you register Claude Desktop as an OAuth client, perform one of the following tasks to connect it to Tanium Atlas MCP Server:

- Connect Claude Desktop through an organization-wide custom connector on page 20
- Connect Claude Desktop through a personal custom connector on page 22

Note:

If Claude Desktop fails to connect, check the connector error log for the specific error. For more information, see Claude Desktop connection errors on page 28.

For more information about custom connectors, see Get started with custom connectors using remote MCP in the Claude Support center.

CONNECT CLAUDE DESKTOP THROUGH AN ORGANIZATION-WIDE CUSTOM CONNECTOR

About this task

Use an organization-wide connector if multiple users in your organization must use MCP clients to access Tanium tools.

The primary Claude owner or Claude team/enterprise owner performs the following steps as a one-time setup.

Important: This one-time setup is the only part of the connection workflow that affects the connector configuration. No other user on the team repeats the steps and no one creates a second connector.

©2026 Tanium Inc. All Rights Reserved

Note: For more information about organization-wide connectors, see Authorize MCP connectors for your entire organization in the Claude Support center.

1. Open Claude Desktop and go to **Organization settings → Connectors**.

   Tip: If you are accessing Claude through a web browser, go to claude.ai/admin-settings/connectors instead.

2. Click **Add**, hover over **Custom**, and select **Web**.
3. Enter a **Name** to identify the connector.
4. Enter the MCP endpoint URL `https://<tanium-server>/mcp`, where `<tanium-server>` is the FQDN or IP address of your Tanium Server.
5. Click **Continue**.
   Claude finds the authorization server and verifies the OAuth configuration. Claude automatically sets **Authentication** to **Always required** and sets **OAuth client** to **Use your own OAuth client**. Claude detects these settings because Tanium does not support hosted client metadata (CIMD) or dynamic client registration (DCR). Do not change these settings.
6. Enter the **Client ID** into the **OAuth Client ID** field. The field is required and the connection fails without it.
   Leave the **OAuth Client Secret (optional)** blank.
7. Click **Add** to finish.

Next steps

After you finish the one-time setup, all other users who access Tanium tools through Claude must perform the following steps:

1. Open Claude Desktop and go to **Customize → Connectors**.

   Tip: Users who access Claude through a web browser can go to claude.ai and then select **Customize → Connectors**.

2. Find the connector that the Claude owner added. The connector might be labeled **Custom** or

©2026 Tanium Inc. All Rights Reserved

use Tanium branding if the URL matches a directory listing.

3. Click **Connect**, sign in to the Tanium UI if prompted, and approve the request on the Tanium **Authorize Access** page. For more information, see Tanium Console User Guide: Authorize access.

CONNECT CLAUDE DESKTOP THROUGH A PERSONAL CUSTOM CONNECTOR

About this task

Use a personal custom connector only in one of the following cases:

- Your Claude plan is individual Pro/Max.
- Your organization has not yet configured an organization-wide connector and you want to test the connection independently.

Perform the following steps to connect through a personal connector:

1. Open Claude Desktop and go to **Customize → Connectors**.
2. Select **Add > Add custom connector**.
3. Enter a **Name** to identify the connector.
4. Enter the MCP endpoint URL `https://<tanium-server>/mcp`, where `<tanium-server>` is the FQDN or IP address of your Tanium Server.
5. Click **Continue**.
   Claude finds the authorization server and verifies the OAuth configuration. Claude automatically sets **Authentication** to **Always required** and sets **OAuth client** to **Use your own OAuth client**. Claude detects these settings because Tanium does not support hosted client metadata (CIMD) or dynamic client registration (DCR). Do not change these settings.
6. Enter the **Client ID** into the **OAuth Client ID** field. The field is required and the connection fails without it.
   Leave the **OAuth Client Secret (optional)** blank.
7. Click **Add** and click **Connect** on the new row for the custom connector.
8. Complete the Tanium consent flow. For more information, see Tanium Console User Guide: Authorize access.

©2026 Tanium Inc. All Rights Reserved

Connect other MCP clients to Tanium Atlas MCP Server

About this task

After you register an MCP client as an OAuth client, you must connect it to Tanium MCP. Each MCP client has its own method for configuring an MCP server connection. Generally, you require the following items to configure a connection:

- The Atlas MCP Server endpoint URL `https://<tanium-server>/mcp`, where `<tanium-server>` is the FQDN or IP address of your Tanium Server.
- The pre-registered client ID and (if OAuth 2.0 support is enabled) client secret.

Each user must complete the OAuth consent flow for the first connection from the MCP client to Tanium Atlas MCP Server. For the steps, see Tanium Console User Guide: Authorize access.

Filter tools

About this task

By default, an MCP client can access all the tools that Tanium Atlas MCP Server adds to the tools catalog and that the client user has RBAC permission to access. However, in cases where you want to limit access to a subset of the catalog, you can add filters based on specific toolsets or the readonly flag.

The following scenarios are examples of cases where you might want to filter the tools:

- To prevent access to tools that relate to deploying software, add a filter that lists all the toolsets except the toolset for Tanium Deploy.
- To prevent access to tools that change endpoint state, add a filter that allows access only to read-only tools.

You can add filters through headers in the MCP client configuration or through the MCP endpoint URL.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Add filters through headers if your MCP client supports that option. Add filters through the MCP endpoint URL only if the client configuration exposes a server URL field but not headers.

Add filters through headers in the MCP client configuration

About this task

Configure any of the following headers in your MCP client configuration to specify which tools the client can access on behalf of users. If you add headers that list both toolsets and tools, the client can access the tools across both lists. If you do not add a filter header, the client can access all the tools in the tool catalog. For the specific steps to configure headers, see the documentation for your client.

- `X-Tanium-MCP-Toolsets: <toolset name 1>,<toolset name 2>...`: Enter a comma-separated list of toolsets. Each toolset maps to a Tanium solution. For example, the `patch` toolset contains all the tools that Tanium Patch provides. For a list of all the toolset names, see Reference: Core tools, toolsets, and resources on page 32.
- `X-Tanium-MCP-Readonly: true`: The MCP client can access only the tools that have the readOnlyHint annotation set to true.

Add filters through the MCP endpoint URL

About this task

Your MCP client requires an MCP endpoint URL to connect to Tanium Atlas MCP Server. The URL follows the pattern `https://<tanium-server>/mcp`, where `<tanium-server>` is the FQDN or IP address of your Tanium Server. You can append any of the following suffixes to the URL to specify which tools the client can access on behalf of users. By default, the client can access all the tools in the tool catalog if you do not add a suffix.

- `/x/<toolset>`: Specify one toolset. Each toolset maps to a Tanium solution. For example, the `patch` toolset contains all the tools that Tanium Patch provides. For a list of all the toolset names, see Reference: Core tools, toolsets, and resources on page 32.
- `/readonly`: The MCP client can access only the tools that have the readOnlyHint annotation set to true.

©2026 Tanium Inc. All Rights Reserved

- `/x/<toolset>/readonly`: The MCP client can access only the tools that are in the specified toolset and that have the readOnlyHint annotation set to true.

©2026 Tanium Inc. All Rights Reserved

Troubleshooting Tanium Atlas MCP Server

About this task

If Tanium Atlas MCP Server is not performing as expected, you might need to troubleshoot issues or change settings.

Export MCP tool-call audit data

You can retrieve and archive persisted MCP tool-call evidence for investigation or for your own tooling. For example, you can enter the following prompt in an MCP client:

```
Show how many times any users invoked MCP tools in the past week in my Tanium environment.
```

The Atlas MCP Server tools then export the data through the MCP client. Each exported record includes the name of the called tool, the caller, the time the call started, the outcome, and the duration. A record also includes the stored request parameters and result evidence when these are available. The evidence retention period is 90 days.

Every record indicates one of the following call outcomes:

- `success`: The call completed and returned a result.
- `incorrect_parameters`: The arguments passed schema validation, but the upstream Tanium API rejected them as not valid. For example, an argument might have an incorrect ID or an unsupported value.
- `upstream_error`: An upstream or connectivity issue caused the call to fail.
- `denied_policy`: A router policy denied the call before it reached the upstream API. The risk-evaluator gate is an example of such a policy.

©2026 Tanium Inc. All Rights Reserved

Note:

You must authenticate with a user account that is assigned the **Admin** reserved role to export tool-call audit data.

Connection errors

403 RBACInsufficientPrivilege

This error indicates that the MCP client session token for your user account does not have the **Atlas MCP Server Api execute** permission. Verify that the **Atlas MCP Server User** role is assigned to your user account. For more information, see Set up Tanium Atlas MCP Server users on page 17.

If the error persists after the role assignment and token refresh, check the RBAC log on the Tanium Server for instances of `RBAC Exception`. For more information, see Tanium Appliance User Guide: RBAC log.

Tool catalog is missing an expected tool

About this task

Verify that your environment meets the following conditions if a user or agentic pipeline cannot find an expected tool:

1. Verify that the Tanium solution that provides the tool is installed. For more information, see Tanium Console User Guide: Managing Tanium solutions.
2. Verify that the roles that are assigned to the user include the RBAC permissions that the tool requires. If the user does not have the permissions, Tanium Atlas MCP Server returns a JSON-RPC error and the tool does not run. To check the effective permissions of a user and to update role assignments, see Tanium Console User Guide: Managing access permissions through roles.
3. Verify that the allowed roles of the OAuth client include the required permission. For more information, see Tanium Console User Guide: Edit an OAuth client registration.
4. Verify that Tanium Atlas MCP Server completed its first catalog refresh after a recent restart.

©2026 Tanium Inc. All Rights Reserved

Wait one minute for the catalog to refresh and retry the tool request.

OAuth and authentication errors

Tanium consent page shows "No role overlap for any persona"

After each user first connects an MCP client to Tanium Atlas MCP Server, the Tanium consent page opens in a browser for the user to complete the OAuth consent flow. The page shows the message `No role overlap for any persona` if the allowed roles of the OAuth client do not overlap with any role that is assigned to any persona that the user can select. Ensure that the allowed roles of the OAuth client include at least one such role.

For the steps, see Tanium Console User Guide: Edit an OAuth client registration.

Refresh token rejected

About this task

Tanium revokes the entire token family for a refresh token if it is used after revocation. For example, this might happen due to token rotation or an explicit revocation. The user or service account must sign out of the MCP client, sign in again, and repeat the consent flow. For the steps, see Tanium Console User Guide: Authorize access.

Claude Desktop connection errors

If Claude Desktop fails to connect to Tanium Atlas MCP Server, check the connector log at ~/Library/Logs/Claude/mcp-server-tanium-mcp-router.log.

Error messages and resolutions for Claude Desktop connectivity

Claude Desktop connection errors

Log message	Issue and resolution
Streamable HTTP error: 403 RBACInsufficientPrivilege	See 403 RBACInsufficientPrivilege on page 27 .
Connection error: ... self	Your network is intercepting TLS through a corporate proxy or similar device. In the environment

©2026 Tanium Inc. All Rights Reserved

Log message	Issue and resolution
signed certificate	configuration of the connector, set one of the following variables: • Set `NODE_EXTRA_CA_CERTS` to a PEM bundle that contains your corporate root certificate authority (CA) certificate. • Set `NODE_OPTIONS=--use-system-ca` to trust the certificate store of your operating system. Do not set `NODE_TLS_REJECT_UNAUTHORIZED=0`, which disables TLS verification entirely.
Redirect URI mismatch or "invalid redirect_uri" during the OAuth consent flow	Confirm the redirect URI registered on the Tanium OAuth client exactly matches what your MCP client sends, including the host, port, and path. For more information, see Tanium Console User Guide: Edit an OAuth client registration.

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

Reference: Tool availability

Tool availability based on RBAC

About this task

After each user first connects an MCP client to Tanium Atlas MCP Server, the user must perform the OAuth consent flow. The flow generates an access token that authorizes the client to request tools through Tanium Atlas MCP Server. The effective RBAC permissions of the token are the intersection of the following roles:

- The roles that an administrator assigned to the OAuth client during registration. For more information, see Tanium Console User Guide: Enabling third-party authentication through OAuth clients.
- The roles of the persona that a user selected during the OAuth consent flow. For more information, see Tanium Console User Guide: Authorize access.

Tanium Atlas MCP Server dynamically evaluates this intersection at the time of each tool request from an MCP client. If the roles of a user change after a token is issued, the change takes effect on the next request and no token rotation is required.

When a user initiates a tool request through an MCP client, Tanium Atlas MCP Server automatically filters the tool catalog at runtime to show only the tools that the token has RBAC permissions to call. The user can be an MCP client user or an AI agent acting on behalf of the user, such as an agentic pipeline. This filtering reduces context waste and improves the reliability of automated workflows by ensuring that AI agents do not waste their context window on tools that they cannot use.

Tool availability based on installed solutions

About this task

At startup, Tanium Atlas MCP Server polls each Tanium solution to discover available Tanium REST API routes. Thereafter, Tanium Atlas MCP Server polls the solutions again at each catalog refresh interval. Upon discovering a route, Tanium Atlas MCP Server registers the route as an MCP tool with its name, description, input schema, safety annotations, and RBAC authorization requirement. After

©2026 Tanium Inc. All Rights Reserved

you import a solution, Tanium Atlas MCP Server registers the tools for that solution at the next catalog refresh. If you remove a solution, Tanium Atlas MCP Server normally removes its tools within one minute.

> **Note:** If a user operation or agentic pipeline fails because it depends on a tool that disappears from the catalog, the most likely cause is that the associated Tanium solution was removed. Verify solution availability before diagnosing other causes. For more information, see Tanium Console User Guide: Managing the Tanium license.

Tool availability based on filters

About this task

Optionally, you can add filters that limit which tools an MCP client can access in the tool catalog. For more information, see Filter tools on page 23.

©2026 Tanium Inc. All Rights Reserved

Reference: Core tools, toolsets, and resources

The following tables describe core tools and resources for Tanium Atlas MCP Server, and describe all the toolsets that Tanium solutions provide to the tools catalog. For information about these concepts, see MCP tools, tool catalog, and toolsets on page 7.

Core tools

Core tools for Atlas MCP Server

Tool	Description
tanium_catalog	Entry-point tool that lists the Tanium capability domains (toolsets) currently visible to the user in an MCP client session.
tanium_search_tools	Cross-domain search that returns candidate tool names for a task, across all visible toolsets.
tanium_describe_tool	Returns the full schema, risk profile, and usage guidance for a tool. The MCP client reads the schema to provide tool inputs. The response also includes the response schema of the tool, when available, alongside its input schema.
tanium_call_read_only_tool	Runs any read-only Tanium operation (list/get/query/count) selected through the tanium_search_tools and tanium_describe_tool tools.
tanium-skill	Reads shared reference resources (Tanium expert guidance) for a domain, or the risk-evaluator guidance, before a gated action. For more information, see Core resources on page 32 .

Core resources

Resources reside in the skill://tanium-expert/ namespace and are fetched through the tanium-skill tool, where skill="tanium-expert" and path="references/<file>.md" (omit the path for the entry point). The risk-evaluator skill is published as its own top-level skill outside the tanium-expert namespace.

©2026 Tanium Inc. All Rights Reserved

Core Atlas MCP Server resources

Resource	Description
SKILL.md	The first file that the MCP client reads when the skill loads. It specifies the routing logic, mandatory safety-gate summary, module boundaries, and cross-module workflow chains.
risk-evaluator/ SKILL.md	The same risk-assessment content republished as a standalone skill at skill://risk-evaluator/ , fetched with skill="risk-evaluator" and no path.
references/direct-questions.md	Guidance for asking questions directly through the Tanium question interface.

Toolsets and reference resources

Tanium solutions provide the following toolsets to Atlas MCP Server.

The entry-point tool for every toolset works the same way: call with action=search to find the exact operation and action=describe for its schema[, then run it through tanium_call_read_only_tool or tanium_call_action_tool]. This flow describes how the AI agent interacts with the tools; users do not enter these commands. For more information about entry-point tools, see MCP tools, tool catalog, and toolsets on page 7.

The MCP client reads the references/<file>.md guidance resource for each toolset before the first use of the toolset domain according to the required-context pointer of the domain.

Toolset entry-point tools and reference resources for Atlas MCP Server

Toolset	Entry-point tool	Description	Reference resource
Apple Endpoint Management	tanium_apple_endpoint_management_tools	Apple MDM: enrolled-device inventory, MDM-command status, FileVault escrow, Activation Lock, enrollment/SCEP, tags, sensor catalog	references/ apple-endpoint-management.md
Asset	tanium_asset_tools	Asset inventory and reporting (installed software, hardware, SBOM); also tenant-wide OT/ICS protocol-restriction policy and	references/ asset.md

©2026 Tanium Inc. All Rights Reserved

Toolset	Entry-point tool	Description	Reference resource
		satellite-configuration lifecycle	
Automate	tanium_automate_tools	Playbook and deployment-plan lifecycle; trigger enable/disable and risk-gated write operations for automated remediation workflows	references/automate.md
Benchmark	tanium_benchmark_tools	Security operations posture compared to industry peer percentiles, per-endpoint Risk Score (1–1000), Tanium Risk Assessment (TRA) report lifecycle	references/benchmark.md
Certificate Manager	tanium_certificate_manager_tools	Endpoint-discovered X.509/SSL/TLS/JKS certificate inventory, trust-store and cipher policy, scan locations, certificate replacement workflow	references/certificate-manager.md
Client Management	tanium_client_management_tools	Tanium Client lifecycle: deployments, credentials, settings/index configurations, recovery passwords (BitLocker/FileVault), versions, manifests	references/client-management.md
Cloud Workloads	tanium_cloud_workloads_tools	Kubernetes/OpenShift cluster registration, container registries, image inventory, SBOMs, per-endpoint image run history	references/cloud-workloads.md
Comply	tanium_comply_tools	Compliance (CIS/SCAP/STIG) and vulnerability (CVE) assessment results, exceptions, custom profiles, benchmarks, vulnerability-source management	references/comply.md
Connect	tanium_connect_tools	Export saved-question/audit/module-report data to Splunk, Sentinel, S3, SQL Server, SMB, Elasticsearch, email, or ServiceNow on a schedule	references/connect.md

©2026 Tanium Inc. All Rights Reserved

Toolset	Entry-point tool	Description	Reference resource
Criticality	tanium_criticality_tools	Contextual importance scoring (Critical/ High/Medium/Low) for endpoints, AD users and user groups, and Microsoft Entra users and user groups	references/ criticality.md
Deploy	tanium_deploy_tools	Third-party software package management and deployment: catalog, bundles, deployments, templates, maintenance windows, self-service, removal	references/ deploy.md
Device Management (Google)	tanium_device_management_google_tools	Google device management for Chrome OS and Android MDM inventory and workflows	*(not yet authored)*
Direct Connect	tanium_direct_connect_tools	Satellite fleet management, connect tokens, connection testing, zone proxies, endpoint-connection configuration for endpoints that the Tanium Server cannot reach directly and connects to through satellites	references/ direct-connect.md
Directory Query	tanium_directory_query_tools	Configures directory service connectors that feed the Tanium identity graph: on-premises AD domain controllers and Entra tenant connections	references/ directory-query.md
Discover	tanium_discover_tools	Network discovery: discovered interfaces (managed/unmanaged), networks, scan profiles, labels, location hierarchy	references/ discover.md
Endpoint Configuration	tanium_endpoint_configuration_tools	Delivers per-solution configuration items and endpoint tools to Tanium Clients; governs approvals and staged Tanium solution toolset/Client upgrade rings	references/ endpoint-config.md
Endpoint Provider	tanium_endpoint_provider_tools	MDM action history for Intune-managed devices (wipe/lock/retire status) and	references/ endpoint-

©2026 Tanium Inc. All Rights Reserved

Toolset	Entry-point tool	Description	Reference resource
		provider service health	provider.md
Enforce	tanium_enforce_tools	Centralized policy management for Windows/macOS/Linux/Kubernetes: anti-malware, BitLocker/FileVault, AppLocker, firewall, device control, remediation actions	references/enforce.md
Engage	tanium_engage_tools	Author and deliver surveys, on-screen notifications, and remediation tasks tied to user responses	references/engage.md
Gateway	tanium_gateway_tools	Live Direct Connect endpoint sessions: open a session, read live process/performance/alert data, terminate processes	references/gateway.md
Guide (Feed)	tanium_guide_tools	Operator notification feed (Guardian issues, guidance, custom alerts): read, dismiss, pin, snooze, administer notification configurations	references/guide.md
Impact	tanium_impact_tools	Active Directory attack-path scoring: lateral-movement and administrative-relationship blast radius across computers, users, groups	references/impact.md
Integrity Monitor	tanium_integrity_monitor_tools	File-integrity monitoring: watched file/registry paths bound to computer groups, rule-based auto-labeling of change events	references/integrity-monitor.md
Investigate	tanium_investigate_tools	Investigation case container with artifacts, comments, and search; cross-module evidence hub for alerts, anomalies, and audit entries	references/investigate.md
Iris	tanium_iris_tools	Read-only Entra sync-eligibility sets: which Entra group filters scope a profile sync, with match counts and status	references/iris.md

©2026 Tanium Inc. All Rights Reserved

Toolset	Entry-point tool	Description	Reference resource
Jump Gate	tanium_jump_gate_tools	Policy-gated privileged remote sessions (RDP/PowerShell/Bash/AWS): requests, approvals, command records, AI summaries, audit trail	references/jump-gate.md
MCP Router	tanium_mcp_router_tools	MCP tool-call audit evidence export for administrators: caller and tool filters, a fixed time window, cursor pagination, and stored parameter and result evidence. For more information, see Export MCP tool-call audit data on page 26 .	references/mcp-router.md
Operational Technology	tanium_operational_technology_tools	OT/ICS device discovery, satellite-bound protocol access (EtherNet/IP, PROFINET), protocol-restriction workflows	references/operational-technology.md
Patch	tanium_patch_tools	OS-patch catalog and applicability (installed/missing/pending), deployments, ADCs, patch/block lists, maintenance windows, scan configuration	references/patch.md
Performance	tanium_performance_tools	Endpoint resource monitoring: alert monitors, monitored applications, process groups, single-endpoint CPU/memory summaries	references/performance.md
Platform	tanium_platform_tools	Tanium Server core API: packages and actions (run, schedule, approve, stop), computer/filter/action group targeting primitives, sensor and question reads, role-based access control (RBAC) and content sets, multi-org tenancy, server configuration	references/platform.md
Provision	tanium_provision_tools	Bare-metal OS imaging/refresh: OS bundles, PXE satellites, deployment inspection, ODJ	references/provision.md

©2026 Tanium Inc. All Rights Reserved

Toolset	Entry-point tool	Description	Reference resource
		pre-staging, device retirement (lock/wipe/ BitLocker freeze)	
Reporting	tanium_reporting_tools	Read-only access to the report and dashboard catalog and current report data	references/ reporting.md
Reputation	tanium_reputation_tools	File-hash verdict aggregation from VirusTotal, Recorded Future, ReversingLabs, WildFire, with custom verdict overrides	references/ reputation.md
Reveal	tanium_reveal_tools	Sensitive-data discovery in file content on managed endpoints: rule sets (PCI/HIPAA/ GDPR/CCPA), custom patterns, validations, profile deployment	references/ reveal.md
Screen Sharing	tanium_screen_sharing_tools	Observability for ScreenMeet remote-takeover sessions: audit trail, licensing, deployment status, alert thresholds	references/ screen-sharing.md
TDS	tanium_tds_tools	Sensor-data harvest/cache layer backing Reporting and Atlas: sensor registration, cache health, endpoint identity, on-demand queries across cached sensor data	references/ tds.md
Threat Response	tanium_threat_response_tools	Detection operations and threat-hunt inventory: alerts, intel docs/sources, detection profiles, quarantine/response configuration, Threat Navigator hunts	references/ threat-response.md
Zero Trust	tanium_zero_trust_tools	Drives Entra Conditional Access from endpoint posture through device extension attributes; read-only rule, posture, and audit access	references/zero-trust.md

©2026 Tanium Inc. All Rights Reserved