Tanium™ Direct Connect User Guide

Version 1.1.0

September 03, 2019

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

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

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

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

Table of contents

Direct Connect overview

Direct Connect provides a central location for configuring and administering all direct endpoint connections across Tanium modules. With Direct Connect, you can configure the connection settings that are shared by Tanium modules for establishing direct endpoint connections. Direct Connect manages the fully qualified domain name (FQDN) and port information that direct endpoint connections use, and generates and installs certificates that authenticate connections between endpoints and the Tanium Module Server.

Active endpoint sessions

You can review active endpoint connections across Tanium modules. Use active endpoint connections to see the active connections on the server.

Getting started

1. Install Tanium Direct Connect. For more information, see Installing Direct Connect on page 11.
2. Provide configuration settings for connecting to endpoints. For more information, see Set up Direct Connect on page 11.

Direct Connect requirements

Review the requirements before you install and use Direct Connect.

Tanium dependencies

In addition to a license for Direct Connect, make sure that your environment also meets the following requirements.

Component	Requirement
Platform	Version 7.2.314.2831 or later. For more information, see Tanium Core Platform Installation Guide: Installing Tanium Server.
Tanium Client	7.2.314.3211 or later
Tanium™ solutions that use the endpoint recorder	If you are using any of the following Tanium solutions that use the endpoint recorder, you must use the specified versions: • Tanium™ Integrity Monitor 1.7.0.0035 or later • Tanium™ Map 1.1.1.0006 or later • Tanium™ Threat Response 1.2.0.0037 or later • Tanium™ Trace 2.9.0.0035 or later

Tanium Module Server

Direct Connect is installed and runs as a service on the Module Server. The impact on the Module Server is minimal and depends on usage.

Endpoints

Direct Connect supports Windows, Linux, and macOS endpoints.

Host and network security requirements

Specific ports are needed to run Direct Connect.

Ports

The following ports are required for Direct Connect communication.

Component	Port	Direction	Purpose
Module Server	17475	Inbound	Connecting to the Module Server for direct connections to endpoints.

User role requirements

Use role-based access control (RBAC) permissions to restrict access to Direct Connect functions.

Table 1: Tanium Direct Connect User Role Privileges

Permission	Direct Connect Administrator	Direct Connect Read Only User	Direct Connect Service Account	Direct Connect User
Direct Connect API Read Allows viewing of the Direct Connect workbench	✓[1]	✓	✓[1]	✓[1]
Direct Connect API Write Perform operations using the API	✓[1]	✗	✓[1]	✓
Direct Connect Cron Exec Allows performing service account user work	✓	✗	✓	✗
Direct Connect Endpoint Config Read Allows viewing endpoint configuration settings	✓[1]	✓	✗	✓
Direct Connect Endpoint Config Write Allows modification of endpoint configuration settings	✓	✗	✗	✗

Permission	Direct Connect Administrator	Direct Connect Read Only User	Direct Connect Service Account	Direct Connect User
Direct Connect Endpoint Connect Allows creating and using endpoint connections	✓	✗	✗	✓
Direct Connect Logs Read Allows viewing logs	✓	✓	✗	✓
Direct Connect Service User Read Allows viewing the service account user	✓[1]	✓	✗	✓
Direct Connect Service User Write Allows modification of the service account user	✓	✗	✗	✗
Direct Connect Session Read Allows viewing endpoint connections	✓[1]	✓[1]	✓[1]	✓[1]
Direct Connect Session Write Allows managing endpoint connections	✓	✗	✗	✗

[1] Denotes a provided permission.

Table 2: Provided Advanced user role permissions for Tanium 7.1.314.3071 or later

Permission	Content Set for Permission	Direct Connect Administrator	Direct Connect Read Only User	Direct Connect Service Account	Direct Connect User
Read Sensor	Reserved	✓	✓	✗	✓

Permission	Content Set for Permission	Direct Connect Administrator	Direct Connect Read Only User	Direct Connect Service Account	Direct Connect User
Read Sensor	Base	✓	✗	✗	✓
Read Sensor	Direct Connect	✓	✓	✓	✓
Read Action	Direct Connect	✓	✓	✓	✓
Read Own Action	Direct Connect	✓[1]	✓[1]	✓[1]	✓[1]
Write Action	Direct Connect	✓	✗	✓	✓
Show Preview	Direct Connect	✓[1]	✗	✓[1]	✓[1]
Read Plugin	Direct Connect	✓[1]	✓[1]	✓[1]	✓[1]
Execute Plugin	Direct Connect	✓	✓	✓	✓
Read Package	Direct Connect	✓[1]	✓	✓[1]	✓[1]
Write Package	Direct Connect	✓	✗	✓	✓
Read Saved Question	Reserved	✓	✗	✓	✓
Read Saved Question	Base	✓	✗	✗	✗
Read Saved Question	Direct Connect	✓	✓	✓	✓

[1] Denotes a provided permission.

For more information and descriptions of content sets and permissions, see the Tanium Core Platform User Guide: Users and user groups.

Installing Direct Connect

You can install Direct Connect from the **Tanium Solutions** page.

Before you begin

- Read the Release Notes.
- Review the Direct Connect requirements on page 7.

Import Direct Connect

Import Direct Connect from the **Tanium Solutions** page.

1. In the **Tanium Content** section, select the **Direct Connect** row and click **Import Solution**.
2. In the **Content Import Preview** window, review the Tanium content that is being installed. Click **Import**.
3. After the installation process completes, refresh your browser.
4. From the Main menu, in the **Tanium Services** section, click **Direct Connect**. The Direct Connect **Home** page displays.

Verify installation

To verify that Direct Connect is installed, go to the **Supported Solutions** tab in the **Tanium Content** section of the **Tanium Solutions** page and check the **Imported Version**. To check the installed version from the Direct Connect **Home** page, click Info .

Set up Direct Connect

Configure the Direct Connect action group

The action group defines the set of endpoints to which you are deploying the Direct Connect packages. By default, the **Computer Group Targets** setting for the Direct Connect action group is set to **No Computers**. You can set the action group to **All Computers** or any computer groups that you have defined.

1. From the Direct Connect **Home** page, in the **Configuration** section, click the **Configure Action Group** step and click **Configure Action Group**.
2. Select the computer group for the group of endpoints that you want to use for Direct Connect. Click **Save**.

Configure service account

The Direct Connect service account runs background processes for the Direct Connect service. The credentials that you provide must be reconfigured after each upgrade of Direct Connect. The Direct Connect service account should have the **Direct Connect Cron Exec** permission.

1. From the Direct Connect **Home** page, in the **Configuration** section, click the **Configure Service Account** step and click **Configure Service Account**.
2. Enter the Tanium credentials and click **Save**.

> **Note:** You can also set or update the service account from the Direct Connect settings. Click Settings ⚙, and update the service account settings on the **Service Account** tab. Click **Save**.

Configure Endpoint Connection settings

Specify Endpoint Connection settings to define the domain name to use to connect to the Tanium Module Server, certificates to authenticate connections to the Tanium Module server and endpoints, and the port to use for connections.

1. From the Direct Connect **Home** page, in the **Configuration** section, click the **Configure Endpoint Connection** step and click **Configure Endpoint Connection**.
2. In the **FQDN** section, provide a domain name to use to connect to the Tanium Module server. The domain name that you provide must resolve to the Tanium Module Server from all endpoints in all direct endpoint connections. Direct Connect validates the name you provide to ensure the format. Verify the accuracy of the domain name you provide.
3. The **Port** is set to 17475 by default and cannot be modified. Make sure that incoming connections to this port are allowed by applicable firewall configurations.
4. In the **Server Certificate** section, the **Install a new certificate** option is selected by default and cannot be modified during the initial configuration. A certificate is generated and installed to authenticate the server when an endpoint starts a connection.

   After a certificate is installed on the server, the expiration date for the certificate displays. If a certificate is installed, you can select **Install a new certificate** to generate and install a new certificate.

5. In the **Client Certificate** section, the **Install a new certificate** option is selected by default and cannot be modified during the initial configuration. A certificate is generated, installed, and deployed to endpoints to authenticate that the endpoint is a Tanium client with permission to connect to the server.
   After a certificate is installed, the expiration date for the certificate displays. If a certificate is installed, you can select **Install a new certificate** to generate and install a new certificate.
6. Click **Save**.

If the **Fully Qualified Domain Name** validates successfully, success messages display:

```
The endpoint connection settings saved successfully.
Content build is in progress. Connection settings will deploy
to endpoints once complete.
```

If an error occurs, correct the fully qualified domain name and save again. If the information validates and saves successfully, packages for each supported operating system are created with the configuration information that is needed to use Direct Connect. These packages are distributed using a scheduled action to the Tanium Direct Connect action group.

Upgrade Direct Connect

Upgrade Direct Connect to the latest version from the **Tanium Solutions** page.

1. From the Main menu, click **Tanium Solutions**.
2. Locate Direct Connect and click **Upgrade to X.X.X.XX**.
3. Click **OK**.
   The Import Solution window opens with a list of all the changes and import options.
4. Click **Proceed with Import** and enter your password.
   The installation and configuration process begins.
5. To confirm the upgrade, return to the **Tanium Solutions** page and check the **Installed: X.X.X.XX** version for Direct Connect.

> **Tip:** If the Direct Connect version is not updated, refresh your browser window.

What to do next

See Getting started on page 6 for more information about using Direct Connect.

Reviewing active endpoint sessions

Use Direct Connect to gain visibility into all the connections between endpoints and the Tanium Module Server. The connections that Direct Connect displays are created by Tanium Modules that use direct connection capabilities.

1. From the Direct Connect menu, click **Active Endpoint Sessions**. All current sessions across Tanium modules display in the results grid.
2. The results grid displays these details for each active session:
   - **Host Name**: Endpoint computer name.
   - **Tanium Client ID**: Endpoint ID that is used for the connection.
   - **IP Address**: Endpoint IP Address.
   - **Action Status**: Current status of the `Open Session` action. Possible values are `Creating`, `Downloading`, `Running`, `Error`, `Succeeded`, `Not Succeeded`, `Complete`, or `Closed`.
   - **Session Status**: Current status of the session.
   - **Duration**: Time passed since the connection was first established from the endpoint.
   - **Last Message**: Time passed since the last message was received from the endpoint.

Troubleshooting Direct Connect

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

Collect logs

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

1. From the Direct Connect **Home** page, click Help, then the **Troubleshooting** tab.
2. Click **Collect**. When the status shows that the package is complete, click the **Download** link.
3. A ZIP file downloads to the local download directory.
4. Attach the ZIP file to your Tanium Support case form or send it to your TAM.

Uninstall Direct Connect

If you need to uninstall Direct Connect, first clean up the Direct Connect artifacts on endpoints and then uninstall Direct Connect from the server.

> **CAUTION:** Direct Connect is a shared service that is used by several Tanium solutions. If Direct Connect is in use by another Tanium solution, uninstalling Direct Connect or removing the tools from endpoints could have unintended consequences. Consult your TAM to determine whether uninstalling Direct Connect is advisable in your environment.

Remove Direct Connect content and tools from endpoints

Each operating system has its own remove action. Therefore, you must select a group of endpoints for cleanup that has the same operating system.

1. From the Main menu, click **Interact**.
2. Ask a question to target the endpoints from which you want to remove Direct Connect content and tools. For example, `Get Direct Connect - Tools Version from all machines`.
3. Select the row for the endpoints from which you want to remove the Direct Connect tools (either **Windows Package Installed**, **Mac Package Installed** or **Linux Package Installed**).

4. Click **Deploy Action**.
5. On the **Deploy Action** page, enter `Direct Connect - Remove` in the **Enter package name here** field.
6. Select the **Direct Connect - Remove Tools [*operating system*]** action, where *operating system* matches the operating system of the endpoints that you selected.
7. Click **Show preview to continue**.
8. A results grid displays at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

Remove the Direct Connect solution from the Tanium Module Server

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