Tanium™ Direct Connect User Guide

Version 1.10.41

October 14, 2021

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

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

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

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

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

Tanium is committed to the highest accessibility standards 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 and has most recently completed certification against the WCAG 2.1 / VPAT 2.3 standards for all major product modules in summer 2021. In the recent testing the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.1 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 best efforts to address any gaps quickly, as is feasible, given the severity of the issue and scope of the changes. These objectives are factored into the ongoing delivery schedule of features and releases with our existing resources.

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

Table of contents

Direct Connect overview

Direct Connect provides a communication channel for other Tanium™ modules and a central location for configuring and administering direct endpoint connections across modules.

With Direct Connect, you can configure the connection settings that are shared by Tanium modules for establishing direct endpoint connections. Since Direct Connect uses mutual authentication, both IP addresses and self-signed certificates are supported.

Active endpoint sessions

You can review open and pending endpoint sessions across Tanium modules. Use active endpoint connections to see the active connections on the server. For more information, see Reviewing active endpoint sessions.

Integration with other Tanium products

Tanium™ Client Management

Client Management uses Direct Connect to access client health information from endpoints. For more information, see Tanium Client Management User Guide: Monitoring client health in the Client Management service.

Tanium™ Enforce

Enforce encryption management policies use Direct Connect to transfer encryption keys securely from the client to the recovery key database during the encryption process. For more information see Enforce User Guide: Encryption management.

Tanium™ Performance

Use Direct Connect with Performance to view historical process-level data from a single endpoint for analysis and troubleshooting. For more information, see Performance User Guide: Connecting directly to endpoints.

Tanium™ Reveal

Reveal uses Direct Connect to view files on endpoints that match configured rules and patterns. For more information, see Reveal User Guide: Investigating rule matches and Reveal User Guide: Validating pattern matches.

Tanium™ Threat Response

Threat Response uses Direct Connect to connect to live endpoints and explore data. For more information, see Threat Response User Guide: Connecting to live endpoints and exploring data.

Getting started

Step 1: Install and configure Direct Connect

Install and configure Direct Connect, either through automatic configuration with default settings (Tanium Core Platform 7.4.2 or later only) or through manual configuration with custom settings.

For more information, see Installing Direct Connect on page 15.

Step 2: Configure a zone proxy

If you want to use Direct Connect with endpoints that connect to the Module Server through a Zone Server, you must configure a zone proxy.

For more information, see Configure Zone Proxies.

Direct Connect requirements

Review the requirements before you install and use Direct Connect.

Tanium dependencies

Component	Requirement
Tanium™ Core Platform	• 7.3.314.4250 or later • 7.4.1.1939 or later
Tanium™ Appliance	(Optional) If you are using a Tanium Appliance for your Zone Server, you must use Tanium operating system (TanOS) 1.5.2 or later. • For TanOS 1.5.2 - 1.5.4, you must use the TanOS shell to install the Direct Connect Zone Proxy. • For TanOS 1.5.5 and later, you can install the Direct Connect Zone Proxy through the Tanium Operations menu on the Zone Server appliance. For more information, see Appliance Deployment Guide: Install the Direct Connect Zone Proxy. To install the Direct Connect Zone Proxy on a Tanium Appliance with the All-in-One role, use the TanOS shell.
Tanium™ Client	Any supported version of Tanium Client. For the Tanium Client versions supported for each OS, see Tanium Client Management User Guide: 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.
Tanium™ solutions	If you clicked **Tanium Recommended Installation** when you installed Direct Connect, the Tanium Server automatically installed all your licensed solutions at the same time. Otherwise, you must manually install any other solutions you are using, as described under Tanium Console User Guide: Import, re-import, or update specific solutions. The following solution is required for features of Direct Connect to function. The given version is the minimum required: • Tanium™ Endpoint Configuration 1.2 or later (installed as part of Tanium™ Client Management 1.5 or later) The following solutions are optional: • Tanium™ Enforce • Tanium™ Performance The following solutions are optional, but Direct Connect requires the specified minimum versions to work with them: • 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 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

Supported internet protocols

Direct Connect supports only endpoints that have IPv4 addresses.

Supported operating systems

The following endpoint operating systems are supported with Direct Connect.

Operating System	Version	Notes
Windows	• Windows 7 Service Pack 1 or later • Windows Server 2008 R2 Service Pack 1 or later	Windows 7 Service Pack 1 requires Microsoft KB2758857.
macOS	Same as Tanium Client support. See Tanium Client Management User Guide: Client version and host system requirements.	
Linux	Same as Tanium Client support. See Tanium Client Management User Guide: Client version and host system requirements.	

Host and network security requirements

Specific ports and processes are needed to run Direct Connect.

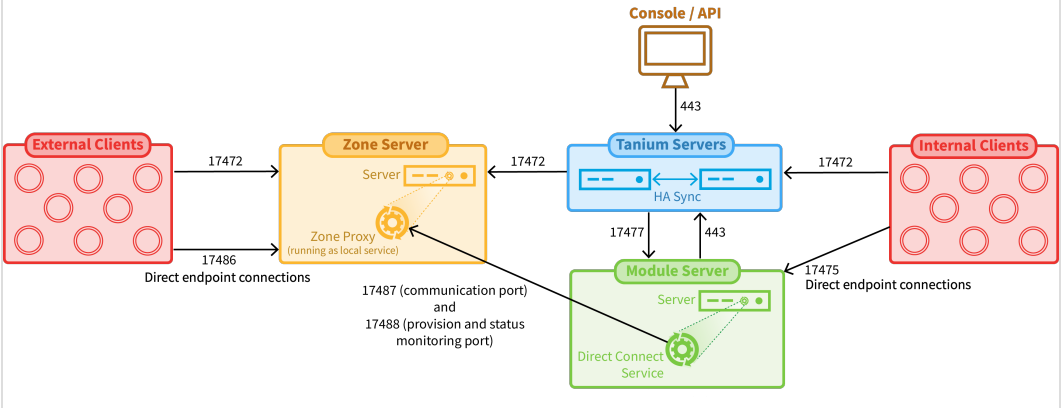
Ports

The following ports, which communicate over HTTPS using TLS 1.2 (RSA 2048-bit), are required for Direct Connect.

Source	Destination	Port	Protocol	Purpose
Tanium Client (internal)	Module Server	17475	TCP	Used by the Module Server for endpoint connections to internal clients.
Tanium Client (external)	Zone Server[1]	17486	TCP	Used by the Zone Server for endpoint connections to external clients. This port begins listening after the Zone Proxy provisioning process is complete on port `17488`. The default port number is `17486`. If needed, you can specify a different port number when you configure the zone proxy.

Source	Destination	Port	Protocol	Purpose
Module Server	Zone Server[1]	17487	TCP	Used by the Zone Server for Module Server connections. This port begins listening after the Zone Proxy provisioning process is complete on port `17488`. The default port number is `17487`. If needed, you can specify a different port number when you configure the zone proxy.
		17488	TCP	Used by the Module Server to provision the Zone Proxy on the Zone Server. After the Zone Proxy is provisioned, used for connection status and diagnostics. On TanOS, the Direct Connect Zone Proxy installer automatically configures the firewall on the Zone Server to open port `17488`. You must manually configure the firewall to open this port on Windows. This port number is not configurable.
Tanium Server	Module Server	17477	TCP	Tanium Server initiates connections to the Module Server on port `17477`.

[1] These ports are required only when you use a Zone Server.



Direct Connect supports the following cipher suites for encrypting information in TLS communication:

- `ECDHE-ECDSA-AES256-GCM-SHA384`
- `ECDHE-RSA-AES256-GCM-SHA384`
- `ECDHE-ECDSA-AES128-GCM-SHA256`
- `ECDHE-RSA-AES128-GCM-SHA256`
- `ECDHE-ECDSA-AES256-SHA384`
- `ECDHE-RSA-AES256-SHA384`
- `ECDHE-ECDSA-AES128-SHA256`
- `ECDHE-RSA-AES128-SHA256`

Security exclusions

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

Direct Connect security exclusions

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\direct-connect-service\node.exe`
		Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`
Zone Server		Process	`<Tanium Installation Directory>\Tanium Direct Connect Zone Proxy\node.exe`
Windows endpoints		Process	`<Tanium Client>\TaniumClientExtensions.dll`
		Process	`<Tanium Client>\TaniumClientExtensions.dll.sig`
		Process	`<Tanium Client>\extensions\TaniumDEC.dll`
		Process	`<Tanium Client>\extensions\TaniumDEC.dll.sig`
	7.2.*x* clients; requires SHA2 support to allow installation	Process	`<Tanium Client>\Python27\TPython.exe`
	7.4.*x* clients; requires SHA2 support to allow installation	Process	`<Tanium Client>\Python38\TPython.exe`
		Process	`<Tanium Client>\TaniumCX.exe`
	7.4.*x* clients	Folder	`<Tanium Client>\Python38`

Direct Connect security exclusions (continued)

Target Device	Notes	Exclusion Type	Exclusion
macOS endpoints		Process	`<Tanium Client>/libTaniumClientExtensions.dylib`
		Process	`<Tanium Client>/libTaniumClientExtensions.dylib.sig`
		Process	`<Tanium Client>/extensions/libTaniumDEC.dylib`
		Process	`<Tanium Client>/extensions/libTaniumDEC.dylib.sig`
	7.2.*x* clients	Process	`<Tanium Client>/python27/bin/pybin`
	7.4.*x* clients	Process	`<Tanium Client>/python38/bin/pybin`
		Process	`<Tanium Client>/TaniumCX`
Linux endpoints		Process	`<Tanium Client>/libTaniumClientExtensions.so`
		Process	`<Tanium Client>/libTaniumClientExtensions.so.sig`
		Process	`<Tanium Client>/extensions/libTaniumDEC.so`
		Process	`<Tanium Client>/extensions/libTaniumDEC.so.sig`
	7.2.*x* clients	Process	`<Tanium Client>/python27/bin/pybin`
	7.4.*x* clients	Process	`<Tanium Client>/python38/bin/pybin`
		Process	`<Tanium Client>/TaniumCX`

Zone Proxy server requirements

BEST PRACTICE Configure firewall policies to open ports for Tanium traffic with TCP-based rules instead of application identity-based rules. For example, on a Palo Alto Networks firewall, configure the rules with service objects or service groups instead of application objects or application groups.

If you want to use Direct Connect to connect to endpoints that route to the module server through a Zone Server, you must install and configure the Direct Connect Zone Proxy on that Zone Server. For more information, see Configure zone proxies.

IMPORTANT For best results, do not use a load balancer in front of your Zone Server. If you must use a load balancer, it must be configured for persistent TCP connections and the port that you configure in the Direct Connect Zone Proxy for the **Endpoint Inbound Port** must be open on the load balancer. By default, this port is `17486`.

User role requirements

The following tables list the role permissions required to use Direct Connect. To review a summary of the predefined roles, see Set up Direct Connect users on page 20.

For more information about role-based access control (RBAC), role permissions, and associated content sets, see Tanium Core Platform User Guide: Managing RBAC.

Direct Connect user role permissions

Permission	Direct Connect Administrator[1,2]	Direct Connect User[1]	Direct Connect Read Only User[1]	Direct Connect Service Account[2,3]	Direct Connect Endpoint Configuration Approver[1,2]
Direct Connect Cron Allows performing service account work	✗	✗	✗	✓ EXEC	✗
Direct Connect Endpoint Configuration Approve Endpoint Configuration items for Direct Connect	✗	✗	✗	✗	✓ APPROVE
Direct Connect Logs Access Direct Connect logs	✓ READ	✗	✗	✗	✗
Direct Connect Session Access endpoint connections	✓ READ WRITE	✓ READ WRITE	✓ READ	✗	✗
Direct Connect Settings Access Direct Connect settings	✓ READ WRITE	✗	✗	✗	✓ READ

Direct Connect user role permissions (continued)

Permission	Direct Connect Administrator[1,2]	Direct Connect User[1]	Direct Connect Read Only User[1]	Direct Connect Service Account[2,3]	Direct Connect Endpoint Configuration Approver[1,2]
Directconnect View the Direct Connect workbench	✓ SHOW	✓ SHOW	✓ SHOW	✗	✓ SHOW

[1] This role provides module permissions for Tanium Interact. You can view which Interact permissions are granted to this role in the Tanium Console. For more information, see Tanium Interact User Guide: Tanium Data Service permissions.

[2] This role provides module permissions for Tanium Endpoint Configuration. You can view which Endpoint Configuration permissions are granted to this role in the Tanium Console. For more information, see Tanium Endpoint Configuration User Guide: User role requirements.

[3] If you installed Tanium Client Management, Endpoint Configuration is installed, and by default, configuration changes initiated by the module service account (such as tool deployment) require approval. You can bypass approval for module-generated configuration changes by applying the **Endpoint Configuration Bypass Approval** permission to this role and adding the relevant content sets. For more information, see Tanium Endpoint Configuration User Guide: User role requirements.

Provided Direct Connect platform content permissions

Permission	Direct Connect Administrator	Direct Connect User	Direct Connect Read Only User	Direct Connect Service Account	Direct Connect Endpoint Configuration Approver
Action	✓ READ WRITE	✗	✗	✓ READ WRITE	✓ READ
Own Action	✓ READ	✗	✗	✓ READ	✓ READ
Package	✓ READ	✗	✗	✓ READ WRITE	✓ READ
Plugin	✓ READ	✓ READ	✓ READ	✓ READ EXECUTE	✓ READ

Provided Direct Connect platform content permissions (continued)

Permission	Direct Connect Administrator	Direct Connect User	Direct Connect Read Only User	Direct Connect Service Account	Direct Connect Endpoint Configuration Approver
Saved Question	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ
Sensor	✓ READ	✗	✗	✓ READ	✓ READ
You can view which content sets are granted to any role in the Tanium Console.					

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

Installing Direct Connect

Use the **Solutions** page to install Direct Connect and choose either automatic or manual configuration:

- **Automatic configuration with default settings** (Tanium Core Platform 7.4.2 or later only): Direct Connect 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 details about the automatic configuration for Direct Connect, see Import Direct Connect with default settings on page 15.
- **Manual configuration with custom settings**: After installing Direct Connect, you must manually configure required settings. Select this option only if Direct Connect requires settings that differ from the recommended default settings. For more information, see Import Direct Connect with custom settings on page 16.

Use the **Automatic configuration with default settings** option.

Before you begin

- Read the Release Notes.
- Review the Direct Connect requirements on page 7.
- If you are upgrading from a previous version, see Upgrade Direct Connect.
- Assign the correct roles to users for Direct Connect. Review the User role requirements on page 12.
    - To import the Direct Connect solution, you must be assigned the Administrator reserved role or a role that has the **Import Signed Content** permission.
    - To configure the Direct Connect action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Action Group** write permission.
- Determine if some endpoints connect to the Module Server through a Tanium™ Zone Server. To enable connections to endpoints through a Zone Server, you must configure a zone proxy after you import Direct Connect. For more information, see Configure zone proxies on page 21.

Import Direct Connect with default settings

(Tanium Core Platform 7.4.5 or later only) You can set the Direct Connect action group to target the **No Computers** filter group by enabling restricted targeting before importing Direct Connect. This option enables you to control tools deployment through scheduled actions that are created during the import and that target the Tanium Direct Connect action group. For example, you might want to test tools on a subset of endpoints before deploying the tools to all endpoints. In this case, you can manually deploy the tools to an action group that you configured to target only the subset. To configure an action group, see Tanium Console User Guide: Managing action groups. To enable or disable restricted targeting, see Tanium Console User Guide: Dependencies, default settings, and tools deployment.

When you import Direct Connect with automatic configuration, the following default settings are configured:

Setting	Default Value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group
Service account	The service account is set to the account that you used to import the module. Configuring a unique service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization. See Configure service account on page 18.
Fully Qualified Domain Name for the module server	The **Fully Qualified Domain Name** setting in the **Endpoint Connection** settings is set to the first-detected IPv4 address that is closest to the Tanium Server IP address. (This is often the IP address of the module server.) The IP address or FQDN that is specified for this setting must resolve to the Module Server from all endpoints in all direct endpoint connections. After the initial installation and configuration completes, you can verify this value on the **Endpoint Connection** tab in the **Direct Connect** settings and update it if needed.

To import Direct Connect and configure default settings, see Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed: see Verify Direct Connect version on page 17.

Import Direct Connect with custom settings

To import Direct Connect without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** check box while performing the steps in Tanium Console User Guide: Import, re-import, or update specific solutions. After the import, verify that the correct version is installed: see Verify Direct Connect version on page 17.

To configure the service account, see Configure service account on page 18.

To configure the Direct Connect action group, see Configure the Direct Connect action group on page 19.

To configure Endpoint Connection settings, see Configure Endpoint Connection settings on page 19.

To configure connection certificates, see Configure certificates on page 20.

Manage dependencies for Tanium solutions

When you start the Direct Connect workbench for the first time, the Tanium console ensures that all of the required dependencies for Direct Connect are installed at the required version. You must install all required Tanium dependencies before the Direct Connect workbench can load. A banner appears if one or more Tanium dependencies are not installed in the environment. The Tanium Console lists the required Tanium dependencies and the required versions.

1. From the Main menu, go to **Administration > Configuration > Solutions**.
2. Select the required solutions, click **Import Selected**, and then click **Begin Import**. When the import is complete, you are returned to the **Tanium Solutions** page.
3. From the Main menu, go to **Administration > Shared Services > Direct Connect** to open the Direct Connect **Overview** page after you import all of the required Tanium dependencies.

Upgrade Direct Connect

For the steps to upgrade Direct Connect, see Tanium Console User Guide: Import, re-import, or update specific solutions. After the upgrade, verify that the correct version is installed: see Verify Direct Connect version on page 17.

For the steps to upgrade a Direct Connect Zone Proxy, see Install or upgrade the Direct Connect Zone Proxy on page 22.

Verify Direct Connect version

After you import or upgrade Direct Connect, verify that the correct version is installed:

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

Configuring Direct Connect

If you did not install Direct Connect with the **Apply All Tanium recommended configurations**, you must enable and configure certain features. Additionally, if you want to enable connections to endpoints through a Tanium™ Zone Server, you must configure a zone proxy.

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 Configuration is installed as a part of Tanium Client Management. For more information, see the Tanium Client Management User Guide: Installing Client Management.

Additionally you can use Endpoint Configuration to manage configuration approval. For example, configuration changes are not deployed to endpoints until a user with approval permission approves the configuration changes in Endpoint Configuration. For more information about the roles and permissions that are required to approve configuration changes for Direct Connect, see User role requirements on page 12.

To use Endpoint Configuration to manage approvals, you must enable configuration approvals.

1. From the Main menu, go to **Administration > Shared Services > Endpoint Configuration** to open the Endpoint Configuration **Overview** page.
2. Click Settings and click the **Global** tab.
3. Select **Enable configuration approvals**, and click **Save**.

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

If you enabled configuration approvals, you must approve the deployment of Direct Connect tools in Endpoint Configuration before they deploy to endpoints.

Configure Direct Connect

Configure service account

The Direct Connect service account runs background processes for the Direct Connect service. This user requires the **Direct Connect Service Account** role. If you installed Tanium Client Management, Endpoint Configuration is installed, and by default, configuration changes initiated by the module service account (such as tool deployment) require approval. You can bypass approval for module-

generated configuration changes by applying the **Endpoint Configuration Bypass Approval** permission to this role and adding the relevant content sets. For more information, see Tanium Endpoint Configuration User Guide: User role requirements.

For more information about Direct Connect permissions, see User role requirements on page 12.

> NOTE
>
> If you imported Direct Connect with default settings, the service account is set to the account that you used to perform the import. Configuring a unique service account for each Tanium solution is an extra security measure to consider in consultation with the security team of your organization.

1. On the Direct Connect**Overview** page, click Settings and then click **Service Account** if needed.
2. Provide a user name and password, and then click **Save**.

Configure the Direct Connect action group

Importing the Direct Connect module automatically creates an action group to target specific endpoints. Select the computer groups to include in the Direct Connect action group.

> BEST PRACTICE
>
> Set the action group to **All Computers**, unless you want to block direct connections to some endpoints.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Click **Tanium Direct Connect**.
3. Select the computer groups 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.

Configure Endpoint Connection settings

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

1. From the Direct Connect**Home** page, click Settings and open the **Endpoint Connection** tab.
2. In the **Fully Qualified Domain Name** section, provide an IP address or FQDN to use to connect to the Module Server. The IP address or FQDN that you provide must resolve to the Module Server from all endpoints in all direct endpoint connections.
3. The **Port** is set to 17475 by default. If needed, you can modify this port. Make sure that incoming connections to this port are allowed by applicable firewall configurations.
4. In the **Action Lock** section, specify the behavior that you want for Direct Connect when action lock is enabled on endpoints:
   - **Block All Direct Connection Actions**
   - **Allow New Connections**
   - **Allow New Connections and Configuration Changes**

For more information about action locks, see Tanium Console User Guide: Managing action locks.

5. Click **Save**.

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

```
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.

Configure certificates

Configure certificates to authenticate connections to the Tanium Module server and endpoints.

1. From the Direct Connect**Home** page, click Settings and open the **Certificates** tab.
2. 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 is shown. If a certificate is installed, you can select **Renew** to renew the certificate.
3. 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 is shown. If a certificate is installed, you can select **Renew** to renew the certificate.
4. Click **Save**.
5. Enter your password and click **OK**.

Set up Direct Connect users

You can use the following set of predefined user roles to set up Direct Connect users.

To review specific permissions for each role, see User role requirements on page 12.

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

Direct Connect Administrator

Assign the **Direct Connect Administrator** role to users who manage the configuration and deployment of Direct Connect functionality to endpoints.

This role can perform the following tasks:

- Configure Direct Connect settings
- Test direct endpoint connections
- View own active endpoint sessions

Direct Connect User

Assign the **Direct Connect User** role to users who test direct endpoint connections and who can review their own active endpoint sessions.

Direct Connect Read Only User

Assign the **Direct Connect Read Only User** role to users who can only review their own active endpoint sessions.

Direct Connect Service Account

Assign the **Direct Connect Service Account** role to the account that performs background processes for Direct Connect. For more information, see Configure service account on page 18.

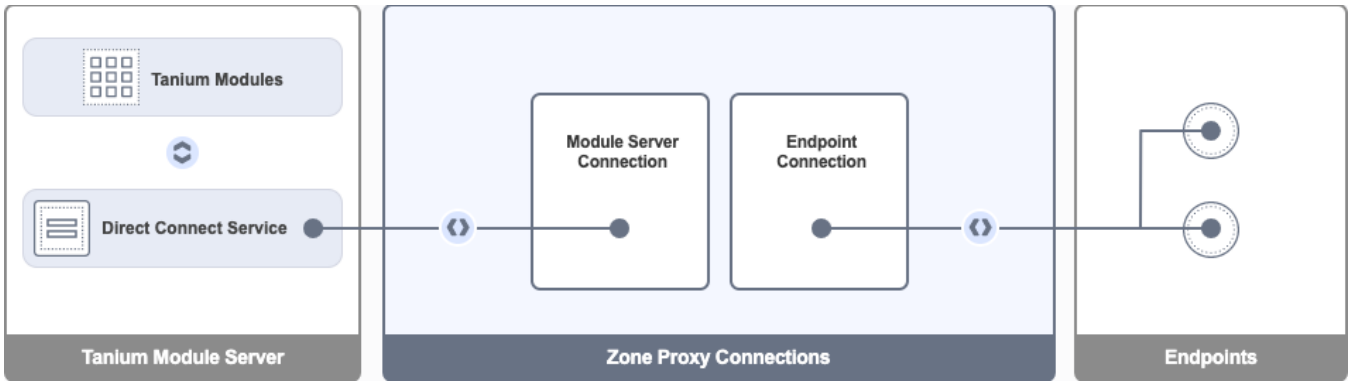
Direct Connect Endpoint Configuration Approver

Assign the **Direct Connect Endpoint Configuration Approver** role to a user who approves or rejects Direct Connect configuration items in Tanium Endpoint Configuration.

Configure zone proxies

You can optionally configure a zone proxy to enable connections to endpoints through a Zone Server. This configuration is required to use Direct Connect with endpoints that connect to the Module Server through a Zone Server.

Zone Proxy Server Overview



IMPORTANT For best results, do not use a load balancer in front of your Zone Server. If you must use a load balancer, it must be configured for persistent TCP connections and the port that you configure in the Direct Connect Zone Proxy for the **Endpoint Inbound Port** must be open on the load balancer. By default, this port is `17486`.

BEFORE YOU BEGIN

Contact Tanium Support to obtain the Direct Connect Zone Proxy Installer file for your Zone Server operating system. For more information, see Contact Tanium Support on page 30.

Confirm that all required ports are available. For more information, see Host and network security requirements.

INSTALL OR UPGRADE THE DIRECT CONNECT ZONE PROXY

1. Copy the Direct Connect Zone Proxy Installer to the Zone Server.
2. Run the Direct Connect Zone Proxy Installer on the Zone Server to install or upgrade the Direct Connect Zone Proxy.

   - You must use the TanOS shell to install the Direct Connect Zone Proxy on TanOS 1.5.2 - 1.5.4.
   - You can install the Direct Connect Zone Proxy through the Tanium Operations menu on the Zone Server appliance on TanOS 1.5.5 and later. For more information, see Appliance Deployment Guide: Install the Direct Connect Zone Proxy.
3. If you are performing initial installation of the Direct Connect Zone Proxy, copy the provision secret and certificate (known as the *provision payload*) for use in the configuration in Direct Connect.

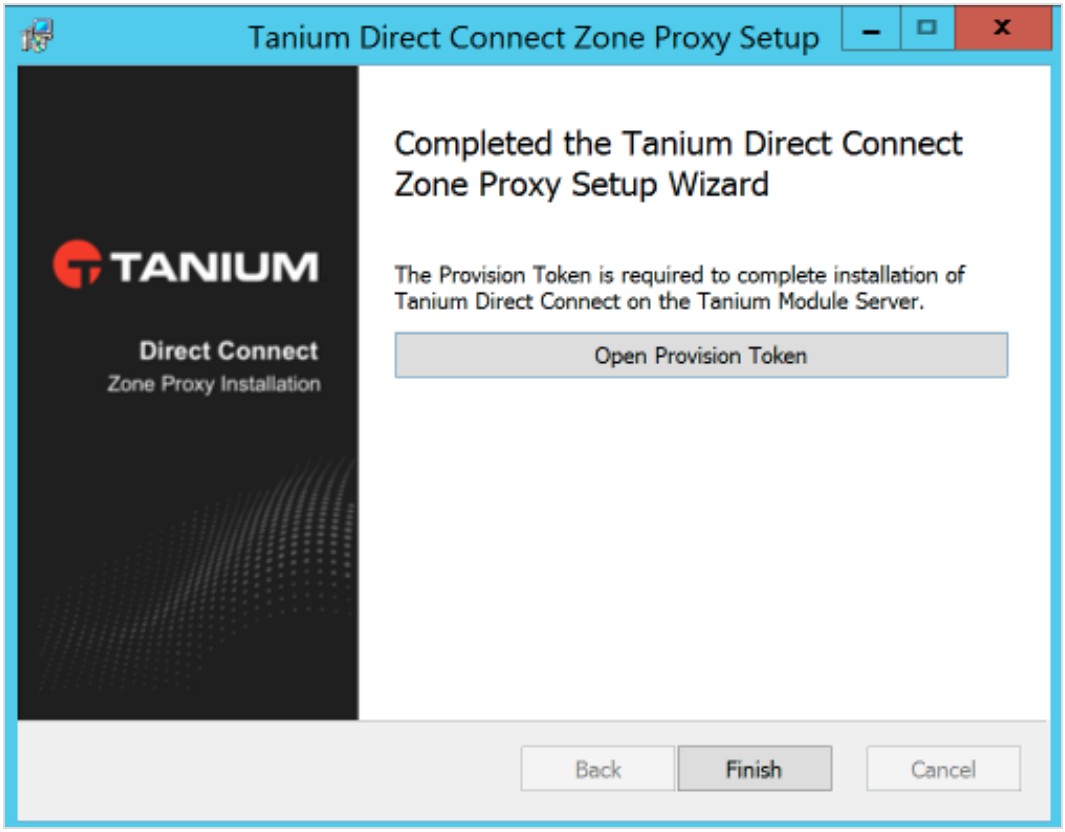
   The provision payload is stored in `provision.txt`, which is located in the following directories:

   - **TanOS**: *<Tanium Installation Directory>*`/TaniumDirectConnectZoneProxy/settings/PROVISION.txt`

     During the installation process on TanOS, the `Provision Secret` and `Certificate` also appear in the console where you run the installation. You can copy the `Provision Secret` and `Certificate` from the console or from the `PROVISION.txt` file.

- **Windows**: *<Tanium Install Directory>*\Tanium Direct Connect Zone Proxy\settings\PROVISION.txt

  At the end of the installation on Windows, click **Open Provision Token** to open PROVISION.txt. You can copy the Provision Secret and Certificate from this file.



Either copy these during the install or retrieve them from provision.txt for use during the subsequent configuration steps. For example:

```
-----BEGIN PROVISION SECRET-----
+EPQlEuUloBizbexjtshLuoxhNHA0JuMeOAEwFq/OKpEk6+jUJbFPx8Dol+vL22F
geNrd4/+wbsZwTgL3EUsqg==
-----END PROVISION SECRET-----
-----BEGIN CERTIFICATE-----
MIIC7TCCAdWgAwIBAgIgAwi2sO+h6dq/XIroZ1vK96/sHqxcMRWvkLXFrZrb5pAw
r3AxeSY2NpzDmVcQFNlYUhyR8QOr5hRE7AF9gGKDei6A
-----END CERTIFICATE-----
```

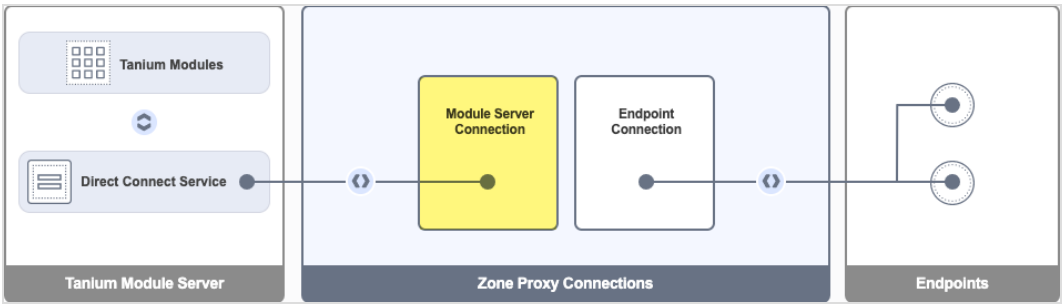
> NOTE
>
> The preceding figure is provided as an example of the `Provision Secret` and `Certificate` values to copy during the installation. The content is intentionally truncated and cannot be used as-is. You must use the values from your installation for the certificate pinning to work. If you use this example `Provision Secret` and `Certificate` in your environment, your configuration will fail.

To complete the configuration for an initial installation, return to Direct Connect. No further configuration is necessary during an upgrade.

CONFIGURE THE DIRECT CONNECT ZONE PROXY

After you complete the initial installation of a Direct Connect Zone Proxy, you must configure it in Direct Connect. This configuration is not necessary during an upgrade.

1. From the Direct Connect menu, click **Zone Proxies**.
2. Click **Add Zone Proxy**.
3. Specify the zone proxy **Name**.
4. Paste the `Provision Secret` and `Certificate` that you saved during the installation into the **Provision Payload** field.
5. Configure the **Module Server Connection**:



   a. Specify the **Zone Proxy Host**.

      This value is the host name or IP address that is used by the Module Server to connect to the Zone Server. It is the Zone Server's internal IP address, host name, or fully qualified domain name that can be resolved by the Module Server. For example, `DMZZoneServer.internal.local`.

   b. Specify the **Bind IP Address**.

      This value is the binding IP address that is used by the Zone Server for Module Server connections. It is the Zone Server's internal IP address that can be reached by the Module Server.

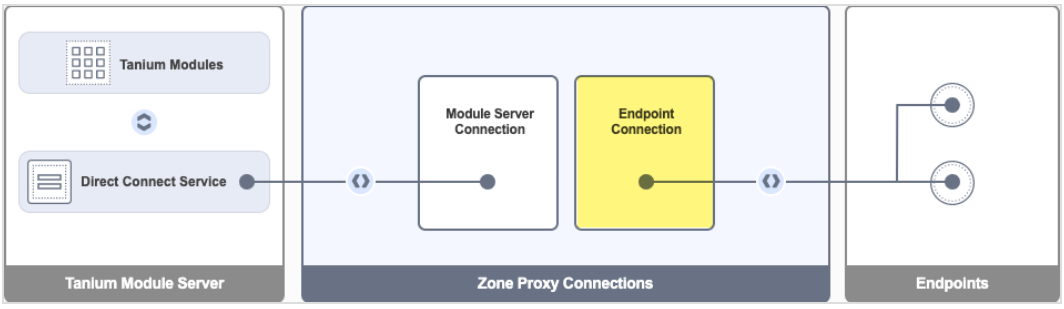
      Use this value to specify the IPv4 interface on the Zone Server to bind to for module server connections on multihomed servers. To listen on all interfaces, specify `0.0.0.0`.

      > NOTE
      >
      > In most environments, this value is not the same as the IP address of the Module Server.

c. Specify the **Port**.

This value is the binding port that is used by the Zone Server for module server connections. The default value is `17487`.

6. Configure the **Endpoint Connection**:



a. Specify the **Zone Proxy Host**.

This value is the host name or IP address that is used by endpoints to connect to the Zone Server. It is the Zone Server's external IP address or fully qualified domain name that can be resolved by endpoints. This value is a public, internet-routable IP address or host name. For example, `MyZoneServer.company.com`.

b. Specify the **Bind IP Address**.

This value is the binding IP address that is used by the Zone Server for endpoint connections. It is the Zone Server's external IP address that can be reached by endpoints. This value is a public, internet-routable IP address.

Use this value to specify the IPv4 interface on the Zone Server to bind to for endpoint connections on multihomed servers. To listen on all interfaces, specify `0.0.0.0`.

c. Specify the **Port**.

This value is the binding port that is used by the Zone Server for endpoint connections. The default value is `17486`.

7. Click **Save**.

8. Enter your password and click **OK**.

The status of the zone proxy shows in the **Status** column. When the configuration is complete, the status is **Connected**.

Due to the provisioning process, you cannot modify existing zone proxy configurations. If needed, you can delete the configuration and recreate it with different values. To delete a configuration, hover over the configuration and click **Delete**.

You can also see the status and activity for existing Zone Proxies from this page.

Reviewing active endpoint sessions

Use Direct Connect to gain visibility into your currently active connections between endpoints and the Module Server. The active connections list on the Direct Connect **Overview** page shows your current Direct Connect sessions across Tanium modules.

The active connections list does not include connections that other users initiated.

The grid shows details for each active session:

- **Computer Name**: Endpoint computer name.
- **Tanium Client ID**: Endpoint ID that is used for the connection.
- **IP Address**: Endpoint IP Address.
- **Direct Connect Proxy**: Name of the proxy server, if applicable.
- **Direct Connect 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.

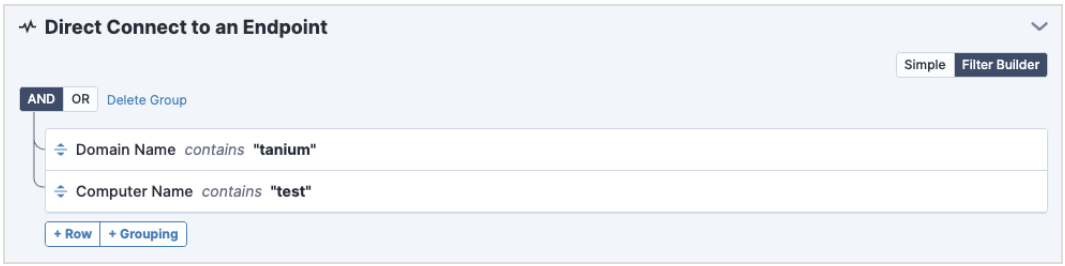
Testing direct endpoint connections

Use Direct Connect to test connections to endpoints without formally creating a connection. Test connections are a helpful tool to ensure that users of Tanium modules can make connections to endpoints and to troubleshoot connection issues if they occur.

Search for the endpoint in the **Direct Connect to an Endpoint** section of the Direct Connect **Home** page.

- To use the simple search, enter the IP address or Computer Name (exactly as it appears in the Computer Name sensor) for the endpoint to which you want to test a connection. Select the endpoint from the results.

- To use a filter, click **Filter Builder**. Build a query to search for the endpoint using advanced filters to filter question results based on match conditions.



  Click **+** and use the controls to add filter conditions:

  - **Add Row**: Add one or more conditions.
  - **Add Group**: Select this option to nest a Boolean operator and then use **Add Row** to build the nested expression.

If the test connection is unsuccessful, see Troubleshooting Direct Connect on page 28.

Troubleshooting Direct Connect

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

Generate a support package

Collect information about the current state of the Direct Connect service to use for troubleshooting. 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 **Generate Support Package**.
3. Click **Download Support Package** to download the ZIP file 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 30.

Change the logging level

If you need greater verbosity in the logs, you can change the log level.

1. From the Direct Connect **Home** page, click Help, then the **Troubleshooting** tab.
2. Adjust the **Log Level** as needed.
   Possible values are: **trace**, **debug**, **info** (default), **warn**, **error**, **fatal**.

> NOTE
> This update changes the log level for future logging. It does not affect the data that is available in the support package for previously logged events.

Troubleshoot endpoint connection issues

When you attempt an endpoint connection, Direct Connect iterates through the configured Tanium Servers or Zone Servers for an endpoint in this order until a successful connection occurs:

1. **LastGoodServerName** (if available)
2. The last server used for a successful connection
3. Server with the most successful connections
4. **ServerName** (if specified)
5. Any servers specified in the **ServerNameList**

For more information about **LastGoodServerName**, **ServerName**, and **ServerNameList**, see Tanium Client Management User Guide: Settings for connections to Tanium Core Platform servers.

If you are unable to establish an endpoint connection, check the status of the `Deploy Direct Connect - Open Session - operating system - session ID` action from the **Action History** page.

If the action ran, but was not successful, check the `<Tanium Client>/Logs/extensions0.txt` log on the endpoint. Make sure that the endpoint can connect to the Module Server using the **Fully Qualified Domain Name** and **Port** that you configured on the **Endpoint Connection** tab in the Direct Connect settings.

If the action did not run on the endpoint, make sure that the endpoint is a member of the Direct Connect action group and has the latest tools installed.

Troubleshoot connection issues through a zone proxy

To use Direct Connect with endpoints that connect to the Module Server through a Zone Server, you must install and configure the Direct Connect Zone Proxy. For more information, see Configure Zone Proxies.

If you are unable to establish an endpoint connection after installing and configuring the Direct Connect Zone Proxy, check the Direct Connect Zone Proxy log for errors: `<Tanium>/TaniumDirectConnectZoneProxy/logs/proxy.log`.

Remove Direct Connect tools from endpoints

You can deploy an action to remove Direct Connect tools from an endpoint or computer group. Separate actions are available for Windows and non-Windows endpoints.

1. In Interact, target the computers from which you want to remove the tools. For example, ask a question that targets a specific operating system:
   `Get Endpoint Configuration - Tools Status from all machines with Is <OS> equals True`, for example:
   `Get Endpoint Configuration - Tools Status from all machines with Is Windows equals True`
2. In the results, select the row for **Direct Connect**, drill down as necessary, and select the targets from which you want to remove Direct Connect tools. For more information, see Tanium Interact User Guide: Drill Down.
3. Click **Deploy Action**.
4. On the **Deploy Action** page, enter `Endpoint Configuration - Uninstall` in the **Enter package name here** box, and select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
5. For **Tool Name**, select **Direct Connect**.
6. (Optional) By default, after the tools are removed they cannot be reinstalled. To allow tools to be automatically reinstalled, clear the selection for **Block reinstallation**. Re-installation occurs almost immediately.

   NOTE

   If reinstallation is blocked, you must unblock it manually:

   - To allow Direct Connect to reinstall tools, deploy the **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]** package (depending on the targeted endpoints).

NOTE

- If you reinstall tools manually, select **Unblock Tool** when you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package.

7. (Optional) To remove all Direct Connect databases and logs from the endpoints, clear the selection for **Soft uninstall**.
8. (Optional) To also remove any tools that were dependencies of the Direct Connect tools that are not dependencies for tools from other solutions, select **Remove unreferenced dependencies**.
9. Click **Show preview to continue**.
10. 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**.

NOTE

If you have enabled Endpoint Configuration, tool removal must be approved in Endpoint Configuration before tools are removed from endpoints.

Uninstall Direct Connect

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. Contact support@tanium.com to determine whether uninstalling Direct Connect is advisable in your environment.

1. From the Main menu, go to **Administration > Configuration > Solutions**.
2. In the **Content** section, select the **Direct Connect** row.
3. Click Delete Selected and then click **Uninstall** to complete the process.

Contact Tanium Support

To contact Tanium Support for help, sign in to https://support.tanium.com.