Tanium™ Client Management User Guide

Version 1.6.195

March 03, 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 to make interaction with Tanium software more intuitive and to accelerate the time to success. To ensure high accessibility standards, Tanium complies with the U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. We have conducted third-party accessibility assessments over the course of product development for many years, and most recently a comprehensive audit against the WCAG 2.1 / VPAT 2.3 standards for all major product modules was completed in September 2019. 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

Client Management overview

With Client Management, you can rapidly deploy the Tanium™ Client to targeted sets of endpoints, and you can upgrade or reinstall existing clients as needed. You can also continuously monitor the health of all installed clients to help quickly identify, diagnose, and resolve issues with clients.

Client deployment

Deploy the Tanium™ Client to targeted sets of Windows, Linux, macOS, Solaris, or AIX endpoints.

Before you begin the deployment process, determine the set of endpoints that you are going to target. You can target by single IP, computer name, IP or CIDR range, or label that you defined in Tanium™ Discover.

To deploy clients, configure client settings and credentials. You can then use those configurations to create deployments, which are targeted at specific sets of unmanaged endpoints. The Tanium Module Server installs the Tanium Client on the targeted endpoints. Depending on the results, you can reuse the configurations to try deployments again or target different sets of endpoints.

If you are deploying the Tanium Client to endpoints that cannot be reached directly from the Tanium Module Server, such as those connected to a Zone Server, you can configure client settings, and then download and manually deploy an installation bundle.

Client settings

Configure client settings that are specific to a deployment. These settings include the version of the Tanium Client to deploy and the Tanium Server or Zone Server with which to associate the client. Client settings can also contain tags, which identify the endpoints after the client is installed.

Credentials

Configure a list of credentials that the Module Server uses to sign in to endpoints for installation of the Tanium Client. The Module Server attempts to sign in to each endpoint with each set of credentials in the order in which you defined them.

Deployments

Create and run a deployment that defines the targeted endpoints and deploys the Tanium Client to those endpoints. You can also choose whether to upgrade or reinstall existing clients that are in the targeted group.

Client health monitoring

After clients are installed, you can use Client Management to continuously monitor client health. Quickly identify outliers and issues by viewing aggregated information for clients on supported operating systems. Diagnose specific issues with Windows, Linux, and macOS clients by directly connecting and exploring

individualized client health information.

Integration with other Tanium products

Discover

You can apply labels to the unmanaged interfaces that are identified with Discover, and then you can target endpoints using those labels.

Trends

Client Management features Trends boards that provide data visualization of Client Management concepts, including successful and failed deployments, and the versions of the Tanium Client that were deployed. The following panels are in the **Tanium Client Management** board:

- Tanium Client versions deployed
- Tanium Client versions deployed - latest
- Successful installations
- Deployment failures

> **Note:** The **Successful installations** and **Deployment failures** panels apply only to deployment using Client Management.

For more information about how to import the Trends boards that Client Management provides, see Tanium Trends User Guide: Importing the initial gallery.

Getting started

1. Install and configure Tanium Client Management. For more information, see Installing Client Management on page 20.
2. Configure client configuration settings. These configurations define the properties of the clients that you want to install on the endpoint, including platform, client version, and the Tanium Server name. For more information, see Configure client settings on page 25.
3. Configure credentials. These credentials specify the user names and passwords that are required to install the clients. The priority of credentials defines the order to try each user name and password combination. For more information, see Configure client credentials on page 28.
4. Deploy Tanium Client. Specify settings for the deployment, including the configured client configuration and credentials settings. Target the endpoints on which you want to install the Tanium Client, schedule the deployment, and define the method you want to use to deploy. For more information, see Configure a deployment on page 29.
5. Monitor deployment results. View the results of the deployment, and re-deploy if necessary. For more information, see Deploy clients on page 31.
6. Monitor client health. View the status of deployed clients over time and maintain them as necessary. For more information, see Monitoring client health on page 34.

Client Management requirements

Review the requirements before you install and use Client Management.

Tanium dependencies

In addition to a license for Client Management, make sure that your environment meets the following requirements.

Component	Requirement
Tanium™ Core Platform	7.3 or later
Tanium™ Client	Client Management does not require a pre-existing installation of Tanium Client. Using client health features, including using Tanium™ Direct Connect to access detailed client health information, requires a supported Tanium Client. For the Tanium Client versions supported for each OS, see Tanium Client User Guide: Client version and host system requirements.
Tanium products	If you clicked **Install with Recommended Configurations** when you installed Client Management, the Tanium Server automatically installed all your licensed modules at the same time. Otherwise, you must manually install any other modules you are using, as described under Tanium Console User Guide: Manage Tanium modules. Client Management requires the given minimum versions to work with the following modules: • Tanium™ Interact 2.4.50 or later • Tanium™ Discover 3.1 or later (target endpoints based on Discover tags) • Tanium™ Trends 3.6 or later (view charts on the Client Management overview page) • Tanium Direct Connect 1.4.3 or later (connect to endpoints to access detailed client health information)

Note: Tanium™ Endpoint Configuration is automatically installed when you install Client Management 1.5 or later. You must upgrade Client Management to version 1.5 or later to support the latest versions of Tanium solutions that use Endpoint Configuration to deploy tools and configuration changes to endpoints. For more information about Endpoint Configuration, see Tanium Endpoint Configuration User Guide.

Tanium™ Module Server

Client Management is installed and runs as a service on the Module Server host computer. The impact on the Module Server is minimal and depends on usage.

For more information, see Tanium Core Platform Installation Guide: Host system sizing guidelines.

Endpoints

For a list of supported operating systems for the Tanium Client, see Tanium Client Guide: Host system requirements.

Supported operating systems

The following endpoint operating systems are supported with Client Management.

Operating System	Version
Microsoft Windows Server	2008 R2 with Service Pack 1 or later
Microsoft Windows Workstation	7 or later
macOS	Same as Tanium Client support. See Tanium Client User Guide: Host system requirements.
Linux	Same as Tanium Client support. See Tanium Client User Guide: Host system requirements. **Note:** Using Direct Connect to access detailed client health information on a CentOS client requires CentOS version 6.0 or later.
Solaris	Same as Tanium Client support. See Tanium Client User Guide: Host system requirements. **Note:** You cannot use Direct Connect to access detailed client health information with Solaris.
AIX	Same as Tanium Client support. See Tanium Client User Guide: Host system requirements. **Note:** You cannot use Direct Connect to access detailed client health information with AIX.

Account permissions

During client installation using Client Management, you must have an account configured with the appropriate permissions on each endpoint. You add credentials for these accounts during the deployment process. For more information, see Configure client credentials on page 28. These accounts and permissions are necessary only during deployment, and they can be removed or changed after you successfully deploy clients.

Tip: To protect credentials that are used for client deployment, use one of the following methods:

- Use a temporary account that is removed after deployment.
- Disable or change the password for the account after client deployment is complete.

WINDOWS ENDPOINTS

On each Windows endpoint, you must have an account with Local Administrator rights, or a local or domain account configured that has the following abilities:

- Remotely connect to the endpoint and authenticate using SMB.
- Create folders in the `C:\Program Files (x86)\` directory for 64-bit Windows, or the `C:\Program Files\` directory for 32-bit Windows.
- Write and execute files in the `C:\Program Files (x86)\Tanium\` directory for 64-bit Windows, or the `C:\Program Files\Tanium\` directory for 32-bit Windows.

NON-WINDOWS ENDPOINTS

On each non-Windows endpoint, you must have an account configured that can remotely connect to the endpoint and authenticate using SSH. You must use *one* of the following options to configure a user with elevated privileges to perform installation:

- The root user
- A user that is listed in the sudoers file on each endpoint, to allow the account you are using for installation to use **sudo**

  > **Note:** If you restrict user commands in the sudoers file, contact Tanium support to help determine the necessary commands to allow.

Amazon Linux requires key-based authentication. On the endpoint, be sure to enable SSH key-based authentication and enable `NOPASSWD` in the sudoers file for the admin user account. Add this user name and password to the credentials list. This configuration ensures that the key, and not a password, is used to elevate the admin permissions of the user so that the user can install the Tanium Client and start the service.

Other distributions or your specific environment might have different authentication requirements.

Host and network security requirements

Specific ports and processes are needed to run Client Management.

For information about preparing endpoints for remote installation, see Prepare for deployment to Linux, macOS, or UNIX endpoints on page 23 and Prepare for deployment to Windows endpoints on page 24.

Ports

The following ports are required for Client Management communication.

Source	Destination	Port	Protocol	Purpose
Module Server	Endpoints (non-Windows)	22	TCP	Used for SSH communication from the module server to the target endpoint during client installation.

Source	Destination	Port	Protocol	Purpose
Module Server	Endpoints (Windows)	135	TCP	Used for WMI communication from the module server to the target endpoint during client installation.
		445	TCP	Used for SMB communication from the module server to the target endpoint during client installation.
Tanium Client (internal)	Module Server	17475	TCP	Used for direct connection to endpoints for detailed client health information.
Tanium Client (external)	Zone Server[1]	17486	TCP	Used for direct connection to endpoints for detailed client health information. The default port number is `17486`. If needed, you can specify a different port number when you configure the Zone Proxy.
Module Server	Zone Server[1]	17487	TCP	Used by the Zone Server for Module Server connections. The default port number is `17487`. If needed, you can specify a different port number when you configure the Zone Proxy.
		17488	TCP	Allows communication between the Zone Server and the Module Server. On TanOS, the Direct Connect Zone Proxy installer automatically opens port `17488` on the Zone Server. This port must be manually opened on Windows.

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

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.

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.

The *<Tanium Client>* variable refers to the Tanium Client installation path, which is configurable during client deployment. For default client installation paths, see Tanium Client User Guide: Tanium Client installation paths.

The *<Module Server>* variable refers to the Tanium Module server installation path.

Note: Security exclusions for the Tanium Core Platform are also required to install Tanium clients using Client Management. For a list of these exclusions, see Tanium Core Platform Deployment Reference Guide: Tanium Core Platform folders and Tanium Core Platform Deployment Reference Guide: Tanium Core Platform system processes.

Client Management security exclusions

Target Device	Notes	Process
Module Server		*<Module Server>*\services\client-management-service\node.exe
		<Module Server>\services\twsm-v1\twsm.exe
Windows x86 endpoints	During client installation	\Program Files\Tanium\TaniumClientBootstrap.exe
	During client installation	\Program Files\Tanium\SetupClient.exe
	During client installation	*<Tanium Client>*\SetupClient.exe
		<Tanium Client>\TaniumClientExtensions.dll
		<Tanium Client>\TaniumClientExtensions.dll.sig
		<Tanium Client>\extensions\TaniumDEC.dll
		<Tanium Client>\extensions\TaniumDEC.dll.sig
		<Tanium Client>\TaniumCX.exe
Windows x64 endpoints	During client installation	\Program Files (x86)\Tanium\TaniumClientBootstrap.exe
	During client installation	\Program Files (x86)\Tanium\SetupClient.exe
	During client installation	*<Tanium Client>*\SetupClient.exe
		<Tanium Client>\TaniumClientExtensions.dll
		<Tanium Client>\TaniumClientExtensions.dll.sig
		<Tanium Client>\extensions\TaniumDEC.dll
		<Tanium Client>\extensions\TaniumDEC.dll.sig
		<Tanium Client>\TaniumCX.exe

Client Management security exclusions (continued)

Target Device	Notes	Process
macOS endpoints	During client installation	/Library/Tanium/TaniumClientBootstrap
	During client installation	/Library/Tanium/SetupClient
	During client installation	<*Tanium Client*>/SetupClient
		<*Tanium Client*>/libTaniumClientExtensions.dylib
		<*Tanium Client*>/libTaniumClientExtensions.dylib.sig
		<*Tanium Client*>/extensions/libTaniumDEC.dylib
		<*Tanium Client*>/extensions/libTaniumDEC.dylib.sig
		<*Tanium Client*>/TaniumCX
Linux endpoints	During client installation	/opt/Tanium/TaniumClientBootstrap
	During client installation	/opt/Tanium/SetupClient
	During client installation	<*Tanium Client*>/SetupClient
		<*Tanium Client*>/libTaniumClientExtensions.so
		<*Tanium Client*>/libTaniumClientExtensions.so.sig
		<*Tanium Client*>/extensions/libTaniumDEC.so
		<*Tanium Client*>/extensions/libTaniumDEC.so.sig
		<*Tanium Client*>/TaniumCX
Solaris and AIX endpoints	During client installation	/opt/Tanium/TaniumClientBootstrap
	During client installation	/opt/Tanium/SetupClient
	During client installation	<*Tanium Client*>/SetupClient

Internet URLs

If security software is deployed in the environment to monitor and block unknown URLs, your security administrator might need to add the following URL to the approved list.

- https://content.tanium.com

User role requirements

The following tables list the role permissions required to use Client Management. For more information about role permissions and associated content sets, see Tanium Core Platform User Guide: Managing RBAC.

> **Note:** To install Client Management, you must have the **Import Signed Content** micro admin permission (Tanium Core Platform 7.4 or later) or the reserved role of Administrator.

Client Management user role permissions

Permission	Client Management Administrator[1]	Client Management User[1]	Client Management API User	Client Management Auditor	Client Management Operator	Client Management Read-Only User[1]
Show Clientmanagement View the Client Management workbench	✓	✓	✓	✓	✓	✓
Client-management Configurations Read Read client and deployment configurations	✓	✓	✗	✗	✗	✓
Client-management Configurations Write Create and modify client and deployment configurations	✓	✗	✗	✗	✗	✗
Client-management Credentials Read Read credentials list, but not view associated passwords or key data	✓	✓	✗	✗	✗	✓

Client Management user role permissions (continued)

Permission	Client Management Administrator[1]	Client Management User[1]	Client Management API User	Client Management Auditor	Client Management Operator	Client Management Read-Only User[1]
Client-management Credentials Write Create and modify credentials lists	✓	✗	✗	✗	✗	✗
Client-management Deployments Read View data about client deployments	✓	✓	✗	✗	✗	✓
Client-management Deployments Write Create deployments of Tanium Client to unmanaged endpoints	✓	✓	✗	✗	✗	✗
Client-management Direct Connect Connect to an endpoint using Direct Connect and read data from that endpoint	✓	✗	✗	✗	✓	✗
Client-management Settings Write Write access to global settings in the Client Management module	✓	✗	✓	✗	✗	✗
Client-management Read Audit Log Read audit log with API	✓	✗	✗	✓	✗	✗

Client Management user role permissions (continued)

Permission	Client Management Administrator[1]	Client Management User[1]	Client Management API User	Client Management Auditor	Client Management Operator	Client Management Read-Only User[1]
Client-management Use API Write access to global settings in the Client Management module	✓	✗	✓	✗	✗	✗
Direct Connect Session Read Allows users to view endpoint connections	✓	✗	✗	✗	✓	✗
Direct Connect Session Write Allows users to create and manage endpoint connections	✓	✗	✗	✗	✓	✗

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

Provided Client Management Micro Admin and Advanced user role permissions

Permission	Role Type	Content Set for Permission	Client Management Administrator	Client Management User	Client Management API User	Client Management Auditor	Client Management Operator	Client Management Read-Only User
Read System Status	Micro Admin		✓	✗	✗	✗	✓	✗
Read Sensor	Advanced	Tanium Client Management	✓	✓	✓	✓	✓	✓
Read Sensor	Advanced	Reserved	✓	✓	✓	✓	✓	✓
Read Sensor	Advanced	Base	✓	✓	✓	✓	✓	✓
Read Sensor	Advanced	Client Extensions	✓	✓	✓	✓	✓	✓

Provided Client Management Micro Admin and Advanced user role permissions (continued)

Permission	Role Type	Content Set for Permission	Client Management Administrator	Client Management User	Client Management API User	Client Management Auditor	Client Management Operator	Client Management Read-Only User
Read Sensor	Advanced	Direct Connect	✓	✗	✗	✗	✓	✗
Read Action	Advanced	Reserved	✓	✗	✗	✗	✓	✗
Read Action	Advanced	Direct Connect	✓	✗	✗	✗	✓	✗
Write Action	Advanced	Reserved	✓	✗	✗	✗	✓	✗
Write Action	Advanced	Direct Connect	✓	✗	✗	✗	✓	✗
Execute Plugin	Advanced	Tanium Client Management	✓	✓	✓	✓	✓	✓
Execute Plugin	Advanced	Reserved	✓	✓	✓	✗	✗	✓
Read Package	Advanced	Reserved	✓	✗	✗	✗	✓	✗
Read Package	Advanced	Direct Connect	✓	✗	✗	✗	✓	✗
Write Package	Advanced	Reserved	✓	✗	✗	✗	✓	✗
Write Package	Advanced	Direct Connect	✓	✗	✗	✗	✓	✗
Read Saved Question	Advanced	Tanium Client Management	✓	✓	✓	✓	✓	✓
Read Saved Question	Advanced	Reserved	✓	✓	✓	✗	✓	✓
Read Saved Question	Advanced	Direct Connect	✓	✗	✗	✗	✓	✗
Read Filter Group	Advanced	Tanium Client Management	✓	✓	✓	✓	✓	✓
Read Filter Group	Advanced	Reserved	✓	✓	✓	✓	✓	✓
Read Filter Group	Advanced	Default Filter Groups	✓	✓	✓	✓	✓	✓

Optional roles for Client Management

Role	Enables
Discover Read Only User	For service account: Deploy to endpoints based on Discover labels

For more information and descriptions of content sets and permissions, see Tanium Core Platform User Guide: Managing roles.

Installing Client Management

Use the **Tanium Solutions** page to install Client Management and choose either automatic or manual configuration:

- **Automatic configuration with default settings** (Tanium Core Platform 7.4.2 or later only): Client Management 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 Client Management, see Import and configure Client Management with default settings on page 20.
- **Manual configuration with custom settings**: After installing Client Management, you must manually configure required settings. Select this option only if Client Management requires settings that differ from the recommended default settings. For more information, see Import and configure Client Management with custom settings on page 20.

Endpoint Configuration is automatically installed when you install Client Management. For more information about Endpoint Configuration, see Tanium Endpoint Configuration User Guide.

Before you begin

- Read the release notes.
- Review the Client Management requirements on page 9.
- Assign the correct roles to users for Client Management. Review the User role requirements on page 15. To import the Client Management solution, you must be assigned the Administrator reserved role.

Import and configure Client Management with default settings

When you import Client Management with automatic configuration, the Client Management service account is set to the account that you used to import the module.

To import Client Management and configure default settings, be sure to select the **Apply Tanium recommended configurations** check box while performing the steps in Tanium Console User Guide: Manage Tanium modules. After the import, verify that the correct version is installed: see Installing Client Management on page 20.

Import and configure Client Management with custom settings

To import Client Management without automatically configuring default settings, follow the steps in Tanium Console User Guide: Manage Tanium content packs. After the import, verify that the correct version is installed: see Installing Client Management on page 20.

Configure service account

The service account is a user that runs several background processes for Client Management. This user requires the following roles and access:

- **Content Administrator** and **Tanium Client Administrator**, or **Tanium Administrator**
- (Optional) **Discover Read Only User** role, to deploy to endpoints based on labels created in Tanium Discover

For more information about Client Management permissions, see User role requirements on page 15.

1. From the Main menu, click **Administration > Shared Services > Client Management** to open the Client Management **Home** page.
2. Click Settings and open the **Service Account** tab.
3. Update the service account settings and click **Save**.

Verify installation

To verify that Client Management is installed, go to the **Tanium Solutions** page and check the installed version.

(Tanium 7.2.x, 7.3.x only) Upload Tanium public key

If you are using Tanium Server 7.2.x or 7.3.x, upload the Tanium public key. This public key enables the connection between the clients you are installing and the Tanium Server. This configuration occurs automatically with Tanium Server 7.4 and later.

1. From the Client Management home page, click Settings.
2. Click **Choose File** and select the `tanium.pub` file for your Tanium Server. The `tanium.pub` file is in the top-level installation directory for the Tanium Server.
3. Click **Upload**.

Add client installation files for air-gapped environments

If you cannot enable communication between your Tanium Module Server and content.tanium.com, contact Tanium Support for help with configuring client installers on the Tanium Module Server.

What to do next

See Getting started on page 8 for more information about using Client Management.

Deploying Tanium Client

To deploy Tanium Client to unmanaged endpoints, configure your endpoints to accept connections from the Module Server. Create sets of client settings and credentials to define the types of clients to deploy and the information that is needed to log into the endpoints to perform the installations. Finally, use these configurations to create a deployment that targets a specific set of endpoints.

> **Note:** When you use Client Management to deploy the Tanium Client to endpoints, Client Management also installs Client Management tools on the endpoints to provide client health information. For more information, see Monitoring client health on page 34.

Plan deployment targeting

You can deploy the Tanium Client to a single IP address or computer name, an IP or CIDR range, or a Discover label.

If you want to deploy to unmanaged interfaces that get defined in Discover, you can create a label and use the label as a deployment target. For example, you might create a `New Computers` label with the condition: `First Seen in the last 30 minutes AND Computer Id = "0"`. For more information about creating labels in Discover, see Tanium Discover User Guide: Labels.

If you are deploying the Tanium Client to endpoints that cannot be reached directly from the Tanium Module Server, such as those connected to a Zone Server, you can configure client settings, and then download and manually deploy an installation bundle.

Upgrade or reinstall the Tanium Client

By default, a deployment installs the Tanium Client only on unmanaged endpoints and ignores any endpoints where the client is already installed. However, you can also configure the deployment to reinstall or upgrade the client.

Configure a deployment to upgrade existing clients if you want to install the version that you specify in client settings on any endpoint where an earlier version is currently installed. You can optionally disable new installations if you want *only* to upgrade existing client installations.

Configure a deployment that reinstalls existing clients to repair disabled or corrupt clients. With the default selections for advanced options, the deployment reinstalls clients only on endpoints where the client is not communicating properly with the Tanium Server and where the currently installed version is earlier than or the same as the version that you configure in client settings. Any data that the client has collected is also left in place. However, you can configure the deployment to reinstall the client even if it is currently communicating with the server, or to wipe all data before reinstallation. If you configure the deployment to

wipe data, the version that you are deploying replaces *any* existing version, since the deployment first removes any version of the client found on the endpoint. You can also optionally disable new installations if you want *only* to reinstall existing clients.

Prepare for deployment to Linux, macOS, or UNIX endpoints

1. Configure password-based or SSH key-based authentication based on the authentication requirements on the endpoints.

   On each non-Windows endpoint, you must have an account configured that can remotely connect to the endpoint and authenticate using SSH. You must use *one* of the following options to configure a user with elevated privileges to perform installation:

   - The root user
   - A user that is listed in the sudoers file on each endpoint, to allow the account you are using for installation to use **sudo**

     > **Note:** If you restrict user commands in the sudoers file, contact Tanium support to help determine the necessary commands to allow.

   Amazon Linux requires key-based authentication. On the endpoint, be sure to enable SSH key-based authentication and enable `NOPASSWD` in the sudoers file for the admin user account. Add this user name and password to the credentials list. This configuration ensures that the key, and not a password, is used to elevate the admin permissions of the user so that the user can install the Tanium Client and start the service.

   Other distributions or your specific environment might have different authentication requirements.
2. Allow traffic from the Module Server to endpoints on TCP port 22 (SSH port, configurable), and allow SFTP access. For more information, see Host and network security requirements on page 11
3. Configure any host-based firewalls or other security tools on the endpoint that might interfere with a remote installation that is initiated through SSH. For more information, see Host and network security requirements on page 11.
4. If you use the root account to install, make sure the sshd_config allows root login.
5. Verify that you can log in to the remote system with SSH, using the same credentials that you will use for the Tanium Client deployment.

> **Tip:** To protect credentials that are used for client deployment, use one of the following methods:
>
> - Use a temporary account that is removed after deployment.
> - Disable or change the password for the account after client deployment is complete.

Prepare for deployment to Windows endpoints

1. Configure local or domain accounts with the necessary permissions.

   On each Windows endpoint, you must have an account with Local Administrator rights, or a local or domain account configured that has the following abilities:

   - Remotely connect to the endpoint and authenticate using SMB.
   - Create folders in the `C:\Program Files (x86)\` directory for 64-bit Windows, or the `C:\Program Files\` directory for 32-bit Windows.
   - Write and execute files in the `C:\Program Files (x86)\Tanium\` directory for 64-bit Windows, or the `C:\Program Files\Tanium\` directory for 32-bit Windows.

2. Enable Windows file-and-print sharing and administrative shares on the target endpoint, and make sure the Windows Management Instrumentation (WMI) service is enabled and started.

   > **Tip:** Enabling these settings and services is required only for installation. You can disable sharing and WMI as needed after the installation.

3. Configure any host-based firewalls or other security tools on the endpoint that might interfere with WMI, which uses port 135, or file sharing, which uses port 445. For more information, see Host and network security requirements on page 11.

4. Allow TCP traffic on ports 135 and 445 from the Tanium Module Server host computer to the endpoints on which you want to deploy the Tanium Client. For more information, see Host and network security requirements on page 11.

5. If you are using a non-default Administrator account and the machine is not joined to a domain, edit the Windows registry to disable User Account Control (UAC) remote restrictions, which normally prevent access to administrative shares and remote installations under these conditions. To disable UAC remote restrictions, add the following registry value and restart the machine:

   ```
   Subkey: HKEY_LOCAL_
   MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
   Data type: REG_DWORD
   Value name: LocalAccountTokenFilterPolicy
   Value data: 1
   ```

   > **Note:** If you use the default local Administrator account, you do not need to make this registry change.

   > **IMPORTANT:** Administrative shares are not available in Home editions of Windows operating systems.

6. Verify that you can log in to the remote system `wmic` and `net use` commands with the same credentials that you will use for the Tanium Client deployment. For example:

- **Port 135:** `wmic /node:"192.168.1.130" /user:"Administrator" useraccount list brief`
- **Port 445:** `net use p: \\192.168.1.130\C$ password /user:Administrator`

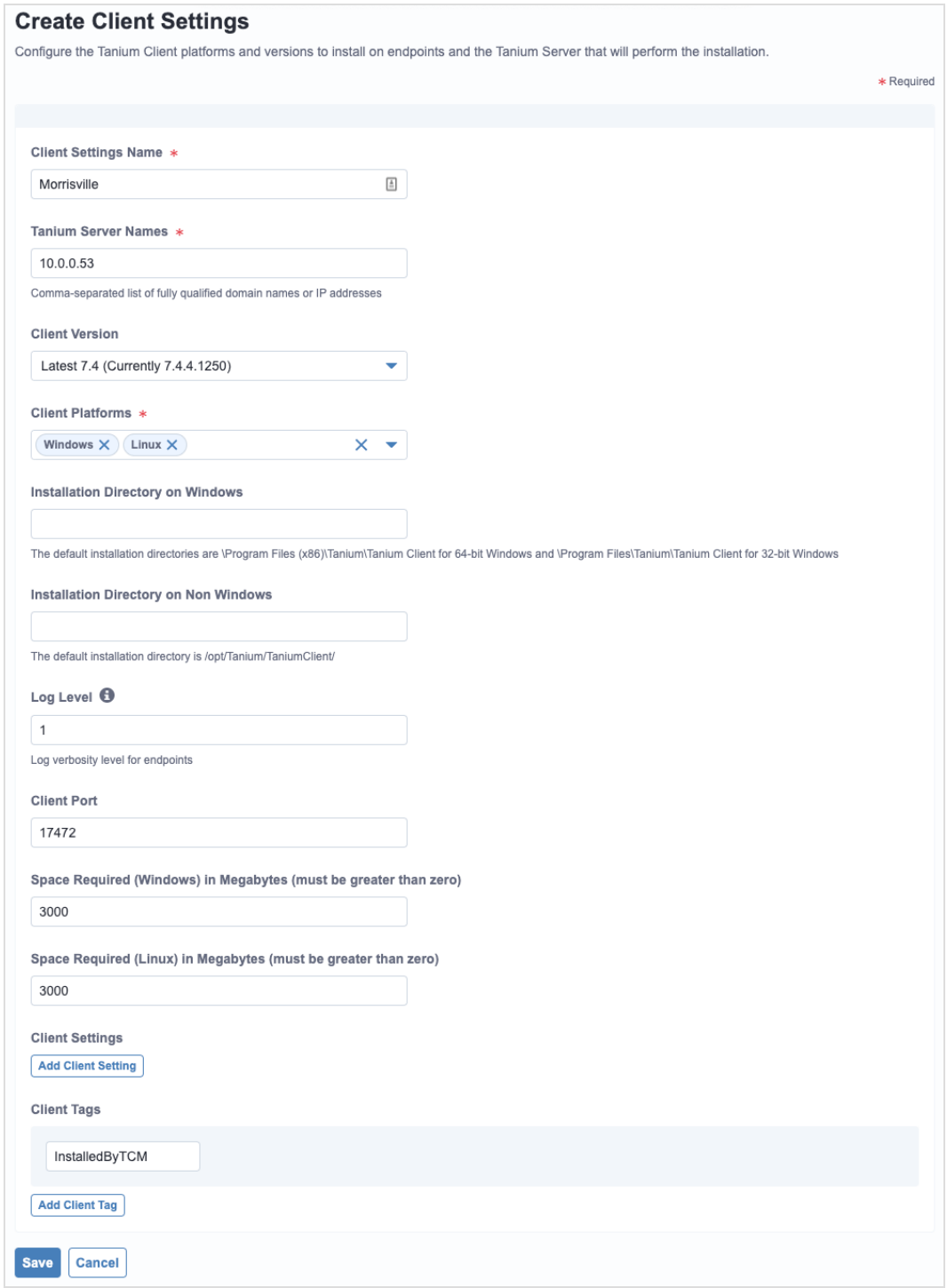
Tip: To protect credentials that are used for client deployment, use one of the following methods:

- Use a temporary account that is removed after deployment.
- Disable or change the password for the account after client deployment is complete.

Configure client settings

Client settings define the Tanium Server, platforms, and installation directories for your client deployment. You can configure multiple client settings to deploy to different types of environments.

1. From the Client Management menu, click **Client Settings**, and then click **Create**.
2. Specify a descriptive name for the client settings.
3. Specify the IP address or fully qualified domain name of the Tanium Server. In high-availability deployments and deployments with Zone Servers, you can enter a comma-separated list of all servers, such as: `ts1.example.com,ts2.example.com,zs1.example.com`.



> **Note:** The Tanium Module Server must have a connection to endpoints in order to automatically deploy the Tanium Client using Client Management. If you are deploying the Tanium Client to endpoints that cannot be reached directly from the Tanium Module Server, such as those connected to a Zone Server, you can download and manually deploy an installation bundle. For more information, see Download and deploy the installation bundle on page 33.

4. Select the **Client Version** to install.
5. Select the **Client Platforms** of the endpoints to which you are installing Tanium Client. You can leave the installation directories as their default values, or specify custom installation directories.
6. Leave the installation directories blank to use the defaults, or enter a custom **Installation Directory on Windows** or **Installation Directory on Non Windows**.

   > **Note:** You cannot customize the installation directory on macOS. The fixed installation directory for macOS is `/Library/Tanium/TaniumClient`.

7. Enter a **Log Level**.
   The following decimal values are best practices for specific use cases:
   - `0`: Disable logging. This is the best practice value for clients installed on sensitive endpoints or virtual desktop infrastructure (VDI) endpoints.
   - `1`: This is the best practice value during normal operation.
   - `41`: This is the best practice value during troubleshooting.
   - `91` or higher: Enable the most detailed log levels for short periods of time only.
8. Leave the default **Server Port**, or enter a custom port.
9. In the **Space Required** for each operating system, enter the space that should be available on a targeted endpoint for the client to be installed.
10. To change a default client settings, click **Add Client Setting**, and then enter a **Key** and **Value**. For information about specific client settings, see Tanium Client User Guide: Tanium Client settings.
11. To add a custom tag to the client during deployment, click **Add Client Tag** and enter a tag name. The `InstalledByTCM` tag is included by default so that you can later easily target clients that were installed using Client Management.

    > **Note:** Do not include spaces in a tag name.

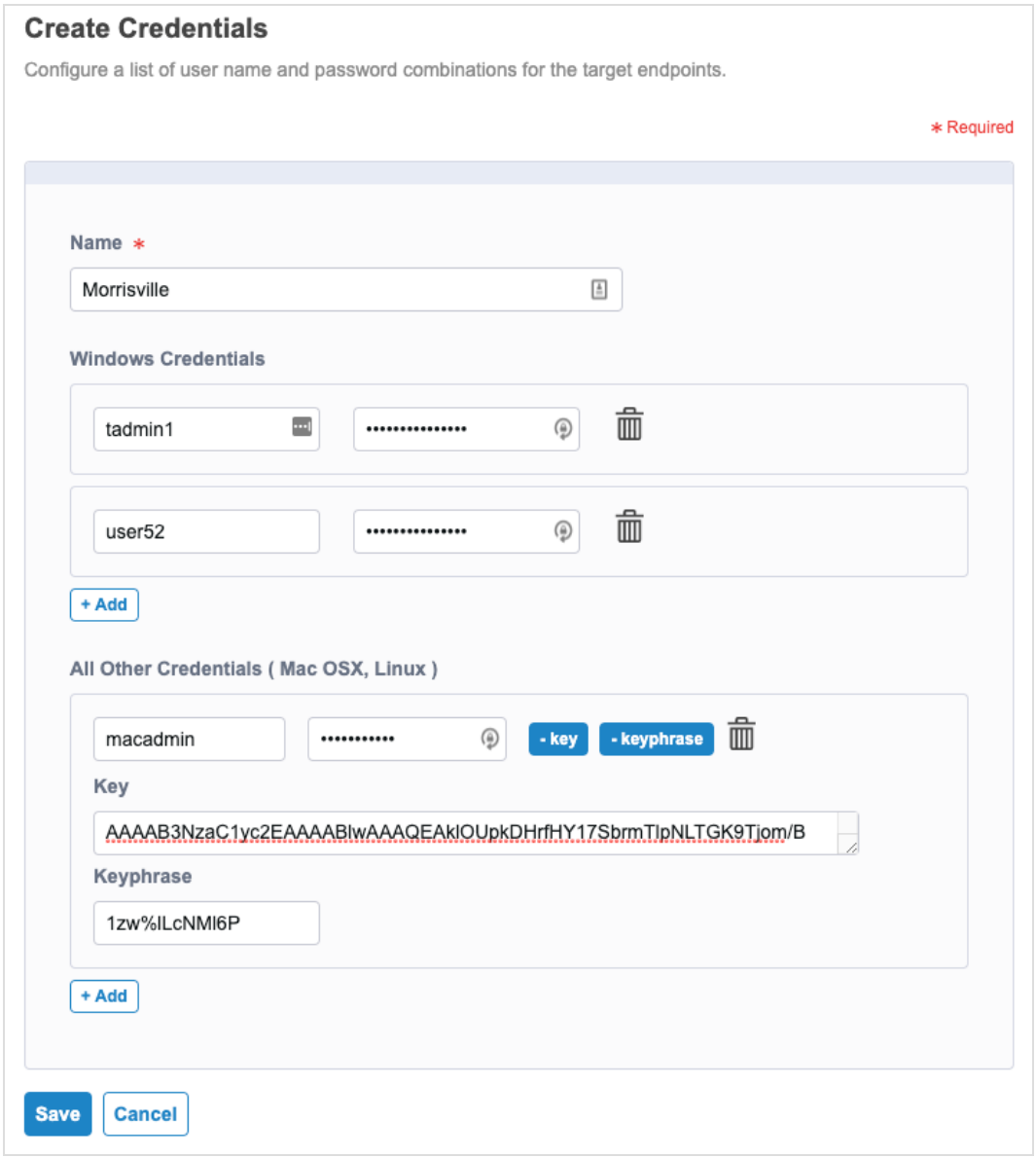
12. Click **Save**.

Configure client credentials

Client credentials are a list of user name and password combinations for the target endpoints on which you want to install Tanium Client. For specific requirements for authentication and permissions, see Account permissions on page 10.

1. From the Client Management menu, click **Credentials**. Click **Create**.
2. Enter a name for the credentials list.
3. Add a set of credentials to try for each operating system type.
   - For Windows endpoints, if you are using domain credentials, you must enter the user name in the format `domain\username`. If you are using local credentials, enter only `username` for the user name.
   - On non-Windows endpoints, you can also add an SSH key. If you are using an SSH key, the private key is required. Click **+ key**, copy the contents of the private key, and paste the contents in the **Key** field. If the key requires a passphrase, click **+ keyphrase** and enter the passphrase in the **Keyphrase** field. When you use an SSH key for authentication, a user name

is required, and a password is optional.



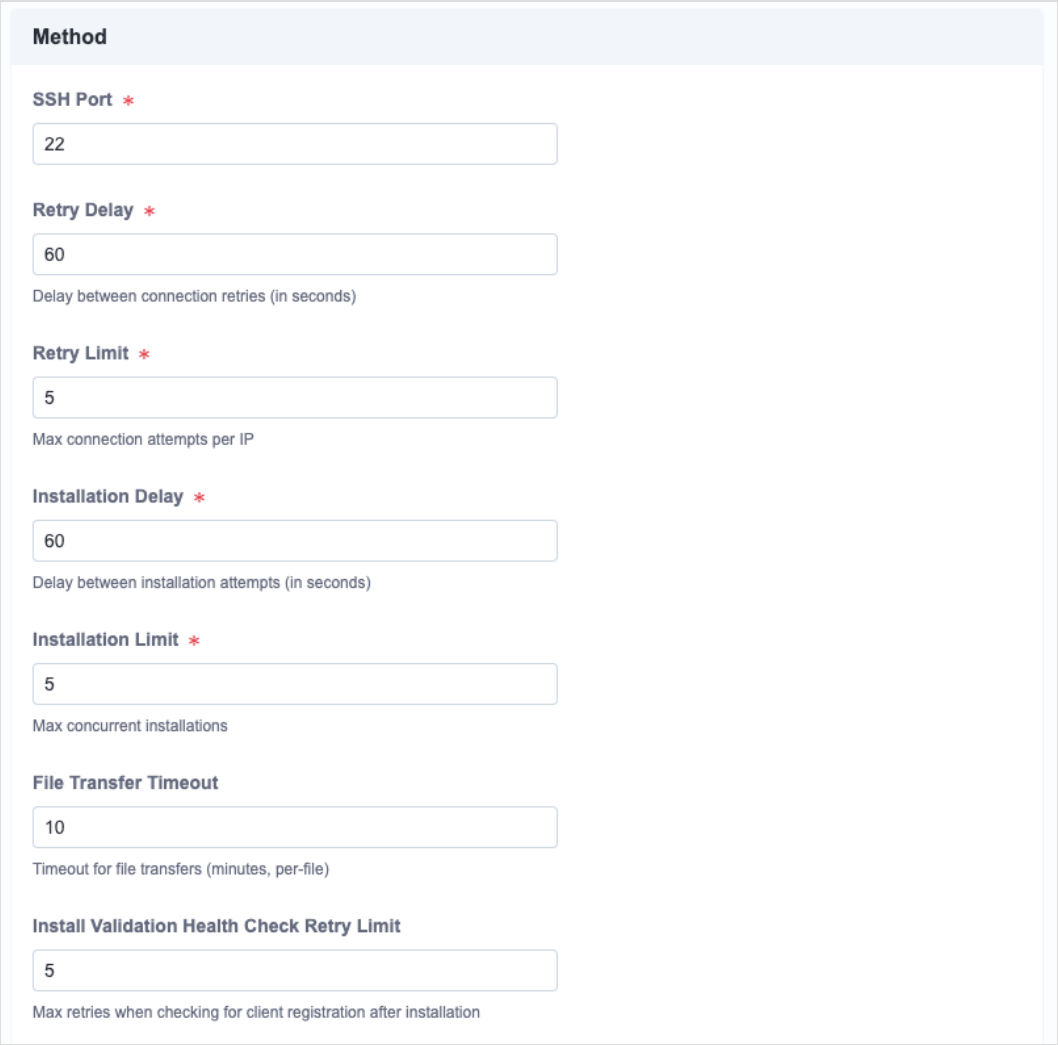
4. Click **Save**.

Configure a deployment

1. From the Client Management menu, click **Deployments**, and then click **Create**.
2. Specify a descriptive name for the deployment, and select the client configuration and credentials that you configured.
3. Configure targeting. You can target endpoints by a single IP address, a list of IP addresses, a computer name, an IP or CIDR range, or a Discover label. For information about configuring Discover labels, see Tanium Discover User Guide: Labels.

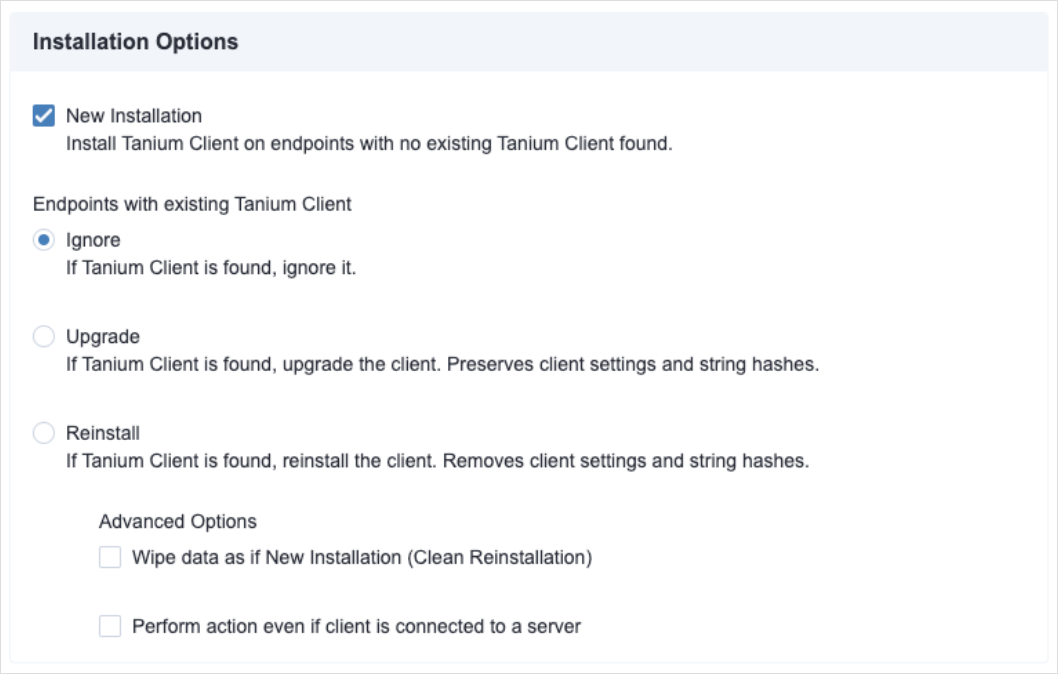
To define an additional target for the deployment, click **Add Target**. To remove a target, click Delete .

4. Configure the settings in the **Method** section as needed.



5. Configure the settings in the **Installation Options** section.
   - To install the client on unmanaged endpoints, make sure **New Installation** is selected.

- To determine how to manage endpoints where the client is already installed, select **Ignore**, **Upgrade**, or **Reinstall**. For more information, see Upgrade or reinstall the Tanium Client on page 22.



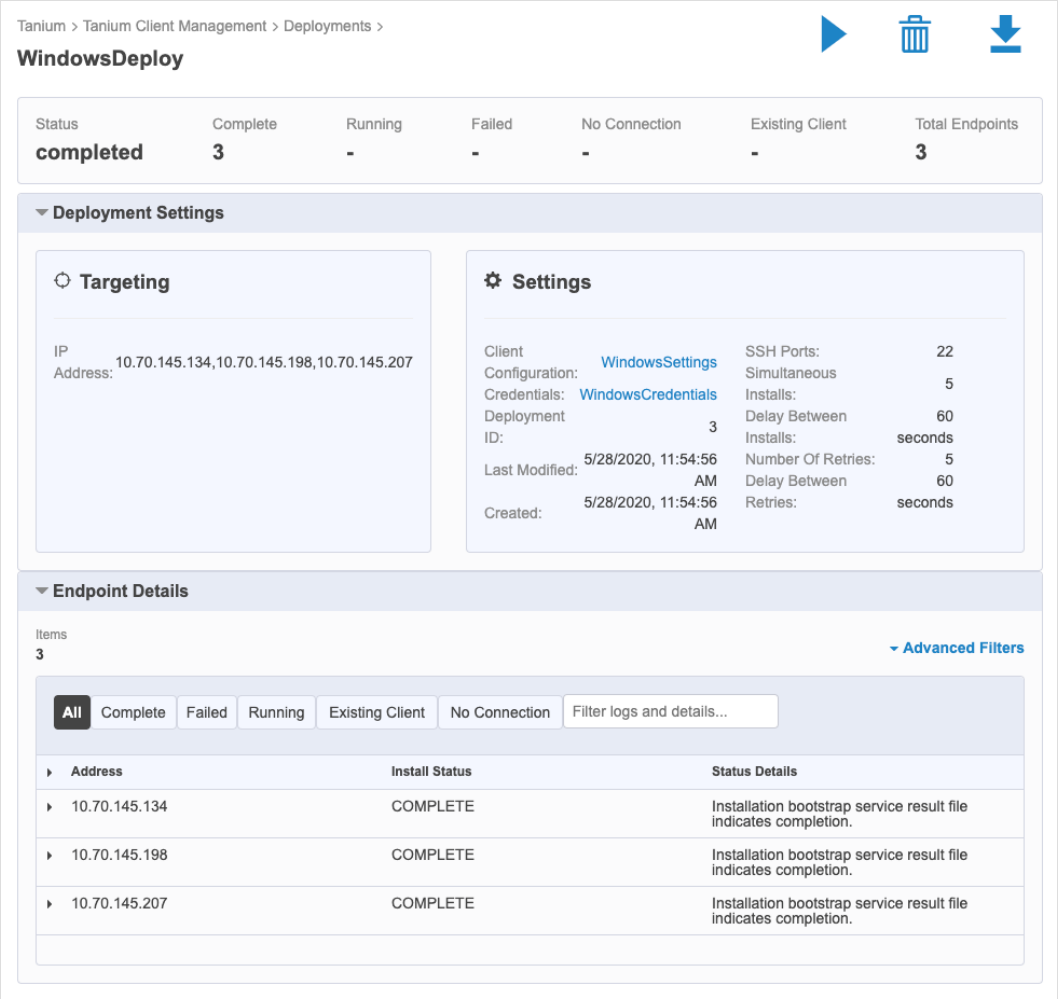
6. Click **Save** to save the deployment without running, or **Save and Deploy** to immediately deploy.

Deploy clients

From the Client Management menu, click **Deployments**. In the **Name** column, click the name of a deployment.

To run the deployment, click Start .

You can then view the status of the deployment, including viewing a list of the targeted endpoints.



Deployment steps

When you start a deployment, the Module Server takes the following actions to install the Tanium Client:

1. Pings the targeted endpoints to verify they are online.
2. Detects the operating system of the endpoints that respond to the ping.
3. Tries the credentials in the defined credentials list to log into the endpoint for installation.
4. Checks for the space required on the endpoint as specified in the client settings.
5. Copies the Tanium public key file for the Tanium Server to the endpoint.
6. Installs Tanium Client on the endpoint. The version and installation location are defined in the client configuration for the deployment.
7. Displays the deployment status.

Deployment status

Each successful deployment reports a status of `COMPLETE` in the **Installation Status** column.

Filter the endpoints by clicking the status buttons in the grid, or enter filter text in the **Filter logs and details** box.

For more information about other status messages and troubleshooting deployments, see Troubleshoot deployments on page 41.

Download and deploy the installation bundle

For endpoints that are connected to a Zone Server or that cannot be reached directly from the Tanium Module Server for any other reason, you can download and manually deploy the installation bundle associated with client settings.

> **Note:** After creating or updating client settings, the Module Server must retrieve the necessary client installers before you can download the installation bundle. The Download Bundle button becomes available when the download is ready.

1. From the Client Management menu, click **Client Settings**
2. To download the installation bundle associated with a set of client settings, click Download Bundle in the **Actions** column.
3. Deploy the installation bundle to the appropriate endpoints.

For more information about deploying the client using an installation package, see:

- Tanium Client User Guide: Deploying the Tanium Client to Windows endpoints
- Tanium Client User Guide: Deploying the Tanium Client to macOS endpoints
- Tanium Client User Guide: Deploying the Tanium Client to Linux endpoints
- Tanium Client User Guide: Deploying the Tanium Client to Solaris endpoints
- Tanium Client User Guide: Deploying the Tanium Client to AIX endpoints

Verify client installation

To verify the installation on an endpoint has completed:

1. From Interact, enter a question in the **Ask a Question** field to verify that the endpoints respond to the following query: `Get Computer Name and Operating System and Tanium Client Version and Tanium Server Name from all machines`
2. Review the **Question Results** grid to verify that all endpoints where you deployed Tanium Client software are reporting.
3. (Optional) From the main menu, go to **Administration > Management > System Status** to review recent client registration details.

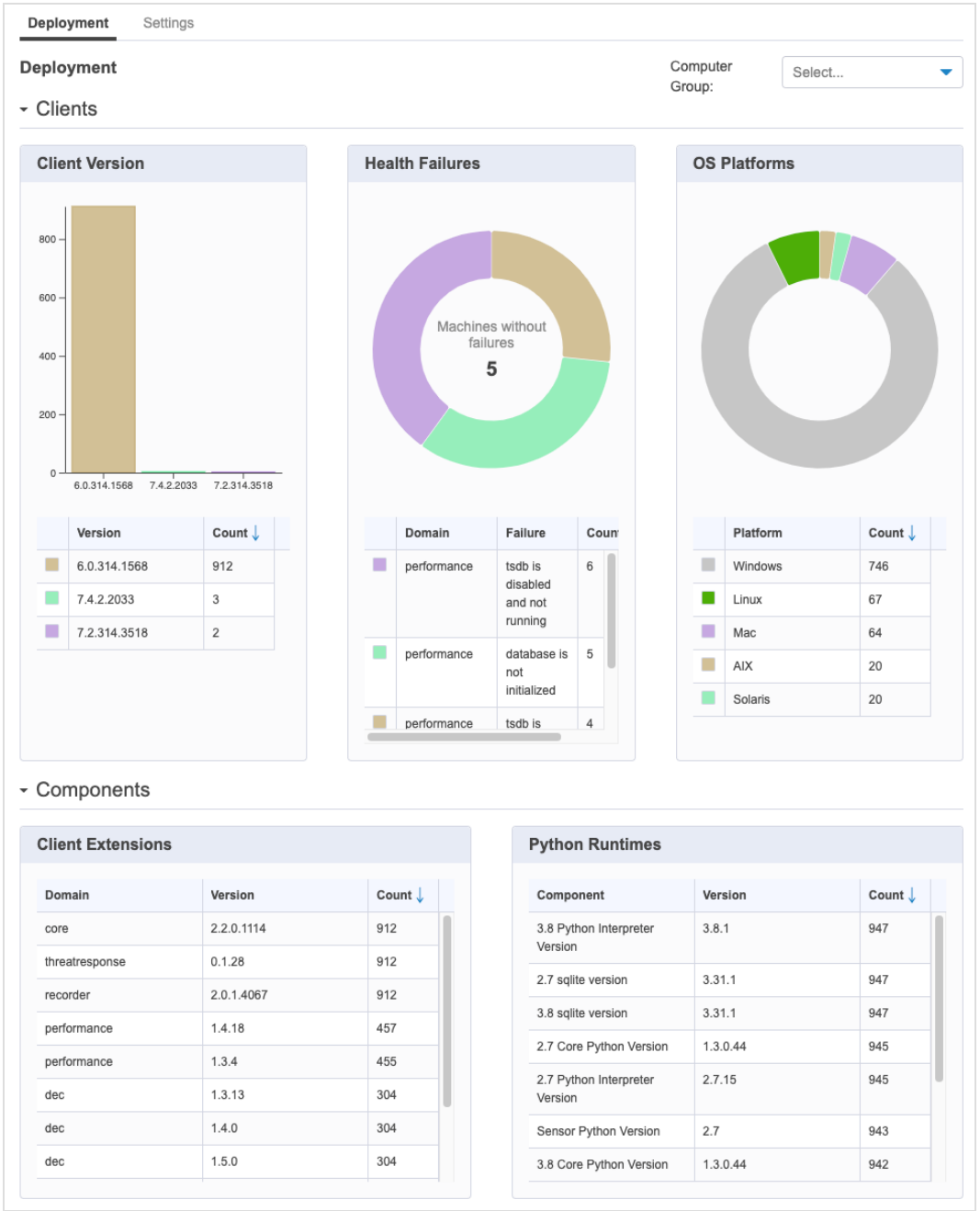
Monitoring client health

Review health information about deployed clients.

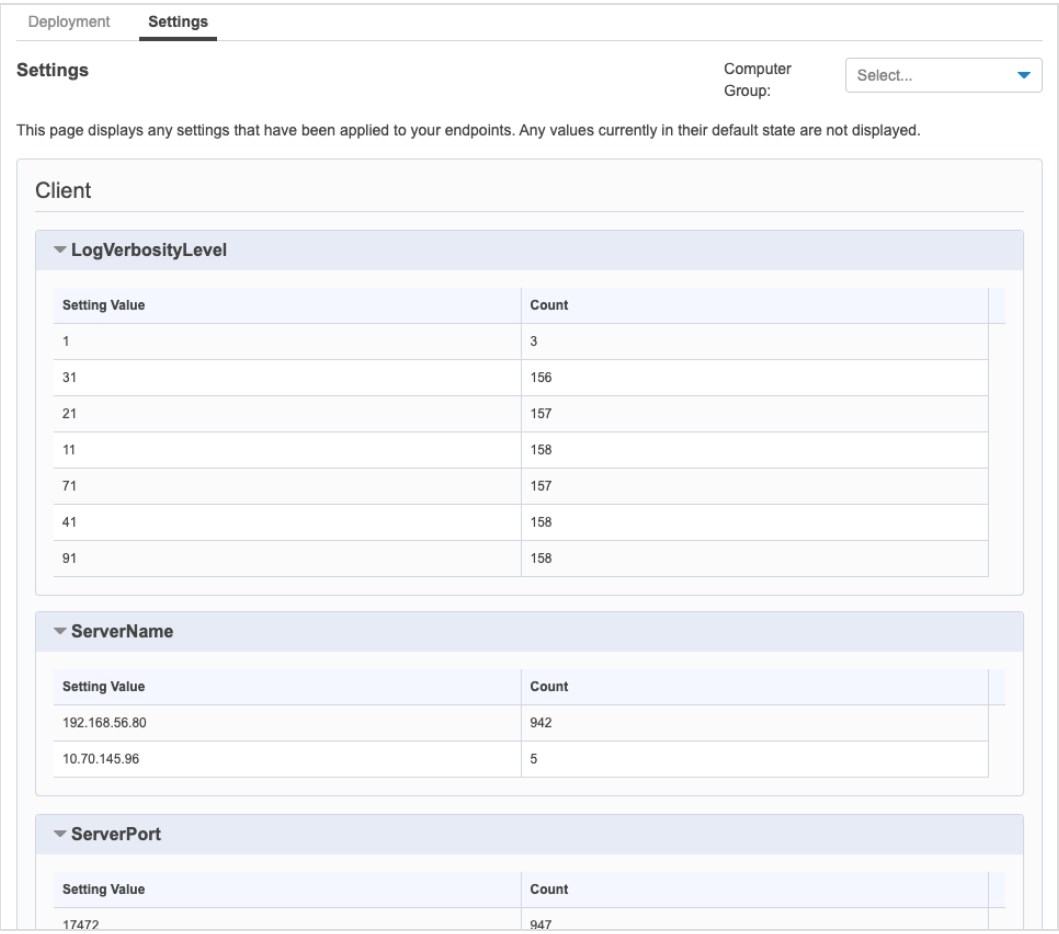
View a summary of client health information

From the **Client Management** menu, go to **Client Health**.

The **Deployment** tab displays a summary of client deployment information, such as client versions, health check failures, operating systems, installed client extensions, and Python runtime versions.



The **Settings** tab displays a summary of client settings, such as log verbosity level, server name, server port, and various component information. This overview can help identify settings that have been changed from defaults.



On either tab, you can select a **Computer Group** to filter the summary information.

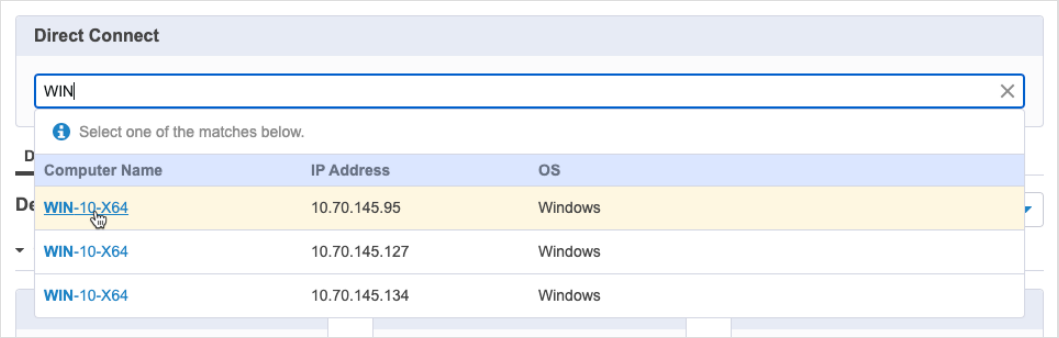
To further investigate a data set using the associated question results, click View question results in Interact . For more information about working with question results, see Tanium Interact User Guide: Managing question results.

View detailed client health information for an endpoint

You can directly connect to a Windows, Linux, or macOS endpoint to view more detailed client health information.

1. From the Client Management menu, go to **Client Health**.
2. In the **Direct Connect** search box, enter all or part of an IP address or a computer name. Matching results are displayed after the search completes.

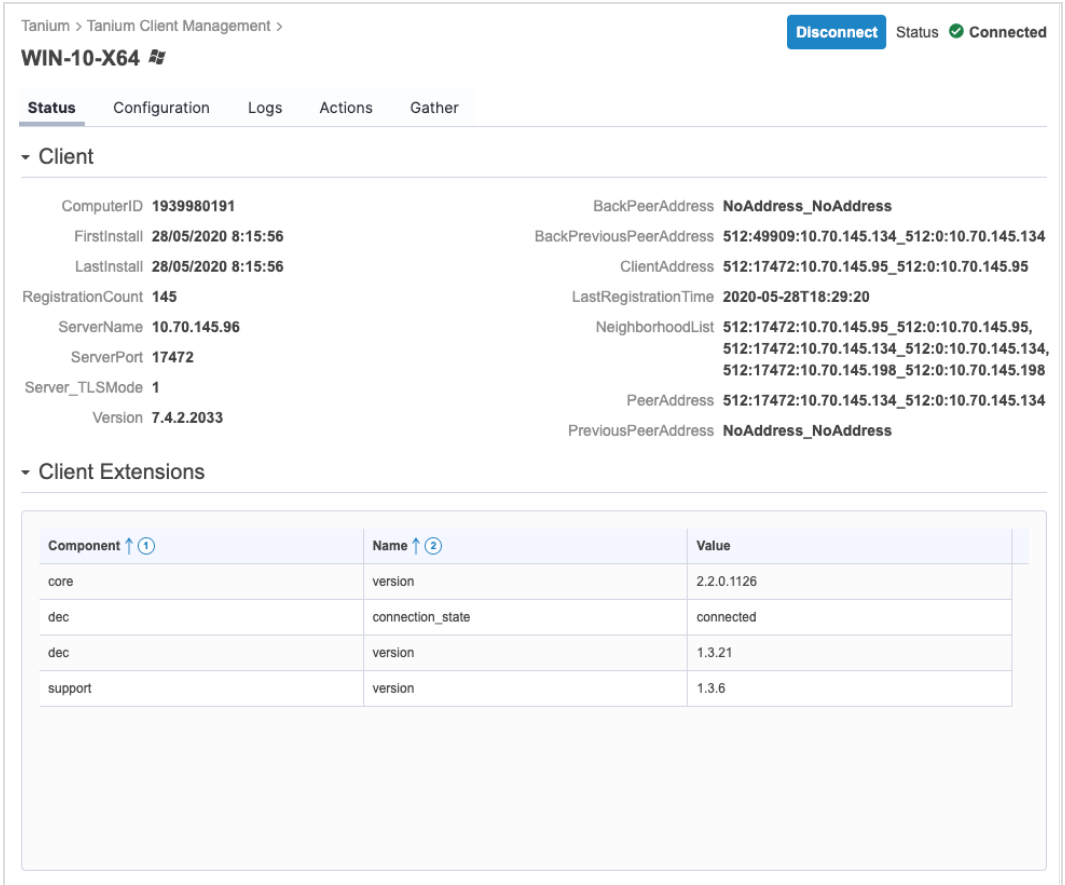
3. From the search results, click the computer name to connect to the endpoint.



Note: If the connection to the endpoint times out, click **Reconnect** to reestablish the connection.

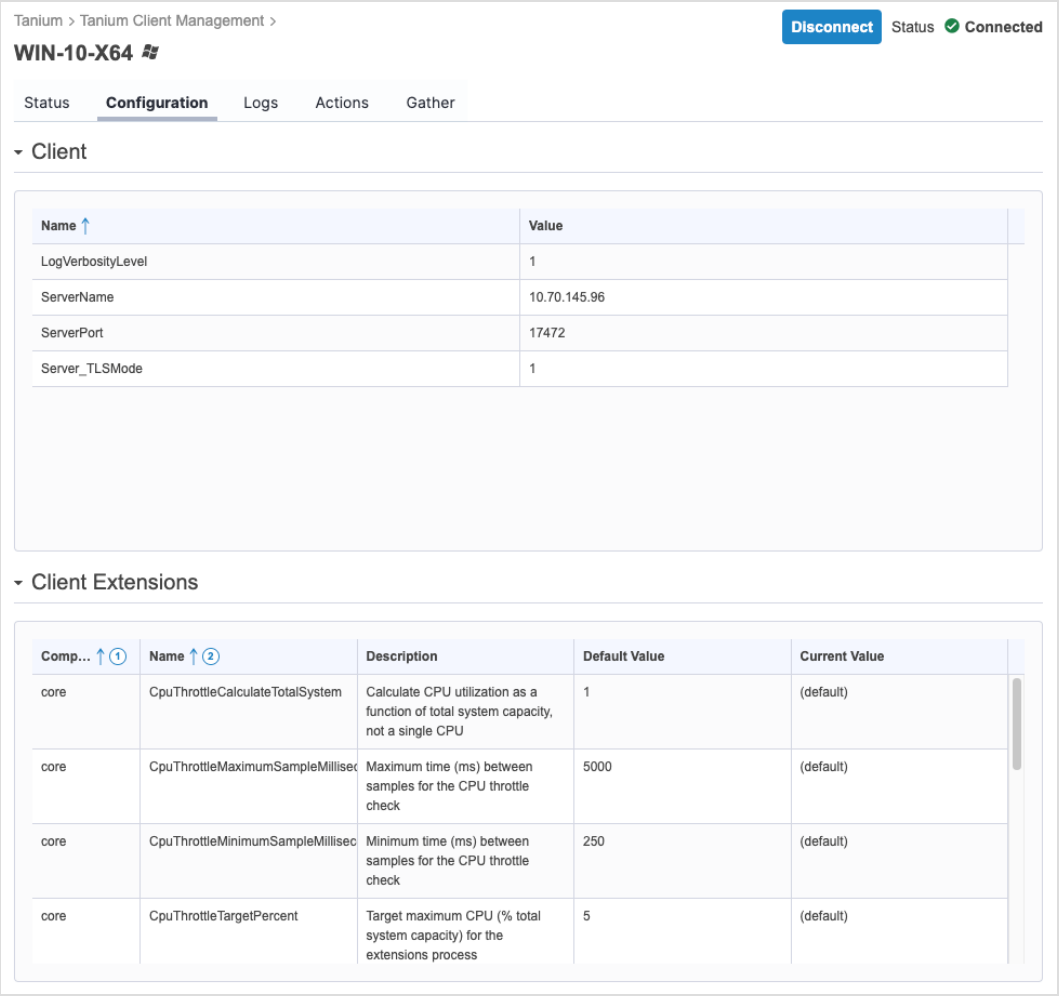
View detailed status information

Click the **Status** tab to view detailed client status information about the connected endpoint, such as the computer ID, the first and last client installation time stamps, the installed client version, client and peer address information, and client extension information, including any health check failures.



View detailed client settings information

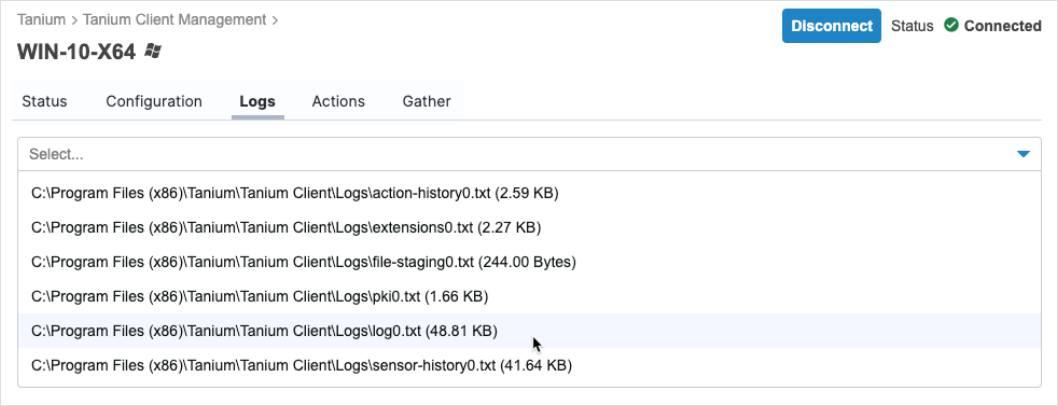
Click the **Configuration** tab to view detailed information about client settings for the connected endpoint, such as log verbosity level, server name, server port, and various settings for client extensions.



View logs from the connected client

To view logs from the connected client, click the **Logs** tab, and select a log to view.

To download the currently selected log, click **Download**.



For information about reviewing logs for troubleshooting, see Tanium Client User Guide: Troubleshooting.

View action logs from the connected client

To view action logs from the connected client, click the **Actions** tab, and select a previously run action for which you want to view the log.

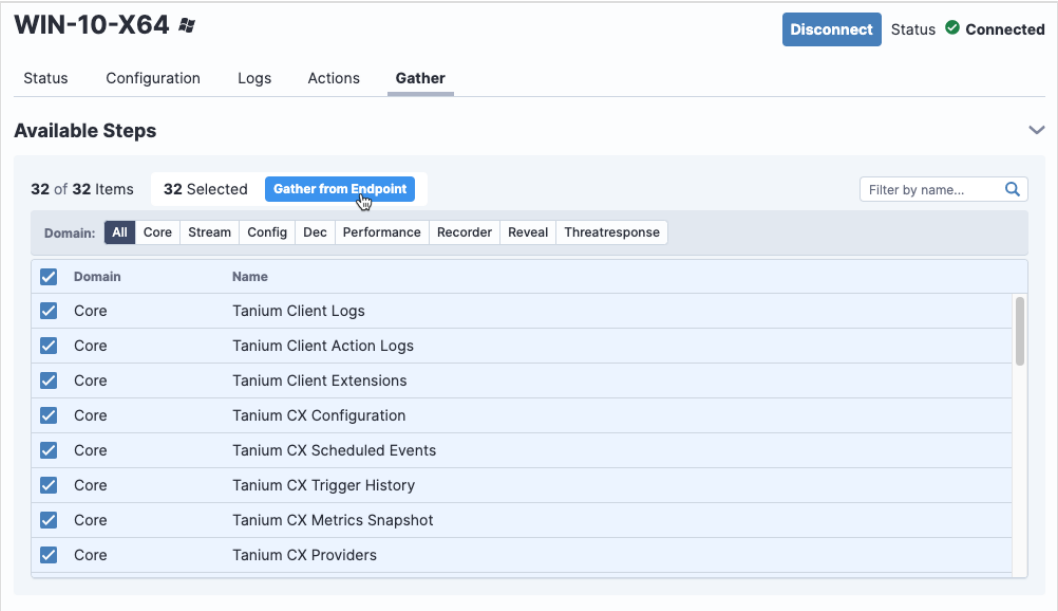
To download the currently selected log, click **Download**.

For information about reviewing action logs for troubleshooting, see Tanium Client User Guide: Action_logs.

Collect troubleshooting information from endpoints

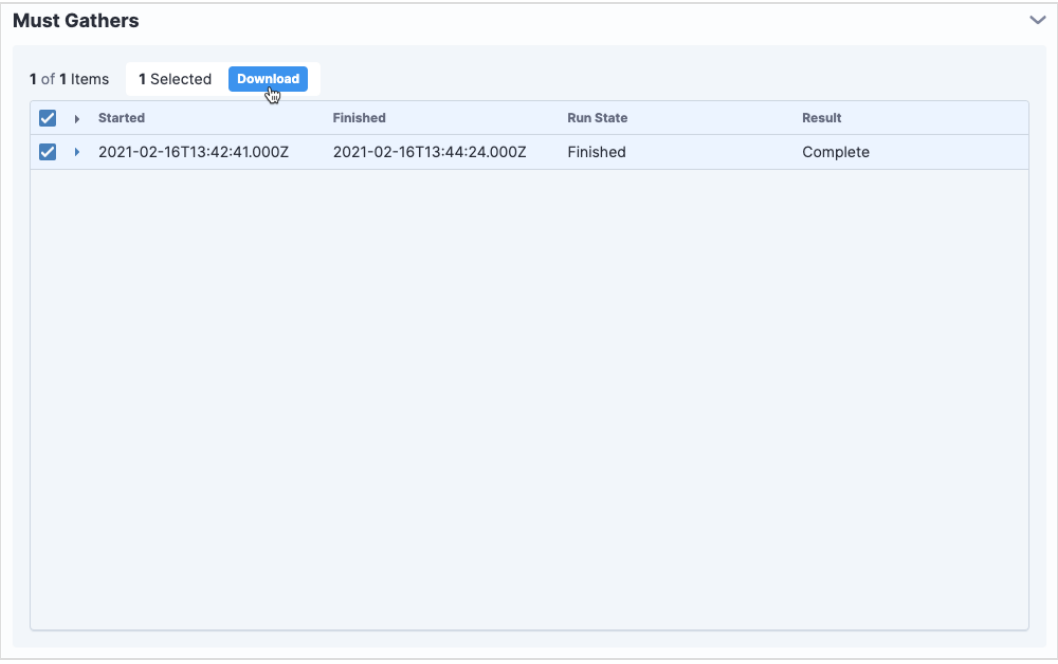
You can collect a bundle of logs and other artifacts from a connected endpoint to help resolve issues.

1. Click the **Gather** tab. To filter the available logs and artifacts, click a button in the **Domain** section.
2. Click **Gather from Endpoint**.



The selected logs and artifacts are gathered from the endpoint. The package appears in the **Must Gathers** section, named with its time stamp.

3. When **Finished** appears in the **Run State** column, select the package and click **Download** to download a ZIP file that contains the troubleshooting information.



Disconnect and return to summary information

To disconnect from the endpoint and return to the client health summary, click **Disconnect**.

Troubleshooting Client Management

To 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 Client Management home page, click Help, then the **Troubleshooting** tab.
2. Click **Download Debug Package**.
   A `tanium-client-management-support.zip` file downloads to the local download directory.
3. Attach the ZIP file to your Tanium Support case form or contact Tanium Support.

Tanium Client Management maintains logging information in the `client-management.log` file in the `\Program Files\Tanium\Tanium Module Server\services\client-management-files` directory.

Download deployment information

You can download a JSON file that includes deployment settings and endpoint details for a deployment.

1. From the Client Management menu, click **Deployments**.
2. In the **Name** column, click the name of a deployment.
3. Click Download to download the JSON file.

Troubleshoot deployments

Problem: A new deployment instantly switches to the Completed status with no attempted deployments to endpoints

The Module Server is having trouble downloading the client binaries.

SOLUTION

Check the TDownloader log for download errors. For information about where to find this log, see Tanium Core Platform Deployment Reference Guide: TDownloader logs.

Problem: Endpoint Installation Status = ERROR_ACQUIRE_LOGS_FAIL

Log messages for the deployment contain the following message:

```
Deployment Result Generated: Necessary file(s) missing on disk: C:\Program
Files\Tanium\Tanium Module Server\services\client-management-files\deployment-
runner-data\bc6bf6fd-0388-4f2d-9120-860cac75e8d4\tanium.pub
```

SOLUTION

Upload the `tanium.pub` file. See (Tanium 7.2.x, 7.3.x only) Upload Tanium public key on page 21.

Problem: Endpoint Installation Status = ERROR_ACQUIRE_LOGS_FAIL

Log messages for the deployment contain the following message:

```
Error creating/starting the installation bootstrap service on the target: Error:
cli_rpc_pipe_open_noauth: rpc_pipe_bind for pipe svcctl failed with error NT_
STATUS_CONNECTION_DISCONNECTED Could not initialise pipe svcctl. Error was NT_
STATUS_CONNECTION_DISCONNECTED
```

SOLUTION

Verify that the firewall allows WMI, RPC, and SMB traffic between Tanium servers and endpoints. For more information, see Host and network security requirements on page 11.

> **Note:** Firewalls with application-based control might not allow this traffic for Tanium by default.

Problem: Endpoint Installation Status = ERROR_CONNECTION_FAIL

Log messages for the deployment contain the following message:

```
Deployment Result Generated: All 1 connection attempt(s) resulted in no response
from the target.
```

SOLUTION

- Check the user name provided with the credentials. Credentials must be active and not disabled. Check that the domain is added correctly, for example: `domain\username` for a domain account, or `username` for a local endpoint account.
- Check the password provided with the credentials to ensure it is not disabled or expired.
- Check both the target endpoint firewall and network device firewalls. The Module Server might be blocked from initiating a connection to the target endpoint by a firewall. WMI port 135, SMB port 445, and SSH port 22 must be open. Use the following testing techniques to check the ports:

    - Test Network connections:
        - Windows PowerShell: `Test-NetConnection -computer ip_address -port port_number`
        - Linux: `telnet`, `nc` / `netcat`
    - Check TanOS network status: See Tanium Appliance Deployment Guide: Support menu.
- If you are using a non-default Administrator account and the machine is not joined to a domain, edit the Windows registry to disable User Account Control (UAC) remote restrictions, which normally prevent access to administrative shares and remote installations under these conditions. To disable UAC remote restrictions, add the following registry value and restart the machine:

```
Subkey: HKEY_LOCAL_
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
Data type: REG_DWORD
Value name: LocalAccountTokenFilterPolicy
Value data: 1
```

> **Note:** If you use the default local Administrator account, you do not need to make this registry change.

> **IMPORTANT:** Administrative shares are not available in Home editions of Windows operating systems.

Problem: Endpoint Installation Status = ERROR_CONNECTION_FAIL

Log messages for the deployment contain the following message:

```
Command resulted in error: Error: Connection to 'SSH Client for '192.168.24.11''
was not established
```

SOLUTION

- Verify the client configuration and deployment settings. You might be targeting a Windows endpoint with a deployment while only using SSH as a connection method.
- Verify that the targeted Linux endpoint has SSH enabled and is configured on port 22.
- Check the user name provided with the credentials. Credentials must be active and not disabled. Check that the domain is added correctly, for example: `domain\username` for a domain account, or `username` for a local endpoint account.
- Check the password provided with the credentials to ensure it is not disabled or expired.

Problem: Endpoint Installation Status = ERROR_ACQUIRE_LOGS_FAIL

Log messages for the deployment contain the following message:

```
SMB 'mkdir' command exited with exit code 1.
```

SOLUTION

Verify that you are not trying to deploy to an endpoint that already has the Tanium Client installed. The endpoint could have a Tanium Client that was not fully removed, or a Tanium Client installation that points to a different Tanium Server.

Uninstall Client Management

1. From the Main menu, click **Administration > Configuration > Solutions**.
2. In the **Content** section, select the **Client Management** row.
3. Click Delete Selected  . Click **Uninstall** to complete the process.

Contact Tanium Support

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