



Tanium™ Client Management User Guide

Version 1.0.9

May 22, 2020

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 TAM, sales representative, or email accessibility@tanium.com to make further inquiries.

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

© 2020 Tanium Inc. All rights reserved.

Table of contents

- Client Management overview 7**
 - Deployment process overview 7
 - Client configurations 7
 - Client credentials 7
 - Target endpoints 7
 - Integration with other Tanium products 7
 - Discover 7
 - Trends 8
- Getting started 9**
- Client Management requirements 10**
 - Tanium dependencies 10
 - Tanium™ Module Server 10
 - Endpoints 10
 - Supported operating systems 10
 - Host and network security requirements 11
 - Ports 11
 - Security exclusions 12
 - Internet URLs 12
 - User role requirements 13
- Installing Client Management 22**
 - Before you begin 22
 - Import and configure Client Management with default settings 22
 - Import and configure Client Management with custom settings 22

| | |
|---|-----------|
| Configure service account | 23 |
| Verify installation | 23 |
| (Tanium 7.2.x, 7.3.x only) Upload Tanium public key | 23 |
| Add client installation files for air-gapped environments | 23 |
| What to do next | 24 |
| Deploying Tanium Client | 25 |
| Plan deployment targeting | 25 |
| Prepare for deployment to Linux, macOS, or UNIX endpoints | 25 |
| Prepare for deployment to Windows endpoints | 26 |
| Configure client settings | 27 |
| Configure client credentials | 30 |
| Configure a deployment | 31 |
| Monitor deployments | 34 |
| Deployment steps | 34 |
| Deployment status | 35 |
| Verify client installation | 35 |
| Troubleshooting Client Management | 36 |
| Collect logs | 36 |
| Troubleshoot deployments | 36 |
| Problem: A new deployment instantly switches to the Completed status with no attempted deployments to endpoints | 36 |
| Solution | 36 |
| Problem: Endpoint Install Status = ERROR_ACQUIRE_LOGS_FAIL | 36 |
| Solution | 37 |
| Problem: Endpoint Install Status = ERROR_CONNECTION_FAIL | 37 |

| | |
|--|----|
| Solution | 37 |
| Problem: Endpoint Install Status = ERROR_CONNECTION_FAIL | 38 |
| Solution | 38 |
| Problem: Endpoint Install Status = ERROR_ACQUIRE_LOGS_FAIL | 38 |
| Solution | 39 |
| Uninstall Client Management | 39 |

Client Management overview

With Client Management, you can deploy the Tanium™ Client to targeted sets of Windows, Linux, Mac, Solaris, or AIX endpoints.

Deployment process overview

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 configurations 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.

Client configurations

A client configuration includes client settings specific to a deployment, including the version of the Tanium Client to deploy, and the Tanium Server with which to associate the client. Client configurations can also contain tags, which identify the endpoints after the client is installed.

Client credentials

Client credentials are a list of credentials the Module Server uses to log in to endpoint computers for installation of the Tanium Client. This list of credentials is tried in the defined order for each endpoint in the deployment.

Target endpoints

When you create and run a deployment, you can target endpoints by IP address or range, computer name, or labels from Tanium™ Discover.

Integration with other Tanium products

Discover

You can apply labels to the unmanaged interfaces that are identified with Tanium™ Discover,

Trends

Client Management features Tanium™ 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

For more information about how to import the Trends boards that are provided by Client Management, 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 22](#).
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.
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.
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.
5. Monitor results. View the results of the deployment, and re-deploy if necessary.

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 | 7.2 or later |
| Tanium products | <p>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 Tanium Discover, as described under Tanium Console User Guide: Manage Tanium modules.</p> <ul style="list-style-type: none">• (Optional) Tanium Discover 3.1 or later. With Discover, you can target endpoints based on Discover tags.• (Optional) Tanium Trends 2.4 or later. |

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.

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 |

| Operating System | Version |
|-------------------------------|---|
| Microsoft Windows Workstation | 7 and 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 . |
| Solaris | Same as Tanium Client support. See Tanium Client User Guide: Host system requirements . |
| AIX | Same as Tanium Client support. See Tanium Client User Guide: Host system 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 25](#) and [Prepare for deployment to Windows endpoints on page 26](#).

Ports

The following ports are required for Client Management communication.

| Component | Port | Direction | Purpose |
|-----------------------------|---|----------------------|---|
| Module Server (Windows) | 22/TCP 135/TCP 139/TCP 445/TCP | Outbound | Communicate with endpoints during client installation RPC must be enabled from the module server |
| Module Server (Non-Windows) | 22/TCP 135/TCP 445/TCP | Outbound | Communicate with endpoints during client installation |
| Endpoints (Windows) | 17472, 135, 445 | Inbound, Outbound | Communicate with Module Server during client installation |

| Component | Port | Direction | Purpose |
|----------------------------|-----------|----------------------|---|
| Endpoints (Non-Windows) | 17472, 22 | Inbound, Outbound | Communicate with Module Server during client installation Tip: This port is opened automatically on macOS systems |

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.

Table 1: Client Management security exclusions

| Target Device | Process |
|---------------|---|
| Module Server | "<Tanium Module Server>\services\client-management-service\node.exe" service.js |
| | <Tanium Module Server>\services\twsm-v1\twsm.exe |
| Endpoints | <Tanium> (during client installation) <Tanium Client> |

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 whitelist.

- <https://content.tanium.com>

User role requirements

Table 2: Client Management user role permissions

| Permission | Client Management Administrator | Client Management User | Client Management API User | Client Management Auditor | Client Management Credentials Administrator | Client Management Read-Only User |
|---|---------------------------------|------------------------|----------------------------|---------------------------|---|----------------------------------|
| Show Client-management¹ View the Client Management workbench | ✓ ² | ✓ ² | ✓ ² | ✓ | ✓ ² | ✓ ² |
| Client-management Configurations Read Read client and deployment configurations | ✓ ² | ✓ | ✗ | ✗ | ✗ | ✓ |

| Permission | Client Management Administrator | Client Management User | Client Management API User | Client Management Auditor | Client Management Credentials Administrator | Client Management Read-Only User |
|---|---------------------------------|------------------------|----------------------------|---------------------------|---|----------------------------------|
| Client-management Configurations Write Create and modify client and deployment configurations | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ |

| Permission | Client Management Administrator | Client Management User | Client Management API User | Client Management Auditor | Client Management Credentials Administrator | Client Management Read-Only User |
|---|---------------------------------|------------------------|----------------------------|---------------------------|---|----------------------------------|
| Client-management Credentials Read Read credentials list, but not view associated passwords or key data | ✓ ² | ✓ | ✗ | ✗ | ✓ ² | ✓ |
| Client-management Credentials Write Create and modify credentials lists | ✓ | ✗ | ✗ | ✗ | ✓ ² | ✗ |

| Permission | Client Management Administrator | Client Management User | Client Management API User | Client Management Auditor | Client Management Credentials Administrator | Client Management Read-Only User |
|---|---------------------------------|------------------------|----------------------------|---------------------------|---|----------------------------------|
| Client-management Credentials View View passwords or key data for credentials lists | ✘ | ✘ | ✘ | ✘ | ✔ | ✘ |
| Client-management Deployments Read View data about client deployments | ✔ ² | ✔ ² | ✘ | ✘ | ✘ | ✔ |

| Permission | Client Management Administrator | Client Management User | Client Management API User | Client Management Auditor | Client Management Credentials Administrator | Client Management Read-Only User |
|--|---------------------------------|------------------------|----------------------------|---------------------------|---|----------------------------------|
| Client-management Deployments Write Create deployments of Tanium Client to unmanaged endpoints | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ |
| Client-management Settings Write Write access to global settings in the Client Management module | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ |

| Permission | Client Management Administrator | Client Management User | Client Management API User | Client Management Auditor | Client Management Credentials Administrator | Client Management Read-Only User |
|---|---------------------------------|------------------------|----------------------------|---------------------------|---|----------------------------------|
| Client-management Read Audit Log Read audit log with API | ✘ | ✘ | ✔ | ✘ | ✘ | ✘ |
| Client-management Use API Write access to global settings in the Client Management module | ✘ | ✘ | ✔ | ✘ | ✘ | ✘ |
| Trends Data Read³ Run data queries against sources | ✔ | ✔ | ✘ | ✘ | ✘ | ✔ |

| Permission | Client Management Administrator | Client Management User | Client Management API User | Client Management Auditor | Client Management Credentials Administrator | Client Management Read-Only User |
|--|---------------------------------|------------------------|----------------------------|---------------------------|---|----------------------------------|
| Trends API Board Read³ View boards, sections, and panels for specified content sets | ✔ | ✔ | ✘ | ✘ | ✘ | ✔ |
| Trends API Board Write³ Create, edit, delete, and configure boards, sections, and panels for specified content sets | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ |

| Permission | Client Management Administrator | Client Management User | Client Management API User | Client Management Auditor | Client Management Credentials Administrator | Client Management Read-Only User |
|---|---------------------------------|------------------------|----------------------------|---------------------------|---|----------------------------------|
| Trends API Source Read³ View and list sources for specified content sets | ✔ | ✔ | ✘ | ✘ | ✘ | ✔ |
| Trends API Source Write³ Create, edit, and delete sources for specified content sets | ✔ | ✘ | ✘ | ✘ | ✘ | ✘ |

¹ To install Client Management, you must have the reserved role of Administrator.

² Denotes a provided permission.

³ Denotes a permission that applies to the Reserved content set.

Table 3: Provided Client Management Advanced user role permissions

| Permission | Content Set for Permission | Client Management Administrator | Client Management User | Client Management API User | Client Management Auditor | Client Management Credentials Administrator | Client Management Read-Only User |
|----------------|----------------------------|---------------------------------|------------------------|----------------------------|---------------------------|---|----------------------------------|
| Execute Plugin | Tanium Client Management | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Execute Plugin | Reserved | ✗ | ✓ | ✓ | ✗ | ✗ | ✓ |

Table 4: 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 22](#).
- **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 22](#).

Before you begin

- Read the [release notes](#).
- Review the [Client Management requirements on page 10](#).
- Assign the correct roles to users for Client Management. Review the [User role requirements on page 13](#). 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 22](#).

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 22](#).

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 13](#).


1. From the Main menu, click **Tanium Services > Tanium 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 your TAM to configure client installers on the Tanium Module Server.

What to do next

See [Getting started on page 9](#) 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.

IMPORTANT: You can only install on endpoints that do not have a Tanium Client already installed. To upgrade the Tanium Client, see [Tanium Client User Guide: Upgrading Tanium Clients](#).

Plan deployment targeting

You can deploy the Tanium Client to a single IP, computer name, 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 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](#).

Prepare for deployment to Linux, macOS, or UNIX endpoints

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

For all Linux distributions, macOS, and UNIX, use one of the following options to configure a user with elevated privileges to perform installation:

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

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). 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.

Prepare for deployment to Windows endpoints

1. Enable Windows file-and-print sharing and remote procedure calls (RPCs) on the target endpoints. Enabling these settings is required only for installation. You can disable the sharing and RPCs after the installation.
2. Configure any host-based firewalls or other security tools on the endpoint that might interfere with a remote installation initiated through RPC. For more information, see [Host and network security requirements on page 11](#).
3. 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](#).
4. Verify that you can log in to the remote system with PSEXEC or WMIC command line utilities with the same credentials that you will use for the Tanium Client deployment.

For example:

```
psexec \\192.168.1.130 -u Administrator cmd /c dir  
C:\Users\Administrator\Documents  
wmic /node:"192.168.1.130" /user:"Administrator" useraccount list brief
```

CAUTION: Windows credential handling during login events might expose the user name and password in command line arguments on the source system that is initiating the deployment, and in memory on the remotely accessed endpoints. 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**. Click **Create**.
2. Specify the IP address or host name of the Tanium Server from which you want to perform the deployment.
3. Select the 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. and then use the label as a deployment target

Create Client Settings

Configure the Tanium Client platforms and versions to install on endpoints and the Tanium Server that will perform the installation.

* Required

Name *

Morrisville

Tanium Server Names *

ts1.tam.local

Comma-separated list of fully qualified domain names or IP addresses

Client Platforms *

MacOS x

Windows x

Installation Directory on Windows

C:\Program Files (x86)\Tanium\Tanium Client

Installation Directory on Linux

/opt/Tanium/Tanium Client/

Log Level

1

Log verbosity level for endpoints

Client Port

17472

Client Version

Install latest 7.4 client

Client Settings


Add Client Setting

Client Tags

InstalledByTCM

Add Client Tag

4. Click **Save**.

Tip: To download an installer bundle associated with a set of client settings, click Download Bundle  in the **Actions** column.

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.

1. From the Client Management menu, click **Credentials**. Click **Create**.
2. Specify a name for the credentials list, and a set of user names and passwords to try for each operating system type. On macOS and Linux endpoints, you can also specify

a key or keyphrase.

Create Credentials

Configure a list of user name and password combinations for the target endpoints.

* Required

Name *

Windows Credentials

[+ Add](#)

All Other Credentials (Mac OSX, Linux)

[- key](#) [- keyphrase](#)

Key

Keyphrase

[+ Add](#)

[Save](#) [Cancel](#)

3. Click **Save**.

Configure a deployment

1. From the Client Management menu, click **Deployments**. 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, computer name, IP or CIDR range, or Discover label. For information about configuring Discover labels, see [Tanium Discover User Guide: Labels](#).
4. Tune the settings in the **Method** section as needed.

Create Deployment

Select a configuration and client configuration, and configure the deployment of Tanium Client

* Required

Deployment Name *

Morrisville

Description

Client Configuration *

Morrisville

Credentials List *

Morrisville

Targeting

Single IP or Comma-delimited List of IPs

192.168.1.1-192.168.1.50

Method

SSH Port *

22

Retry Delay *

60

Delay between connection retries (in seconds)

Retry Limit *

5

Max connection attempts per IP

Install Delay *

60

Delay between install attempts (in seconds)

Install Limit *

5

Max concurrent installs

Save

Save And Deploy

Cancel

- Click **Save** to save the deployment without running, or **Save and Deploy** to immediately deploy. To start the deployment after you save, click Start Deployment ▶

Monitor deployments

From the Client Manage

Tanium > Tanium Client Management > Deployments >

Install to all Unmanaged Devices

| Status | Complete | Not Started | Running | Failed | N/A | Total Endpoints |
|------------------|-----------|-------------|----------|----------|----------|-----------------|
| completed | 61 | - | - | 7 | 2 | 70 |

Items
70

| Address | Install Status | Status Details |
|---------------|-------------------------|--|
| ▶ 10.0.16.6 | COMPLETE | Cleanup via SSH successful. |
| ▶ 10.0.16.13 | ERROR_ACQUIRE_LOGS_FAIL | Log acquisition failed. |
| ▶ 10.0.16.16 | ERROR_ACQUIRE_LOGS_FAIL | Log acquisition failed. |
| ▶ 10.0.16.20 | COMPLETE | Cleanup via SSH successful. |
| ▶ 10.0.16.38 | COMPLETE | Cleanup via SSH successful. |
| ▶ 10.0.16.48 | FAILED | Failed to distribute installation files to endpoint. |
| ▶ 10.0.16.92 | FAILED | Installation failed. |
| ▶ 10.0.16.130 | FAILED | Installation failed. |
| ▶ 10.0.16.132 | COMPLETE | Cleanup via SSH successful. |
| ▶ 10.0.16.160 | COMPLETE | Cleanup via SSH successful. |
| ▶ 10.0.16.182 | FAILED | Failed to distribute installation files to endpoint. |
| ▶ 10.0.16.187 | COMPLETE | Cleanup via SSH successful. |
| ▶ 10.0.16.193 | COMPLETE | Cleanup via SSH successful. |
| ▶ 10.0.16.206 | COMPLETE | Installation bootstrap service result file indicates completion. |
| ▶ 10.0.16.209 | COMPLETE | Installation bootstrap service result file |

ment menu, click **Deployments**. Click the name in the **Name** column. 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. Ping the targeted endpoints to verify they are online.
2. Detect the operating system of the endpoints that respond to the ping.

3. Try the credentials in the defined credentials list to log into the endpoint for installation.
4. Copy the Tanium public key file for the Tanium Server to the endpoint.
5. Install Tanium Client on the endpoint. The version and installation location are defined in the client configuration for the deployment.
6. Display deployment status.

Deployment status

Deployments can have the following status:

- Install completed
- Install failed
- Not applicable

For more information about troubleshooting deployments, see [Troubleshoot deployments on page 36](#).

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 the **Administration > System Status** page to review recent client registration details.

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 send it to your Technical Account Manager (TAM).

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.

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 Install 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 23](#).

Problem: Endpoint Install 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. SMB ports on 139 and 445 must be open. 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](#).
- (Windows endpoints) If the client is non-domain joined, you must edit the Windows registry to allow remote installations. In most Active Directory environments, admin shares are already available. For standalone machines that have not joined the domain, you might have to enable admin shares so that a user can reach `c$` with sufficient permissions. In Windows 7

and 8 machines, enable the admin shares of a standalone machine by adding the following registry key and restarting the computer:

```
Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\Policies\System
Name: LocalAccountTokenFilterPolicy
Data Type: REG_DWORD
Value: 1
```

IMPORTANT: Admin shares are not available in Home editions of Windows operating systems.

Problem: Endpoint Install 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 Install 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 **Tanium Solutions**.
2. In the **Tanium Content** section, select the **Client Management** row.
3. Click **Uninstall Solution**. Click **Uninstall** to complete the process.