Tanium™ Deploy User Guide

Version 2.20.131

July 25, 2023

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

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

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

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

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

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years and has most recently completed certification against the WCAG 2.1 / VPAT 2.3 standards for all major product modules in summer 2021. In the recent testing the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.1 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

As new products and features are continuously delivered, Tanium will conduct testing to identify potential gaps in compliance with accessibility guidelines. Tanium is committed to making best efforts to address any gaps quickly, as is feasible, given the severity of the issue and scope of the changes. These objectives are factored into the ongoing delivery schedule of features and releases with our existing resources.

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

Table of contents

Deploy overview

Deploy is a software management module that you can use to rapidly install, update, and remove software across large organizations with minimal infrastructure requirements. You can create deployments to run during a maintenance window that is convenient for your IT operations.

You can deploy applications or a group of applications to a flexible set of targets, including computer groups, user groups, departments, locations, individual computers, and individual users. You can also update existing software installation to the latest available versions, and create custom packages to install, update, and remove applications.

Software packages

A Tanium Deploy *software package* is a combination of source files, metadata, detection logic, and actions that are used to detect, install, update, and remove software from Tanium managed devices.

Each software package contains the following elements:

Package Files

The files needed to install, update, remove, or configure an application. This typically includes installation files, but can also be any files that are used by the software package.

Package Details

The product vendor, name, version, and platform of the software package. A Self Service display name, description, or package icon can optionally be added.

System Requirements

The requirements to install or update the software package on a managed endpoint: minimum RAM and disk space, system architecture, or specific operating systems that are supported.

Deploy Operations

The changes that the software package can make when it is deployed to endpoints: installing, updating, or removing the package. Software packages can have any combination of these operations defined, or they can have no operations and be used only for reporting and auditing purposes.

Installation Requirements

The conditions that must be met to install the software package, such as prerequisite applications.

Update Detection

The conditions that must be met to update the software package. Typically, this is the presence of a previous version of the product.

Install Verification

The conditions that must be met to identify that the software package is installed.

For more information, see Create a software package on page 54.

Software bundles

A Tanium Deploy *software bundle* is a list of Deploy software packages that can be deployed and executed in an ordered sequence. Software bundles are used to deploy a list of packages that are used by specific departments or user types.

For more information, see Create a software bundle on page 69.

Predefined Package Gallery

The Tanium Deploy *Predefined Package Gallery* is a collection of software packages that you can use to distribute software package templates. These templates include all of the required information for you to import and deploy third-party software. The Predefined Package Gallery is updated hourly. For a list of packages in the Predefined Package Gallery, see Reference: Predefined Package Gallery on page 122.

For more information, see Import a software package from the Predefined Package Gallery on page 61.

Applicability scans

You can configure how often applicability scans run for the software packages that are in the Deploy software package catalog, and how frequently the applicability status cache is updated.

Applicability scans evaluate endpoints against the required operating system, minimum disk space, memory, and requirements. Applicability scans run under the following circumstances to determine if a Tanium managed device is eligible to install, is eligible for update, installed, or has failed requirements:

- On a schedule according to the **Scan Interval** setting (Default: 24 hours)
- When the endpoint receives a new deployment for the first time or a new or updated software package
- When a deployment is about to run or has finished running a software package operation
- When a user logs onto a Windows computer or opens the Self Service Client

Install Eligible

The count of systems where the software is not installed and system requirements are met.

Update Eligible

The count of systems where one or more of the previous versions of the application are detected, and the software package can update those systems.

Installed

The count of systems where the software package is already installed.

Update Ineligible

The count of systems where one or more of the previous versions of the application are detected, but the system requirements are not met.

Not Applicable

The count of systems where the system requirements or prerequisites are not met.

For information about how Deploy determines software package applicability, see View software package applicability on page 64.

Deployments

A deployment is a one-time or recurring action to install, update, or remove applications on targeted endpoints. For more information, see Deploying software on page 71.

Deployment templates can be used to save settings for a deployment that you can issue repeatedly. For more information, see Create a deployment template on page 71.

Maintenance windows

Maintenance windows designate the permitted times that the targeted computer groups are open for deployments to run. You can have multiple maintenance windows, even with overlapping times. Maintenance windows do not interfere with each other. For a deployment to take effect, the deployment and maintenance window times must be met. For more information, see Managing maintenance windows on page 90.

Self service profiles

With the Self Service Client application, you can publish software to Windows endpoints so that users can install software on their own without the need for IT to install for them. Deploy self service profiles and the Self Service Client application are used in conjunction with End-User Notification profiles in Tanium™ End-User Notifications 1.5 or later. For more information, see Managing End-User Self Service on page 93.

Interoperability with other Tanium products

Deploy works with other Tanium products to provide additional features and reporting.

API Gateway

Use API Gateway to access the Deploy API. For information about what features are available through the API Gateway, see Tanium API Gateway User Guide: Schema reference.

End-User Notifications

Deploy uses Tanium™ End-User Notifications to notify users about deployments to Windows and macOS endpoints, and to configure End-User Self Service capabilities. You can create a message with your deployment to notify the user that the system is about to begin a deployment, has completed a deployment, and if postponements are enabled, to give the user the option to postpone the deployment or restart now. For more information, see Tanium End-User Notifications.

Reporting

If you have Tanium Reporting 1.12 or later, Deploy uses Tanium™ Reporting to create the charts on the Deploy **Overview** page. For more information, see Tanium Reporting.

Trends

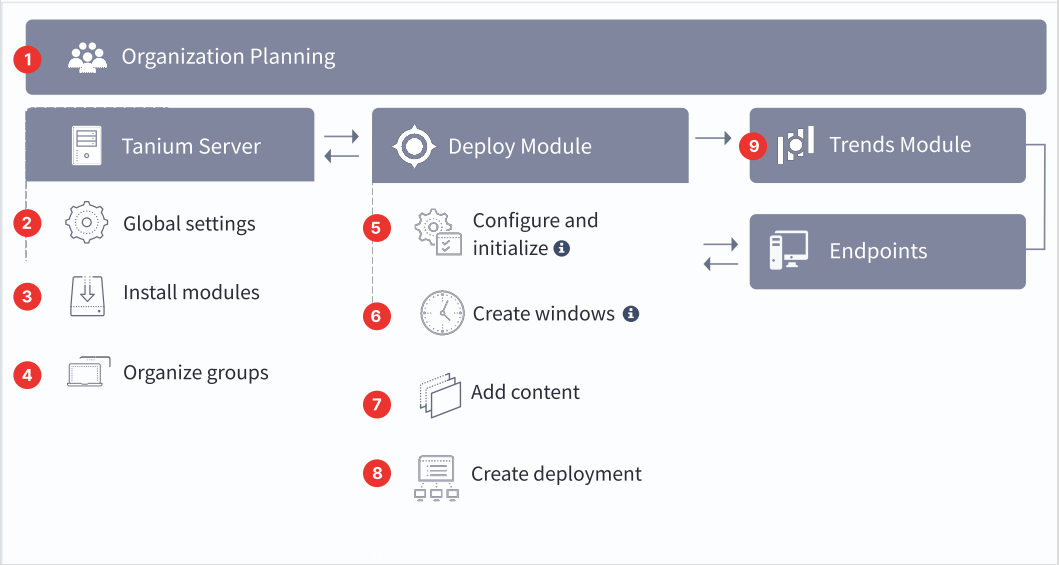
Deploy has built in integration with Tanium™ Trends to provide data visualization. The **Deploy** board displays metrics related to software deployment, including machines running Deploy and gallery packages that are installed. The following panels are in the **Deploy** board:

- Summary
    - Deploy Coverage
    - Endpoints Missing Software Updates Released Over 30 Days Ago
    - Mean Time to Deploy Software
    - Software Installed by Self Service User Request
- Gallery Updates
    - Top 25 Gallery Packages Installed
    - Top 25 Gallery Package Updates Needed
- Endpoint Status
    - Online - Endpoints Running Deploy
    - Historical - Endpoints Running Deploy

For more information about how to import the Trends board that is provided by Deploy, see Tanium Trends User Guide: Importing the initial gallery.

Succeeding with Deploy

Follow these best practices to achieve maximum value and success with Tanium Deploy. These steps align with the key benchmark metrics: increasing deploy coverage, reducing endpoints missing software updates released over 30 days and mean time to deploy, and optimizing software installed by self service user requests.



Step 1: Gain organizational effectiveness

Complete the key organizational governance steps to maximize Deploy value. For more information about each task, see Gaining organizational effectiveness on page 18.

- ☐ Develop a dedicated change management process.
- ☐ Define distinct roles and responsibilities in a RACI chart.
- ☐ Validate cross-functional organizational alignment.
- ☐ Track operational metrics.

Step 2: Configure platform settings

- ☐ Increase the client cache size to 2 GB to accommodate package distribution.

See Configure advanced settings on page 46.

Step 3: Install and configure Tanium modules

☐ Install Tanium End-User Notifications. See Tanium End-User Notifications User Guide: Installing End-User Notifications.

☐ Install Tanium Deploy. See Installing Deploy on page 43.

> If you installed Deploy using the **Apply All Tanium recommended configurations** option, the service account is automatically set to the account that you used to install Deploy.

☐ Install Tanium Trends. See Tanium Trends User Guide: Installing Trends.

☐ Install Tanium Client Management, which provides Tanium Endpoint Configuration. See Tanium Client Management User Guide: Installing Client Management.

☐ Import the **IT Operations Metrics** board from the Trends initial gallery. See Tanium Trends User Guide: Importing the initial gallery.

> If you installed Trends using the **Apply All Tanium recommended configurations** option, the **IT Operations Metrics** board is automatically imported.

Step 4: Organize computer groups and set the Deploy action group

☐ Create computer groups. See Tanium Console User Guide: Create a computer group.

Additional computer groups might be required to fulfill the requirements of your organization. See Organize computer groups on page 48.

☐ Configuring Deploy on page 46.

> If you installed Deploy using the **Apply All Tanium recommended configurations** option, the Deploy action group is automatically set to the `All Computers` computer group.

☐ Ensure that all operating systems that are supported by Deploy are included in the Deploy action group.

Step 5: Configure and initialize endpoints

☐ Create an End-User Notifications profile for End-User Self Service. See Tanium End-User Notifications User Guide: Customizing the end-user interface.

> If you installed Tanium End-User Notifications using the **Apply All Tanium recommended configurations** option, a default End-User Notifications profile is automatically created.

☐ Initialize End-User Notifications endpoints. See Tanium End-User Notifications User Guide: Initialize endpoints.

☐ Initialize Deploy endpoints on page 53.

Step 6: Create maintenance windows

☐ Create a maintenance window that properly overlaps with deployment times and change control process timelines.

> If you installed Deploy using the **Apply All Tanium recommended configurations** option, an **Always On** maintenance window is automatically created and enforced against the `All Computers` computer group.

☐ Verify that the **Computers with Enforced Maintenance Windows** chart in the **Health** section of the Deploy **Overview** page shows 100% enforcement.

See Managing maintenance windows on page 90.

Step 7: Add content

☐ Import software packages from the Predefined Package Gallery or create your own custom packages. See Managing software on page 54.

☐ Assign packages to software bundles. See Create a software bundle on page 69.

☐ Create a self service profile on page 93 to include the packages or bundles.

Step 8: Create deployments

☐ Create a deployment template for quick application of defaults in a deployment. See Create a deployment template on page 71.

☐ Create a deployment to install software for each of the supported operating systems in your environment.

☐ Ensure that deployment windows are long enough for endpoints to download and install the software, and properly overlap with maintenance window times.

☐ Use the **Make available before start time** option for deployments that are set for the future.

☐ If the software requires a restart, use the **Restart** and **Notify User** options and set the **Duration of Postponement** value to less than one day.

See Deploying software on page 71.

Step 9: Monitor Deploy metrics

☐ From the Trends menu, go to **Boards** and then click **IT Operations Metrics** to view the **Deploy Coverage**, **Endpoints Missing Software Updates Released Over 30 Days**, **Mean Time to Deploy Software**, and **Software Installed by Self Service User Request** panels in the **Deploy** section.

☐ Monitor and troubleshoot Deploy coverage on page 98.

☐ Monitor and troubleshoot endpoints missing software updates released over 30 days on page 99.

☐ Monitor and troubleshoot mean time to deploy software on page 100.

☐ Monitor and troubleshoot software installed by self service user request on page 100.

Gaining organizational effectiveness

The four key organizational governance steps to maximizing the value that is delivered by Deploy are as follows:

- Develop a dedicated change management process. See Change management on page 18.
- Define distinct roles and responsibilities. See RACI chart on page 18.
- Validate cross-functional alignment. See Organizational alignment on page 22.
- Track operational maturity. See Operational metrics on page 22.

Change management

Develop a tailored, dedicated change management process for software management, taking into account the new capabilities provided by Tanium.

- Update SLAs with elevated expectations, from software identification to software deployment.
- Identify key resources in your organization to review and approve software, to achieve effective software deployment results (example, aligned to an organizational-specific RACI chart).
- Align activities to key resources for Tanium software management activities across IT Security, IT Operations, and IT Risk/Compliance teams.
- Designate change or maintenance windows for all software management scenarios (example: emergency upgrades to general software, to achieve optimized software management efficacy).
- Create a Tanium steering group (TSG) for software management activities, to expedite reviews and approvals of processes that align with SLAs.

RACI chart

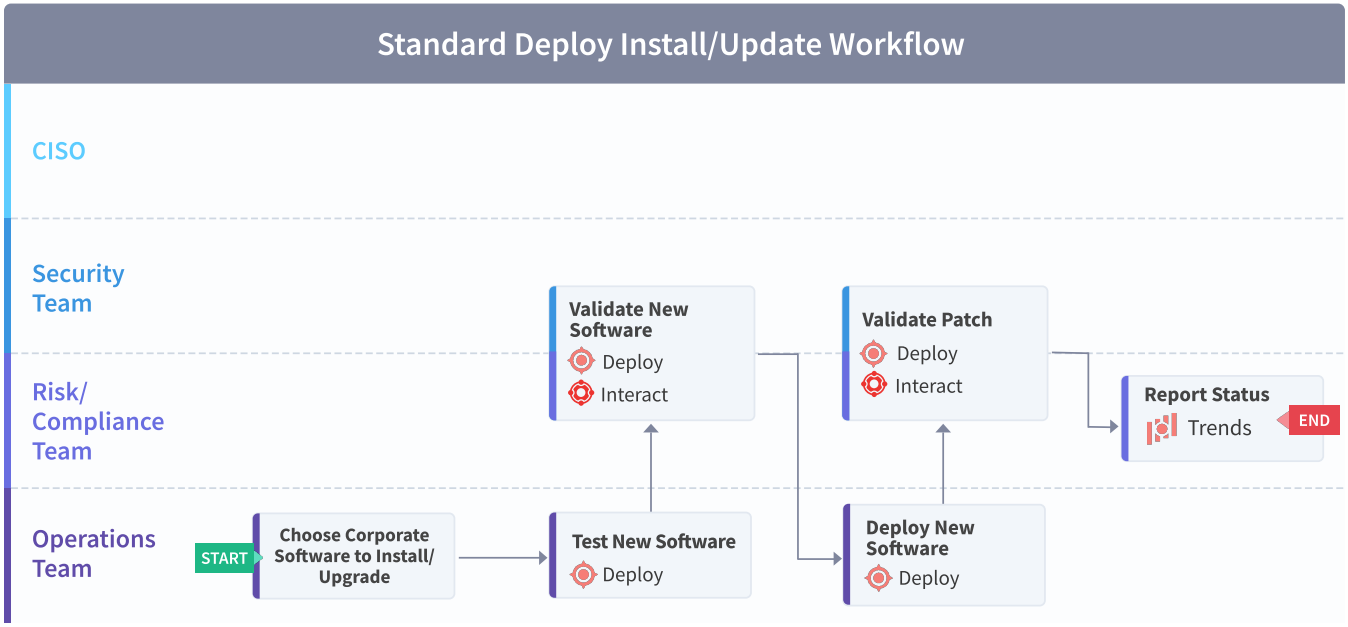
A RACI chart identifies the team or resource who is **R**esponsible, **A**ccountable, **C**onsulted, and **I**nformed, and serves as a guideline to describe the key activities across the security, risk/compliance, and operations teams. Every organization has specific business processes and IT organization demands. The following table represents Tanium's point of view for how organizations should align functional resources against patch management. Use the following table as a baseline example.

Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Deploy new or update existing corporate software See Standard Deploy install/update workflow on page 21.	I	A/R	I	-	Deployment of existing, approved corporate software and updating software versions is owned by the operations team. Include predefined notifications so that the security and risk/compliance teams are informed.
Deploy newly introduced corporate software See Standard Deploy install/update workflow on page 21.	C	A/R	I	-	Deployment of newly introduced corporate software is owned by the operations team. Include predefined notifications so that the security team is consulted and team risk/compliance team is informed.
Update or remove software due to threat intel/vulnerability See Standard threat intel/vulnerability update/remove workflow on page 22.	A	R	C	I	Updating or removal of corporate software that could be a threat to the environment is executed by the operations team, while the security team is ultimately accountable because the threat is deemed a risk to the environment. The risk/compliance team is consulted to ensure complete update or removal. The executive team is informed of the progress.

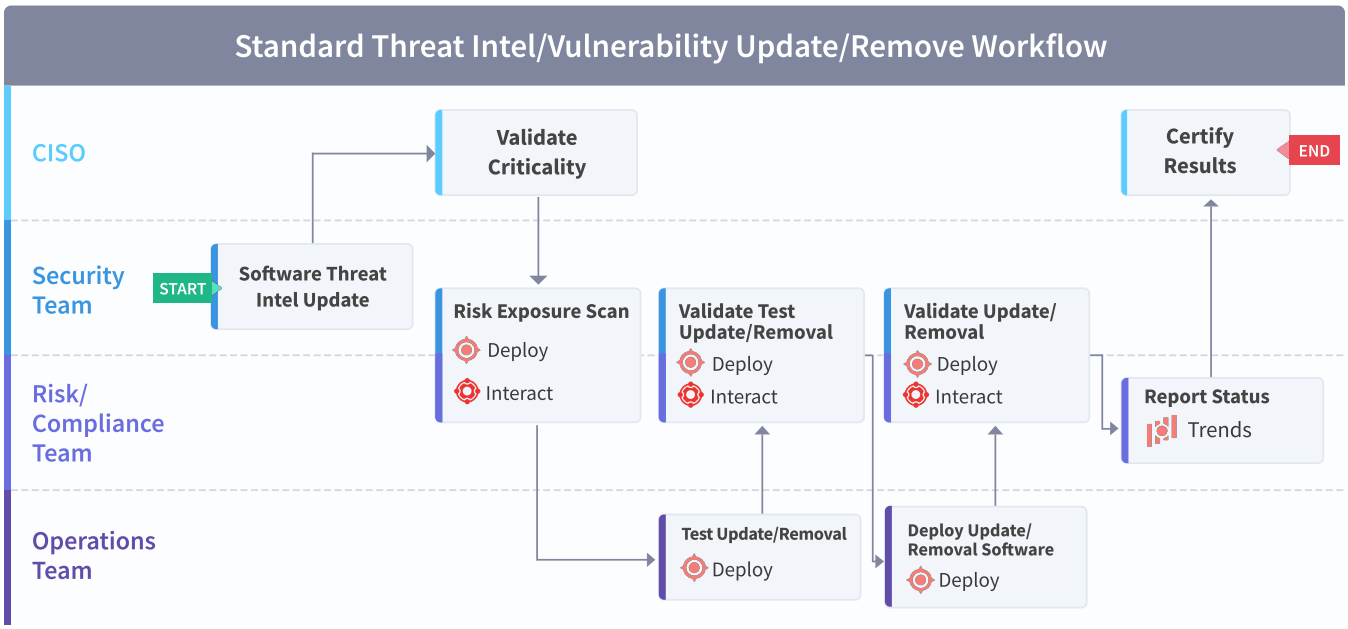
Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Testing of new or updated software	I	A/R	C	-	New corporate software should be tested to ensure compliance to current standards. The operations team owns the execution and responsibility of testing, with consultation from the risk/compliance team. The security team is informed that new software can be deployed.
User acceptance testing (UAT) and deployment to production	I	A/R	C	-	New corporate software should be tested to ensure compliance to current standards before deployment to production. The operations team owns the execution and responsibility of testing, with consultation from the risk/compliance team. The security team is informed that new software is being deployed.
Publish optional software to the Self Service application	I	A/R	I	-	The operations team is responsible and accountable for offering the user the Self Service application with the ability to add or remove software as the user chooses. The risk/compliance and security teams are informed of the options that are presented to the user.

Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Reporting metrics/dashboard of deployment or removal	C	A/R	C	I	The operations team is responsible and accountable for the deployment or removal process, consulting with the security and risk/compliance teams on any questions or concerns. The executive team is informed of key metrics that impact the environment.

Standard Deploy install/update workflow



Standard threat intel/vulnerability update/remove workflow



Organizational alignment

Successful organizations use Tanium across functional silos as a common platform for high-fidelity endpoint data and unified endpoint management. Tanium provides a common data schema that enables security, operations, and risk/compliance teams to assure that they are acting on a common set of facts that are delivered by a unified platform.

In the absence of cross-functional alignment, functional silos often spend time and effort in litigating data quality instead of making decisions to improve software management.

Operational metrics

Deploy maturity

Managing a software management program successfully includes operationalization of the technology and measuring success through key benchmarking metrics. The four key processes to measure and guide operational maturity of your Tanium Deploy program are as follows:

Process	Description
Usage	How and when Tanium Deploy is used in your organization
Automation	How automated Tanium Deploy is, across endpoints
Functional integration	How integrated Tanium Deploy is, across IT security, IT operations, and IT risk/compliance teams
Reporting	How automated Tanium Deploy is and who the audience of software management reporting is

Benchmark metrics

In addition to the key software deployment processes, the four key benchmark metrics that align to the operational maturity of the Tanium Deploy program to achieve maximum value and success are as follows:

Executive Metrics	Deploy Coverage	Endpoints Missing Software Updates Released Over 30 Days	Mean Time to Deploy Software	Software Installed by Self Service User Request
Description	Number of endpoints in each of these categories: • **Optimal**: Endpoints where Deploy is operational • **Needs Attention**: Endpoints that do not have the Deploy tools installed, are not targeted by a profile, or do not have a supported version of the Tanium Client installed • **Unsupported** : Endpoints with an operating system version that is not supported by Deploy	Percentage of endpoints that require an update.	Average number of days it takes to install or upgrade software on workstations.	Percentage of software that is installed through the Self Service Client application.
Instrumentation	Uses the `Deploy - Coverage Status` sensor to determine the endpoints where Deploy is optimal, needs attention, or unsupported.	Number of endpoints that are reporting at least one software application that is eligible for an update for more than 30 days / number of endpoints managed by Deploy.	The time it takes from software availability date to software installation date averaged by system, in the last three months.	Number of successful deployments through self-service / the total number of successful deployments on an endpoint in the last three months.

Executive Metrics	Deploy Coverage	Endpoints Missing Software Updates Released Over 30 Days	Mean Time to Deploy Software	Software Installed by Self Service User Request
Why this metric matters	Low percentage of **Optimal** against total manageable endpoints indicates that Deploy is not being used to its full potential and maximum ROI is not being achieved because you are covering only part of the environment. You cannot deploy software and update 3rd party applications to devices that are not under management (member of the Deploy action group). You also cannot provide full visibility of your environment without the tools being installed.	High percentage indicates lack of 3rd party update process or current process is not working. High percentage indicates configuration drift and could indicate a wider issue(for example, all users have admin rights). The Predefined Package Gallery can also provide insight into the overall state of the environment before import.	If it takes you too long to deploy software and validate that it was applied, you are at risk of being exploited by the vulnerabilities that are addressed by that software. Tanium is great at sending the software catalog and deployments and getting visibility of the enterprise. Package building is simple and quick with Deploy and even more so with using the Predefined Package Gallery and starting with a pre-built template to edit or test directly.	A moderate percentage means that users are installing software on their own without the use of IT resources like a help desk. A high percentage indicates too much dependency on user-installed applications and implies that administrative software installations are down, which can show a lack of control of software installations. A low or zero number indicates that either the feature is underused or not used at all.

Use the following table to determine the maturity level for Tanium Deploy in your organization.

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Deploy configured; Known common software imported from the Predefined Package Gallery	Piloting deployment of new software; Creating packages and bundles; Deploy is used by exception	Deploy is used for software updates, new software, and removal of software to audit legacy tooling	Deploy is used as the default tooling for software updates, new software deployment, and removal of software; Legacy tooling is used for audit	Deploy is used as the default tooling for software updates, new software deployment, and removal of software; Legacy tooling is sunset

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
	Automation	Manual	Manual	Partially automated (>50% of software deployment process automated)	Partially automated (>75% of software deployment process automated); Software available on endpoint for end user self service	Fully automated (>90% of patch deployment process automated); Software available on endpoint for end user self service
	Functional integration	Consult with software packaging or deployment teams and application owners	Consult with software packaging or deployment teams and application owners	Consult with help desk or support and IT Leadership or peers in enterprise vulnerability management and threat management	Deploy, Asset, Connect, and Trends integrated into enterprise vulnerability management, threat management, and asset management tools, such as Flexera and ServiceNow	Deploy, Asset, Connect, and Trends integrated into enterprise vulnerability management, threat management, and asset management tools, such as Flexera and ServiceNow; Approval workflow integration for tracking of licensed applications
	Reporting	Manual; Reporting for Operators only	Manual; Reporting for Operators and peer group only	Automated; Reporting for Operators and peer group only	Automated; Reporting tailored to stakeholders ranging from Operator to Executive	Automated; Reporting tailored to stakeholders ranging from Operator to Executive

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Metrics	Deploy Coverage	0-92%	93-94%	95-96%	97-98%	99-100%
	Endpoints Missing Software Updates Released Over 30 Days	> 15%	11-15%	6-10%	2-5%	0-1%
	Mean Time to Deploy Software	> 30 days	26-30 days	21-25 days	15-20 days	1-14 days
	Software Installed by Self Service User Request	0-19%	20-35%	36-50%	51-75%	76-100%

Deploy requirements

Review the requirements before you install and use Deploy.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes Deploy
- **Tanium™ Core Platform servers:** 7.4.3.1204 or later
- **Tanium™ Client:** Any supported version of Tanium Client. For the Tanium Client versions supported for each OS, see Tanium Client Management User Guide: Client version and host system requirements.
  If you use a client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed client versions.

Computer group dependencies

When you first sign in to the Tanium Console after a fresh installation of Tanium Server, the server automatically imports the `All Computers` computer group, which Deploy requires.

For earlier versions of the Tanium Server, or after upgrading from an earlier version, you must manually create the computer groups. See Tanium Console User Guide: Create a computer group.

Solution dependencies

Other Tanium solutions are required for Deploy to function (required dependencies) or for specific Deploy features to work (feature-specific dependencies). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.

Some Deploy dependencies have their own dependencies, which you can see by clicking the links in the lists of Required dependencies on page 29 and Feature-specific dependencies on page 29. Note that the links open the user guides for the latest version of each solution, not necessarily the minimum version that Deploy requires.

Tanium recommended installation

If you select **Tanium Recommended Installation** when you import Deploy, the Tanium Server automatically imports all your licensed solutions at the same time. See Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Deploy to import and are using Tanium Core Platform 7.5.2.3531 or later with Tanium Console 3.0.72 or later, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are earlier than the minimum required for Deploy, the server automatically updates those dependencies to the latest available versions.

If you select only Deploy to import and you are using Tanium Core Platform 7.5.2.3503 or earlier with Tanium Console 3.0.64 or earlier, you must manually import or update required dependencies. See Tanium Console User Guide: Import, re-import, or update specific solutions.

Required dependencies

Deploy has the following required dependencies at the specified minimum versions:

- Tanium™ Endpoint Configuration 1.2 or later (installed as part of Tanium Client Management 1.5.112 or later)
- Tanium™ Interact 2.4.74 or later (use the latest version of Interact for best results)
- Tanium Trends 3.6.323 or later
- Tanium End-User Notifications 1.14.55 or later
- Tanium™ System User Service 1.0.77 or later

Feature-specific dependencies

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

- Tanium™ Reporting 1.16.58 or later. Review charts on the **Overview** page. If Reporting is not installed, Trends creates the charts.
    - Tanium™ Blob Service 1.0.6 or later
    - Reporting Content 1.0.24 or later

Tanium Server and Module Server

Deploy 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 about Tanium Server and Module Server sizing guidelines, see Tanium Core Platform Installation Guide: Host system sizing guidelines.

Endpoints

Contact Tanium Support on page 110 for customized tuning to your environment. For more information, see Tanium Platform User Guide: Managing Tanium Core Platform Settings.

Supported operating systems

Operating System	Version	Notes
Windows Server	Windows Server 2008 R2 Service Pack 1 or later	• Windows Server Core not supported for End-User Notifications functionality. • Windows Server 2008 R2 Service Pack 1 requires Microsoft KB2758857. • Windows Server 2012 R2 requires Microsoft KB2919394 or KB2919355 for End-User Self Service functionality.
Windows Workstation	Windows 7 Service Pack 1 or later	• Windows 7 Service Pack 1 requires Microsoft KB2758857. • Windows 8.1 requires Microsoft KB2919394 or KB2919355 for End-User Self Service functionality. • IMPORTANT Deploy does not support Arm-based Windows endpoints.
macOS	• macOS 13 Ventura • macOS 12 Monterey • macOS 11 Big Sur • macOS 10.15 Catalina • macOS 10.14.6 Mojave • macOS 10.13.6 High Sierra	IMPORTANT Apple does not provide security updates for macOS 10.15 and earlier versions and Tanium does not test these versions. macOS 10.13 has known issues with file extraction and other features may not work as expected. For full Deploy functionality and support, upgrade to macOS 11 or later.

Supported operating systems (continued)

Operating System	Version	Notes
Linux	• AlmaLinux 8.x, 9.x • Amazon Linux 1 or later • CentOS 6 or 7 • Debian 8 or later • openSUSE Linux 11.x Service Pack 3 or later, 12.x, 15.x • Oracle Linux 6.x, 7.x, 8.x, 9.x • Red Hat Enterprise Linux (RHEL) 6.x, 7.x, 8.x, 9.x • Rocky Linux 8.x, 9.x • SUSE Linux Enterprise Desktop 11.3, 11.4, 12.x, 15.x • SUSE Linux Enterprise Server 11.3, 11.4, 12.x, 15.x • Ubuntu 14.04 or later	

Windows System environment variables

The use of environment variables when you refer to file paths in Deploy is recommended over the use of explicit file paths. This method provides independence from differing paths based on operating system language or architecture, and allows the construction of a dynamic path at the time of execution.

Process Architecture	System Environment Variable	Path
32-bit process on 32-bit Windows	`%PROGRAMFILES%`	`C:\Program Files`
	`%COMMONPROGRAMFILES%`	`C:\Program Files\Common Files`
32-bit process on 64-bit Windows	`%PROGRAMFILES%`	`C:\Program Files (x86)`
	`%PROGRAMFILESX86%`	`C:\Program Files (x86)`
	`%COMMONPROGRAMFILES%`	`C:\Program Files (x86)\Common Files`
	`%COMMONPROGRAMFILES(X86)%`	`C:\Program Files (x86)\Common Files`
	`%COMMONPROGRAMW6432%`	`C:\Program Files\Common Files`
	`%PROGRAMW6432%`	`C:\Program Files`

NOTE Additional environment variables that are available to the System account, such as `%SystemDrive%`, `%SystemRoot%`, `%WinDir%`, are also supported.

Host and network security requirements

Specific ports, processes, and URLs are needed to run Deploy.

Ports

The following ports are required for Deploy communication.

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17463	TCP	Internal purposes; not externally accessible

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, Tanium recommends that a security administrator create exclusions to allow the Tanium processes to run without interference. The configuration of these exclusions varies depending on AV software. For a list of all security exclusions to define across Tanium, see Tanium Core Platform Deployment Reference Guide: Host system security exclusions.

For Windows endpoints, review and follow the Microsoft antivirus security exclusion recommendations for enterprise computers. For more information, see Microsoft Support: Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows (KB822158).

Deploy security exclusions

Target Device	Notes	Exclusion Type	Exclusion
Module Server		Process	`<Module Server>\services\deploy-service\node.exe`
	Required when Endpoint Configuration is installed	Process	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`
Windows endpoints	Required only for the Microsoft InPlace Upgrade packages	Folder	`C:\Deploy\Tanium`
		Process	`<Tanium Client>\Python38\TPython.exe`
		Folder	`<Tanium Client>\Python38`
		Process	`<Tanium Client>\Tools\SoftwareManagement\7za.exe`
		Process	`<Tanium Client>\TaniumCX.exe`
		File	`<Tanium Client>\extensions\TaniumSoftwareManager.dll`
		File	`<Tanium Client>\extensions\TaniumSoftwareManager.dll.sig`
		File	`<Tanium Client>\Tools\SoftwareManagement\data\software-management.db`
		File	`<Tanium Client>\Tools\SoftwareManagement\data\software-management.db-wal`
		File	`<Tanium Client>\Tools\SoftwareManagement\data\software-management.db-shm`

Deploy security exclusions (continued)

Target Device	Notes	Exclusion Type	Exclusion
Linux endpoints		Process	<*Tanium Client*>/python38/python
		Folder	<*Tanium Client*>/python38
		Process	<*Tanium Client*>/TaniumCX
		File	<*Tanium Client*>/Tools/SoftwareManagement/data/software-management.db
		File	<*Tanium Client*>/Tools/SoftwareManagement/data/software-management.db-wal
		File	<*Tanium Client*>/Tools/SoftwareManagement/data/software-management.db-shm
		File	<*Tanium Client*>/extensions/libTaniumSoftwareManager.so
		File	<*Tanium Client*>/extensions/libTaniumSoftwareManager.so.sig
macOS endpoints		Process	<*Tanium Client*>/python38/python
		Folder	<*Tanium Client*>/python38
		Process	<*Tanium Client*>/TaniumCX
		File	<*Tanium Client*>/extensions/libTaniumSoftwareManager.dylib
		File	<*Tanium Client*>/extensions/libTaniumSoftwareManager.dylib.sig

Internet URLs

If security software is deployed in the environment to monitor and block unknown URLs, your security administrator must allow the following URLs on the Tanium Server and the Tanium Module Server for the Deploy service.

The Tanium Server and the Tanium Module Server require access to the following websites to download binaries for the Predefined Package Gallery templates.

Software Package	Domain	Port
Adobe Acrobat DC[1]	download.adobe.com	443
Adobe Acrobat Reader DC	ardownload2.adobe.com	443
	download.adobe.com	
Adobe AIR	download.macromedia.com	443

Software Package	Domain	Port
Adobe Digital Editions	adedownload.adobe.com	443
Adobe Flash Player	fpdownload.macromedia.com	443
Adobe Shockwave EOL[2]	fpdownload.macromedia.com	443
AgileBits 1Password 7	c.1password.com	443
Apache Tomcat	dlcdn.apache.org	443
Apple iTunes	secure-appldnld.apple.com	443
Apple macOS Upgrade (Big Sur, Monterey, and Ventura)	swscan.apple.com swcdn.apple.com swdist.apple.com	443
Arco Software CutePDF Writer	www.cutepdf.com	443
Arduino IDE	downloads.arduino.cc	443
Atlassian Sourcetree	product-downloads.atlassian.com	443
Bare Bones BBEdit	s3.amazonaws.com/BBSW-download	443
BlueJeans Network, Inc BlueJeans	swdl.bluejeans.com	443
Box Inc. Box Drive	e3.boxcdn.net	443
Cisco Jabber	binaries.webex.com	443
Cisco Network Recording Player	akamai.webex.com	443
Cisco Webex Recorder and Player	welcome.webex.com	443
Citrix Workspace (formerly Citrix Receiver)	downloadplugins.citrix.com	443
Corel Corporation WinZip	download.winzip.com	443
DB Browser for SQLite Team DB Browser for SQLite	sqlitebrowser.org	443
Devolutions Inc. Remote Desktop Manager	http://cdn.devolutions.net	443
Discord, Inc Discord	dl.discordapp.net	443
Docker Desktop	desktop.docker.com	443
	www.docker.com/products/docker-desktop/	
Dropbox Desktop Client	clientupdates.dropboxstatic.com	443

Software Package	Domain	Port
Eclipse Adoptium Temurin JDK/JRE	github.com	443
Evernote Corporation Evernote	cdn1.evernote.com	443
Extensis Universal Type Client	bin.extensis.com	443
Foxit Software Inc PDF Reader	cdn01.foxitsoftware.com	443
George Nachman iTerm2	iterm2.com	443
GN Audio Jabra Direct	jabraxpressonlineprdstor.blob.core.windows.net	443
Google Android Studio	*.gvt1.com	443
Google Chrome	dl.google.com	443
Google Drive File Stream	dl.google.com	443
Helios TextPad	www.textpad.com	443
Igor Pavlov 7-Zip	crl.identrust.com	80
	7-zip.org	443
iterate GmbH Cyberduck	update.cyberduck.io	443
JAM Software TreeSize Free	downloads.jam-software.de	443
JetBrains DataGrip	download.jetbrains.com	443
JetBrains GoLand	download-cdn.jetbrains.com	443
JetBrains PyCharm	download-cdn.jetbrains.com	443
Licecap Licecap	https://www.cockos.com/licecap/	443
KeePass KeePass 1 and 2	sourceforge.net	443
MacPaw The Unarchiver	dl.devmate.com	443
Martin Prikryl WinSCP	sourceforge.net	443
Microsoft .NET Framework	download.visualstudio.microsoft.com	443
Microsoft Edge	msedge.sf.dl.delivery.mp.microsoft.com	443
	officecdn-microsoft-com.akamaized.net	
Microsoft Feature Update to Windows 10, version 21H2 (KB5003791)	catalog.s.download.windowsupdate.com	443
Microsoft Office 2019	officecdn-microsoft-com.akamaized.net	443

Software Package	Domain	Port
Microsoft Office 2019 with Teams	officecdn-microsoft-com.akamaized.net	443
Microsoft Office Click-to-Run	download.microsoft.com	443
Microsoft Power BI Desktop	download.microsoft.com	443
Microsoft Skype Desktop Client	download.skype.com	443
Microsoft SQL Server Management Studio	aka.ms	443
Microsoft Teams	statics.teams.cdn.office.net	443
Microsoft Visual Studio Code	code.visualstudio.com	443
Microsoft Windows 10 Upgrade[3]	content.tanium.com	443
Mozilla Firefox	releases.mozilla.org	443
	download-installer.cdn.mozilla.net	
Node.js Foundation NodeJS	nodejs.org	443
Notepad++ Team Notepad++	download.notepad-plus-plus.org	443
Oracle Java Runtime	javadl.oracle.com	443
	sdlc-esd.oracle.com	
Oracle MySQL Community	dev.mysql.com	443
Oracle VirtualBox	download.virtualbox.org	443
pgAdmin pgAdmin 4	ftp.postgresql.org	443
Piriform Software CCleaner Standard	bits.avcdn.net	443
Postman Postman	postman.com	443
Royal Apps GmbH Royal TS	download.royalapplications.com	443
Running with Crayons Ltd Alfred 5	cachefly.alfredapp.com	443
Scooter Software Beyond Compare	www.scootersoftware.com	443
Simon Tatham PuTTY	the.earth.li	443
Slack Slack	downloads.slack-edge.com	443
Splunk Universal Forwarder	download.splunk.com	443
	docs.splunk.com	

Software Package	Domain	Port
Stamps.com, Inc Stamps.com	resources.stamps.com	443
Tableau Reader	downloads.tableau.com	443
TechSmith Camtasia	download.techsmith.com	443
	support.techsmith.com	
TechSmith Snagit	download.techsmith.com	443
	support.techsmith.com	
The Wireshark developer community Wireshark	2.na.dl.wireshark.org	443
3T Software Labs Ltd Studio 3T (Arm) and (Intel)	download.studio3t.com	443
TortoiseSVN TortoiseSVN	osdn.net	443
VideoLAN VLC Media Player	download.videolan.org	443
VMware Tools	packages.vmware.com	443
VMware Workstation Player[4]	download3.vmware.com	443
win.rar GmbH WinRAR 32-bit and WinRAR 64-bit	www.win-rar.com	443
Yubico Authenticator	developers.yubico.com	443
Zoom Outlook Plugin	zoom.us	443
Zoom Rooms NOTE On macOS, the MDM profile needs to allow access to camera, microphone, and screen sharing to avoid permission prompts on the endpoint.	d11yldzmag5yn.cloudfront.net	443
	zoom.us	
Zoom Zoom	d11yldzmag5yn.cloudfront.net	443
	zoom.us	

[1] Update operation only.

[2] Remove operation only.

[3] Windows 10 Operating System media is not included in this package template. For more information, see Use case: Upgrading Windows on page 1.

[4] Update and Remove operations only.

User role requirements

The following tables list the role permissions required to use Deploy. To review a summary of the predefined roles, see Set up Deploy users on page 48.

IMPORTANT On installation, Deploy creates a **Deploy** user to automatically manage the Deploy service account. Do not edit or delete the **Deploy** user.

For more information about role permissions and associated content sets, see Tanium Core Platform User Guide: Managing RBAC.

Deploy user role permissions

Permission	Deploy Administrator [1,2,3,4]	Deploy Endpoint Configuration Approver[1,2]	Deploy Operator [1,2,3,4]	Deploy Package Administrator [1,2,3,4]	Deploy Read Only User[2,3,4]	Deploy User[1,2,3]
Deploy View the Deploy workbench	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW
Deploy API Perform Deploy operations using the API	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE	✓ EXECUTE
Deploy Deployments Create and modify deployments	✓ WRITE	✗	✓ WRITE	✗	✗	✓ WRITE
Deploy Endpoint Configuration APPROVE: Approve Deploy items for Endpoint Configuration REGISTER: Register with Endpoint Configuration	✗	✓ APPROVE	✗	✗	✗	✗
Deploy Maintenance Windows Create, modify, and remove maintenance windows	✓ WRITE	✗	✓ WRITE	✗	✗	✓ WRITE

Deploy user role permissions (continued)

Permission	Deploy Administrator [1,2,3,4]	Deploy Endpoint Configuration Approver[1,2]	Deploy Operator [1,2,3,4]	Deploy Package Administrator [1,2,3,4]	Deploy Read Only User[2,3,4]	Deploy User[1,2,3]
Deploy Module Read and write access to the Deploy module, including creating, editing, deleting, and importing software packages	✓ READ WRITE	✓ READ	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ WRITE
Deploy Operator Settings Write access to a subset of platform settings in the Deploy module	✓ WRITE	✗	✓ WRITE	✗	✗	✗
Deploy Profiles Create, modify, and delete self service profiles	✓ WRITE	✗	✓ WRITE	✗	✗	✓ WRITE
Deploy Settings Write access to platform settings in the Deploy module	✓ WRITE	✗	✗	✗	✗	✗

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

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

[3] 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.

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

Provided Deploy administration and platform content permissions

Permission	Permission Type	Deploy Administrator [1,2,3,4]	Deploy Endpoint Configuration Approver[2,3,4]	Deploy Operator [1,2,3,4]	Deploy Package Administrator [1,2,3,4]	Deploy Read Only User[2,3,4]	Deploy User[2,3,4]
User	Administration	✓ READ	✗	✓ READ	✗	✗	✗
Action	Platform Content	✓ READ WRITE	✓ READ	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ WRITE
Approve Action	Platform Content	✓ SPECIAL	✗	✓ SPECIAL	✓ SPECIAL	✗	✓ SPECIAL
Filter Group	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ
Own Action	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ	✓ READ
Package	Platform Content	✓ READ WRITE	✓ READ	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ WRITE
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	Platform Content	✓ READ WRITE	✓ READ	✓ READ WRITE	✓ READ WRITE	✓ READ	✓ READ WRITE

Provided Deploy administration and platform content permissions (continued)

Permission	Permission Type	Deploy Administrator [1,2,3,4]	Deploy Endpoint Configuration Approver[2,3,4]	Deploy Operator [1,2,3,4]	Deploy Package Administrator [1,2,3,4]	Deploy Read Only User[2,3,4]	Deploy User[2,3,4]
Sensor	Platform Content	READ	READ	READ	READ	READ	READ

To view which content set permissions are granted to a role, see Tanium Console User Guide: View effective role permissions.

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

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

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

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

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

Installing Deploy

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

- **Automatic configuration with default settings** (Tanium Core Platform 7.4.2 or later only): Deploy 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 Deploy, see Import Deploy with default settings on page 43.
- **Manual configuration with custom settings** After installing Deploy, you must manually configure required settings. Select this option only if Deploy requires settings that differ from the recommended default settings. For more information, see Import Deploy with custom settings on page 44.

Before you begin

- Read the release notes.
- Review the Deploy requirements on page 28.
- If you are upgrading from a previous version, see Upgrade Deploy on page 45.

Import Deploy with default settings

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

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

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group
Deploy deployment templates	The following deployment templates are created: • **[Standard Deployment]** - default • **[Deployment with Reboot]** • **[Deployment with Pre-Notification]**

Setting	Default value
Deploy maintenance windows	An `Always On` maintenance window is created, and enforced against the `All Computers` computer group.
Deploy configurations	For action locked machines, only applicability scanning is enabled, so that deployments cannot run on action locked machines.
Deploy software packages	The following Predefined Package Gallery packages are automatically imported: • Adobe Digital Editions • Adobe Acrobat Reader DC (en-us) • Adobe Acrobat Reader DC (en-us) (64-bit) • Adobe Acrobat Reader DC (MUI) • Adobe Acrobat Reader DC (MUI) (64-bit) • Microsoft Power BI Desktop (x64) • Microsoft Power BI Desktop • Microsoft Teams (x64) • Microsoft Teams (x86) • Microsoft Visual Studio Code (x64 en-us) • Microsoft Visual Studio Code (x86 en-us) • Mozilla Firefox (x64 en-US) • Mozilla Firefox (x86 en-US) • VideoLAN VLC media player (32-bit) • VideoLAN VLC media player (64-bit) • Zoom Zoom • Zoom Zoom (64-bit)

To import Deploy and configure default settings, be sure to select the **Apply All Tanium recommended configurations** check box while performing the steps in Tanium Console User Guide: Import, re-import, or update specific solutions. After the import, verify that the correct version is installed: see Verify Deploy version on page 45.

Import Deploy with custom settings

To import Deploy without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** check box while performing the steps in Tanium Console User Guide: Import, re-import, or update specific solutions. After the import, verify that the correct version is installed: see Verify Deploy version on page 45.

To organize computer groups, see Organize computer groups on page 48.

To configure the Deploy action group, see Configuring Deploy on page 46.

Manage solution dependencies

Other Tanium solutions are required for Deploy to function (required dependencies) or for specific Deploy features to work (feature-specific dependencies). See Solution dependencies.

Upgrade Deploy

IMPORTANT

In Deploy 2.19, the steps required to configure the service account are no longer necessary due to the adoption of the System User Service, which performs these tasks automatically. After upgrading to Deploy 2.19, it might take time for the RBAC privileges and other updates to sync properly. This could lead to issues and error messages when you first query the Tanium Console. These issues usually resolve on their own after a few minutes, but could take up to an hour or longer depending on system resources and the amount of data to migrate.

For the steps to upgrade Deploy, see Tanium Console User Guide: Import all modules and services. After the upgrade, verify that the correct version is installed: see Verify Deploy version on page 45.

Verify Deploy version

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

1. Refresh your browser.
2. From the Main menu, go to **Modules > Deploy** to open the Deploy **Overview** page.
3. To display version information, click Info .

Configuring Deploy

If you did not install Deploy with the **Apply All Tanium recommended configurations** option, you must enable and configure certain features.

Configure advanced settings

You can configure the Tanium platform for optimal delivery of larger payloads, which are typically associated with downloading and installing software.

1. From the Main menu, go to **Administration > Configuration > Settings > Advanced Settings**.
2. To increase the client cache size, click **Add Setting**, provide the following information, and click **Save**.
   Setting Type: `Client`
   Platform Setting Name: `ClientCacheLimitInMB`
   Value Type: `Numeric`
   Value : `2048`

Changes to platform settings can take up to five hours to propagate to clients.

Install and configure Tanium End-User Notifications

With the Tanium End-User Notifications solution, you can create a notification message with your deployment to Windows and macOS endpoints to notify the user that the system is about to begin a deployment, has completed a deployment, and if postponements are enabled, to give the user the option to postpone the deployment or restart now.

For more information, see Tanium End-User Notifications User Guide: End-User Notifications overview.

Install and configure Tanium Endpoint Configuration

Manage solution configurations with Tanium Endpoint Configuration

Tanium Endpoint Configuration delivers configuration information and required tools for Tanium Solutions to endpoints. Endpoint Configuration consolidates the configuration actions that traditionally accompany additional Tanium functionality and eliminates the potential for timing errors that occur between when a solution configuration is made and the time that configuration reaches an endpoint. Managing configuration in this way greatly reduces the time to install, configure, and use Tanium functionality, and improves the flexibility to target specific configurations to groups of endpoints.

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

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Deploy, see User role requirements on page 39. For more information about enabling and using configuration approvals in Endpoint Configuration, see Tanium Endpoint Configuration User Guide: Managing approvals.

IMPORTANT For solutions to perform configuration changes or tool deployment through Endpoint Configuration on endpoints with action locks turned on, you must enable the **Manifest Package Ignore Action Lock** and **Deploy Client Configuration and Support Package Ignore Action Lock** settings. To access these settings, from the Endpoint Configuration **Overview** page, click Settings and select **Global**. For more information about action locks, see Tanium Console User Guide: Managing action locks.

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

If you enabled configuration approvals, the following configuration changes must be approved in Endpoint Configuration before they deploy to endpoints:

- Creating, stopping, or reissuing deployments
- Adding or removing maintenance window enforcements
- Creating, editing, or removing self service profiles
- User-initiated actions, such as initializing endpoints, distributing the software package catalog, updating Deploy Settings

Configure Deploy

Configure the Deploy action group

Importing the Deploy module automatically creates an action group to target specific endpoints. If you did not use automatic configuration or you enabled restricted targeting when you imported Deploy, the action group targets **No Computers**.

If you used automatic configuration and restricted targeting was disabled when you imported Deploy, configuring the Deploy action group is optional.

Select the computer groups to include in the Deploy action group.

BEST PRACTICE Clear the selection for **No Computers** and make sure that all operating systems that are supported by Deploy are included in the Deploy action group.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Click **Tanium Deploy**.
3. Select the computer groups that you want to include in the action group and click **Save**.
   If you select multiple computer groups, choose an operator (AND or OR) to combine the groups.

Organize computer groups

One way to deploy packages or bundles is by computer group. Create relevant computer groups to organize your endpoints. Some options include:

- Endpoint type, such as servers or employee workstations
- Endpoint location, such as by country or time zone
- Endpoint priority, such as business-critical machines

Set up Deploy users

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

To review specific permissions for each role, see User role requirements on page 39.

On installation, Deploy creates a **Deploy** user to automatically manage the Deploy service account. Do not edit or delete the **Deploy** user.

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

Deploy Administrator

Assign the **Deploy Administrator** role to users who manage the configuration and deployment of Deploy functionality to endpoints.
This role can perform the following tasks:

- Manage all Deploy settings
- Manage deployments, maintenance windows, and Self Service profiles

Deploy Endpoint Configuration Approver

Assign the **Deploy Endpoint Configuration Approver** role to a user who approves or rejects Deploy configuration items in Tanium Endpoint Configuration.
This role approves, rejects, or dismisses changes that target endpoints where Deploy is installed.

Deploy Operator

Assign the **Deploy Operator** role to users who manage the configuration and deployment of Deploy functionality to endpoints.
This role can perform the following tasks:

- Create, edit, import, or delete software packages and software bundles
- Manage deployments, maintenance windows, and Self Service profiles

Deploy Package Administrator

Assign the **Deploy Package Administrator** role to users who manage the configuration of Deploy functionality. This role can perform the following tasks:

- Reject or dismiss Deploy configuration changes
- Create, edit, import, or delete software packages and software bundles
- View all configurations, graphs, and reporting data in Deploy

Deploy Read Only User

Assign the **Deploy Read Only User** role to users who need visibility into Deploy data. This role can view all configurations, graphs, and reporting data in Deploy.

Deploy User

Assign the **Deploy User** role to users who manage the deployment of Deploy functionality to endpoints. This role can manage deployments, maintenance windows, and Self Service profiles.

Do not assign the **Deploy Service Account** role to users. This role is for internal purposes only.

Configure module settings

1. On the Deploy **Overview** page, click Settings and then click **Configuration Settings** if needed.
2. In the **Endpoint Process Settings** section, configure the following options:

   Scan Interval

   Specify how frequently in hours that endpoints complete a full catalog scan. The default value is 24 hours but can be set lower to improve responsiveness to changes on endpoints, such as software that is installed, updated, or removed by programs other than Deploy.

   File Download Retry Limit

   Specify how many times Deploy will attempt to download a file that has failed to download. Setting this option to a higher number can help work around temporary issues, such as bad network connectivity.

   File Download Retry Delay

   Specify the amount of time in seconds, minutes, or hours before the endpoint tries to download a file that has failed to download. Setting this option to a relatively low number, such as 1-5 minutes, can help work around temporary issues without causing an excessive number of download requests.

   File Download Timeout

   Specify the amount of time in hours or days before a download attempt will time out. Setting this option to at least 24 hours helps ensure that large downloads on bandwidth-constrained endpoints have time to complete.

When Action Lock Enabled

This option specifies how Deploy behaves on action-locked endpoints. For best results, select either **Applicability Scanning Only** or **Ignore Action Lock** to ensure the accuracy of workbench data.

> NOTE
>
> The Deploy action lock setting does not override the Endpoint Configuration action lock setting. If you do not select **Manifest package ignore action lock** in Endpoint Configuration settings, then action-locked endpoints do not receive changes to Deploy configurations. For more information, see Tanium Endpoint Configuration User Guide: Reference: Settings and Tanium Console User Guide: Managing action locks.

Enable Debug Logging

Select this option to set the Deploy logs on all endpoints to be at the most verbose level. You should use this setting only with guidance from Tanium Support. To configure log verbosity, use the `Deploy - Set Logging Options` Tanium packages.

Max Log Size (in MBs)

Specify the maximum size of logs (in MBs) on an endpoint. Specify an option that allows readability and sufficient logging on an endpoint without utilizing too much disk space.

Number of Logs to Keep

Specify the number of log files to keep on an endpoint. Specify an option that allows readability and sufficient logging on an endpoint without utilizing too much disk space.

3. In the **Deployment Retry Settings** section, configure the following options:

   Retry Limit

   Specify how many times Deploy will retry a failed deployment on an endpoint. When Deploy reaches this limit, it will not retry the failed deployment until the **Reset Frequency** time has been reached.

   Reset Frequency (in hours)

   Specify the amount of time in hours before Deploy will attempt to retry failed downloads after the **Retry Limit** has been reached. Setting this option to a value less than 24 hours lets failed deployments run multiple times in the same day and can help work around temporary issues.

4. In the **General Settings** section, configure the following options:

   Client API Nonce Roundoff (in minutes)

   This setting enables a timestamp-based nonce for all Tanium Client API calls to avoid reusing previously cached URLs. You should use this setting only with guidance from Tanium Support.

   UNC Path Host Allowed List (comma separated)

   Specify the hostnames and IP addresses, separated by commas, for which the system allows access via UNC paths. The asterisk (*) character is a wildcard that matches any characters or none in a target hostname or IP address.

Software Package Gallery

For air-gapped environments, select **Enable Alternate Software Package Gallery Location** and then specify a location in the **Alternate Software Package Gallery Location** field. For more information, see Configure an alternate location for the Predefined Package Gallery on page 51.

Auto-Distribute Catalog

If you want the software package catalog to be automatically distributed, you must select **Enable Auto-Distribute Catalog**. New installations of Deploy automatically distribute the software package catalog to endpoints when changes are detected. If you do not enable this option, you are prompted to distribute the software package catalog each time an update is detected, and must click **Distribute Catalog**.

5. Click **Save**.

Configure an alternate location for the Predefined Package Gallery

The Predefined Package Gallery in Tanium Deploy provides a collection of common software packages that are hosted at `content.tanium.com`. These packages are preconfigured and ready to deploy to endpoints. By default, the Tanium Server in an air-gapped environment cannot directly access Deploy Gallery package definitions. To address this scenario, you can configure an alternative Gallery location so that a Tanium Server in an air-gapped environment can still download the Gallery.

To ensure the Tanium Server can download the Gallery, use a computer that is connected to the internet to download the software package definitions and then place the definitions in a location defined on your local network that is accessible to your Tanium Server.

For more information about using the Deploy Gallery, see Import a software package from the Predefined Package Gallery on page 61.

Stage the Predefined Package Gallery in a location accessible to the Tanium Server

Download the Package Gallery ZIP file and place it where it can be accessed by the Tanium Server.

- The network location that you specify must be accessible by the Tanium Server. To use a UNC path or a credential-protected URL, configure the settings based on the Tanium Server version and operating system.
  - **Tanium Server 7.5.3.3503 and later:** You must configure a downloads authentication entry for the UNC path or credential-protected URL. For information about configuring a downloads authentication entry, see Tanium Console User Guide: Managing downloads authentication.
  - **(TanOS) Tanium Server earlier than 7.5.3.3503:** You must configure credentials in the TanOS Tanium Operations menu. For information, see Tanium Appliance Deployment Guide: Add an authentication user for TDownloader

IMPORTANT

- **(Windows) Tanium Server earlier than 7.5.3.3503:** You must configure the Tanium Server service account to run as a Windows user with sufficient permissions. For information, see Tanium Appliance Deployment Guide: Add an authentication user for TDownloader
- Tanium does not support hidden or administrative shares.

The Package Gallery ZIP file contains JSON content for each software package in the Gallery. In environments that are not air-gapped, this JSON content is downloaded automatically from `content.tanium.com`. Because air-gapped environments do not have access to the internet, the ZIP file must be staged in a location that the Tanium Server can access.

Configure the alternate Gallery location

1. On the Deploy **Overview** page, click Settings and then click **Configuration Settings**.
2. In the **General Settings** section, select **Enable Alternate Software Package Gallery Location** and then specify a location in the **Alternate Software Package Gallery Location** field.
   For example, a UNC location might look like this: `\\myserver.example.local\files\deploy-software-package-gallery.zip`.
3. Click **Save** and then confirm your changes.
4. On the Deploy **Overview** page, click Help, and then click **Support > Initialize Endpoints**.
5. In the **Support** tab, click **View Job Status** and confirm that **Sync Software Gallery** appears with a green check mark.
6. Close the window and let the Package Gallery synchronize to Deploy. This process typically takes 5-10 minutes.

Add files to a software package

When you import a software package from the Gallery, the Tanium Server attempts to download the files associated with that software package. However, air-gapped Tanium Servers cannot download the files, which causes a `Sync Software Package` warning to appear. For information about fixing the error so that the imported software package can be used by the air-gapped Tanium Server, see Deploy cannot access the origin of a software package file on page 104.

Create a custom operating system

To make a specific operating system version available for use in the **Restrict Operating System** menu for software packages, you can create a new operating system in the Deploy settings.

1. On the Deploy **Overview** page, click Settings and then click **Operating Systems**.
2. Click **Add Operating System**.
3. Select the OS platform, and then specify a name and version.

4. Configure the following settings as needed:
    - (Windows) In the **Type** drop-down menu, specify whether the OS is for servers or workstations.
    - (Linux) In the **Distribution** drop-down menu, specify the type of Linux distribution for the OS.
5. Click **OK**.

Initialize Deploy endpoints

Deploy installs a set of tools on each endpoint that you have targeted. Initializing the endpoints starts the Deploy service and starts the Deploy process on every endpoint where it is not running.

1. On the Deploy **Overview** page, click Help  , and then click **Support** if needed.
2. Click **Initialize Endpoints** and confirm your action.

After deploying the tools for the first time, endpoints can take up to four hours to display status.

Managing software

Use software *packages* to install, update, or remove software on a set of target computers. Use software *bundles* to specify a sequenced list of software packages to deploy. Deploy also provides a gallery of common software packages in the **Predefined Package Gallery**.

The **Predefined Package Gallery** page lists predefined software package templates that you can import. Use the Predefined Package Gallery to import third-party software package templates to install, update, or remove software on a set of target computers.

NOTE

Tanium does not repackage or redistribute third-party software installers. The Tanium software package templates provide you with the remote file paths to directly download the software installer from the third-party vendor. You must review any applicable third-party End User Licensing Agreement (EULA) before you import third-party software to the Tanium software package catalog. Tanium is not responsible for accepting, nor does it accept, any EULAs from third-party software vendors on your behalf.

Before you begin

For applicability checks and command-line operations, make sure that all endpoints have the required system environment variables defined. For more information, see Windows System environment variables on page 32.

Create a software package

1. From the Deploy menu, go to **Software** and then click **Create Software Package**.
2. In the **Package Files** section, click **Add Package Files** to add a local or remote file or remote folder.

   These are the files that are needed to install an application on a managed device. They include, but are not limited to, MSI or EXE installers, resource files or folders, package files, configuration files, custom scripts, custom registry files, or license keys.

   You can select multiple files at once, but you cannot upload entire folder structures as a local file. To use an entire folder, first compress the folder contents into a compressed archive file (such as a ZIP file), then add the compressed file to the software package. For information about using Deploy to extract a file, see File/Folder actions on page 58.

   IMPORTANT

   If you select a remote file or remote folder, ensure that the Tanium Module Server service account can access the remote location and has sufficient permissions.

   - Windows Module Servers: Use a domain-joined account for seamless access to remote shares.
   - Appliance Module Servers: Add an authentication user. For more information, see Tanium Appliance Deployment Guide: Add an authentication user for TDownloader.
3. In the **Package Details** section, provide the general product information, select the OS platform, and specify the Self Service display name and icon to upload for self service deployments.

- If the package files include one or more Windows Installer packages (MSI file format), you can click **Inspect MSI to Populate Fields** to extract information from the `.msi` file and verify the pre-populated information. Using this feature does not overwrite any information that you previously entered manually.
- The account that is set for the Deploy service account must have access to execute PowerShell on the Tanium Module Server.

OS Platform

Specify an operating system platform. If the software package should only be run on certain versions of the platform, click **Restrict Operating Systems** in the **System Requirements** section.

4. In the **System Requirements** section, provide the minimum system requirements for the software package to run on the endpoint.

Disk Space Required

Configure the minimum available system disk space required. For best results, specify at least three times the total size of the package files.

Minimum Ram

Configure the minimum physical RAM required.

Architecture

Configure the allowed architectures for the software package based on the platform. On endpoints where the architecture does not match, the software package will show a status of `Not Applicable`.

(Windows) Select **x86** for software that cannot be installed on 64-bit Windows systems. Select **x64** for software that can be installed on 64-bit Windows systems. Select **Select All** for x86 software that can be installed on 64-bit Windows.

(macOS) Select **x64** for software that should only be installed on Intel-based Mac endpoints. Select **ARM64** for software that has only a native ARM64 binary. Select **Select All** for software that has a universal binary, does not install a binary, or can run using Rosetta.

(Linux) Select **x86**, **x64**, or **ARM64** based on the platform for which the software is compiled. Select any combination of the three options for software packages that do not install compiled code or that do so in a platform-agnostic fashion.

Restrict Operating Systems

Click **Restrict Operating Systems** and then select the supported operating systems on which to allow Deploy to install or update the software package. The software package will still be considered installed if the **Install Verification** criteria are met on non-restricted operating systems. Specific operating systems can be targeted for deployments and self service profiles without making a selection in the software package.

> NOTE Specify an operating system only if the software package should never be installed or updated on other operating systems. If you need an operating system that is not available, you can add one in Deploy settings. For more information, see Create a custom operating system on page 52.

5. In the **Deploy Operations** section, select which operations you want to enable: **Install**, **Update**, or **Remove**, and add conditional commands for any of the Deploy operations that you enabled for this package. For each operation, select the **Require Source Files** option if any of the files in the **Package Files** section are required to perform the operation. If you do not select this option, the package files are not downloaded. (Windows) For more information, see Variables for Windows applicability scans and command-line operations on page 58.

> TIP If you chose to inspect the MSI, some operations are already enabled and information is pre-populated. You can verify or update any of the pre-populated information.

Check for Running Processes

Specify a process name, for example, `Chrome.exe`, and select either **Terminate process** or **Pause until process is no longer running**. If you choose to pause the process, the wait time is five minutes.

Run Command

Specify an install, update, or remove command to run and choose whether to run the command as the **System** or the **Active User** on Windows endpoints. If any part of the path in a command contains a space, use double quotation marks, even if you use variables.

File/Folder

Extract a compressed file, copy a file or folder, create a folder, delete a file or folder, or rename a file or folder. For more information, see File/Folder actions on page 58.

Tanium Client File Request

Specify an HTTP(S) address or a UNC file path and file name. Any URI that you enter must be allowed on the Tanium Server. For more information, see Tanium Platform User Guide: Managing allowed URLs.

> TIP
> - To use any of these actions with a file attached to this software package, enter the file name in the source field.
> - (Linux) To install a file attached to the software package using the **apt** command, specify an absolute or relative path and escape the slash, for example `apt --yes install .\/zoom_amd64.deb`. To install a file attached to the software package without specifying a path, use the **dpkg** command.
> - To extract or copy a file or folder to the working directory used for running this software package, enter a period in the destination field. If the file or folder should go to a different location, specify the fully qualified path, such as `"C:\Program Files"` or `/opt/Tanium`.

6. In the **Installation Requirements**, **Update Detection**, and **Install Verification** sections, configure applicability rules that determine whether this software package is install eligible, update eligible, or installed, respectively. For detailed information about how Deploy determines applicability, see Software package applicability in Deploy on page 68.

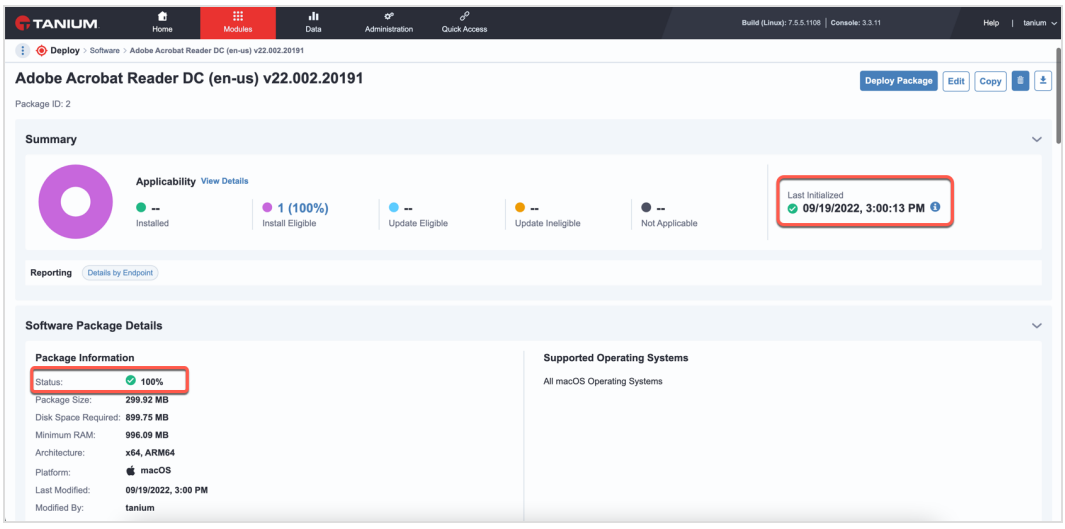
   IMPORTANT Deploy automatically encloses file and registry paths in double quotation marks, so you do not need to use quotation marks for file or path names that contain spaces.

   TIP
   - You can refer to file and registry paths specific to the active user of a Windows endpoint. You can also refer to the 32-bit `Program Files` or native `Program Files` directory with a single rule. For more information, see Variables for Windows applicability scans and command-line operations on page 58.
   - You can use a Windows Management Instrumentation (WMI) query to query information from WMI classes for any of the detection rules within a software package. If you use a WMI query, you cannot query against the `Win32_Product` WMI class. For more information, see Microsoft Documentation: Win32_Product class.
   - Specify registry DWORD values as decimals.

7. Click **Create Package**. You can also click **Save and Finish Later** to finish creating the package later.

Next steps

- On the software package page, wait up to 10 minutes to allow the initialization to complete and the **Status** in **Package Information** to be 100%.



NOTE The initialization must be complete and package status at 100% before proceeding to the next steps.

- Distribute the software package catalog on page 63, if not automatically done.

  NOTE It takes up to five minutes before the new software package is distributed to endpoints.

- (Optional) View software package applicability on page 64.
- (Optional)Deploy a software package or bundle on page 72.
- (Optional) Add to a software bundle. See Edit a software package or bundle on page 69.
- (Optional) Add to a self-service profile. See Edit a self service profile on page 94.

Variables for Windows applicability scans and command-line operations

When you create a Windows software package, you can use `||PROGRAMFILES32BIT||`, `||PROGRAMFILES||`, `||ACTIVEUSERPROFILE||`, or `||ACTIVEUSERREGISTRY||` as variables for applicability scans and command-line operations. For the **Requirements**, **Update Detection**, and **Install Verification** sections, you can use these variables if you select the **Registry Path**, **Registry Data**, **File Path** or **File Version** filter fields.

Installer Architecture	Variable	Path
32-bit on 32-bit endpoint	`||PROGRAMFILES32BIT||`	Path to Program Files folder (example: `C:\Program Files`)
32-bit on 64-bit endpoint	`||PROGRAMFILES32BIT||`	`C:\Program Files (x86)`
64-bit on 32-bit endpoint	`||PROGRAMFILES||`	`C:\Program Files`
64-bit on 64-bit endpoint	`||PROGRAMFILES||`	`C:\Program Files`
Any	`||ACTIVEUSERPROFILE||`	Profile directory of the active authenticated user (example: `C:\users\john.smith`)
Any	`||ACTIVEUSERREGISTRY||`	Registry hive of the active authenticated user (example: `HKEY_USERS\USER-SID\`)

IMPORTANT Use double quotation marks (") if any part of the path in a command contains a space, even if you use variables.

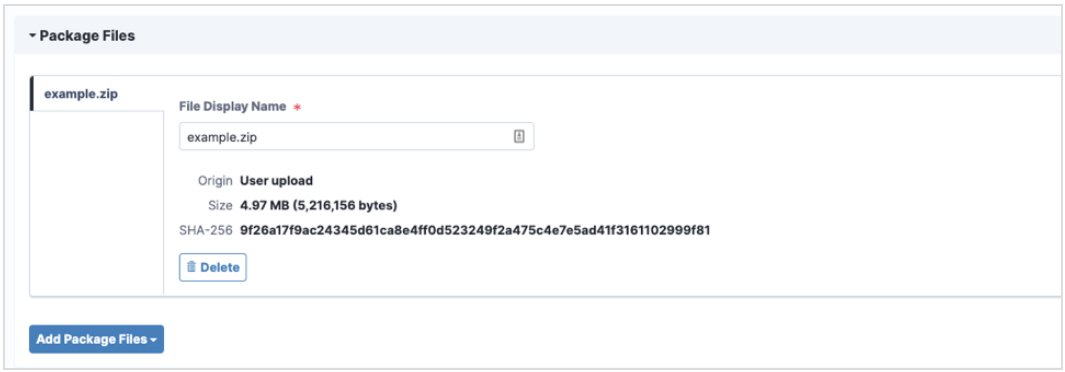
File/Folder actions

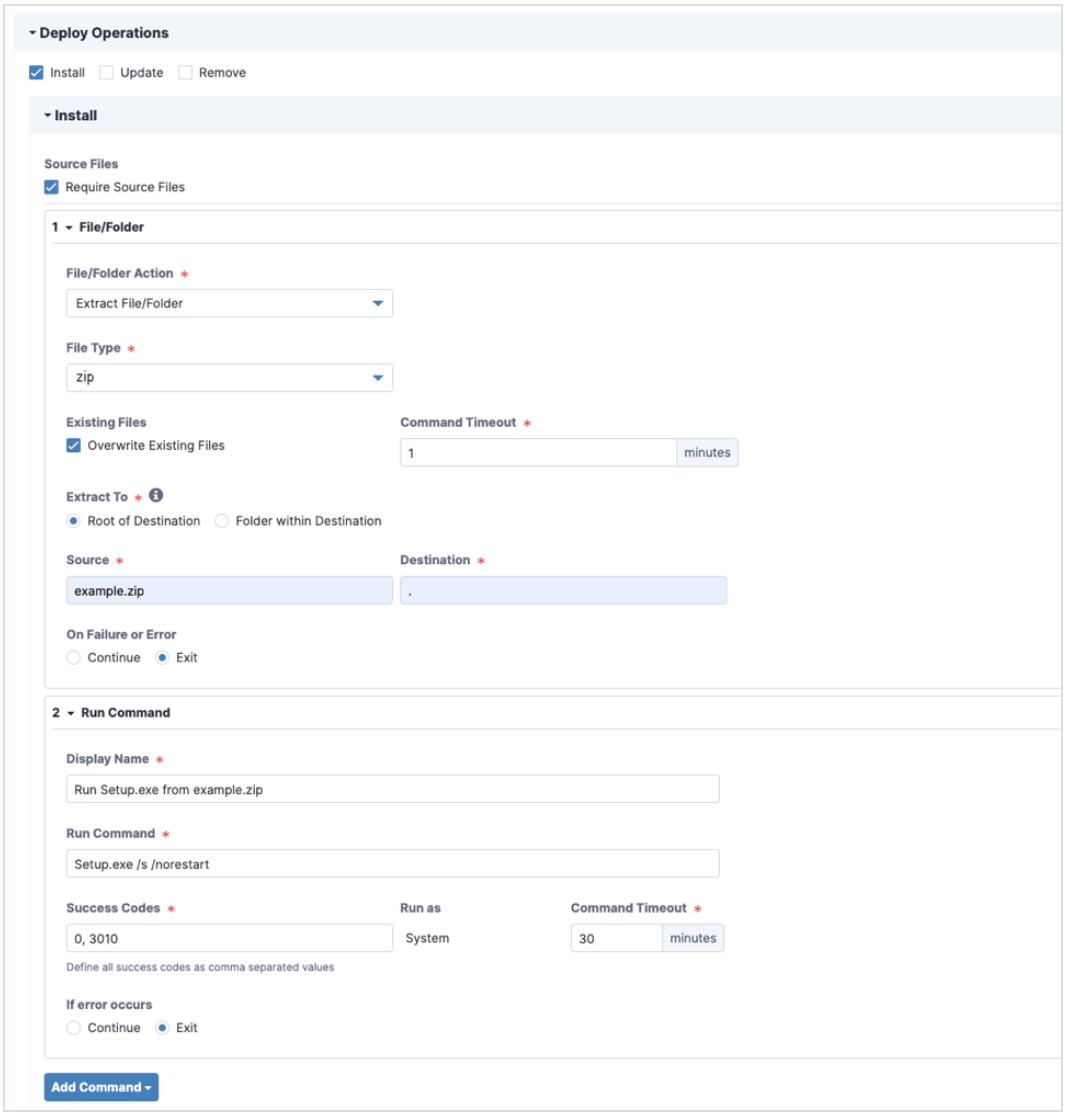
You can perform the following actions for files and folders.

IMPORTANT Do not use quotation marks in the folder path or file name in File/Folder actions.

- **Copy File/Folder**: Specify the fully qualified path and file name. If the destination is a folder, Deploy copies the source to the destination folder; it does not replace an existing folder. For example, a command to copy `firefox.app` to `/Applications/firefox.app` with overwrite enabled produces the following results, depending on whether `/Applications/firefox.app` is an existing folder:
    - If `/Applications/firefox.app` is not an existing folder, Deploy creates `/Applications/firefox.app`.
    - If `/Applications/firefox.app` exists, Deploy creates `/Applications/firefox.app/firefox.app`.

  To always replace `/Applications/firefox.app`, set the destination to `/Applications` instead of `/Applications/firefox.app`.
- **Create Folder**: Creates a folder. If you specify a parent folder path that does not exist, it is created. For example, `c:\temp\myfiles` creates `c:\temp` folder and `myfiles` subfolder.
- **Delete File/Folder**: Any subfolders of the folder that you specify are also deleted.
- **Extract File/Folder**: Supported file types for extracting a file are 7Z, TAR, ZIP, BZIP2, GZIP, XZ, and Z. You can specify the following options for extract commands.
    - Specify whether to overwrite existing files. If there is an existing file, however, you must also select **Continue** in the **On Failure or Error** section; otherwise, the extract command fails and Deploy retries the software package operation.
    - Specify a **Command Timeout** in minutes. The extract operation will time out after the number of minutes you specify. For best results, specify 1 minute for each 50 MB of file size. For example, if your file is 1 GB, specify a **Command Timeout** value of 20 minutes.
    - In the **Extract To** section, specify an option. **Root of Destination** extracts the contents of the compressed file in the specified destination. **Folder within Destination** creates a folder in the specified destination with the same name as the compressed file, and then extracts the file to the newly created folder.
    - As an example, to use the contents of an attached package file `example.zip` in a software package, specify `example.zip` as the **Source** and `.` as the **Destination**. Select **Root of Destination** and **Overwrite Existing Files**. Then, if `example.zip` contains a `Setup.exe` file that should be executed in this software package operation, add a **Run Command** step with `Setup.exe` at the start of the **Run Command**.





- **Rename File/Folder**: Specify the existing (source) and new (updated) fully qualified path and file names.

Export a software package

You can export a software package so that you can later import the package on a different server or recreate a deleted package.

1. From the Deploy menu, go to **Software**.
2. Click the name of your package and then click Export.

The ZIP file is available in your downloads folder.

Import a software package

You can import a previously exported software package on a different server or recreate a deleted package.

1. From the Deploy menu, go to **Software** and then click **Import Package**.
2. Browse to the previously exported ZIP file and click **Import**.
3. Click **(Download File)** for any required files.
4. Click **Import** or **Import Duplicate** if you are importing a duplicate package.

Import a software package from the Predefined Package Gallery

You can select one of two ways to import a software package:

- You manually import a software package from the Predefined Package Gallery.
- Deploy automatically imports the software package if Tanium updates the package or adds a new version of the package.
  If you installed Deploy with the **Apply All Tanium recommended configurations** option, certain packages are automatically imported by default. For the list of packages, see Import Deploy with default settings on page 43. You can modify the default import setting.

For guidance on determining the import setting for a software package, see Impact of software package import setting and deployment settings on ease of use on page 62.

For a complete list of the software packages available in the *Predefined Package Gallery*, see Reference: Predefined Package Gallery on page 122.

1. From the Deploy menu, go to **Software** and then click **Predefined Package Gallery**.
2. Select the packages you want to import and click **Import Settings**.
   a. Select the import type.
   If you select the automatic import option, the package is immediately imported. Subsequent automatic imports occur hourly as needed, according to the software package gallery update schedule. If a package is automatically imported by Tanium, you can select the manual import option to stop the automatic import.

   NOTE Packages that are automatically imported are marked as **In Use** on the **Software Packages** page.

b. Select if you want to enable package cleanup. If you enable cleanup, enter how many versions to keep of a software package.

   Package cleanup deletes the oldest version of the software package when a new version is imported that exceeds the specified limit. Package cleanup occurs hourly.

c. Click **Save**.

3. If you selected manual import, import the package by clicking Import package in the **Actions** column.

   Or you might import a package to reset it to the out-of-box configuration.

   > NOTE You cannot manually import the packages that Tanium automatically imports, unless you have changed the default import setting.

After you import a package and distribute the catalog, you can deploy, edit, delete, or export the package. If a package is marked as **Tanium Managed** on the **Software Packages** page, you cannot edit or delete it unless you change the import setting to manual.

If Deploy cannot access the origin of a software package file, you can edit the package and manually add any inaccessible files. For more information, see Deploy cannot access the origin of a software package file on page 104.

> TIP If you import the Oracle Java 8 package and want to remove previous versions of Java, you can add `REMOVEOUTOFDATEJRES=1` to the end of the run command in the **Update Command** field of the software package.

Impact of software package import setting and deployment settings on ease of use

Review the following table to understand how the software package import setting and the deployment type and settings impact what you need to do to keep software packages and deployments up-to-date.

Software package import setting	Package included in software package deployment	Package included in software bundle deployment
Manual import	• You must monitor the software package gallery for changes to the specific package version and additional package versions. • When Tanium updates a package or releases a new package version, add the package to the deployment.	

Software package import setting	Package included in software package deployment	Package included in software bundle deployment
Automatically import updated and new versions as they are released	• If Tanium updates a specific package version, the deployment automatically uses the updated package. • When Tanium creates a new package version, add the package to the deployment.	• If a software package in a bundle uses the **Latest Applicable** version and Tanium updates a specific package version or creates a new package version, the deployment automatically uses the updated or new package. To configure the **Latest Applicable** setting, see Create a software bundle on page 69. BEST PRACTICE To maximize ease of use, automatically import software packages and use software bundles with the **Latest Applicable** version in deployments. • If the software bundle does not use the **Latest Applicable** version and Tanium updates a specific package version, the deployment automatically uses the updated version. If Tanium creates a new package version, the deployment is updated with the new package, but you need to select the most recent version to deploy.

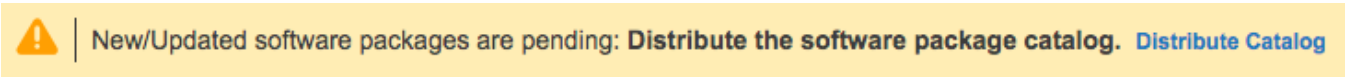
Distribute the software package catalog

After you create or edit a software package, the updated software package catalog must be distributed to the endpoints. When the endpoints receive the updated software package catalog, you can view the package applicability.

New installations of Deploy automatically distribute the software package catalog to endpoints when changes are detected.

If you upgraded from Deploy 2.1.9 or earlier and want the software package catalog to be automatically distributed, you must enable the **Auto-Distribute Catalog** option in the **Configuration Settings** tab of the Deploy Settings. If you do not enable this option, you are prompted to distribute the software package catalog each time an update is detected, and must click **Distribute Catalog**.

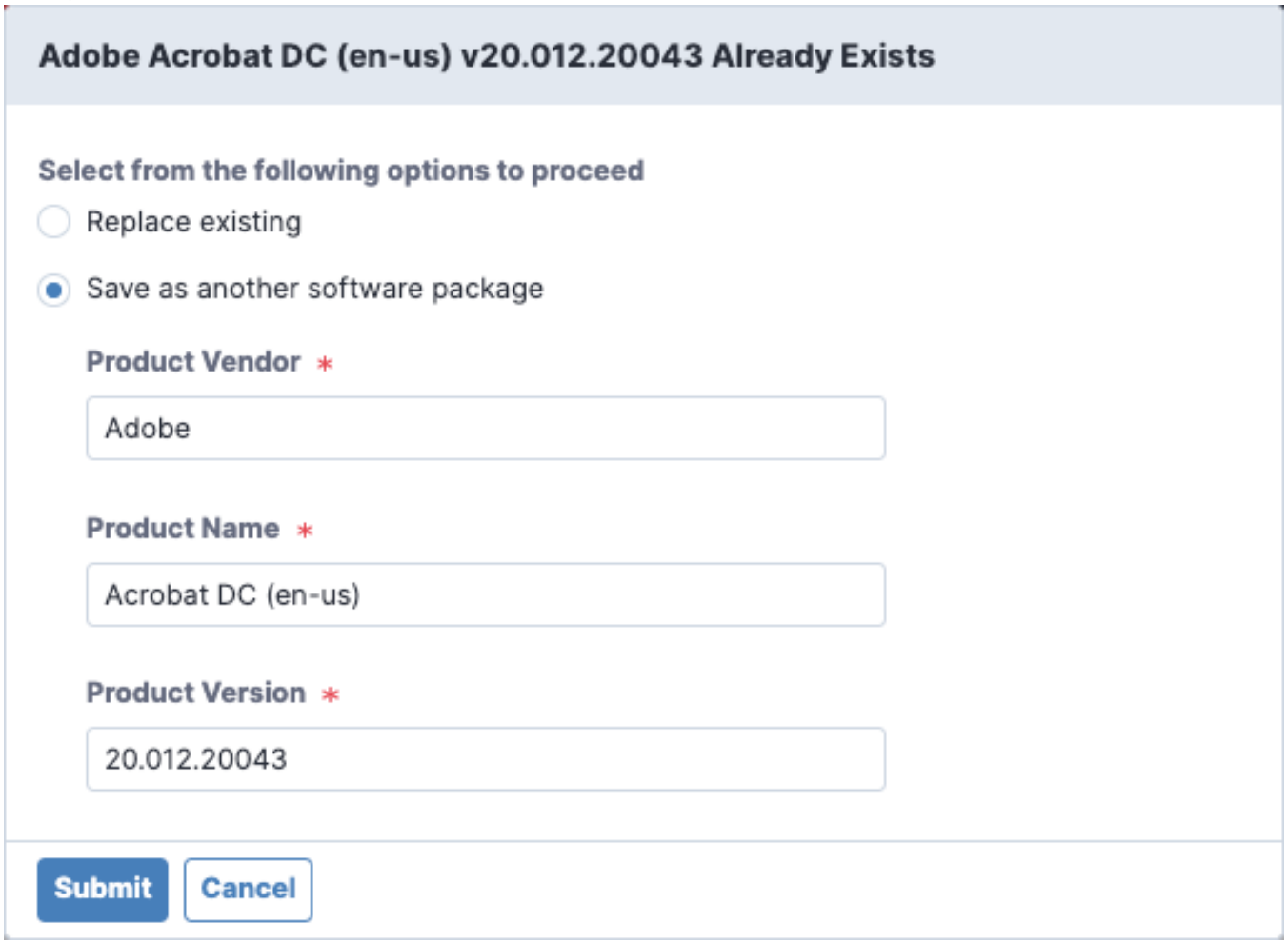
Distribute software package catalog



Manually replace or add a new package to the software package catalog

If a software package that is being manually imported already exists in the software package catalog, you are presented with two options prior to importing again. If you want to replace the existing package, select **Replace existing**. If you want to import the package, but also keep the existing one, select **Save as another software package**. You must then update at least one of the fields to create a unique record in the software package catalog.

Package already exists

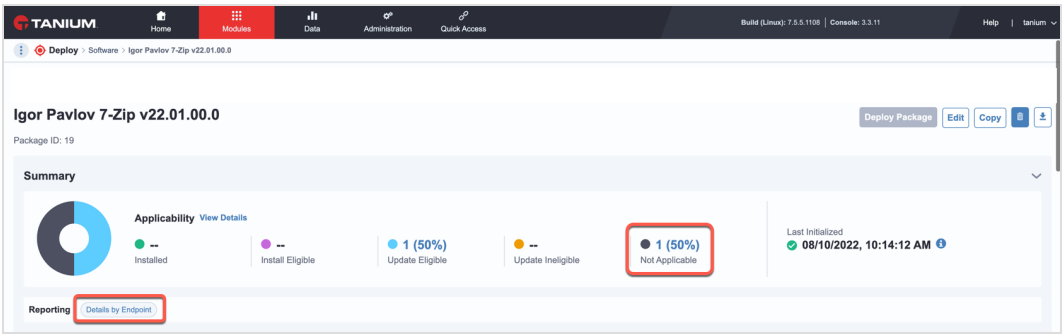


View software package applicability

To view software package applicability and understand the results, review the Interact question results, software package details, and endpoint log files. The following example describes how to view and understand the applicability results for the **Igor Pavlov 7-Zip v22.01.00.0** software package on one endpoint.

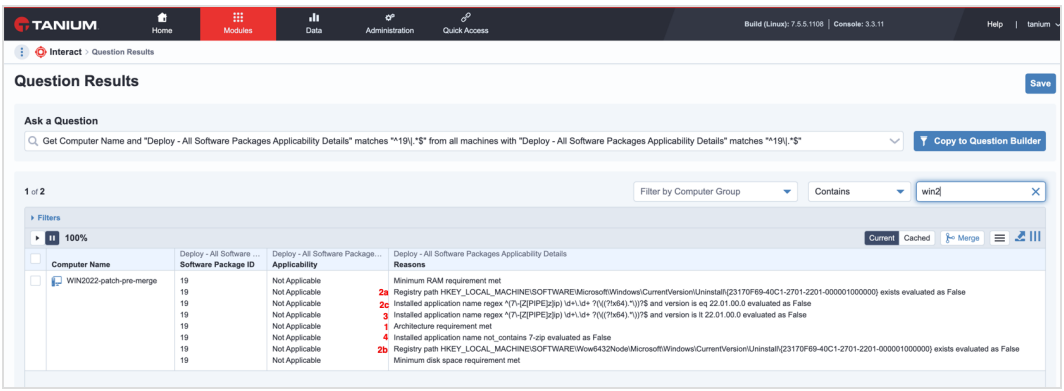
1. From the Deploy menu, go to **Software > Software Packages** and click the **7-Zip** package. Note that the 7-Zip package is not applicable on one endpoint.
   You can also view the software package applicability by expanding the package name.

Software package not applicable on an endpoint



2. For more details about a specific applicability state, click **Details by Endpoint > View Online Data** or **View Cached Data**. In this example, `WIN2022-patch-pre-merge` is an endpoint with **Not Applicable** results.

Endpoint results

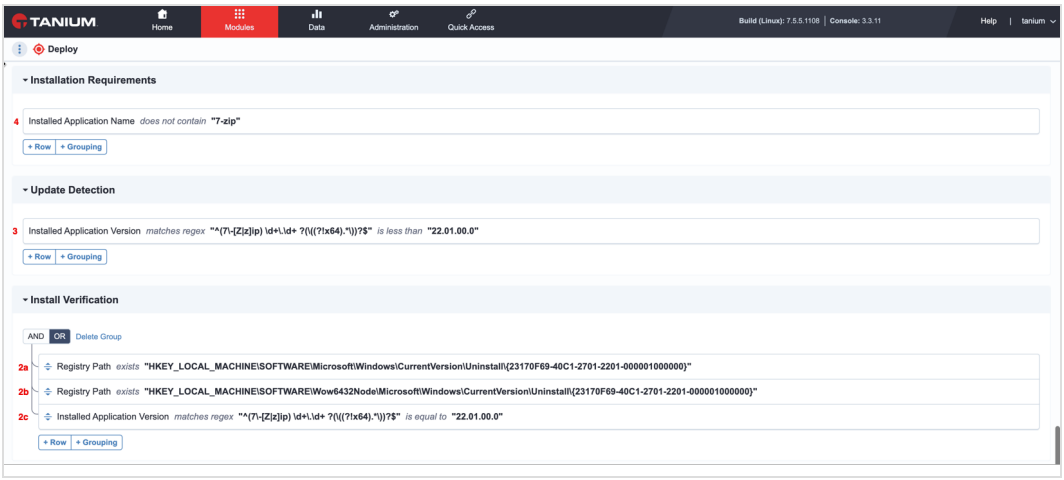


3. In Interact, review the **Reasons** column. Consider the following information:

   - Each answer in the **Reasons** column is the result of the evaluation of one of the applicability rules in the software package.
   - Each **Applicability** result does not directly relate to each **Reason**. If one result is **Not Applicable**, for example, all **Applicability** results are **Not Applicable**.
   - The answers are not displayed in evaluation order. In the image in step 2, each answer is numbered according to the evaluation order specified in Software package applicability in Deploy on page 68. For example, the answer marked with 1 corresponds with the **System architecture** criteria, the answers marked with 2 correspond with the **Install Verification** criteria, and so on.

4. To identify which item corresponds with each criteria, compare the results in the **Reasons** column to the software package details. The following image shows the **Install Verification** , **Update Detection**, and **Installation Requirements** sections.

Software package details



This software package is not **Installed** on this endpoint because the **Install Verification** criteria are not met. The two registry paths do not exist and there is not an installed application that matches the regular expression of a 32-bit 7-Zip 22.01.00.0.

The software package is not **Update Eligible** because the **Update Detection** criteria is not met. There is not an installed application that matches the regular expression of a 32-bit 7-Zip 22.01.00.0 or older.

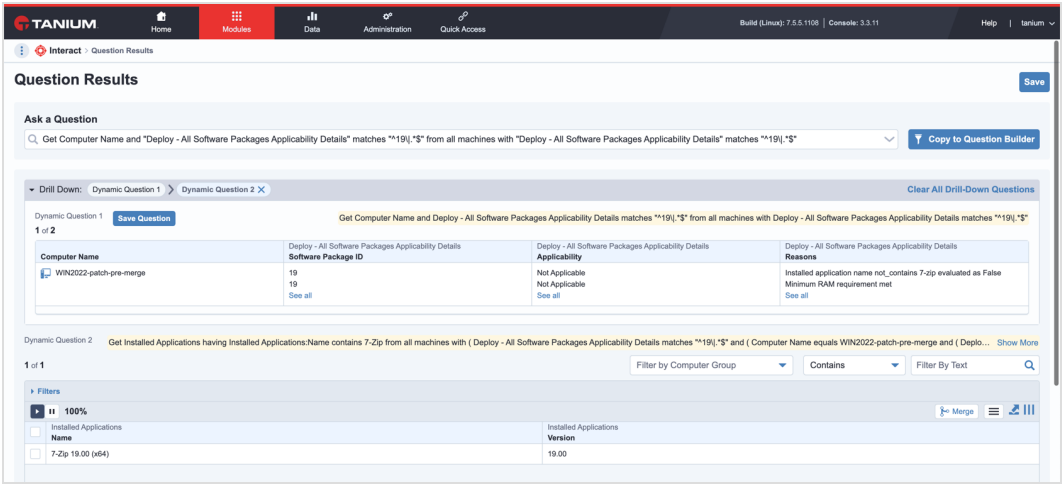
The software package is **Not Applicable** instead of **Install Eligible** because the **Installation Requirements** criteria is not met. There is an installed application name that contains 7-Zip. The results of the **Install Verification** and **Update Detection** criteria indicate that this endpoint does not have 32-bit 7-Zip 22.01.00.0 or older installed. So either a newer version of 32-bit 7-Zip is installed or a 64-bit version of 7-Zip is installed.

5. To quickly evaluate which version of 7-Zip is installed on the endpoint, ask Interact questions on the impacted endpoint.

   a. On the **Questions Results** page, drill down on the impacted endpoint.

   b. In this example, build a question using the **Installed Applications** filter with the name of **7-Zip**.

Drill down on endpoint



This package is not applicable on the endpoint because the endpoint has a 64-bit version of 7-Zip and the software package specifies a non-64-bit version of 7-Zip.

6. To see an ordered list of applicability results for easier analysis, review the impacted endpoint's `software-management.log` file. For the log location, see Collect Deploy troubleshooting information from endpoints on page 103. Search for `Determining applicability status for software package 19` to find the most recent instance of this line. `19` is the ID of the software package.

   The log provides more details than are available in Interact. The log identifies that the `Installed application` rule matches the installed application name of `7-zip 19.00 (x64)`.

```
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Determining applicability status for software package 19
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Registry path HKEY_LOCAL_
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{23170F69-40C1-
2701-2201-000001000000} exists evaluated as False
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Registry path HKEY_LOCAL_
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{23170F69-40C1-
2701-2201-000001000000} exists evaluated as False
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Registry path HKEY_LOCAL_
MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\
{23170F69-40C1-2701-2201-000001000000} exists evaluated as False
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Evaluating installed application rule: name regex "^(7\-
[Z|z]ip) \d+\.\d+ ?(\((?!x64).*\))?$", version eq 22.01.00.0
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Find application: name=^(7\-[Z|z]ip) \d+\.\d+ ?(\
((?!x64).*\))?$, operator=regex, version=22.01.00.0, operator=eq
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Installed application rule evaluated as False
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Evaluating installed application rule: name regex "^(7\-
[Z|z]ip) \d+\.\d+ ?(\((?!x64).*\))?$", version lt 22.01.00.0
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Find application: name=^(7\-[Z|z]ip) \d+\.\d+ ?(\
((?!x64).*\))?$, operator=regex, version=22.01.00.0, operator=lt
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Installed application rule evaluated as False
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Evaluating installed application rule: name not_contains "7-
zip", version None None
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
```

```
package_scan]: Find application: name=7-zip, operator=contains, version=None,
operator=None
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Found matching application: Name: 7-zip 19.00 (x64), Version:
19.0
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Installed application rule evaluated as False
2022-09-19 18:41:55Z INFO [PID 1088] [Software Package Scan][software_
package_scan]: Install requirements NOT met. Package is not applicable
```

For information about configuring applicability scans, see Applicability scans on page 11.

Software package applicability in Deploy

When determining software package applicability, Deploy checks the criteria specified in the software package in the following order, stopping at the first section with matching criteria.

1. System architecture on the endpoint: If the architecture does not match any of the architectures defined in **System Requirements**, Deploy marks the software package as `Not Applicable` and moves on to the next software package.
2. **Install Verification** criteria: If those criteria match, Deploy marks the software package as `Installed` and moves to the next software package.
3. **Update Detection**: If an **Update** operation exists, Deploy then checks the **Update Detection** criteria. If those criteria are met, Deploy checks **System Requirements**:
    - If **System Requirements** match, Deploy marks the software package as `Update Eligible` and moves to the next software package.
    - If **System Requirements** do not match, Deploy marks the software package as `Update Ineligible` and moves to the next software package.
4. **Installation Requirements** criteria: If **Installation Requirements** criteria do not match, Deploy marks the software package as `Not Applicable` and moves on to the next software package. If **Installation Requirements** criteria match, Deploy then checks **System Requirements**:
    - If **System Requirements** match, Deploy marks the package as `Install Eligible` and moves on to the next software package.
    - If **System Requirements** do not match, Deploy marks the package as `Not Applicable` and moves on to the next software package.

Keep the following clarifications in mind as you review software package applicability:

- **Installation Requirements** affect only **Install** operations, not **Update** operations.
- If you do not specify **Installation Requirements**, then the software package is marked `Install Eligible` if the endpoint meets **System Requirements** criteria for the software package.

- Deploy evaluates **Installation Requirements** criteria, even if the software package does not contain an Install operation. As a result, Deploy marks a software package as `Install Eligible` even if it cannot be installed. To prevent this behavior, add a rule that cannot be true; for example, add the following **Registry Path** check to the **Installation Requirements**: `HKLM\Software does not exist`.

Create a software bundle

1. From the Deploy menu, go to **Software** and then click **Software Bundles**.
2. Click **Create Software Bundle**.
3. In the **Bundle Details** section, specify the bundle name and optionally a description.
4. In the **Bundle Workflow** section, select software options.
   a. Click **Add** to select the software packages to add to the bundle.

   You can filter packages by typing the platform, vendor name, or package title.

   b. Select a specific version, or choose **Latest Applicable** to automatically select the latest available version for each endpoint.
   c. Select the operation: **Install Or Update**, **Install**, **Update**, or **Remove**.
   d. Select whether you want the bundle to exit or continue or if the package fails.

   You can change the order of the packages by dragging the package.
5. Click **Create Bundle**.

Edit a software package or bundle

To edit a package or bundle, click the name of your package or bundle and then click **Edit**.

When a bundle is edited and saved, all existing deployments continue to use the version that was specified at the time of deployment. To prevent the previous version of the bundle from being used, stop any active deployments of the bundle before making changes.

Copy a software package or bundle

To copy a package or bundle, click the name of your package or bundle and then click **Copy**.

When a software package or bundle is copied, the name is automatically prepended with **Copy -** .

Delete a software package or bundle

To delete a package or bundle, click the name of your package or bundle and then click Delete  .

To delete multiple packages simultaneously, select the packages from the **Software Packages** page and then click **Delete**.

You can delete a software package or bundle only if it is not referenced in an active deployment or self service profiles.

Deploying software

Use deployments to install, update, or uninstall software on a set of target computers. Deployments can run once or be ongoing to meet requirements such as:

- Maintain operational hygiene and system baselines.
- Manage systems which may be online for short periods.
- Rerun packages which become applicable as system states change.

IMPORTANT Deployments do not run outside of a maintenance window unless the **Override maintenance window** option is selected in the deployment options. You must create at least one maintenance window for other deployments to run. For more information about creating a maintenance window, see Managing maintenance windows on page 90.

Before you begin

- To create a software package deployment, ensure that you have at least one software package. See Create a software package on page 54 or Import a software package on page 61.
- To create a software bundle deployment, ensure that you have at least one software bundle. See Create a software bundle on page 69.
- If you want to notify the end users of your Windows and macOS endpoints about the start of deployments or restarts that occur after deployments, install the Tanium End-User Notifications solution. See Tanium End-User Notifications User Guide: Installing End-User Notifications and Configure end user notifications on page 74.

Create a deployment template

You can create a deployment template to save settings for a deployment that you can issue repeatedly. You can either create a deployment template from the **Deployment Templates** menu item, or you can select an option when you create a deployment to save the options as a template.

1. From the Deploy menu, go to **Deployment Templates** and then click **Create Deployment Template**.
2. Specify a name and optionally a description for your deployment template.
3. Select deployment options. These options are the same as the options you can configure in an individual deployment. For more information, see Deploy a software package or bundle on page 72.

   BEST PRACTICE For self service deployments that are set for the future, use the **Make Available Before Start Time** option.

4. Click **Create Deployment Template**.

You can use this template when you create a deployment.

Set the default deployment template

The default deployment template is applied when you create deployments. Importing Deploy with automatic configuration creates three deployment templates and sets one of them as the default. You can change the default template or remove a template as the default.

1. From the Deploy menu, go to **Deployment Templates**.
2. Select a template and click **Set as Default**.
3. To remove the default designation from a template, select the default template and click **Remove as Default**.

Delete a deployment template

1. From the Deploy menu, go to **Deployment Templates**.
2. Select one or more templates and click **Delete Deployment Templates**.

You can also click the name of your deployment template and then click Delete .

Deploy a software package or bundle

1. From the Deploy menu, go to **Deployments** and then click **Create Deployment**.

   TIP You can also create a deployment from the Software page. Select a software package and click **Deploy Package**.

2. Provide a name for the deployment and optionally provide a description.
3. Do one of the following, as needed:
   - Select **Software Package**, select the package from the drop-down list, and then select the software package operation. You can filter packages by typing the platform, vendor name, or package title.
   - Select **Software Bundle** and then select the bundle from the drop-down list.

     NOTE A software bundle is platform-specific and each software package evaluates and installs independently, but is available only for the specified OS platform. If an individual package fails to install during a bundle deployment, you can decide if the bundle should continue and install the remaining packages, or you can choose to stop on failure and report the failure.

4. Add targets.

   Select either or both of the following targeting methods and complete the fields as needed. If you select both targeting methods, then they are joined by an `OR` operator. If you use multiple targets, the deployment applies to endpoints that match any of the targets you specify.

- **Select Computer Groups** provides a drop-down list of computer groups available to be managed in Deploy.
- **Set Targeting Criteria** lets you add any Tanium question filter as a target. When you use this option, you must also select a limiting group from the **Select Limiting Group** drop-down list of computer groups. For example, to target endpoints in the `192.168.1.0/24` subnet, you can type `Tanium Client IP Address starts with 192.168.1` in the **Filter Bar** or use the **Filter Builder** to select the **Tanium Client IP Address** sensor, and then apply the same filter. After that, set the `All Windows 10` computer group as the limiting group to make the deployment apply to all Windows 10 endpoints with an IP address that starts with `192.168.1`.

  IMPORTANT The **Select Computer Groups** and **Set Targeting Criteria** options are joined by an `OR` operator. If you use multiple targets, the deployment applies to endpoints that match any of the targets you specify. If you use Set Targeting Criteria, you must also specify a limiting group that limits all targets. For example, if you select **All Laptops** as the target computer group, the deployment goes to all laptops managed by Deploy. However, if you also add `Tanium Client IP Address starts with 192.168.1` as the targeting criteria, and then select **All Windows 10** as the limiting group, then the deployment goes to all Windows 10 devices that are either laptops or have an IP address starting with `192.168.1`.

  BEST PRACTICE If you set targeting criteria, use criteria based on attributes that cannot be changed by the deployment. If you select attributes that can change, endpoints might become in a state where the deployment is `Not Applicable` with a sub-status of `Configuration not available or not targeted`. For more information about how endpoints might become in this state, see Reference: Deployment status on page 77.

5. Select deployment options.

   a. Choose whether you want to use an existing deployment template. To create a new deployment template based on this template, select **Do not use existing template** and then select **Save Deployment Options as template**. For more information, see Create a deployment template on page 71.

   b. Specify a deployment frequency. You can either do a single deployment with a specific start and end time, or an ongoing deployment that does not have an end time.

   NOTE A software package operation may be interrupted if you stop the deployment, the deployment ends, or the maintenance window closes.

   NOTE After the deployment ends or the maintenance window closes, restarts do not occur, End-User Notification messages do not appear, and remaining steps in a software bundle (if applicable) do not run.

   c. Designate the deployment time. You can choose from the local time on the endpoint or UTC time.

d. Select self service options.

> BEST PRACTICE For self service deployments that are set for the future, use the **Make Available Before Start Time** option.

e. To prepare the endpoints for future deployments by downloading the deployment content before the installation time, select the option for **Download Immediately**.

f. (Windows and macOS endpoints) To enable pre-deployment end user notifications, select **Notify User Before Running** in the **Pre-Notify User** section. To minimize disruptions to end users, configure a notification for Update and Remove operations, as they could affect applications that are in use on an endpoint.

g. To protect shared compute resources in a virtual environment, select **Enabled** for the **Distribute Over Time** option and indicate an amount of time. The value you indicate for **Distribute Over Time** must be less than the deployment duration.

Distribute Over Time randomizes the deployment start time on each endpoint by an amount of time up to the value configured. This option reduces concurrent consumption of shared compute resources in a virtual environment.

> BEST PRACTICE Specify a **Distribute Over Time** value that is at least two hours less than the length of the deployment window and any maintenance windows. If the value exceeds deployment and maintenance windows, some endpoints will not be able to run the deployment or will run a software package operation outside of the maintenance window.

h. If you want to ignore deployment restrictions, select **Override maintenance windows**.

i. (Windows and macOS endpoints) Select whether to restart the endpoint. To avoid suddenly restarting a endpoint while an end user is working, configure a notification if the deployment requires a restart.

j. (Windows and macOS endpoints) Select **Notify User After Running** in the **Post-Notify User** section to configure a post-deployment end user notification.

> BEST PRACTICE Use a post-deployment notification if a deployment also uses a pre-deployment notification to inform users that an operation is complete.

6. Click **Show Preview to Continue** and review the deployment.
7. Click **Deploy Software**.

Configure end user notifications

(Windows and macOS endpoints) You can enable pre- and post-deployment notifications to warn end users about changes to endpoints. Pre-deployment notifications are especially important for Update and Remove operations because they can affect applications that are in use on an endpoint. Post-deployment notifications are especially important for deployments that require restarts because they can occur while end users are working on an endpoint.

Notification Options

- **Duration of Notification Period:** Specify the amount of time before the notification must be accepted. The deadline is calculated by adding this value to the time the deployment completed for each endpoint.
- **Allow User to Postpone:** If you want to give the user an option to defer accepting the notification for a specified amount of time, select this option. A user cannot postpone beyond the deadline.
- **User Postponement Options:** Specify the amount of time a user can postpone the notification. The total amount of time specified must be less than the **Duration of Notification Period** value. Note that this is only the amount of time to defer the notification from being displayed again; it does not affect when the countdown to deadline appears.
- **Final Countdown to Deadline:** Specify the amount of time for end users to accept the notification. The notification also shows a countdown until end users must accept. If end users dismiss the notification and a restart is required, the notification will reappear in the last minute of the final countdown to deadline before the computer restarts.

Message Content

- Specify the title and body of the notification message. Upload optional icon and body images for branding to avoid confusing users and to limit support calls. Optionally, enable additional languages and provide translated title and body text. By default, the notification displays content in the system language on the endpoints. If you enable additional languages, the user can select other languages to display.

  NOTE You can use `||OPERATION||`, `||PACKAGENAME||`, or `||DEPLOYMENTNAME||` as variables in the title or body. If you are deploying a software bundle, the bundle name is used for the `||PACKAGENAME||` variable.

IMPORTANT If your deployment is configured for a pre-notification, but the endpoint does not have the End-User Notifications tools installed, the deployment fails and triggers the following error: `EunIncompatible: EUN is not installed or the version installed is too old.` For more information about installing End-User Notifications tools on endpoints, see Tanium End-User Notifications User Guide: Configuring End-User Notifications.

Deploy a software package to a single endpoint

You can quickly create a deployment to install a software package on a single endpoint through the Endpoint Details page in Tanium Reporting. To create a deployment, you must have the **Deploy Deployments** write permission.

NOTE You can also install a software package on a single endpoint by following the steps in Deploy a software package or bundle on page 72.

1. Open the Endpoint Details page for the endpoint that requires a deployment. See Tanium Reporting User Guide: View endpoint details.
2. Select the **Endpoint Management** tab.
3. In the **Software Package Applicability** section, click **Install** next to the package you want to deploy, and complete the deployment.

Review deployment summary

You can get the deployment results by status, any error messages, and the deployment configuration details.

1. From the Deploy menu, go to **Deployments**.
2. Select the **Active**, **Inactive**, or **Self Service** tab.

   > NOTE
   > A software package or bundle appears in the **Self Service** tab after it is included in a self service profile and applicability counts appear after a user installs, updates, or removes the item in the End-User Self Service Client application.

3. Click the deployment name. The **Status** section shows the status and substatus, links to deployment results, OS, online endpoints, information about the last time the status or initialization was updated, and any error messages.
4. In the Deployment Details area, expand the section you want to see, or click **Expand All** to expand all sections.
   - **Content to deploy** provides all the configuration information, including installation details, execution information, installation workflow and notifications, patch lists, and patches.
   - **Endpoints to target** lists the targeted endpoints for the deployment.
   - **Deployment type and schedule** shows the deployment frequency, time zone, and schedule.
   - **User notifications** has the information about any end user notifications associated with the deployment.

Stop a deployment

You can stop a package or bundle deployment, but it does not remove packages that have already completed installation.

1. From the Deploy menu, go to **Deployments**.
2. On the **Active** tab, click the deployment name, and then click **Stop**.
3. Go to the **Inactive** tab and click the deployment name to verify the status.

Reissue a deployment

You can restart a stopped deployment or reissue a one-time deployment. Reissuing a deployment creates a new deployment with the same configuration and targets.

1. From the Deploy menu, go to **Deployments**.
2. On the **Inactive** tab, click the deployment name, and then click **Reissue**.
3. Make changes if necessary and then click **Deploy**.

Clone a deployment

You can clone an active deployment if you want to create a deployment that is similar to an existing deployment. When a deployment is cloned, the name is automatically prepended with **Clone:** and the targets are removed.

1. From the Deploy menu, go to **Deployments**.
2. On the **Active** tab, click the deployment name, and then click **Clone**.
3. Make changes and then click **Deploy**.

Reference: Deployment status

The following is a list of all possible deployment status groups and the sub-statuses. Endpoints return deployment statuses only if they are targeted endpoints.

Status group	Sub-status	Description and troubleshooting
Not Applicable	Configuration not available or not targeted	The endpoint is no longer targeted by the deployment. Most commonly, this sub-status means the deployment uses targeting criteria that was changed by the deployment. For example, if you create a deployment with an Adobe Acrobat Reader Update bundle and targeting criteria of `Deploy - Software Packages matches ".Adobe Acrobat Reader.*Update Eligible."`, the deployment updates Adobe Acrobat Reader on endpoints. The update changes the response to the **Deploy - Software Packages** sensor so that this deployment no longer applies.  BEST PRACTICE Use deployment targeting criteria based on attributes that cannot be changed by the deployment.

Status group	Sub-status	Description and troubleshooting
	Stopped before the deployment started	

Status group	Sub-status	Description and troubleshooting
	Software package *ID* is no longer applicable after task error. Updating status.	The software package encountered the error in the sub-status but the package is no longer applicable after running. Investigate the error message and endpoint log files for more information.

Status group	Sub-status	Description and troubleshooting

	• All software packages are not applicable to specified operations
	• Software package **Remove** operation sub-status:
	  ◦ Software package is *applicability* instead of Installed
	• Software package **Update** operation sub-statuses:
	  ◦ Software package is Installed instead of Update Eligible
	  ◦ Software package is Update Ineligible (System Requirements not met)
	  ◦ Software package is Install Eligible instead of Update Eligible
	  ◦ Software package is Not Applicable (Update Detection not met)
	• Software package **Install** operation sub-statuses:
	  ◦ Software package is already Installed
	  ◦ Software package is Update Eligible instead of Install Eligible (Update Detection met)
	  ◦ Software package is Update Ineligible (Update Detection met, System Requirements not met)
	  ◦ Software package is Not Applicable (System Requirements not met)
	  ◦ Software package is Not Applicable (Installation Requirements not met)
	  ◦ Software package is Update Ineligible (System Requirements not met)
	• Software package **Install or Update** operation sub-statuses:
	  ◦ Software package is already Installed
	  ◦ Software package is Update Ineligible (System Requirements not met)
	  ◦ Software package is Not Applicable (System Requirements not met)
	  ◦ Software package is Not Applicable (Update Detection and Installation Requirements not met)
		The deployment will not run because the software package operation is not applicable. The sub-status provides the current software package applicability status and high-level reason.
		If this sub-status is unexpected on an endpoint, investigate the software package applicability.

Status group	Sub-status	Description and troubleshooting
Waiting	Download Complete Waiting	The endpoint downloaded all software package files needed for this deployment but is waiting for the deployment start time or a maintenance window to open. This sub-status is most commonly the result of selecting **Download Immediately** and a future start time in the deployment settings.
	Waiting for initial evaluation	Deploy sent the deployment to the endpoint, but Deploy has not yet evaluated it. This sub-status should not persist for more than a few minutes.
	Waiting for maintenance window. Next window is at *time*	
	Waiting for maintenance window. No upcoming maintenance windows	
	Waiting for deployment start time *x*	
	Waiting for notification	
	Waiting for reboot	
	Waiting to run process	
	Waiting for updated software package catalog	The deployment includes a software package that the endpoint does not have. This sub-status should not persist for more than five minutes.
	Waiting for an active user	The deployment includes a software package with a command that runs as active user, but there is no active user logged in. To avoid this sub-status, use an `||ACTIVEUSERPROFILE||` or `||ACTIVEUSERREGISTRY||` applicability rule, which makes the software package **Not Applicable** if there is not an active user. For more information, see Variables for Windows applicability scans and command-line operations on page 58.
	Waiting for notification for deployment *ID* Waiting for deployment *ID* to finish running Waiting for deployment *ID* to finish running task *ID*	Another deployment is running. The current deployment is ready to run but will not run until the referenced deployment has finished running.

Status group	Sub-status	Description and troubleshooting
Downloading	Software package *ID* downloading files *x*%	
	Downloading required files	Software package files are downloading, but a download status cannot be reported yet.
Running	• Software package *ID* command *name* • Software package *ID* killing process *name* • Software package *ID* waiting for process *name* to exit • Software package *ID* copying *source* to *destination* • Software package *ID* deleting *path* • Software package *ID* creating *path* • Software package *ID* renaming *source* to *destination* • Software package *ID* extracting *source* to *destination*	The command step that is running.
Complete	Success	
	Skipped	A command step encountered an error and was skipped. The command step is in a software package or a software package in a bundle that is set to **On Failure or Error: Continue**.
	Success after re-scan	The deployment did not succeed initially, but after re-running an applicability scan, the software package is now in the targeted state. This sub-status most often happens if the software package installs software that is not fully installed until completing some additional activity, such as a security agent that must connect to a management server before it is fully installed. This sub-status might also indicate that something other than Deploy changed the state of this software shortly after this initial deployment did not succeed.
	Success after step error *error details*	One of the software package commands received an error but the targeted software package applicability state is still achieved. This sub-status might indicate the exit code seen in the error details can be safely ignored or that the software package applicability rules are not fully detecting the state of the software.

Status group	Sub-status	Description and troubleshooting
Failed	Software Package *ID* at edit_id *ID* is no longer present in the catalog	The specific revision of a software package was removed after the deployment started running. This sub-status can happen temporarily when a software package is edited during an active deployment. If it persists for more than 24 hours or appears on a new deployment of an unedited software package, this most likely indicates an issue. Gather endpoint logs and contact Tanium Support.

Status group	Sub-status	Description and troubleshooting
	Software Package *name* (id: *ID*) applicability after *operation* is applicability	The deployment ran but did not reach the targeted applicability state (for example, **Installed** for an **Install or Update** deployment). Instead, the deployment resulted in another applicability state (for example, **Not Applicable** for an **Install or Update** deployment). This sub-status most often indicates a misconfiguration with the software package applicability rules. Review the sub-process log and the software package applicability .

Status group	Sub-status	Description and troubleshooting
	Software package is *applicability* after *operation*. Task error *error details*	

Status group	Sub-status	Description and troubleshooting
	Deployment ended before completing	The deployment stopped or reached the configured end time before it could complete. This sub-status might happen for one of the following reasons: • The deployment window was too short to download needed package files. • There was no active maintenance window during the deployment window. • The duration of notification period was too long and the end user did not accept the notification in time. • There was a persistent error and the deployment ended during a retry.

Status group	Sub-status	Description and troubleshooting
	Failed to import configuration	The deployment or software package configuration could not be imported. To investigate this rare status, verify security exclusions for Deploy and Endpoint Configuration. If this status persists or is repeatable, collect a full Endpoint Must Gather and contact Tanium Support.

Status group	Sub-status	Description and troubleshooting
	Software package *ID* applicability reverted to *applicability* after *previous_deployment_status* deployment status and *attempt_count* attempts were made within *retry_reset_hours* hours. Will not retry for *retry_reset_hours* hours.	The deployment ran and initially succeeded but a software package applicability scan later detected the deployment needed to run again. If this happens enough to exceed the configured deployment **Retry Count** during the period of the deployment **Reset Frequency**, Deploy stops re-running the deployment and sets the deployment to this status. For more information, see Configure module settings on page 49. This sub-status might indicate an external system is undoing changes made by Deploy or that another deployment is undoing it. For example, if this is an **Install** deployment, a concurrent deployment that uninstalls this software might cause this problem.
		Deploy cannot download the package icon configured on the software package. This sub-status most commonly happens if the deployment is configured with **Download Immediately** and a future start time, but the deployment runs when the endpoint cannot connect to Tanium. As a workaround, remove the package icon and re-issue the deployment or wait for the deployment to try again after the **Reset Frequency** interval has elapsed. For more information, see Configure module settings on page 49.
		Deploy is persistently failing to refresh the Self Service Client after the post-deployment applicability scan. This sub-status most likely indicates an issue with Deploy or End-User Self Service. Collect a full Endpoint Must Gather and contact Tanium Support.
		Deploy is persistently unable to complete software package applicability scans. The software management logs contain diagnostic information about this issue. Collect a full Endpoint Must Gather and contact Tanium Support.
		Deploy is persistently unable to launch an end user notification configured in this deployment. This sub-status might happen if there is a disconnected Microsoft Remote Desktop session on a Windows computer. If this status persists or is repeatable, collect a full Endpoint Must Gather and contact Tanium Support.

Managing maintenance windows

Maintenance windows control when deployments can run on a computer group. A maintenance window is separate from the deployment start and end time. To run a deployment, a maintenance window must be open during the configured deployment time, or the deployment must have the **Override maintenance windows** option configured.

Deployments do not run outside of a maintenance window unless the **Override maintenance windows** option is selected in the deployment options. You must create at least one maintenance window for other deployments to run.

Maintenance window options

You can configure maintenance windows for the times that are best for your environment. Apply maintenance windows by enforcing them against computer groups. Multiple maintenance windows can affect a computer group, creating several times that deployment activity is permitted.

If you want . . .	After the date and time, select . . .
A one-time window	**Does Not Repeat**
A window that repeats every few days	**Daily** and the number of days between windows
A window that repeats on the same days of the week	**Weekly**, the number of weeks between windows, and which days of the week it opens on
A window that repeats on the same date each month	**Monthly**, the number of months between windows, and **Day of the Month**
A window that repeats on the same day each month	**Monthly**, the number of months between windows, and **Day of the Week**
A window that repeats on the same day of the year	**Yearly** and the number of years between windows

If a maintenance window does not repeat and it is the only one enforced against a computer group, deployments cannot run after the window closes.

Create a maintenance window

You can open multiple maintenance windows to customize when deployments run on your endpoints. For example, you can create windows that allow deployments during periods of low network activity or outside of core working hours.

1. From the Deploy menu, go to **Maintenance Windows** and then click **Create Window**.
2. Name the window.
3. Configure the window options.
   a. (Optional) Select the repetition time frame.
   b. Use the date and time pickers to set the start and end time of the window.

      NOTE If a maintenance window repeats, it does not have an end date. You must remove the enforcement against the target computer groups to stop the maintenance window.

   c. Choose from the local time on the endpoint or UTC time.
   d. If you chose to repeat the window, set additional options, such as how long the window lasts, how often the window repeats, day of the week, or day of the month.
4. (Optional) Add targets.

   Select either or both of the following targeting methods and complete the fields as needed. If you select both targeting methods, then they are joined by an `OR` operator. If you use multiple targets, the maintenance window applies to endpoints that match any of the targets you specify.

   - **Select Computer Groups** provides a drop-down list of computer groups available to be managed in Deploy. Maintenance windows can only target management-rights enabled computer groups.

     NOTE Maintenance window computer groups must be assigned RBAC permissions for the user or group to appear in the list. For more information, see Tanium Console User Guide: RBAC overview.

   - **Set Targeting Criteria** lets you add any Tanium question filter as a target. When you use this option, you must also select a limiting group from the **Select Limiting Group** drop-down list of computer groups. For example, to target endpoints in the `192.168.1.0/24` subnet, you can type `Tanium Client IP Address starts with 192.168.1` in the **Filter Bar** or use the **Filter Builder** to select the **Tanium Client IP Address** sensor, and then apply the same filter. After that, set the `All Windows 10` computer group as the limiting group to make the deployment apply to all Windows 10 endpoints with an IP address that starts with `192.168.1`.

     IMPORTANT The **Select Computer Groups** and **Set Targeting Criteria** options are joined by an `OR` operator. If you use multiple targets, the deployment applies to endpoints that match any of the targets you specify. If you use Set Targeting Criteria, you must also specify a limiting group that limits all targets. For example, if you select **All Laptops** as the target computer group, the deployment goes to all laptops managed by Deploy. However, if you also add `Tanium Client IP Address starts with 192.168.1` as the targeting criteria, and then select **All Windows 10** as the limiting group, then the deployment goes to all Windows 10 devices that are either laptops or have an IP address starting with `192.168.1`.
5. Click **Create Window**. Review any informational messages that appear and perform any updates that are necessary to the maintenance window. Click **Create Window**. Click **Yes** to confirm that you want to create a maintenance window.

Edit a maintenance window

1. From the Deploy menu, go to **Maintenance Windows**.
2. Click the name of a window and click **Edit**.
3. Make your changes and click **Update Window**.

Override a maintenance window

You can run a deployment outside of a maintenance window by configuring the **Override maintenance windows** option during a deployment. For more information, see Deploying software on page 71.

Delete a maintenance window

After the enforcements have been removed, you can delete a maintenance window.

1. From the Deploy menu, go to **Maintenance Windows**.
2. Click the name of a window.
3. If the window is enforced against computer groups, remove all groups.
4. Click Delete  .

Managing End-User Self Service

With the Self Service Client application, you can publish software to Windows endpoints so that users can install software on their own without the need for IT to install them. To use the Self Service Client application on your Windows endpoints, you must create a self service profile in Deploy version 1.2 or later.

Before you begin

- Create or import one or more software packages. For more information, see Managing software on page 54.
- Configure the end-user interface options (logo, title, greeting text, additional language support, shortcut options, and enabling End-User Self Service). For more information, see End-User Notifications User Guide: Customizing the End-User Self Service interface.

Create a self service profile

1. From the Deploy menu, go to **Self Service Profiles** and then click **Create Profile**.
2. Provide a name and optionally a description for the profile.
3. Add targets.
   Select either or both of the following targeting methods and complete the fields as needed. If you select both targeting methods, then they are joined by an `OR` operator. If you use multiple targets, the profile applies to endpoints that match any of the targets you specify.
   - **Select Computer Groups** provides a drop-down list of computer groups available to be managed in Deploy.
   - **Set Targeting Criteria** lets you add any Tanium question filter as a target. When you use this option, you must also select a limiting group from the **Select Limiting Group** drop-down list of computer groups. For example, to target endpoints in the `192.168.1.0/24` subnet, you can type `Tanium Client IP Address starts with 192.168.1` in the **Filter Bar** or use the **Filter Builder** to select the **Tanium Client IP Address** sensor, and then apply the same filter. After that, set the `All Windows 10` computer group as the limiting group to make the deployment apply to all Windows 10 endpoints with an IP address that starts with `192.168.1`.

     IMPORTANT The **Select Computer Groups** and **Set Targeting Criteria** options are joined by an `OR` operator. If you use multiple targets, the deployment applies to endpoints that match any of the targets you specify. If you use Set Targeting Criteria, you must also specify a limiting group that limits all targets. For example, if you select **All Laptops** as the target computer group, the deployment goes to all laptops managed by Deploy. However, if you also add `Tanium Client IP Address starts with 192.168.1` as the targeting criteria, and then select **All Windows 10** as the limiting group, then the deployment goes to all Windows 10 devices that are either laptops or have an IP address starting with `192.168.1`.
4. (Optional) Deselect **Use Latest** if you want to add versions of software packages other than the latest.

5. To choose packages or bundles to include in the profile, click Add next to the available package or bundle.
   You can also select multiple packages or bundles and click Add to add multiple packages or bundles at the same time.
   a. Select whether the package or bundle is allowed to be installed, updated, or removed in the Self Service Client application.
      By default, bundles are allowed only to be installed. Some options cannot be deselected.
   b. If a package or bundle requires a restart of the endpoint, you can select **Restart Required**.
6. Click **Create Profile**.

View self service profiles

From the Deploy menu, go to **Self Service Profiles** to view all self service profiles.

This page displays all currently defined profiles and basic information about those profiles. You can expand the profile to view more detail about the profile, including the defined software packages and the allowed actions that are associated with each package. This expanded detail also shows the targeted groups or questions for the profile.

Edit a self service profile

To edit a self service profile, click the profile name and then click **Edit**.

Delete a self service profile

To delete a self service profile, click the profile name and then click Delete .

Track usage statistics

You can check the status of packages or bundles that are used in the Self Service Client application and track usage statistics of the Self Service Client application on endpoints.

From the Deploy menu, go to **Deployments** and then click **Self Service**. This page displays all software packages and bundles that are included in self service profiles.

Use the Self Service Client application on endpoints

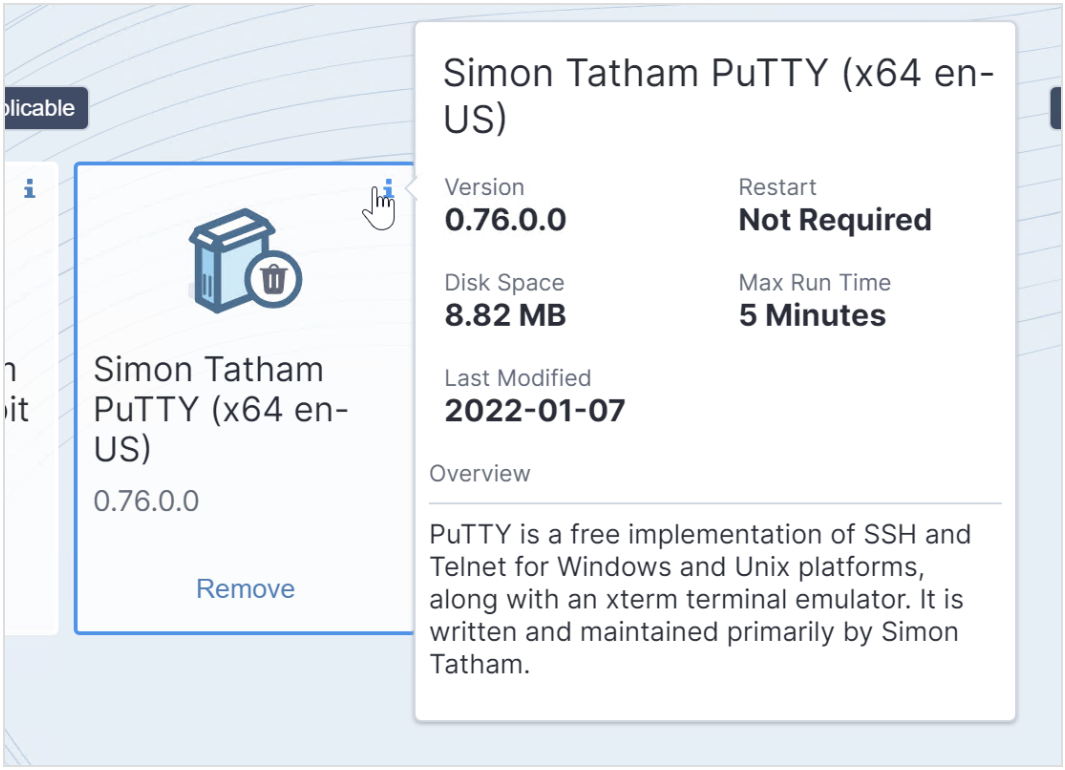
The Self Service Client application lets you install, update, or remove software applications on endpoints. You can customize the End-User Self Service interface with a custom name, support link, logo, and shortcut icon. For more information about customizing the Self Service Client interface, see Tanium End User Notifications User Guide: Customizing the End-User Self Service interface.

The Self Service Client application includes the following tabs:

Catalog

On the **Catalog** tab, you can perform the following actions:

- See a list of all available software applications in the catalog. You can filter to show applications to be installed, removed, or updated, or to show only the applications available to the endpoint. You can also select a gallery or list view, and that view automatically adjusts based on the resolution set on the endpoint.
- See all active deployments, until the install, update, or removal is complete.
- Select additional languages that you have enabled in the End User Notifications settings. For more information, see Tanium End User Notifications User Guide: Customizing the End-User Self Service interface.
- See additional details about each available package. Hover your mouse over the information icon for each package to see additional details about the package. You can configure those details, including the name of the package, on each software package.



For more information, see Create a software package on page 54.

Updates

On the **Updates** tab, you can see updates that are available for installed software applications.

History

On the **History** tab, you can see any completed activities that occurred on the system, as well as who initiated the activity. You can filter results by deployment type, as well as by time period.

Activity

On the **Activity** tab, you can see current and upcoming deployment activity. You can also select **Install** to start the deployment before its scheduled start time. However, you can hide upcoming deployment activity on the **Activity** tab by selecting **Hide from Self Service Client** when you configure the deployment. Similarly, if you do not select **Make Available Before Start Time** when you configure the deployment, then end users cannot start a deployment before its scheduled start time. For more information, see Deploy a software package or bundle on page 72.

Maintaining Deploy

Perform regular maintenance tasks to ensure that Deploy successfully performs scheduled activities on all the targeted endpoints and does not overuse endpoint or network resources. If Deploy is not performing as expected, you might need to troubleshoot issues or change settings. See Troubleshooting Deploy on page 102 for related procedures.

Perform weekly maintenance

Monitor Deploy metrics and update the configurations, if necessary.

1. From the Main menu, go to **Modules > Trends > Boards**.
2. Click **IT Operations Metrics** to view the **Deploy Coverage**, **Endpoints Missing Software Updates Released Over 30 Days**, **Mean Time to Deploy Software**, and **Software Installed by Self Service User Request** panels in the **Deploy** section.
3. Monitor and troubleshoot Deploy coverage on page 98.
4. Monitor and troubleshoot endpoints missing software updates released over 30 days on page 99.
5. Monitor and troubleshoot mean time to deploy software on page 100.
6. Monitor and troubleshoot software installed by self service user request on page 100.

Perform monthly maintenance

Review and remediate Deploy coverage

1. From the Main menu, go to **Modules > Deploy > Overview**.
2. Scroll to the **Health** dashboard to verify that the Deploy process is running on all endpoints.
3. To investigate endpoints that are not running the process, click the number above **False** in the **Running Deploy** panel. The Tanium Server opens the **Deploy - Endpoint Deployment Process Running** report for the affected endpoints.
4. To investigate Deploy coverage issues, scroll up to the **Summary** dashboard and click the number above **Needs Attention** in the **Deploy Coverage** panel. The Tanium Server opens the **Deploy - Coverage Status Details** report for the affected endpoints.
5. To troubleshoot issues related to the Deploy process or coverage, see Troubleshoot Deploy process not running on page 105.

Remove unused Deploy software packages

1. Go to **Modules > Deploy > Software**.
2. Review the **Software Packages** and delete unused packages.
   For example, delete software packages that are not the latest version or software that you are no longer using. For more information, see Managing software on page 54.

Stop unneeded ongoing deployments

1. Go to **Modules > Deploy > Deployments > Active**.
2. Review the deployments and stop any deployments that are no longer needed.

Perform quarterly maintenance

If you install Deploy with default settings, it includes the **Tanium Deploy** action group, to which the **All Computers** computer group is assigned. If you changed computer group assignments for the **Tanium Deploy** action group, or if you created custom action groups for Deploy, review those action groups and, if necessary, update them. For example, if you discover that the Deploy tools are not installed on all the necessary endpoints, you might have to change the computer group assignments in the **Tanium Deploy** action group.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. Use the filters to list only the groups that are for Deploy operations. See Tanium Console User Guide: View action groups. For example, if the custom action groups all have the string "Deploy" in their names, enter `Deploy` in the **Filter items** field.
3. Edit, create, or delete action groups if necessary to ensure Deploy targets the correct computer groups. See Tanium Console User Guide: Managing action groups.

Perform semi-annual maintenance

Review Deploy self-service profiles and, if necessary, update them to ensure that users have access to all the self-service capabilities:

1. From the Main menu, go to **Administration > Modules > Deploy > Self Service Profiles** and review the profiles. Expand  each profile and verify that all the operations are successful  .
2. From the Deploy menu, go to **Deployments > Self Service** and review the **Failures** column.
3. Troubleshoot self-service installations if necessary to resolve issues. See Monitor and troubleshoot software installed by self service user request on page 100.
4. Edit, create, or delete self-service profiles if necessary to resolve issues. See Managing End-User Self Service on page 93.

Monitor and troubleshoot Deploy coverage

The following table lists contributing factors into why the Deploy coverage metric might report endpoints as **Needs Attention** or **Unsupported**, and corrective actions you can make.

Contributing factor	Corrective action
Gaps in Deploy action group membership	Ensure that all endpoints that have a supported configuration for Deploy have the Deploy tools installed. These endpoints should be added to computer groups that can be members of the Deploy action group.

Contributing factor	Corrective action
Gaps in End-User Notifications tools installations	Users cannot receive notifications for actions that are about to happen or configure the Self Service Client application. Ensure that all endpoints that have a supported configuration have the End-User Notifications tools installed. Ensure that any endpoint that is using the Self Service Client application has a properly configured and targeted End User Notification customization profile. Ensure that all other endpoints have a default fallback profile configured in case the tools need to be accessed.
Gaps in Trends metric reports	Ensure that all computer groups that are part of the Deploy action group are also part of the End-User Notifications action group.

Monitor and troubleshoot endpoints missing software updates released over 30 days

The following table lists contributing factors into why the endpoints missing software updates released over 30 days metric might be higher than expected, and corrective actions you can make.

Contributing factor	Corrective action
Gaps in maintenance window coverage	Verify that the **Computers with Enforced Maintenance Windows** chart in the **Health** section of the Deploy **Overview** page shows 100% enforcement. Ensure that endpoints have enough time to download and perform the installation. Use the **Download immediately** option for future deployments so that endpoints are ready when the deployment start time begins. If your business needs require a hard stop, set your maintenance window to end 30 minutes prior to that hard stop to ensure that deployments complete in time to adhere to business needs.
Software is not installing due to maintenance windows being too restrictive	Ensure that maintenance windows properly overlap with deployment times and change control process timelines. Use End-User Notifications to provide users with options to postpone actions, such as installations or updates. Use the **Make Available Before Start Time** option for self service deployments that are set for the future.
Software hits a timeout or does not install properly	Ensure that you have a supported silent installation command-line option that is supported by the vendor. Consult with the vendor or developer of the software for the best practices to install the software.

Contributing factor	Corrective action
The installer does not have a silent installation option	Use a third-party repackaging solution, such as AdminStudio or InstallShield, that offer the ability to assist in making a custom installer. Request that the vendor create a proper silent installer for larger deployments.

Monitor and troubleshoot mean time to deploy software

The following table lists contributing factors into why the mean time to deploy software metric might be higher than expected, and corrective actions you can make.

Contributing factor	Corrective action
Files are not uploading to a package properly	(Windows) Ensure that the permissions are properly set to remote Windows file servers. (Appliance) Ensure that you set up the Module Server TDL to access the shares. For more information, see Tanium Appliance User Guide: Add an authentication user for TDownloader.
Packages are not downloading from the Predefined Package Gallery	Ensure that the Tanium Server can download the packages from the remote URL. Check any proxies, firewalls, or network connectivity. Ensure that your TDL settings are correct. For more information, see Maintaining Deploy on page 97.
It takes too long to test the software and get it ready for production	Reevaluate your process for software testing: • Are there any gaps or delays in the process? • Are there too many points of contact for reporting issues? • Are endpoints being tested that may not be relevant for the deployment? Evaluate conditions that surround problem resolution and retesting. Hold people accountable to timelines. For endpoints that might exhibit compatibility or testing issues, consider a shared solution, such as Terminal, Remote Desktop Server, Citrix XenApp, or App-V.

Monitor and troubleshoot software installed by self service user request

The following table lists contributing factors into why the software installed by self service user request metric might be different than expected, and corrective actions you can make.

Contributing factor	Corrective action
Help desk spends too much time installing software for users	Use self service options for software that is pre-approved, to ease the load on your help desk. Applications that make the best candidates for self service are: • Freeware (example: Chrome or Firefox) • Software that is available for all systems, but are discretionary by business needs (example: Zoom, Notepad++, or specific line of business applications)
Users install unapproved software	Use self service options, but limit the applications that the user has access to, by default. Consider locking down administrative permissions on the endpoints, if available. For software that might require additional approvals, such as software that requires a purchased license, target only endpoints that are approved to install that software.

Troubleshooting Deploy

If Deploy is not performing as expected, you might need to do some troubleshooting or change settings.

TIP For more comprehensive troubleshooting information, registered Tanium customers can sign in to view the Tanium Community: Deploy Troubleshooting Guide.

Collect a troubleshooting package

For your own review or to assist support, you can compile Deploy logs and files that are relevant for troubleshooting.

1. Get the Deploy log.
   a. From the Deploy **Overview** page, click Help.
   b. Click the **Support** tab and click **Collect**.
   c. When the **Status:** is updated, click **Download**.

   The log zip file might take a few moments to download. The files have a timestamp with a deploy-support-*YYYY-MM-DD*T*HH-MM-SS.mmm*Z format.
2. (Optional) On the endpoint, copy the `Tanium\Tanium Client\Tools\SoftwareManagement` folder.

Upgrading to Deploy 2.19

IMPORTANT In Deploy 2.19, the steps required to configure the service account are no longer necessary due to the adoption of the System User Service, which performs these tasks automatically. After upgrading to Deploy 2.19, it might take time for the RBAC privileges and other updates to sync properly. This could lead to issues and error messages when you first query the Tanium Console. These issues usually resolve on their own after a few minutes, but could take up to an hour or longer depending on system resources and the amount of data to migrate.

View job logs to troubleshoot `job failed` errors

You can download job logs to troubleshoot "job failed" errors.

1. From the Deploy **Overview** page, click Help.
2. Click the **Support** tab and click **View Job Status**.
3. In the **Job Detail** window, click **Download Logs** to download a `job-logs.txt` file with more details about recent jobs.

Collect Deploy troubleshooting information from endpoints

You can collect and review endpoint artifacts to troubleshoot Deploy issues on endpoints. For general information about collecting troubleshooting information from endpoints, see Tanium Client Management User Guide: Collect troubleshooting information from endpoints.

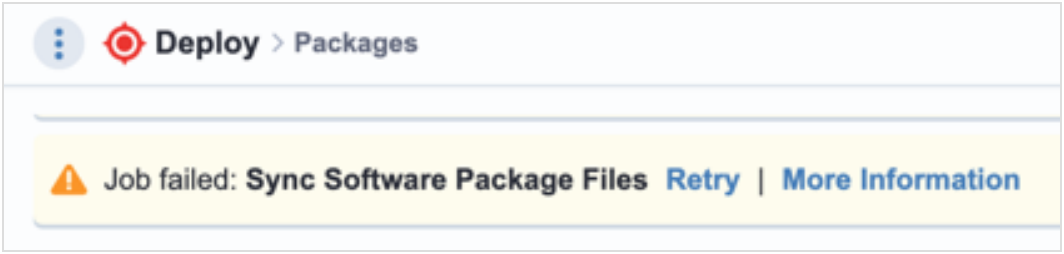
The following files are available on endpoints that have Deploy installed:

File	Location and information
Software Management log files	`Tanium Client\Tools\SoftwareManagement\logs` These logs contain information that can help you troubleshoot multiple problems, including scan issues, deployment issues, and application crashes.
`Deploy subprocess.log`	`Tanium Client\Tools\SoftwareManagement\logs` This log contains information about processes that run outside of Deploy as part of software deployments. For example, it includes install errors during OS upgrades.
`softwaremanagement.db` file	`Tanium Client\Tools\SoftwareManagement\data` Deploy uses this database to read and write information about configurations, stored data files, and the endpoint operating system.

Troubleshoot `Job failed: Sync Software Package Files` error

The `Job failed: Sync Software Package Files` appears in the Deploy workbench if a software package did not synchronize properly. The most common reason for the error is that Deploy cannot cache remote files associated with a package. However, the error can appear for a variety of reasons.

1. Review the information available for the error in the Deploy workbench. If the `Job failed: Sync Software Package Files` error banner includes **More Information**, click the link and review the information.



   You can also retry the synchronization or export, copy, or download the information on this page.

2. Review the logs to identify the issue for the error. See View job logs to troubleshoot job failed errors on page 102.
3. Review Common package synchronization failure issues and resolutions on page 104 for corrective actions.

Common package synchronization failure issues and resolutions

The following table explains different issues that can prevent a software package from syncing properly.

Issue	Explanation and corrective action

Deploy cannot download a remote file at all	• The Tanium Server cannot access the URL for a remote file in a Predefined Gallery package because the URL is blocked by a firewall or proxy. Try one of the following solutions:
	  ◦ Manually add inaccessible files to the affected software package. For more information, see Deploy cannot access the origin of a software package file on page 104.
	  ◦ Review the Tanium Server TDL log for diagnostic information. For information about accessing the Tanium Server TDL log, see Tanium Appliance Deployment Guide: Review Tanium Core Platform logs.
	• When you import a custom package, the Tanium Module Server cannot access the URL for the package because the URL is blocked by a firewall or proxy, or it is inaccessible for another reason. Try one of the following solutions:
	  ◦ Manually add inaccessible files to the affected software package. For more information, see Deploy cannot access the origin of a software package file on page 104.
	  ◦ Review the Tanium Module Server TDL log for diagnostic information. For information about accessing the Tanium Server TDL log, see Collect a troubleshooting package on page 102.

The file hash does not match what is defined in the package definition	This issue is usually caused by a recent release of a new version of the software. Compare the software package version to the latest version published by the vendor, and then try one of the following solutions: • If the version is the same, manually add affected files to the software package. • If the vendor has published a new version, edit the package and update the new version information before manually adding affected files to the software package. Alternatively, wait for a new software package to be published to the Predefined Package Gallery. • For information about manually adding files to a software package, see Deploy cannot access the origin of a software package file on page 104.
A different problem is preventing Deploy from synchronizing the software package	This issue can sometimes be caused by an error with the Tanium Server or with the Endpoint Configuration Service. Review the job logs for basic diagnostic information. Collect a support bundle and review the Deploy service log and Module Server or Tanium Server TDL logs for additional diagnostic information. For more information, see Collect a troubleshooting package on page 102 and Tanium Appliance Deployment Guide: Review Tanium Core Platform logs.

Deploy cannot access the origin of a software package file

If Deploy cannot access the origin of a software package file, you can follow these basic steps to edit the package and manually add any inaccessible files:

1. Download the inaccessible remote file to your computer.
2. Edit the software package.
3. If necessary, expand the **Package Files** section, then click **Add Package Files > Local File** to upload the file from Step 1 to the software package.
4. Ensure that the new package file uses the same value for the **File Display Name** field as the original package file.
5. Delete the original package file and save the package.

   For more information about configuring software packages, see Create a software package on page 54.

End user notifications are not displayed or endpoints have other issues

End user notifications are supported for Windows and macOS endpoints only. If end user notifications are not being displayed on the endpoints or the endpoints have other issues (for example, their statuses are **Needs Attention**):

1. Verify that the Tanium End-User Notifications solution is installed. For more information, see Tanium End-User Notifications User Guide: Installing End-User Notifications.
2. Ask the question: `Get End-User Notifications - Has Tools from all machines` to check if your endpoints have the end user notification tools.
3. Verify that any security software exclusions include the `\Tanium\Tanium End User Notification Tools` directory. For more information, see Security exclusions on page 33.
4. Uninstall the End-User Notifications tools on the endpoints. For more information, see Tanium End-User Notifications User Guide: Remove End-User Notifications tools from endpoints. Then wait up to 10 minutes for the tools to automatically reinstall.

   NOTE You can also reinstall the End-User Notifications tools with the **Endpoint Configuration - Reinstall Tool** package.

Deployment fails with EUN error on endpoint

If your deployment is configured for a pre-notification, but the endpoint does not have the End-User Notifications tools installed, the deployment fails and triggers the following error: `EunIncompatible: EUN is not installed or the version installed is too old.` If you receive this error, ensure that the endpoint has a supported configuration and has the End-User Notifications tools installed. For more information, see Tanium End-User Notifications User Guide: Configuring End-User Notifications.

Troubleshoot Deploy process not running

The **Running Deploy** chart on the **Overview** page or the **Deploy - Is Process Running** sensor report endpoints on which the Deploy process is not running.

The following table explains different issues that can prevent the Deploy process from running.

Issue	Explanation and corrective action
The endpoint does not support Deploy.	1. Ask the question `Get Deploy - Coverage Status from all machines` to identify the endpoints on which Deploy is not supported. 2. Review the Deploy requirements and make necessary changes.
Deploy tools are not installed on the endpoint.	Deploy tools are installed as part of Software Manager CX, which is installed as part of Endpoint Configuration. 1. Ask the question `Get Endpoint Configuration - Tools Status Details from all machines` and drill down on **Software Management**. 2. Review the endpoints on which Deploy and its dependencies are not installed. 3. To reinstall Deploy tools, see Tanium Endpoint Configuration User Guide: Reinstall tools installed by Endpoint Configuration.
The endpoint is not in the Deploy action group.	The endpoint must be in a computer group in the Deploy action group to have the Deploy process started and the Deploy tools installed. Review the computer groups in the Deploy action group. For more information, see Configure the Deploy action group on page 47.
The Deploy process is not running for another reason.	Review endpoint logs. For information on how to collect the logs, see Collect Deploy troubleshooting information from endpoints on page 103. The Software Management logs indicate if the Deploy process starts but then fails. This failure might be from interference with security software, an issue with the Deploy tools on the endpoint, or another issue. As a possible remediation step, reinstall Deploy tools. See Tanium Endpoint Configuration User Guide: Reinstall tools installed by Endpoint Configuration. If the Software Management logs do not exist or do not indicate the Deploy process starting and then crashing, Contact Tanium Support on page 110.

No applicability information for software packages

Software package applicability is calculated on the endpoints by using the applicability rules in the package definition, which is stored in the software package catalog and distributed to the endpoints.

If the applicability information for software packages is not available:

1. Verify that the Deploy process is running on the target endpoint.
    a. Ask the question: `Get Deploy - Is Process Running from all machines`
    b. Check locally for the `\Tanium\Tanium Client\python38\TPython.exe` file on the endpoint.

2. Compare the current and cached results of the **Deploy - Software Packages Applicability** sensor

   a. In Interact, ask the question: `Get Deploy - Software Packages Applicability[1,100000] from all machines`

   b. Toggle between **Current** and **Cached** to ensure that the results match.

   > TIP If you do not see **Current** and **Cached**, ensure that the **Deploy - Software Packages Applicability** sensor is registered for collection in the **Registration & Collection** tab of the Interact Settings for the specific parameter values. For more information, see Tanium Console User Guide: Display sensor collection registration details.

   c. If you see any discrepancies, go to the Interact Settings and click **Collect Now**.

> NOTE For information on troubleshooting unexpected availability, see View software package applicability on page 64.

No software in the Predefined Package Gallery

After you import Deploy 1.1 or later, you must initialize the endpoints again. After the endpoints are initialized, it might take up to one hour to see the software in the **Predefined Package Gallery** page. You can also restart the Tanium Deploy service to reduce this time constraint.

If you still do not see any software in the **Predefined Package Gallery** page:

1. From the Main menu, go to **Administration > Content > Packages**.
2. Search for the `Deploy - Software Package Gallery` package.
3. Verify that this package is cached.
   a. Verify that the **Size** column does not list `Pending`.
   b. If the size stays at `Pending` for more than one hour, Contact Tanium Support on page 110 for assistance.
4. Check to see if the Tanium Deploy service is attempting to gather the Deploy Predefined Package Gallery file.
   a. Collect a troubleshooting package on page 102.
   b. Open the downloaded support bundle and open the `deploy-files\logs\Deploy.log` file.
   c. Search for `Ensuring software package gallery zip package`.
   d. If the `Deploy.log` file does not have that text, Configuring Deploy on page 46 again, wait 10-15 minutes, and then repeat the previous steps to recheck the log file.
5. If you still do not see any software in the **Predefined Package Gallery** page after completing the previous steps, Contact Tanium Support on page 110 for assistance.

Uninstall Deploy

Use only this procedure to uninstall Deploy.

If you need to uninstall Deploy, first clean up the Deploy artifacts on the endpoint, then uninstall Deploy from the server, and then remove Deploy data directories and files from the server.

Remove Deploy artifacts from endpoints

To remove Deploy from endpoints, use the following options in the `Endpoint Configuration - Uninstall` package for Deploy to block reinstallation, perform a hard uninstall, and then remove unreferenced dependencies. For more information, see Remove Deploy tools from endpoints.

Remove Deploy from the Tanium Module Server

1. From the Main menu, go to **Administration > Configuration > Solutions**.
2. Select the check box in the Deploy section, then click **Uninstall** and follow the process.
3. Return to the **Solutions** page and verify that the **Import** button is available for Deploy.

If the Deploy module has not updated in the console, refresh your browser.

Remove packages

1. From the Main menu, go to **Administration > Content > Packages.**
2. In the **Content Set** column, filter on values that contain Deploy.

(Optional) Remove data directories and files

To permanently remove all Deploy data from the Tanium Module Server, manually delete the following directories and files. If you later import the Deploy solution, the previous data is not restored.

WINDOWS:

- `\Program Files\Tanium\Tanium Module Server\services\deploy-files\`
- `\Program Files\Tanium\Tanium Module Server\services\deploy-service\`
- `\Program Files\Tanium\Tanium Module Server\temp\deploy-service\`
- `\Program Files\Tanium\Tanium Module Server\temp\deploy-service-invoker\`
- `\Program Files\Tanium\Tanium Module Server\temp\deploy-service-proxy\`
- `\Program Files\Tanium\Tanium Module Server\temp\deploy-*.bak`

TANOS:

This action requires access to the unrestricted shell. For more information, including how to request a shell key, see Tanium Appliance Deployment Guide: Examine OS processes and files.

- `/opt/Tanium/TaniumModuleServer/deploy-files`
- `/opt/Tanium/TaniumModuleServer/deploy-service`
- `/opt/Tanium/TaniumModuleServer/temp/deploy-*.bak`

Remove Deploy tools from endpoints

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

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

   NOTE

   If reinstallation is blocked, you must unblock it manually:

   - To allow Deploy to reinstall tools, deploy the **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]** package (depending on the targeted endpoints).
   - If you reinstall tools manually, select **Unblock Tool** when you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package.
7. (Optional) To remove all Deploy databases and logs from the endpoints, clear the selection for **Soft uninstall**.

   CAUTION

   When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

8. To also remove any tools that were dependencies of the Deploy tools that are not dependencies for tools from other solutions, select **Remove unreferenced dependencies**.
9. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.
10. Click **Show preview to continue**.
11. A results grid appears at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

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

Contact Tanium Support

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

Use case: Upgrading Windows

Deploy supports two methods for upgrading Windows: enablement package upgrades and in-place upgrades.

Enablement package upgrades use files that are staged on endpoints to upgrade specific versions of Windows 10 to newer versions. This type of upgrade is fast, reliable, and requires no additional configuration.

Other upgrade paths require an in-place upgrade. This type of upgrade requires that you first stage Windows installation media on the endpoints to upgrade, then scan for compatibility, and lastly run Windows Setup to install the new version of Windows.

Overview of enablement package upgrades

To use the enablement package method, import the Feature Update software package from the Predefined Package Gallery and then deploy it to the endpoints you want to target. Enablement packages require no additional setup.

The deployment should include a pre-notification, a post-notification, and a restart to ensure that it completes successfully without end users interrupting it. For information about configuring notifications and restarts, see Deploy a software package or bundle on page 72.

Deploy supports the following enablement package upgrade paths:

Supported enablement package upgrades

Current version with upgrade prerequisites	Enablement package
Windows 10, version 2004 Windows 10, version 20H2 Windows 10, version 21H1 The following updates must also be installed before upgrading: • Servicing stack update Windows 10, version 2004: September 8, 2020 or later • Cumulative update September 14, 2021 – KB5005565 (OS Build 19041.1237) or later	**Feature Update to Windows 10, version 21H2 (KB5003791)**
Windows 10, version 20H2, Enterprise edition Windows 10, version 21H1 Windows 10, version 21H2 The following updates must also be installed before upgrading: • Servicing stack update Windows 10, version 2004: September 8, 2020 or later • Cumulative update July 26, 2022—KB5015878 (19041.1865) or later	**Feature Update to Windows 10, version 22H2 (KB5015684)**

For more information, see Import a software package from the Predefined Package Gallery on page 61.

Overview of in-place upgrades

Deploy supports the upgrade of Windows 7 Service Pack 1 and later to Windows 10 and upgrades of Windows 10 to later builds of Windows. You can use Deploy to handle the Windows upgrade process in three phases:

Phase 1: Download Windows media and scan for compatibility

You can choose from two options for downloading and installing the Windows media in preparation for the upgrade:

- **Phase 1: Pre-Cache**—The Phase 1 Pre-Cache software package invokes a PowerShell script to copy the files that are required for the upgrade to the `C:\Deploy` directory on the endpoint. After the files are in place, the PowerShell script runs Windows Setup to check for upgrade compatibility. The script then takes the information returned from Windows Setup and records the results in the registry. This option is the best choice for updating many Windows endpoints that are in the same physical network location.
- **Phase 1: Direct Cache**—This method uses a script to determine the correct URL for the Windows media that matches the architecture, edition, and language of the endpoint being upgraded and then downloads that media directly from Microsoft. This method is the best choice for updating Windows endpoints that are not peering with other Tanium-managed endpoints, such as those used by remote workers. It is also the best choice for managing many different language versions of Windows.

The following instructions assume that you are using the **Phase 1: Pre-Cache** option for peered Windows endpoints. For information about targeting both peered and non-peered Windows endpoints, see Tanium Community: Managing Windows 10 in a Distributed-Workforce World.

Phase 2: Compatibility remediation and re-scan

If the Phase 1 compatibility scan fails, you must remediate any problems. You can use the Phase 2 software package to force a new scan. Rescanning is necessary if there is a compatibility problem detected in the Phase 1 scan that is later remediated.

Phase 3: Windows Upgrade

The Phase 3 software package invokes a PowerShell script that runs Windows Setup to perform the upgrade.

Before you begin an in-place upgrade

To set up your Windows 10 upgrade, you must have the Windows 10 media (ISO or ESD file) that corresponds to the Windows version, channel, architecture, and language that you want to deploy.

Your security administrator must create security exclusions to ensure successful operation of Tanium Deploy and the Tanium Client. Additional security exclusions for Windows are required for Windows upgrades.

- Microsoft Support: Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows (KB822158).
- Tanium Client Management User Guide: Host system security exclusions
- Security exclusions on page 33

NOTE If you have any questions about implementing Windows upgrades in your environment, Contact Tanium Support on page 110 to discuss your testing and implementation plans.

Step 1: Import software packages

To begin, you must import three software packages from the predefined package gallery. The following examples use Windows 10 Version 21H1, 64-bit. Substitute with the version and architecture you are deploying as needed.

1. From the Deploy menu, go to **Software**, and then click **Predefined Package Gallery**.

   TIP You can use the filter or search options to narrow the list to Microsoft Windows upgrades.

2. Select the following three packages:

   - **InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase1 - Pre-Cache**
   - **InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase2 - Re-Scan**
   - **InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase3 - Upgrade**

3. Click **Import**, confirm the action, and then click **Go To Software Packages**.

   TIP A warning might appear indicating there are pending software package changes and that the catalog must be distributed. You can skip distributing the catalog in this step, as you need to do it again after providing the Windows 10 media.

Step 2: Review and modify software packages

Before you deploy the packages, you must upload the downloaded ISO or ESD files, and then make some modifications to the software packages in the following order:

1. Modify the Phase 1 software package on page 113
2. View the Phase 2 software package on page 114
3. (Optional) Modify the Phase 3 software package on page 114

Modify the Phase 1 software package

1. From the Deploy menu, go to **Software**.
2. Click **InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase1 - Pre-Cache** and then click **Edit**.
3. Expand **Package Files**, and then click **Add Package Files > Local File**.
4. Navigate to the ISO or ESD file and then click **Open**.
   After the upload completes, the file entry with its SHA-256 hash appears.

5. (Optional) If a locale other than en-us is required, edit the **Update Detection** and **Install Verification** rule and change **1033** to the appropriate language ID. For more information and a complete list of all language/region decimal IDs, see Microsoft Documentation: Available languages for Windows.
6. Click **Save Package** and then if prompted, click **Distribute Catalog**.

   NOTE After you update the package, the Module Server transfers files to the Tanium Server. This process could take up to 30 minutes. You cannot deploy the Phase 1 software package to any clients until it completes.

View the Phase 2 software package

This package triggers a new scan after remediating any problems with the Phase 1 scan. Modifications to this software package are not required or supported.

(Optional) Modify the Phase 3 software package

The PowerShell script associated with Phase 3 starts the Windows Setup upgrade process and in most cases should need no modification. The script runs Windows Setup with the following command line arguments:

```
/auto Upgrade /NoReboot /Quiet /DynamicUpdate disable /ShowOOBE none /Telemetry disable /Uninstall enable
```

If you need to append additional arguments to the command line that Windows Setup is using for upgrade, you can complete the following steps:

NOTE If you modify these packages, ensure that you test thoroughly and run them at your own risk.

1. From the Deploy menu, go to **Software**.
2. Click **InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase3 - Upgrade** and then click **Edit**.
3. In the **Update** section of the **Deploy Operations** section, add any arguments to the end of the command in **Run Command**. For example, if you want to keep BitLocker active during a Windows 10 to Windows 10 upgrade, you can append that argument to the end of the command:

   ```
   powershell.exe -executionpolicy remotesigned -noninteractive -command ".\Invoke-Win10Upgrade.ps1" /Bitlocker ForceKeepActive
   ```

   NOTE The full list of commands available to Windows Setup can be found at: Microsoft Documentation: Windows Setup Command-Line Options.

Step 3: Deploy the Phase 1 software package

You cannot complete the following steps until the Windows 10 media you uploaded in Modify the Phase 1 software package on page 113 has finished caching on the Tanium Server.

1. From the Deploy menu, go to **Software**.
2. Select **InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase1 - Pre-Cache** and click **Deploy Package**.
3. Select the desired options according to your environment, click **Show Preview to Continue**, and then click **Deploy Software**.

   NOTE For this deployment, notifications are not necessary because actions are not visible to end users.

   BEST PRACTICE Deploy this package on an ongoing basis. Deploy automatically runs this deployment on endpoints when they enter an eligible state.

Step 4: Review and remediate compatibility results

After deploying the Phase 1 software package, you must check for and remediate any compatibility problems on endpoints. If all targeted endpoints show an applicability status of `Installed` for Phase 1, then you can skip to Deploy the Phase 3 software package on page 118.

Use the following sensors to help you determine endpoint readiness for the Windows 10 upgrade:

Deploy - Windows Upgrade Ready (Optional)

This sensor returns a True/False result as to whether systems are ready and meet the Windows 10 requirements for installation. A False result means that the scan failed for a variety of reasons or that you targeted an ineligible system, such as Windows Server, Mac, or Linux. Use this question for tracking counts of endpoints that are ready for upgrade.

Deploy - Windows Upgrade Scan Details

This sensor provides detailed information from Windows Setup, including specific compatibility blockers. Use this sensor for remediation in the following procedure.

Deploy - Windows Upgrade Scan Results (Optional)

This sensor produces the text of the scan and the result (return code) from Windows Setup. An example of a successful return code from Windows Setup is: `0xc1900210`. Use this sensor for tracking groups of compatibility states. Review Windows Upgrade SCAN Details and remediate errors.

Use the **Deploy - Windows Upgrade Scan Details** sensor to view more detailed information about compatibility failures. For example, some installed software might be incompatible with the upgrade process to this version of Windows. In this scenario, you might need to update or remove software before upgrading Windows.

You can use the **Deploy - Windows Upgrade Scan Results** sensor to review and remediate any conditions that prevent upgrade, such as low disk space or a compatibility block.

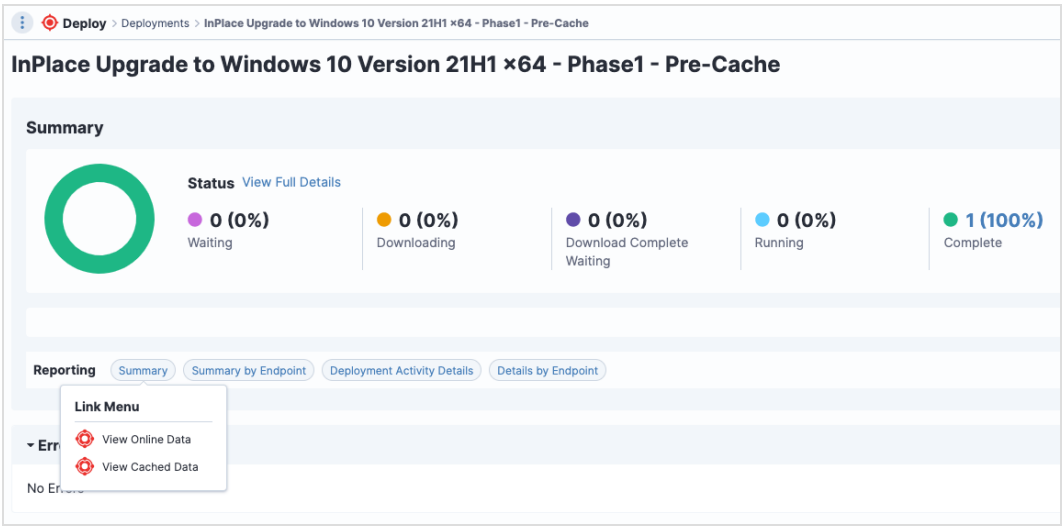
1. Go to the Tanium **Home** page and ask the following question:

```
Get Windows Upgrade Scan Details from all machines
```

2. (Optional) Filter to restrict the question to endpoints that you targeted with the Phase 1 deployment. Feature Update to Windows 10, version 22H2 (KB5015684)

   a. From the Deploy menu, go to **Deployments** and click the **InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase1 - Pre-Cache** deployment.

   b. In the **Summary** section, click **Summary** next to **Reporting** and select **View Online Data**.



   A new Interact page appears with a question filtered to machines that ran this deployment.

   c. Replace the `Get Deploy - Deployments` portion of the question with `Get Deploy - Windows Upgrade Scan Details`.

   d. Select the new question for the filtered view of **Get Deploy - Windows Upgrade Scan Details**.

3. Identify remediation strategies for blocking conditions. For example, if an answer indicates an installed application is not compatible, deploy a Deploy Software Package or Tanium Package to update or remove that application.

4. (Optional) If remediating with a Deploy Software Package or Tanium Package, consider using the **Custom Tagging - Add Tags** Tanium Package to apply a custom tag before deploying the remediation to easily track the remediated endpoints. For more information, see Tanium Community: How to Group Computers Based on Your Organization's Needs Using Custom Tags.

Step 5: Deploy Tanium package: Registry - Set Value

If you have remediated any blocking issues and are ready to re-scan those endpoints for compatibility, you must set a registry value to enable Phase 2 to run.

1. Ask a Tanium question that identifies the remediated endpoints. For example, if you used a custom tag called **Win10remediated** to identify endpoints in the previous step, ask the following question:

   ```
   Get Online from machines with custom tags equals Win10Remediated
   ```

2. Select the answer indicating the remediated endpoints and click **Deploy Action**.
3. Select the Tanium Package: **Registry - Set Value**.
4. Select the **OS Architecture** according to the targeted endpoints.
5. For **Registry Key Name**, enter `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Tanium\Tanium Client\OSD`.
6. For **Value Name**, enter `Status`.
7. For **Value Data**, enter `WIM File Copied`.
8. For **Value**, select **REG_SZ**.

After you are ready to rescan any endpoints, proceed to Deploy the Phase 2 software package on page 117 to force a compatibility re-scan.

Step 6: Deploy the Phase 2 software package

The Phase 2 deployment uses the Windows Setup files to run the same compatibility scan that runs during the Phase 1 deployment. If there were no compatibility errors during the Phase 1 deployment, then the Phase 2 deployment is not required. If errors were remediated and the registry value was set, the Phase 2 software package appears in the `Update Eligible` applicability status on those endpoints and should be deployed.

1. From the Deploy menu, go to **Software**.
2. Select **InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase2 - Re-Scan** and click **Deploy Package**.
3. In the **Targeting** section, select the same targets or a subset of the targets that you configured for the Phase 1 deployment.
4. Select the desired options according to your environment, click **Show Preview to Continue**, and then click **Deploy Software**.

   NOTE For this deployment, notifications are not necessary because you are running a scan that is not visible to end users.

   BEST PRACTICE Deploy this package on an ongoing basis. Deploy automatically runs this deployment on endpoints when they enter an eligible state.

After you deploy the Phase 2 software package, review compatibility results again for any targeted endpoints that are not in `Installed` status for the Phase 2 software package. Some endpoints might take several iterations of remediation before the compatibility scan passes.

Step 7: Deploy the Phase 3 software package

The Phase 3 deployment depends on the successful completion of the Phase 1 and Phase 2 deployments. This deployment executes the Windows Upgrade.

1. From the Deploy menu, go to **Software**.
2. Select **InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase3 - Upgrade**, click **Deploy Package**.
3. In the **Targeting** section, select the same target as the Phase 1 deployment or the desired targets that you want to start the upgrade. Endpoints that are not in `Installed` status for both the Phase 1 and Phase 2 deployments cannot execute this software package operation, so there is no need to restrict targeting based on the previous phase results.
4. Select the desired deployment options based on your environment, click **Show Preview to Continue**, and then click **Deploy Software**.

   Pre-notify the user, post-notify the user, and force a restart as part of the deployment. The upgrade does not complete until the computer is restarted and fails if the user shuts down the computer while it is running. As a result, it is necessary to inform the user that a Windows upgrade is beginning and subsequently that their computer must be restarted.

If the Phase 3 deployment does not complete successfully, action lock might be turned on for some endpoints. For more information about how to find endpoints with action lock enabled and how to disable action lock, see Tanium Console User Guide: Test action lock and Tanium Console User Guide: Turn off action lock.

Deploy Cleanup

After you complete the Phase 3 deployment or run the Phase 1 deployment again, if necessary, use the **Windows Upgrade Cleanup** software package to remove artifacts and enable future usage of Windows upgrade software packages.

1. From the Deploy menu, go to **Software**.
2. Select **Windows Upgrade Cleanup** and click **Deploy Package**.
3. In the **Targeting** section, select **Set Targeting Criteria** for endpoints to remove Windows 10 upgrade artifacts. For example, you can enter the following targeting filter to clean up endpoints that completed the 21H1 x64 upgrade:

   ```
   Deploy - Installed Software Packages matches .*InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase3 - Upgrade.*Installed and Windows OS Release ID matches 21H1
   ```


   If necessary, replace the software package name and release ID to match the package you deployed.

4. Select the desired options according to your environment, click **Show Preview to Continue**, and then click **Deploy Software**.

To check for Phase 3 success, ask the question `Get Operating System?maxAge=60 from all computers`. If an endpoint does not answer with the operating system you deployed, the upgrade was not successful. See Troubleshooting. The `maxAge` parameter ensures that the answer is updated immediately.

For more information about deployment settings, see Deploying software on page 71.

Troubleshooting in-place upgrades

You can access detailed logs for each phase of the Windows Upgrade.

To troubleshoot Windows Setup errors in each phase, review the appropriate log file from an affected endpoint:

- Phase 1 media caching: `%temp%\Win10IPU_PreCache.txt`
- Phases 1 and 2 compatibility scan: `%temp%\Win10IPU_CompatScan.txt`
- Phase 3 Windows setup: `%temp%\Win10IPU_Upgrade.txt`

For problems with Windows Setup, see the appropriate Microsoft log files as described in Microsoft Support: Log files that are created when you upgrade to a new version of Windows.

For general Deploy troubleshooting, see Troubleshooting Deploy on page 102.

Use case: Upgrading macOS

You can use Tanium Deploy to prepare and deploy macOS upgrades to your macOS endpoints. To complete a macOS upgrade, you must understand how to target and deploy software packages in Deploy.

Overview

Deploy supports the upgrade of macOS 10.13.6 through macOS 11 to macOS 11, 12, or 13. You can use Deploy to handle the macOS upgrade process in two phases:

Phase 1: Pre-Cache

This method uses the Tanium platform to download the macOS installer, efficiently sharing parts of the update across endpoints on the same network.

Phase 2: Upgrade

The Phase 2 upgrade runs the macOS installer cached in Phase 1, terminates all applications, and reboots the endpoint.

Import software packages

To begin, you must import at least two software packages from the Predefined Package Gallery. The following examples use macOS Monterey. Substitute with the version you are deploying as needed.

1. From the Deploy menu, go to **Software**, and then click **Predefined Package Gallery**.
2. Select at least one of the following packages:
    - **macOS Monterey - Phase 1 - Pre-Cache**
    - **macOS Monterey - Phase 2 – Upgrade**
3. Click **Import**, confirm the action, and then click **Go To Software Packages**.

Deploy software packages

After the software packages are ready, perform the following steps to complete the upgrade process:

1. Deploy the Phase 1 software package on page 121
2. Deploy the Phase 2 software package with a pre-notification on page 121

Deploy the Phase 1 software package

1. From the Deploy menu, go to **Software**. You can use the filter or search options to narrow the list to macOS upgrades.
2. Select **macOS Monterey - Phase 1 - Pre-Cache** and then click **Deploy Package**.
3. Select the desired options according to your environment, click **Show Preview to Continue**, and then click **Deploy Software**.

   BEST PRACTICE

   - Notifications are not necessary because the Phase 1 actions are not visible to end users.
   - Deploy this package on an ongoing basis so that Tanium Deploy automatically runs this deployment on endpoints when they enter an eligible state.

Deploy the Phase 2 software package with a pre-notification

The Phase 2 software package silently runs the installer command, then it terminates all applications and reboots the computer to perform the upgrade. The process takes up to 30 minutes and does not provide any warning to the end user prior to the reboot.

1. From the Deploy menu, go to **Software**. You can use the filter or search options to narrow the list to macOS upgrades.
2. Select **macOS Monterey - Phase 2 – Upgrade** and click **Deploy Package**.
3. In the **Targeting** section, select the same targets or a subset of the targets that you configured for the Phase 1 deployment.
4. Configure a pre-notification to indicate that the computer will reboot within 30 minutes without further warning.

   BEST PRACTICE Use a clear pre-notification message so that end users can prepare for the reboot. For example:

   ```
   This computer will reboot within 30 minutes to complete a macOS upgrade. You will not be notified again before the reboot. Make sure to save any unsaved work.
   ```

5. Select the desired options according to your environment. Do not include a restart or post-notification.
6. Click **Show Preview to Continue**, and then click **Deploy Software**.

Troubleshooting

Errors encountered while running the macOS installer during Phase 2 are written to the Deploy `subprocess.log` file. The Apple logs for the upgrade are stored in `/var/logs/install`.

For general Deploy troubleshooting, see Troubleshooting Deploy on page 102.

Reference: Predefined Package Gallery

A-B on page 122 | C-E on page 124 | F-L on page 125 | M on page 127 | N-S on page 133 | T on page 135 | U-Z on page 136

A-B

Platform	Vendor	Title
Windows	Adobe	Acrobat (64-bit)
macOS	Adobe	Acrobat DC
Windows	Adobe	Acrobat DC (en-us)
macOS Windows	Adobe	Acrobat Reader DC (en-us)
Windows	Adobe	Acrobat Reader DC (en-us) (64-bit)
Windows	Adobe	Acrobat Reader DC (MUI)
Windows	Adobe	Acrobat Reader DC (MUI) (64-bit)
Windows	Adobe	After Effects CC -- AUDIT ONLY[2]
macOS	Adobe	AIR - Remove Only
Windows	Adobe	Animate CC -- AUDIT ONLY[2]
Windows	Adobe	Audition CC -- AUDIT ONLY[2]
Windows	Adobe	Digital Editions
Windows	Adobe	Dreamweaver CC -- AUDIT ONLY[2]
macOS Windows	Adobe	Flash Player - Remove Only
Windows	Adobe	Illustrator CC -- AUDIT ONLY[2]
Windows	Adobe	InDesign CC -- AUDIT ONLY[2]
Windows	Adobe	Photoshop CC -- AUDIT ONLY[2]
Windows	Adobe	Prelude CC -- AUDIT ONLY[2]
Windows	Adobe	Premiere Pro CC -- AUDIT ONLY[2]

Platform	Vendor	Title
Windows	Adobe	Shockwave EOL
macOS	AgileBits	1Password7
macOS	aONe	Keka
Windows	Apache	Tomcat 10.0
Windows	Apache	Tomcat 9.0
Windows	Apache	Tomcat 8.5
Windows	Apple	iTunes 32-bit
Windows	Apple	iTunes 64-bit
macOS	Apple	macOS Big Sur - Phase1- Pre-Cache
macOS	Apple	macOS Big Sur - Phase2- Upgrade
macOS	Apple	macOS Monterey - Phase1- Pre-Cache
macOS	Apple	macOS Monterey - Phase2- Upgrade
macOS	Apple	macOS Ventura - Phase1 - Pre-Cache
macOS	Apple	macOS Ventura - Phase2- Upgrade
Windows	Arco Software	CutePDF Writer
macOS Windows	Arduino	IDE
macOS Windows	Atlassian	Sourcetree
macOS	Audacity	Audacity
Windows	Audacity	Audacity 32-bit
Windows	Audacity	Audacity 64-bit
macOS	Audacity	Audacity (ARM)
macOS	Bare Bones	BBEdit
Windows	BlueJeans Network, Inc	BlueJeans (Active User)
Windows	BlueJeans Network, Inc	BlueJeans (All Users)

Platform	Vendor	Title
Windows	Box, Inc.	Box Drive (x64 en-us)
Windows	Box, Inc.	Box Drive (x86 en-us)
macOS	Brave Software, Inc	Brave Browser
Windows	Brave Software, Inc	Brave Browser (Active User) (x64)
Windows	Brave Software, Inc	Brave Browser (Active User) (x86)

[2] Audit-only software package templates are used for reporting purposes. No source files or commands are distributed for these packages, but there is logic to determine if the software is installed or out of date.

C-E

Platform	Vendor	Title
Windows	Cisco	Jabber
Windows	Cisco	Network Recording Player
macOS	Cisco	Webex
macOS	Cisco	Webex (ARM)
Windows	Cisco	Webex Recorder and Player
Windows	Corel Corporation	WinZip
macOS	DB Browser for SQLite Team	DB Browser for SQLite
Windows	DB Browser for SQLite Team	DB Browser for SQLite x64
Windows	DB Browser for SQLite Team	DB Browser for SQLite x86
macOS Windows	Devolutions Inc.	Remote Desktop Manager
macOS Windows	Devolutions Inc.	Remote Desktop Manager Free
macOS	Discord, Inc	Discord
macOS	Docker Inc.	Docker Desktop
macOS Windows	Dropbox	Desktop Client

Platform	Vendor	Title
Windows	Eclipse Adoptium	Temurin 11 JDK with Hotspot 32-bit
Windows	Eclipse Adoptium	Temurin 11 JDK with Hotspot 64-bit
Windows	Eclipse Adoptium	Temurin 11 JRE with Hotspot 32-bit
Windows	Eclipse Adoptium	Temurin 11 JRE with Hotspot 64-bit
Windows	Eclipse Adoptium	Temurin 16 JDK with Hotspot 32-bit
Windows	Eclipse Adoptium	Temurin 16 JDK with Hotspot 64-bit
Windows	Eclipse Adoptium	Temurin 17 JDK with Hotspot 32-bit
Windows	Eclipse Adoptium	Temurin 17 JDK with Hotspot 64-bit
Windows	Eclipse Adoptium	Temurin 17 JRE with Hotspot 32-bit
Windows	Eclipse Adoptium	Temurin 17 JRE with Hotspot 64-bit
Windows	Eclipse Adoptium	Temurin 8 JDK with Hotspot 32-bit
Windows	Eclipse Adoptium	Temurin 8 JDK with Hotspot 64-bit
Windows	Eclipse Adoptium	Temurin 8 JRE with Hotspot 32-bit
Windows	Eclipse Adoptium	Temurin 8 JRE with Hotspot 64-bit
macOS	Evernote Corporation	Evernote
Windows	Evernote Corporation	Evernote (Active User)
Windows	Evernote Corporation	Evernote (All Users)
Windows	Extensis	Universal Type Client

F-L

Platform	Vendor	Title
macOS Windows	Foxit Software Inc	PDF Reader
macOS	George Nachman	iTerm2
macOS Windows	gimp.org	GIMP

Platform	Vendor	Title
Windows	Git	Git (x64) Git (x86)
macOS	GitHub	Desktop
Windows	GN Audio	Jabra Direct
Windows	Google	Android Studio 64-bit
macOS	Google	Chrome
Windows	Google	Chrome x64
Windows	Google	Chrome x86
macOS	Google	Drive
Windows	Google	Drive File Stream
macOS Windows	HandBrake	HandBrake
Windows	HCSS	HCSS Client
Windows	Helios	TextPad x64
Windows	Helios	TextPad x86
Windows	Igor Pavlov	7-Zip (x64)
Windows	Igor Pavlov	7-Zip (x86)
Windows	iterate GmbH	Cyberduck
Windows	Jam Software	TreeSize Free
macOS Windows	JetBrains	DataGrip
macOS Windows	JetBrains	GoLand
macOS	JetBrains	GoLand (ARM)
macOS Windows	JetBrains	IntelliJ IDEA Community Edition

Platform	Vendor	Title
macOS	JetBrains	IntelliJ IDEA Community Edition (ARM)
macOS Windows	JetBrains	IntelliJ IDEA Ultimate Edition
macOS	JetBrains	IntelliJ IDEA Ultimate Edition (ARM)
macOS	JetBrains	PyCharm
macOS	JetBrains	PyCharm (ARM)
macOS Windows	JetBrains	PyCharm Community Edition
macOS	JetBrains	PyCharm Community Edition (ARM)
Windows	JetBrains	PyCharm Professional Edition
macOS Windows	JetBrains	WebStorm
macOS	JetBrains	WebStorm (ARM)
Windows	KeePass	KeePass 1
Windows	KeePass	KeePass 2
macOS Windows	KeePassXC Team	KeePassXC
macOS	KeePassXC Team	KeePassXC (ARM)
macOS	Kong	Insomnia
macOS	Licecap	Licecap

M

Platform	Vendor	Title
macOS	MacPaw	The Unarchiver
Windows	Martin Prikryl	WinSCP
Windows	Microsoft	.NET Desktop Runtime 6.0 (x64)

Platform	Vendor	Title
Windows	Microsoft	.NET Desktop Runtime 6.0 (x86)
Windows	Microsoft	.NET Desktop Runtime 7.0 (x64)
Windows	Microsoft	.NET Desktop Runtime 7.0 (x86)
Windows	Microsoft	.NET Framework
Windows	Microsoft	.NET Runtime 6.0 (x64)
Windows	Microsoft	.NET Runtime 6.0 (x86)
Windows	Microsoft	.NET Runtime 7.0 (x64)
Windows	Microsoft	.NET Runtime 7.0 (x86)
Windows	Microsoft	ASP.NET Core Runtime 7.0 (x64)
Windows	Microsoft	ASP.NET Core Runtime 7.0 (x86)
macOS	Microsoft	Edge
Windows	Microsoft	Edge x64
Windows	Microsoft	Edge x86
Windows	Microsoft	Feature Update to Windows 10, version 21H2 (KB5003791) - x64
Windows	Microsoft	Feature Update to Windows 10, version 21H2 (KB5003791) - x86
Windows	Microsoft	Feature Update to Windows 10, version 22H2 (KB5015684) - x64
Windows	Microsoft	Feature Update to Windows 10, version 22H2 (KB5015684) - x86
Windows	Microsoft	IIS URL Rewrite Module 2 x64
Windows	Microsoft	IIS URL Rewrite Module 2 x86
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 1809 x64 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 1809 x64 - Phase2 - Re-Scan
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 1809 x64 - Phase3 - Upgrade
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 1809 x86 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 1809 x86 - Phase2 - Re-Scan
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 1809 x86 - Phase3 - Upgrade

Platform	Vendor	Title
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 - Phase1 - Direct-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 x64 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 x64 - Phase2 - Re-Scan
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 x64 - Phase3 - Upgrade
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 x86 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 x86 - Phase2 - Re-Scan
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 x86 - Phase3 - Upgrade
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H1 - Phase1 - Direct-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 x64 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 x64 - Phase2 - Re-Scan
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 x64 - Phase3 - Upgrade
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 x86 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 x86 - Phase2 - Re-Scan
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 20H2 x86 - Phase3 - Upgrade
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H1 - Phase1 - Direct-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase2 - Re-Scan
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H1 x64 - Phase3 - Upgrade
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H1 x86 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H1 x86 - Phase2 - Re-Scan
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H1 x86 - Phase3 - Upgrade
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H2 - Phase1 - Direct-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H2 x64 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H2 x64 - Phase2 - Re-Scan
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H2 x64 - Phase3 - Upgrade

Platform	Vendor	Title
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H2 x86 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H2 x86 - Phase2 - Re-Scan
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 21H2 x86 - Phase3 - Upgrade
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 22H2 - Phase1 - Direct-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 22H2 x64 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 22H2 x64 - Phase2 - Re-Scan
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 22H2 x64 - Phase3 - Upgrade
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 22H2 x86 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 22H2 x86 - Phase2 - Re-Scan
Windows	Microsoft	InPlace Upgrade to Windows 10 Version 22H2 x86 - Phase3 - Upgrade
Windows	Microsoft	InPlace Upgrade to Windows 11 Build 22000 - Phase1 - Direct-Cache
Windows	Microsoft	InPlace Upgrade to Windows 11 Build 22000 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 11 Build 22000 - Phase2 - Re-scan
Windows	Microsoft	InPlace Upgrade to Windows 11 Build 22000 - Phase3 - Upgrade
Windows	Microsoft	InPlace Upgrade to Windows 11 Build 22621 - Phase1 - Direct-Cache
Windows	Microsoft	InPlace Upgrade to Windows 11 Build 22621 - Phase1 - Pre-Cache
Windows	Microsoft	InPlace Upgrade to Windows 11 Build 22621 - Phase2 - Re-scan
Windows	Microsoft	InPlace Upgrade to Windows 11 Build 22621 - Phase3 - Upgrade
Windows	Microsoft	Latest Cumulative Update for Windows 11 Version 22H2 for x64-based Systems
Windows	Microsoft	Local Administrator Password Solution x64
Windows	Microsoft	Local Administrator Password Solution x86
macOS	Microsoft	Office 2019
macOS	Microsoft	Office 2019 with Teams
Windows	Microsoft	Office Click-to-Run Current Channel (x64)
Windows	Microsoft	Office Click-to-Run Current Channel (x86)

Platform	Vendor	Title
Windows	Microsoft	Office Click-to-Run Monthly Enterprise Channel (x64)
Windows	Microsoft	Office Click-to-Run Monthly Enterprise Channel (x86)
Windows	Microsoft	Office Click-to-Run Office 2019 Perpetual Enterprise (x64)
Windows	Microsoft	Office Click-to-Run Office 2019 Perpetual Enterprise (x86)
Windows	Microsoft	Office Click-to-Run Office 2021 Perpetual Enterprise (x64)
Windows	Microsoft	Office Click-to-Run Office 2021 Perpetual Enterprise (x86)
Windows	Microsoft	Office Click-to-Run Semi-Annual Enterprise Channel (Preview) (x64)
Windows	Microsoft	Office Click-to-Run Semi-Annual Enterprise Channel (Preview) (x86)
Windows	Microsoft	Office Click-to-Run Semi-Annual Enterprise Channel (x64)
Windows	Microsoft	Office Click-to-Run Semi-Annual Enterprise Channel (x86)
Windows	Microsoft	Paint 3D - Remove Only
Windows	Microsoft	Power BI Desktop
Windows	Microsoft	Power BI Desktop (x64)
Windows	Microsoft	Powershell (x64)
Windows	Microsoft	Powershell (x86)
Windows	Microsoft	PowerShell 5.1 x64 for Windows 7 and Windows Server 2008 R2
Windows	Microsoft	PowerShell 5.1 x64 for Windows 8.1 and Windows Server 2012 R2
Windows	Microsoft	PowerShell 5.1 x64 for Windows Server 2012
macOS	Microsoft	Remote Desktop
Windows	Microsoft	Skype Desktop Client (x86 en-us)
Windows	Microsoft	SQL Server Management Studio
macOS	Microsoft	Teams
Windows	Microsoft	Teams (x64)
Windows	Microsoft	Teams (x86)
Windows	Microsoft	Teams Machine-Wide Installer (x64)

Platform	Vendor	Title
Windows	Microsoft	Teams Machine-Wide Installer (x86)
Windows	Microsoft	3D Viewer - Remove Only
Windows	Microsoft	Update for Removal of Adobe Flash Player (KB4577586)
Windows	Microsoft	Visual C++ Redistributable (x64)
Windows	Microsoft	Visual C++ Redistributable (x86)
macOS	Microsoft	Visual Studio Code
Windows	Microsoft	Visual Studio Code (x64 en-us)
Windows	Microsoft	Visual Studio Code (x86 en-us)
Windows	Microsoft	Windows Upgrade Cleanup
macOS	Mozilla	Firefox
Windows	Mozilla	Firefox (x64 da)
Windows	Mozilla	Firefox (x64 de)
Windows	Mozilla	Firefox (x64 en-GB)
Windows	Mozilla	Firefox (x64 en-US)
Windows	Mozilla	Firefox (x64 es-AR)
Windows	Mozilla	Firefox (x64 es-CL)
Windows	Mozilla	Firefox (x64 es-ES)
Windows	Mozilla	Firefox (x64 es-MX)
Windows	Mozilla	Firefox (x64 fr)
Windows	Mozilla	Firefox (x64 it)
Windows	Mozilla	Firefox (x64 nl)
Windows	Mozilla	Firefox (x64 pt-BR)
Windows	Mozilla	Firefox (x64 sv-SE)
Windows	Mozilla	Firefox (x64 tr)
Windows	Mozilla	Firefox (x86 da)

Platform	Vendor	Title
Windows	Mozilla	Firefox (x86 de)
Windows	Mozilla	Firefox (x86 en-GB)
Windows	Mozilla	Firefox (x86 en-US)
Windows	Mozilla	Firefox (x86 es-AR)
Windows	Mozilla	Firefox (x86 es-CL)
Windows	Mozilla	Firefox (x86 es-ES)
Windows	Mozilla	Firefox (x86 es-MX)
Windows	Mozilla	Firefox (x86 fr)
Windows	Mozilla	Firefox (x86 it)
Windows	Mozilla	Firefox (x86 nl)
Windows	Mozilla	Firefox (x86 pt-BR)
Windows	Mozilla	Firefox (x86 sv-SE)
Windows	Mozilla	Firefox (x86 tr)
Windows	Mozilla	Firefox ESR (x64 en-US)
Windows	Mozilla	Firefox ESR (x86 en-US)
macOS	Mozilla	Thunderbird
Windows	Mozilla	Thunderbird (x64)

N-S

Platform	Vendor	Title
macOS	Nmap	Nmap
Windows	Node.js Foundation	Node.js Current x64
Windows	Node.js Foundation	Node.js Current x86
Windows	Node.js Foundation	Node.js LTS x64
Windows	Node.js Foundation	Node.js LTS x86
Windows	Notepad++ Team	Notepad++ 32-bit

Platform	Vendor	Title
Windows	Notepad++ Team	Notepad++ 64-bit
Windows	Oracle	Java SE Runtime Environment 8
Windows	Oracle	Java SE Runtime Environment 8 (x64)
Windows	Oracle	MySQL Community
macOS	Oracle	VirtualBox
Windows	pgAdmin	pgAdmin 4
Windows	Piriform Software	CCleaner Standard
macOS Windows	Postman	Postman
macOS	Postman	Postman (ARM)
Windows	Rocket.Chat	Rocket.Chat (Active User) x64
Windows	Rocket.Chat	Rocket.Chat (Active User) x86
Windows	Rocket.Chat	Rocket.Chat (All Users) x64
Windows	Rocket.Chat	Rocket.Chat (All Users) x86
macOS	Royal Apps	Royal TS
Windows	Royal Apps GmbH	Royal TS
macOS	Running with Crayons Ltd	Alfred 5
macOS	Scooter Software	Beyond Compare
Windows	Scooter Software	Beyond Compare 4
Windows	Simon Tatham	PuTTY (x64 en-US)
Windows	Simon Tatham	PuTTY (x86 en-US)
macOS	Slack	Slack
Windows	Slack	Slack x64
Windows	Slack	Slack x86
Linux	Splunk	Universal Forwarder (x64 DPKG)
Linux	Splunk	Universal Forwarder (x64 RPM)

Platform	Vendor	Title
Windows	Splunk	Universal Forwarder x64
Windows	Splunk	Universal Forwarder x86
Windows	Stairwell	Inception Forwarder
Windows	Stamps.com, Inc	Stamps.com (x64)
Windows	Stamps.com, Inc	Stamps.com (x86)

T

Platform	Vendor	Title
macOS Windows	Tableau	Desktop
Windows	Tableau	Reader
Windows	Tableau	Reader x64
macOS Windows	TechSmith	Camtasia
macOS Windows	TechSmith	Snagit
Windows	The Wireshark developer community	Wireshark 32-bit
Windows	The Wireshark developer community	Wireshark 64-bit
Windows	Thingamahoochie Software	WinMerge 32-bit
Windows	Thingamahoochie Software	WinMerge 64-bit
macOS	3T Software Labs Ltd	Studio 3T (Arm)
macOS	3T Software Labs Ltd	Studio 3T (Intel)
Windows	TortoiseSVN	TortoiseSVN (32-bit)
Windows	TortoiseSVN	TortoiseSVN (64-bit)

U-Z

Platform	Vendor	Title
macOS	VideoLAN	VLC media player
Windows	VideoLAN	VLC media player (32-bit)
Windows	VideoLAN	VLC media player (64-bit)
Windows	VMware	Player
Windows	VMware	VMware Tools (32-bit)
Windows	VMware	VMware Tools (64-bit)
Windows	VMware, Inc	Horizon Client
Windows	win.rar GmbH	WinRAR 32-bit
Windows	win.rar GmbH	WinRAR 64-bit
macOS	Yubico	Authenticator
Windows	Yubico	Authenticator 32-bit
Windows	Yubico	Authenticator 64-bit
Windows	Zoom	Outlook Plugin
macOS Windows	Zoom	Zoom
Windows	Zoom	Zoom (64-bit)
macOS	Zoom	Zoom (ARM)
Linux	Zoom	Zoom (DPKG)
macOS	Zoom	Zoom Gov
macOS	Zoom	Zoom Gov (ARM)
macOS	Zoom	Zoom Rooms
Windows	Zoom	Zoom Rooms (32-bit)
Windows	Zoom	Zoom Rooms (64-bit)

Reference: API Gateway examples for Deploy

For additional API Gateway example syntax, see Tanium API Gateway User Guide: Reference: Filter syntax and Tanium API Gateway User Guide: Reference: API Gateway examples.

Deploy examples

The following queries and mutation require Deploy, retrieve information about software packages deployed in your environment, and allow you to deploy a software package to endpoints.

Deploy a package to all endpoints (`mutation.manageSoftware`)

DEPLOY PACKAGE TO ENDPOINTS

The following mutation deploys a package to `All Computers`.

```
mutation deployPackage ($group:String){
  manageSoftware(
    operation: INSTALL
    softwarePackageID: 2
    start: "2021-10-27T00:00:00Z"
    end: "2021-11-03T00:00:00Z"
    target: {targetGroup: $group}
  ) {
    ID
    name
  }
}
```

Include the computer group variable in the **QUERY VARIABLES** panel or in your variables dictionary:

```
{
  "group": "All Computers"
}
```

Example response:

```
{
  "data": {
    "manageSoftware": {
      "ID": "2",
      "name": "Install Tanium Standard Utilities (Linux)"
    }
  }
}
```

Get package details (`query.packages`)

GET DETAILS OF ALL PACKAGES

The following query retrieves multiple fields for all packages.

```
query PackagesQuery {
  packages {
    items {
      id
      name
      displayName
      command
      commandTimeout
      expireSeconds
      contentSet {
        id
        name
      }
      processGroupFlag
      skipLockFlag
      metadata {
        adminFlag
        name
        value
      }
```

```
      sourceHash
      sourceHashChangedFlag
      sourceID
      sourceName
      parameters {
        key
        value
      }
      rawParameterDefinition
      parameterDefinition {
        parameterType
        model
        parameters {
          model
          parameterType
          key
          label
          helpString
          defaultValue
          validationExpressions {
            model
            parameterType
            expression
            helpString
          }
          promptText
          heightInLines
          maxChars
          values
          restrict
          allowEmptyList
          minimum
          maximum
          stepSize
```

```
      snapInterval
      dropdownOptions {
        model
        parameterType
        name
        value
      }
      componentType
      startDateRestriction {
        model
        parameterType
        type
        interval
        intervalCount
        unixTimeStamp
      }
      endDateRestriction {
        model
        parameterType
        type
        interval
        intervalCount
        unixTimeStamp
      }
      startTimeRestriction {
        model
        parameterType
        type
        interval
        intervalCount
        unixTimeStamp
      }
      endTimeRestriction {
        model
```

```
            parameterType
            type
            interval
            intervalCount
            unixTimeStamp
          }
          allowDisableEnd
          defaultRangeStart {
            model
            parameterType
            type
            interval
            intervalCount
            unixTimeStamp
          }
          defaultRangeEnd {
            model
            parameterType
            type
            interval
            intervalCount
            unixTimeStamp
          }
          separatorText
        }
      }
      verifyExpireSeconds
    }
  }
}
```

Example response:

```
{
```

```
  "data": {
    "packages": {
      "items": [
        {
          "id": "1",
          "name": "Distribute Tanium Standard Utilities",
          "displayName": "Distribute Tanium Standard Utilities",
          "command": "cmd.exe /c cscript.exe //E:VBScript install-standard-utils.vbs \"Tools\\StdUtils\"",
          "commandTimeout": 2700,
          "expireSeconds": 3300,
          "contentSet": {
            "id": "5",
            "name": "Client Management"
          },
          "processGroupFlag": true,
          "skipLockFlag": false,
          "metadata": [],
          "sourceHash": "60b3e906f92929da67341792db9675d5cd91686546f01b57857686c8c6d84fa8",
          "sourceHashChangedFlag": false,
          "sourceID": 0,
          "sourceName": "",
          "parameters": [],
          "rawParameterDefinition": null,
          "parameterDefinition": null,
          "verifyExpireSeconds": 600
        },
        {
          "id": "2",
          "name": "Distribute Tanium Standard Utilities (Linux)",
          "displayName": "Distribute Tanium Standard Utilities (Linux)",
          "command": "/bin/bash distribute-tools.sh STRICT",
          "commandTimeout": 120,
          "expireSeconds": 720,
```

```
          "contentSet": {
            "id": "5",
            "name": "Client Management"
          },
          "processGroupFlag": true,
          "skipLockFlag": false,
          "metadata": [],
          "sourceHash":
"4ed7a30a1ca6c81be5a71b892dfadcdb489122cc641fa4b644f53255134215c9",
          "sourceHashChangedFlag": false,
          "sourceID": 0,
          "sourceName": "",
          "parameters": [],
          "rawParameterDefinition": null,
          "parameterDefinition": null,
          "verifyExpireSeconds": 600
        }
      ]
    }
  }
}
```

Get Deploy packages (`query.softwarePackages`)

GET ALL DEPLOY PACKAGES

The following query retrieves all Deploy packages.

```
query getDeployPackages{
  softwarePackages {
    edges {
      node {
        id
        productName
        productVendor
```

```
        productVersion
      }
    }
  }
}
```

Example response:

```
{
  "data": {
    "softwarePackages": {
      "edges": [
        {
          "node": {
            "id": "19",
            "productName": "Firefox (x64 en-US)",
            "productVendor": "Mozilla",
            "productVersion": "98.0"
          }
        },
        {
          "node": {
            "id": "30",
            "productName": "Power BI Desktop (x64)",
            "productVendor": "Microsoft",
            "productVersion": "2.102.845.0"
          }
        },
        {
          "node": {
            "id": "43",
            "productName": "VLC media player (64-bit)",
            "productVendor": "VideoLAN",
            "productVersion": "3.0.16.0"
```

```
            }
          },
          {
            "node": {
              "id": "46",
              "productName": "Visual Studio Code (x64 en-us)",
              "productVendor": "Microsoft",
              "productVersion": "1.65.2"
            }
          }
        ]
      }
    }
}
```

Get software deployment status (`query.softwareDeployment`)

GET STATUS OF SOFTWARE DEPLOYMENT

The following query retrieves the deployment status of all Deploy packages.

```
query getSoftwareDeploymentStatus {
  softwareDeployment {
    ID
    name
    status {
      completeCount
      downloadCompleteWaitingCount
      downloadingCount
      failedCount
      notApplicableCount
      runningCount
      waitingCount
    }
    errors {
```

```
      error
      count
    }
  }
}
```

Example response:

```
{
  "data": {
    "softwareDeployment": [
      {
        "ID": "5",
        "name": "Install Tanium Standard Utilities",
        "status": {
          "completeCount": 1,
          "downloadCompleteWaitingCount": 0,
          "downloadingCount": 0,
          "failedCount": 0,
          "notApplicableCount": 0,
          "runningCount": 0,
          "waitingCount": 0
        },
        "errors": null
      },
      {
        "ID": "6",
        "name": "Install Tanium Standard Utilities (Linux)",
        "status": {
          "completeCount": 0,
          "downloadCompleteWaitingCount": 0,
          "downloadingCount": 1,
          "failedCount": 0,
          "notApplicableCount": 0,
```

```
            "runningCount": 0,
            "waitingCount": 0
          },
          "errors": null
        }
      ]
    }
}
```