Tanium™ Deploy User Guide

Version 2.5.17

December 15, 2020

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

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

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

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

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

Tanium is committed to the highest accessibility standards to make interaction with Tanium software more intuitive and to accelerate the time to success. To ensure high accessibility standards, Tanium complies with the U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. We have conducted third-party accessibility assessments over the course of product development for many years, and most recently a comprehensive audit against the WCAG 2.1 / VPAT 2.3 standards for all major product modules was completed in September 2019. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

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

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your 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 57.

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 64.

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.

Predefined packages for Windows

The provided applications for Windows include:

- 7-Zip (32/64-bit) - latest version
- Adobe Acrobat DC (Update only) - latest version
- Adobe Acrobat Reader DC - latest version

- Adobe AIR - latest version
- Adobe Digital Editions - latest version
- Adobe Flash Player (ActiveX/NPAPI/PPAPI) - latest version
- Adobe Shockwave EOL (Remove only)
- Box Drive (32/64-bit) - latest version
- DB Browser for SQLite (32/64-bit) - latest version
- Dropbox - latest version
- FileZilla (32/64-bit) - latest version
- Google Android Studio - latest version
- Google Chrome Enterprise (32/64-bit) - latest version
- Google Drive File Stream - latest version
- Microsoft Power BI Desktop (32/64-bit) - latest version
- Microsoft Silverlight (32/64-bit) - latest version
- Microsoft Skype Desktop Client (32-bit) - latest version
- Microsoft Visual Studio Code (32/64-bit) - latest version
- Microsoft Windows 10 Upgrade (32/64-bit) - 1803, 1809, 1903, 1909, 2004
- Mozilla Firefox (32/64-bit) - latest version
- Mozilla Firefox ESR (32/64-bit) - latest version
- NodeJS Current (32/64-bit) - latest version
- NodeJS LTS (32/64-bit) - latest version
- Notepad++ (32/64-bit) - latest version
- Oracle Java 8 Runtime (32/64-bit) - latest version
- Oracle MySQL Community - latest version
- PuTTY (32/64-bit) - latest version
- Royal Apps GmbH Royal TS - latest version
- VideoLAN VLC Media Player (32/64-bit) - latest version
- VMware Workstation Player (Update and Remove only) - latest version
- Wireshark (32/64-bit) - latest version
- Zoom - latest version
- Zoom Outlook Plugin - latest version

The following 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.

- Adobe After Effects CC - latest version
- Adobe Animate CC - latest version
- Adobe Audition CC - latest version
- Adobe Dreamweaver CC - latest version
- Adobe Illustrator CC - latest version
- Adobe InDesign CC - latest version
- Adobe Photoshop CC - latest version
- Adobe Prelude CC - latest version
- Adobe Premiere Pro CC - latest version

Predefined packages for macOS

The provided applications for macOS include:

- Adobe Acrobat Reader DC - latest version
- Google Chrome - latest version
- Microsoft Office 2019 - latest version
- Microsoft Office 2019 with Teams - latest version
- Mozilla Firefox - latest version
- Slack - latest version
- Zoom - latest version

For more information, see Import a software package from the Predefined Package Gallery on page 62.

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. Each software package is evaluated on a routine basis to determine if a Tanium managed device is eligible to install, is eligible for update, installed, or has failed requirements.

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.

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 66.

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 66.

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 76.

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 Using the Self Service Client application on page 79.

Integration with other Tanium products

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

End-User Notifications

Deploy uses Tanium End-User Notifications to notify users about deployments to Windows 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.

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 20.

☐ 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 global settings

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

☐ Increase the hot cache percentage to 80%.

See Configure global settings on page 53.

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 50.

☐ Configure service account on page 55.

> If you installed Deploy using the **Apply 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 Tanium recommended configurations** option, the **IT Operations Metrics** board is automatically imported after the Deploy service account is configured.

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

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

Additional computer groups might be required to fulfill the requirements of your organization. See Organize computer groups on page 55.

☐ Add computer groups to Deploy action group on page 55.

> If you installed Deploy using the **Apply 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 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 56.

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 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 76.

Step 7: Add content

☐ Import software packages from the Predefined Package Gallery or create your own custom packages. See Managing software on page 57.

☐ Assign packages to software bundles. See Create a software bundle on page 64.

☐ Create a self service profile on page 79 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 66.

☐ 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 66.

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 84.

☐ Monitor and troubleshoot endpoints missing software updates released over 30 days on page 85.

☐ Monitor and troubleshoot mean time to deploy software on page 86.

☐ Monitor and troubleshoot software installed by self service user request on page 87.

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 20.
- Define distinct roles and responsibilities. See RACI chart on page 20.
- Validate cross-functional alignment. See Organizational alignment on page 26.
- Track operational maturity. See Operational metrics on page 26.

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 25.	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 25.	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.

Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
Update or remove software due to threat intel /vulnerability See Standard threat intel/vulnerability update/remove workflow on page 26.	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.

Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
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.

Task	IT Security	IT Operations	IT Risk/Compliance	Executive	Rationale
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.
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.

Figure 1: Standard Deploy install/update workflow

Figure 2: 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.

Executive Metrics	Deploy Coverage	Endpoints Missing Software Updates Released Over 30 Days	Mean Time to Deploy Software	Software Installed by Self Service User Request
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 (Needs improvement)	Level 2 (Below average)	Level 3 (Average)	Level 4 (Above average)	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 (Needs improvement)	Level 2 (Below average)	Level 3 (Average)	Level 4 (Above average)	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

		Level 1 (Needs improvement)	Level 2 (Below average)	Level 3 (Average)	Level 4 (Above average)	Level 5 (Optimized)
	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, Connect, and Trends integrated into enterprise vulnerability management, threat management, and asset management tools, such as Flexera and ServiceNow	Deploy, 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 (Needs improvement)	Level 2 (Below average)	Level 3 (Average)	Level 4 (Above average)	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%	76-100%	51-75%	36-50%	20-35%

Requirements

Review the requirements before you install and use Deploy.

Tanium dependencies

In addition to a license for the Deploy product module, make sure that your environment also meets the following requirements.

Component	Requirement
Tanium Core Platform	7.3.314.4250 or later
Tanium Client	7.2.314.3476 or later. • All supported operating systems 7.4 or later. • All supported operating systems • Requires Deploy 1.4.2 or later For more information about supported operating systems, see Supported operating systems on page 36.
Tanium products	If you clicked **Install with Recommended Configurations** when you installed Deploy, the Tanium Server automatically installed all your licensed modules at the same time. Otherwise, you must manually install the modules that Deploy requires to function, as described under Tanium Console User Guide: Manage Tanium modules. Modules at the following minimum versions are required: • Tanium Endpoint Configuration 1.0 or later (installed as part of Tanium Client Management 1.5.112 or later) • Tanium End-User Notifications 1.6.5 or later • Tanium Interact 2.4.74 or later (use the latest version of Interact for best results) • Tanium Trends 3.6 or later
Computer groups	When you first log into the Tanium Console after installing the Tanium Server, the server automatically imports the computer groups that Deploy requires: `All Computers`.

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 89 for customized tuning to your environment. For more information, see Tanium Platform User Guide: Managing Global Settings.

Table 1: 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 Workstation	Windows 7 Service Pack 1 or later	Windows 7 Service Pack 1 requires Microsoft KB2758857.
macOS	• macOS 11.0 Big Sur • macOS 10.15 Catalina • macOS 10.14.6 Mojave • macOS 10.13.6 High Sierra • macOS 10.12 Sierra • OS X 10.11 El Capitan • OS X 10.10 Yosemite	
Linux	• Amazon Linux 1 or later • Oracle Enterprise Linux 6 or later • Red Hat Enterprise Linux (RHEL) 6 or later • CentOS 6 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, your security administrator must create exclusions to allow the Tanium processes to run without interference. For a list of all security exclusions to define across Tanium, see Tanium Core Platform Deployment Reference Guide: Host system security exclusions.

Table 2: Deploy security exclusions

Target device	Notes	Process
Module Server		`<Module Server>\services\deploy-service\node.exe`
	Required when Endpoint Configuration is installed	`<Module Server>\services\endpoint-configuration-service\TaniumEndpointConfigService.exe`
Windows endpoints	Required only for the Microsoft Windows 10 Upgrade packages	`C:\Deploy\Tanium\*`
		`<Tanium Client>\Python27\TPython.exe`
	7.4.*x* clients	`<Tanium Client>\Python38\TPython.exe`
	7.4.*x* clients	`<Tanium Client>\Python38\*.dll`
		`<Tanium Client>\Tools\Deploy\7za.exe`
		`<Tanium Client>\Tools\SoftwareManagement\7za.exe`
		`<Tanium Client>\TaniumCX.exe`

Target device	Notes	Process
Linux endpoints		<*Tanium Client*>/python27/bin/pybin
	7.2.*x* clients	<*Tanium Client*>/python27/pybin
	7.4.*x* clients	<*Tanium Client*>/python38/python
		<*Tanium Client*>/TaniumCX
macOS endpoints		<*Tanium Client*>/python27/bin/pybin
	7.2.*x* clients	<*Tanium Client*>/python27/pybin
	7.4.*x* clients	<*Tanium Client*>/python38/python
		<*Tanium Client*>/TaniumCX

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 Module Server for the Deploy service.

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

Software Package	Domain	Port
7-zip	7-zip.org	443
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
Adobe Digital Editions	adedownload.adobe.com	443
Adobe Flash Player	fpdownload.macromedia.com	443
Adobe Shockwave EOL[2]	fpdownload.macromedia.com	443
Box Drive	e3.boxcdn.net	443
Citrix Workspace (formerly Citrix Receiver)	downloadplugins.citrix.com	443

Software Package	Domain	Port
DB Browser for SQLite	sqlitebrowser.org	443
Dropbox	clientupdates.dropboxstatic.com	443
FileZilla	download.filezilla-project.org	443
Google Android Studio	dl.google.com	443
Google Chrome	dl.google.com	443
Google Drive File Stream	dl.google.com	443
Microsoft Office 2019	officecdn-microsoft-com.akamaized.net	443
Microsoft Office 2019 with Teams	officecdn-microsoft-com.akamaized.net	443
Microsoft Power BI Desktop	downloads.microsoft.com	443
Microsoft Silverlight	go.microsoft.com	443
Microsoft Skype Desktop Client	*.azureedge.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
NodeJS	nodejs.org	443
Notepad++	github.com	443
Oracle Java Runtime	javadl.oracle.com	443
	sdlc-esd.oracle.com	
Oracle MySQL Community	dev.mysql.com	443
PuTTY	the.earth.li	443
Royal Apps GmbH Royal TS	download.royalapplications.com	443
Slack	downloads.slack-edge.com	443
VideoLAN VLC Media Player	download.videolan.org	443
VMware Workstation Player[4]	download3.vmware.com	443
Wireshark	2.na.dl.wireshark.org	443

Software Package	Domain	Port
Zoom	d11yldzmag5yn.cloudfront.net	443
	zoom.us	
Zoom Outlook Plugin	zoom.us	443

[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 Tanium Community: How to execute a Windows 10 upgrade with Tanium Deploy: Setup.

[4] Update and Remove operations only.

User role requirements

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

Table 3: Deploy user role permissions

Permission	Deploy Administrator[1]	Deploy Endpoint Configuration Approver[2]	Deploy Operator[1,2]	Deploy Package Administrator[1,2]	Deploy Read Only User[1]	Deploy Service Account[1,3]	Deploy User[1,2]
Show Deploy View the Deploy workbench							

Permission	Deploy Administrator[1]	Deploy Endpoint Configuration Approver[2]	Deploy Operator[1,2]	Deploy Package Administrator[1,2]	Deploy Read Only User[1]	Deploy Service Account[1,3]	Deploy User[1,2]
Deploy Deployments Write Create and modify deployments							
Deploy Endpoint Configuration Approve Approve endpoint configuration approvals							
Deploy Endpoint Configuration Register Register with Endpoint Configuration							

Permission	Deploy Administrator[1]	Deploy Endpoint Configuration Approver[2]	Deploy Operator[1,2]	Deploy Package Administrator[1,2]	Deploy Read Only User[1]	Deploy Service Account[1,3]	Deploy User[1,2]
Deploy Maintenance Windows Write Create, modify, and delete maintenance windows							
Deploy Module Read Read access to the Deploy module							
Deploy Module Write Write access to the Deploy module							

Permission	Deploy Administrator[1]	Deploy Endpoint Configuration Approver[2]	Deploy Operator[1,2]	Deploy Package Administrator[1,2]	Deploy Read Only User[1]	Deploy Service Account[1,3]	Deploy User[1,2]
Deploy Settings Write Write access to global settings in the Deploy module							
Deploy Operator Settings Write Write access to a subset of global settings in the Deploy module							

Permission	Deploy Administrator[1]	Deploy Endpoint Configuration Approver[2]	Deploy Operator[1,2]	Deploy Package Administrator[1,2]	Deploy Read Only User[1]	Deploy Service Account[1,3]	Deploy User[1,2]
Deploy Profiles Write Create, modify, and delete self service profiles							
Deploy Use Api Perform Deploy operations using the API							

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

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

[3] If you installed Tanium Client Management, this user requires the **Endpoint Configuration Service Account** role. Endpoint Configuration is installed as a part of Tanium Client Management.

Table 4: Provided Deploy Micro Admin and Advanced user role permissions

Permission	Role Type	Content Set for Permission	Deploy Administrator	Deploy Endpoint Configuration Approver	Deploy Operator	Deploy Package Administrator	Deploy Read Only User	Deploy Service Account	Deploy User
Read User	Micro Admin								
Read User Group	Micro Admin								
Read Computer Group	Micro Admin								
Ask Dynamic Questions	Advanced								
Read Sensor	Advanced	Reserved							
Read Sensor	Advanced	Default							
Read Sensor	Advanced	Base							
Read Sensor	Advanced	Deploy Content Set							
Read Action	Advanced	Deploy Content Set							

Permission	Role Type	Content Set for Permission	Deploy Administrator	Deploy Endpoint Configuration Approver	Deploy Operator	Deploy Package Administrator	Deploy Read Only User	Deploy Service Account	Deploy User
Read Action[1]	Advanced	End-User Notifications							
Write Action	Advanced	Deploy Content Set							
Write Action[1]	Advanced	End-User Notifications							
Approve Action	Advanced	Deploy Content Set							
Execute Plugin	Advanced	Deploy Content Set							
Execute Plugin[2]	Advanced	Endpoint Configuration							
Execute Plugin[3]	Advanced	Tanium Data Service							
Execute Plugin[4]	Advanced	Trends							
Read Package	Advanced	Deploy Content Set							

Permission	Role Type	Content Set for Permission	Deploy Administrator	Deploy Endpoint Configuration Approver	Deploy Operator	Deploy Package Administrator	Deploy Read Only User	Deploy Service Account	Deploy User
Read Package[1]	Advanced	End-User Notifications							
Write Package	Advanced	Deploy Content Set							
Read Saved Question	Advanced	Deploy Content Set							
Read Saved Question[1]	Advanced	End-User Notifications							
Write Saved Question	Advanced	Deploy Content Set							
Write Saved Question[1]	Advanced	End-User Notifications							

[1] Denotes a provided permission when the Tanium End-User Notifications shared service is installed.

[2] Denotes a provided permission when Tanium Endpoint Configuration is installed.

[3] Denotes a provided permission when Tanium Interact is installed.

[4] Denotes a provided permission when Tanium Trends is installed.

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 **Tanium 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 and configure Deploy with default settings on page 50.
- **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 and configure Deploy with custom settings on page 51.

Before you begin

- Read the release notes.
- Review the Requirements on page 35.
- If you are upgrading from a previous version, see Upgrade Deploy on page 51.

Import and configure Deploy with default settings

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

- The Deploy service account is set to the account that you used to import the module.
- Computer groups that Deploy requires are imported.
- The Deploy action group is set to the `All Computers` computer group.
- For action locked machines, only applicability scanning is enabled, so that deployments cannot run on action locked machines.
- An `Always On` maintenance window is created, and enforced against the `All Computers` computer group.
- The following deployment templates are created:
  - **[Standard Deployment]** - default
  - **[Deployment with Reboot]**

- **[Deployment with Pre-Notification]**

To import Deploy and configure default settings, be sure to select the **Apply Tanium recommended configurations** check box while performing the steps in Tanium Console User Guide: Manage Tanium modules. After the import, verify that the correct version is installed: see Verify Deploy version on page 52.

Import and configure Deploy with custom settings

To import Deploy without automatically configuring default settings, be sure to clear the **Apply Tanium recommended configurations** check box while performing the steps in Tanium Console User Guide: Manage Tanium modules. After the import, verify that the correct version is installed: see Verify Deploy version on page 52.

To configure the service account, see Configure service account on page 55.

To organize computer groups, see Organize computer groups on page 55.

To configure the Deploy action group, see Add computer groups to Deploy action group on page 55.

Manage dependencies for Tanium solutions

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

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

Upgrade Deploy

For the steps to upgrade Deploy, see Tanium Console User Guide: Manage Tanium modules. After the upgrade, verify that the correct version is installed: see Verify Deploy version on page 52.

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 Tanium recommended configurations** option, you must enable and configure certain features.

Configure global 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 > Management > Global Settings**.
2. To increase the client cache size, click **New Setting**, provide the following information, and click **Save**.
   Setting Name: `ClientCacheLimitInMB`
   Setting Value: `2048`
   Affects: `Client`
   Value Type: `Numeric`
3. To increase the hot cache percentage, click **New Setting**, provide the following information, and click **Save**.
   Setting Name: `HotCachePercentage`
   Setting Value: `80`
   Affects: `Client`
   Value Type: `Numeric`

> **Note:** Changes to global 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 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.

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

Additionally you can use Endpoint Configuration to manage configuration approval. For example, configuration changes are not deployed to endpoints until a user with approval permission approves the configuration changes in Endpoint Configuration. For more information about the roles and permissions that are required to approve configuration changes for Deploy, see User role requirements on page 41.

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

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

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

If you enabled configuration approvals, 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 service account

The service account is a user that runs several background processes for Deploy. This user requires the **Content Administrator, Deploy Service Account**, and **End-User Notifications Read Only User** roles, or the **Tanium Administrator** role. If you installed Tanium Client Management, this user requires the **Endpoint Configuration Service Account** role. Endpoint Configuration is installed as a part of Tanium Client Management. For more information about Deploy permissions, see User role requirements on page 41.

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

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

Manual computer groups are not supported in Deploy. For more information, see Tanium Core Platform User Guide: Managing computer groups.

Add computer groups to Deploy action group

Importing the Deploy module automatically creates an action group to target specific endpoints. Select the computer groups to include in the Deploy action group. By default, Deploy targets No Computers.

> **Best Practice:** Ensure 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. Select **Tanium Deploy** and then click **Edit**.

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 operand (AND or OR) to combine the groups.

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.

> **Note:** 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 36.

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 file, remote file, or remote folder.
   These are the files that are needed to silently 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.

   > **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 click **Choose Icon** to upload an icon for self service deployments.

Tip:
- 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.

4. In the **System Requirements** section, provide the minimum system requirements for the package to run on the endpoint.
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. (Windows) For more information, see Variables for Windows applicability scans and command-line operations on page 59.

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 choose whether to terminate or pause the process.

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**. If any part of the path in a

command contains a space, use double quotation marks, even if you use variables.

File/Folder

Copy a file or folder, create a folder, delete a file or folder, extract a file or folder, or rename a file or folder. For file/folder actions, the source is the folder from which the package is running. If you specify a different folder, for example, c:\`temp`, specify the fully qualified path. The destination requires the fully qualified path. For more information, see File/Folder actions on page 60.

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.

6. In the **Installation Requirements** section, add a list of detection rules for prerequisite software. (Windows) For more information, see Variables for Windows applicability scans and command-line operations on page 59 and WMI queries on page 60.
7. (Optional) If the Update operation is selected, add a list of detection rules for previous versions. (Windows) For more information, see Variables for Windows applicability scans and command-line operations on page 59 and WMI queries on page 60.
8. In the **Install Verification** section, add a list of detection rules for installation verification. For more information, see Variables for Windows applicability scans and command-line operations on page 59 and WMI queries on page 60.
9. Click **Create Package**. You can also click **Save and Finish Later** to finish creating the package later.

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.

WMI queries

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.

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 not, Deploy creates `/Applications/firefox.app`; if so, 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. Specify an existing folder path or a folder path to create. For example, specify file `example.zip` and destination `c:\temp\myunzippedfile`.

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

1. From the Deploy menu, go to **Software** and then click **Predefined Package Gallery**.
2. Click **Import** for the package you want to import.

   > **Tip:** To import multiple packages simultaneously, select the packages that you want to import and click **Import**.

After you import a package and distribute the catalog, you can deploy, edit, delete, or export the package.

> **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.

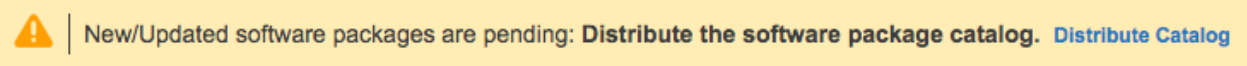
Distribute the software package catalog

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**.

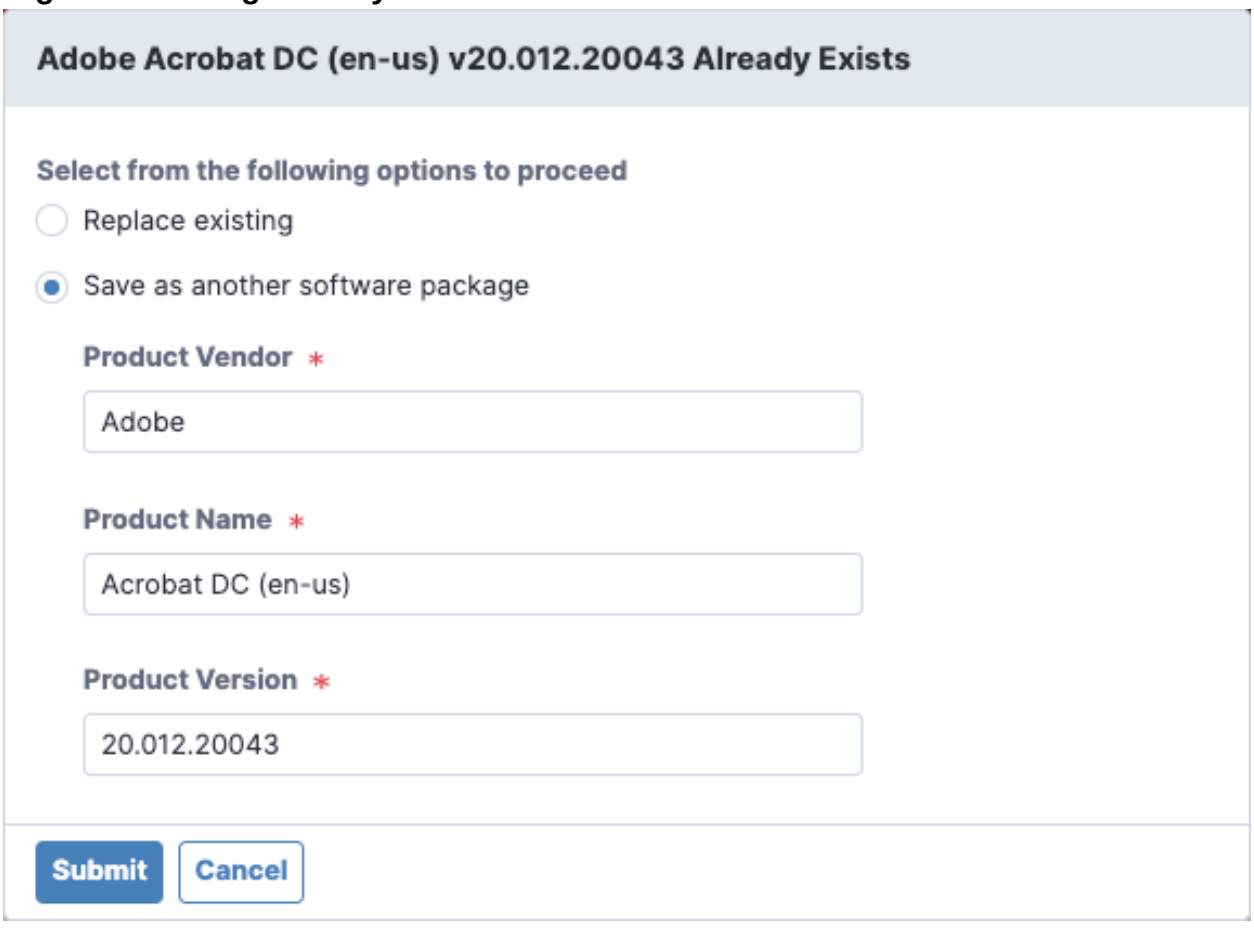
Figure 3: Distribute software package catalog



Replace or add a new package to the software package catalog

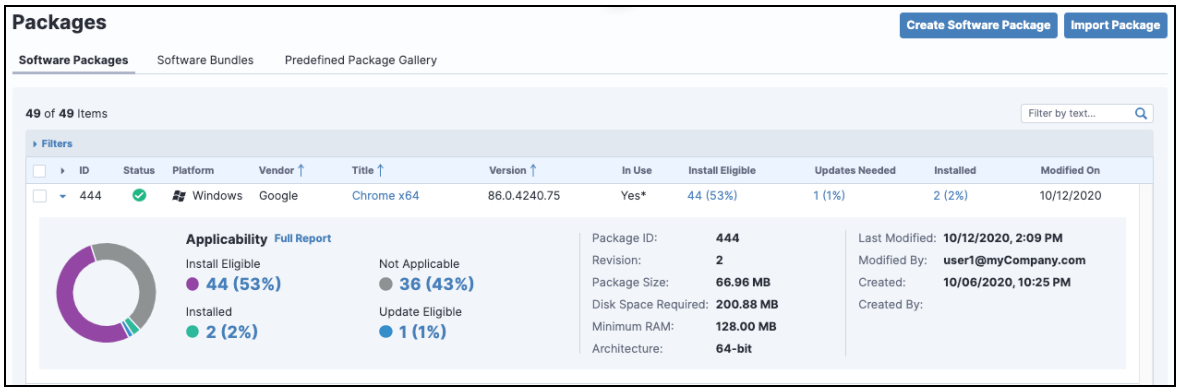
If a software package that is being imported already exists in the software package catalog, you are presented with two options prior to importing again. If you want to replace the existing package, select **Replace existing**. If you want to import the package, but also keep the existing one, select **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.

Figure 4: Package already exists

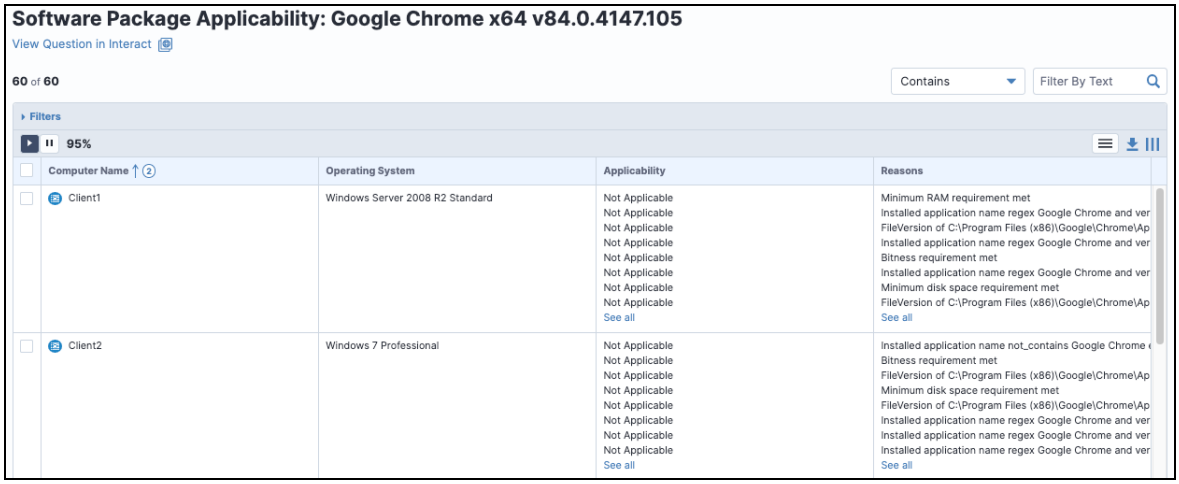


View software package applicability

1. From the Deploy menu, go to **Software** and then expand a package.
   You can also view the software package applicability by additionally clicking your package name.



2. For more details about a specific applicability state, click the link that corresponds to the number and percentage of endpoints in that applicability state.
3. To view the applicability details for the endpoints, click **Full Report**.



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.
   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.

> **Tip:** 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 software package or bundle is edited and saved, the version number of the package or bundle is incremented. All existing deployments continue to use the version that is specified at the time of deployment until the updated software package catalog is distributed.

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 Packages**.

> **Note:** You can delete a software package or bundle only if it is not referenced in an active deployment.

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 76.

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 57 or Import a software package on page 62.
- To create a software bundle deployment, ensure that you have at least one software bundle. See Create a software bundle on page 64.
- If you want to notify the end users of your Windows endpoints about the start of deployments or restarts that occur after deployments, install the Tanium End-User Notification solution. See Tanium End-User Notifications User Guide: Installing End-User Notifications and Windows endpoint restarts on page 70.

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.

   > **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 .

Create a software package deployment

1. From the Deploy menu, go to **Software**.
2. Select a package and then click **Deploy Package**.
3. Verify or provide the deployment details.
4. Select the software package operation.
5. Choose at least one target for the deployment.
6. 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 66.

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.

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.

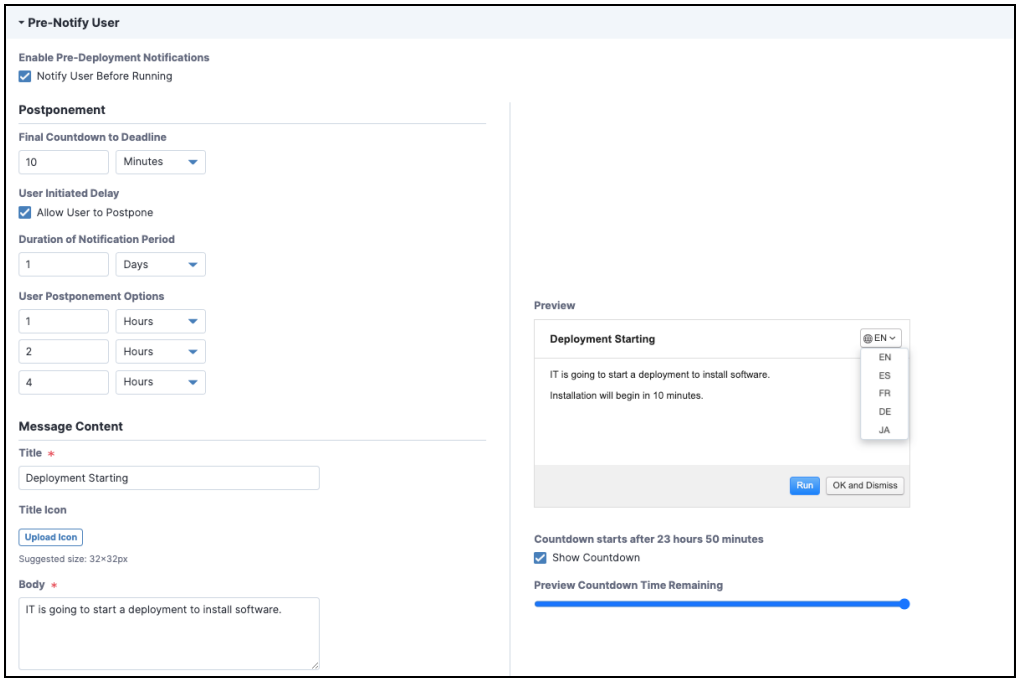
e. If you want the endpoints to download the deployment content before the installation time, select the option for **Download Immediately**.

> **Best Practice:** Select this option for future deployments. Files for the package are downloaded immediately only if the package is applicable.

f. (Windows endpoints) You can enable end user notifications about the deployments. Select **Notify User Before Running** in the **Pre-Notify User** section, and then configure the following settings.

- (Optional) Configure settings that allow the end user to postpone the start of the deployment.
- Configure the **Message Content** that informs the user about the deployment.
- (Optional) Select additional languages and provide translated title and body text for endpoints that are configured for other languages. To view the preview in additional languages, toggle the language drop-down

menu in the preview.



g. To minimize concurrent CPU utilization and disk input/output, select **Enabled** for the **Distribute Over Time** option and indicate a time.

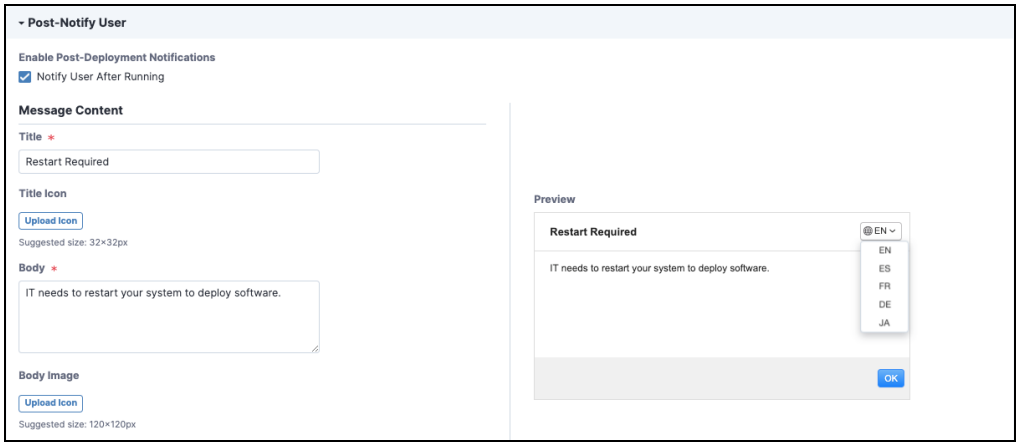
h. If you want to ignore deployment restrictions, select **Override maintenance windows**.

i. Select whether to restart the endpoint. For more information, see Windows endpoint restarts on page 70.

j. (Windows endpoints) You can enable end-user notifications about the completion of a deployment with or without a restart. Select **Notify User After Running** in the **Post-Notify User** section. If you enabled endpoint restarts, you can then configure the following settings that allow the user to postpone the restart:

- Configure the **Message Content** that informs the user about the restart.
- (Optional) Select additional languages and provide translated title and body text for endpoints that are configured for other languages. To view the preview in additional languages, toggle the language drop-down

menu in the preview.



> **Note:** The notification automatically disappears after two minutes if a user does not close it within that time.

7. Click **Deploy Software**.

Windows endpoint restarts

Deploy can trigger a restart of any Windows system after updates have been installed. You can choose between the following options for the restart:

- Restart silently and immediately after deployment. This option is typically used for servers and production machines in conjunction with maintenance windows and change control processes.
- (Windows endpoints) Notify the system user about the pending restart and give the system user the option to defer the restart for a specified amount of time. Configure the following options:

  Final Countdown to Deadline

  Specify the amount of time in minutes, hours, or days to show the final notification before restarting the endpoint. This notification also shows a countdown until restart. If this notification is dismissed, it will reappear after one minute. Set a low value because this option is meant to signal a forced restart that cannot be postponed.

  Allow User to Postpone

If you want to give the user an option to defer the restart for a specified amount of time, select this option. A user cannot postpone beyond the deadline.

Duration of Notification Period

Specify the amount of time in minutes, hours, or days before the endpoint must be restarted. The deadline is calculated by adding this value to the time the deployment completed for each endpoint.

User Postponement Options

Specify the amount of time in minutes, hours, or days that a user can postpone the restart.

Message Content

Specify the title and body of the notification message. 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. Upload optional icon and body images for branding to avoid confusing users and to limit support calls. Enable additional languages and provide translated title and body text. Enabling additional languages requires End-User Notifications 1.6 or later and Deploy 1.3 or later. 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.

Show Countdown

Select this option if you want the notification to show the amount of time that remains.

Tip: End user notifications can be added to existing deployments by stopping, reconfiguring, and reissuing the deployment.

Note: If no user is logged into an endpoint, the endpoint restarts immediately after a deployment completion even if the deployment is configured for a notification.

Create a software bundle deployment

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.

1. From the Deploy menu, go to **Software** and then click **Software Bundles**.
2. Select a bundle and then click **Deploy Bundle**.
3. Verify or provide the deployment details.
4. Verify the software bundle details.
5. Choose at least one target for the deployment.
6. 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 66.
    b. Specify a deployment type. 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.
    c. Designate the deployment time. You can choose from the local time on the endpoint or UTC time.
    d. Select self service options.

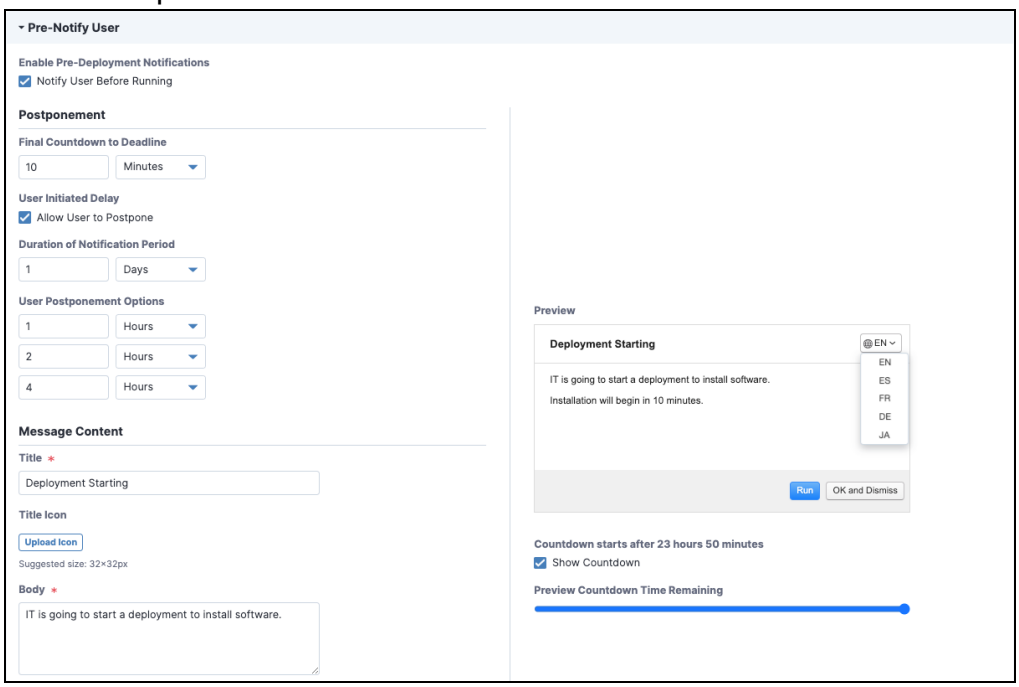
    > **Best Practice:** For self service deployments that are set for the future, use the **Make Available Before Start Time** option.

    e. If you want the endpoints to download the deployment content before the installation time, select the option for **Download immediately**.

    > **Note:** Files for all packages in the bundle are downloaded immediately. Applicability for each package is not checked until the deployment start time.

    f. (Windows endpoints) You can enable end user notifications about the deployments. Select **Notify User Before Running** in the **Pre-Notify User** section, and then configure the following settings.

- (Optional) Configure settings that allow the end user to postpone the start of the deployment.
- Configure the **Message Content** that informs the user about the deployment.
- (Optional) Select additional languages and provide translated title and body text for endpoints that are configured for other languages. To view the preview in additional languages, toggle the language drop-down menu in the preview.



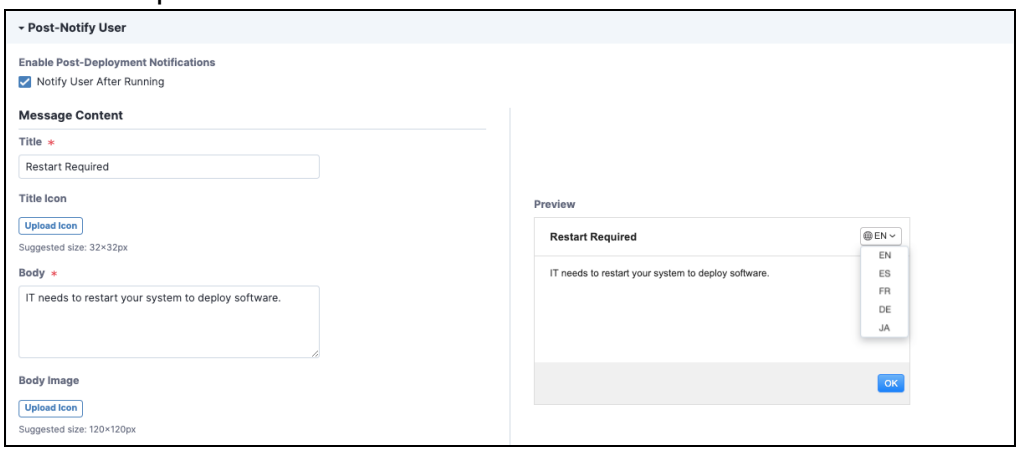
g. To minimize concurrent CPU utilization and disk input/output, select **Enabled** for the **Distribute Over Time** option and indicate a time.

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

i. (Windows) Select whether to restart the endpoint. For more information, see Windows endpoint restarts on page 70.

j. (Windows endpoints) You can enable end-user notifications about the completion of a deployment with or without a restart. Select **Notify User After Running** in the **Post-Notify User** section. If you enabled endpoint restarts, you can then configure the following settings that allow the user to postpone the restart:

- Configure the **Message Content** that informs the user about the restart.
- (Optional) Select additional languages and provide translated title and body text for endpoints that are configured for other languages. To view the preview in additional languages, toggle the language drop-down menu in the preview.



> **Note:** The notification automatically disappears after two minutes if a user does not close it within that time.

7. Click **Deploy Software**.

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 either the **Active** or **Inactive** tab.
3. Click the deployment name.
4. Review the sections.
   - **Deployment Details** provides the deployment details, such as the package or bundle name, status, operation, OS platform, and execution information.
   - **Targeting** lists the targeted computer groups for the deployment.
   - **Error Messages** includes a brief description and the count of affected endpoints, which links to Interact if you want to drill down for more information about specific endpoints.

- **<*Operation*> Workflow and Notifications** shows information about the deployment workflow and notifications.

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 Software**.

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 Software**.

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

IMPORTANT: 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. Click **Create Window** and then add one or more target 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.

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 66.

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 .

Using the Self Service Client application

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

- Install the Tanium End-User Notifications version that is listed in Tanium dependencies on page 35. For more information, see Tanium End-User Notifications User Guide: Installing End-User Notifications.
- Create one or more software packages or bundles. For more information, see Managing software on page 57.

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. Select computer groups or define a group of computers to target.
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. It also shows the number of times a given operation was performed for each package.

Use the Self Service Client application on endpoints

The Self Service Client application includes the following tabs:

Dashboard

The **Dashboard** tab displays the most recently added software applications and any current activity.

Catalog

The **Catalog** tab displays all of the available software applications in the catalog.

History

The **History** tab displays any completed activities that occurred on the system and their results.

Activity

The **Activity** tab displays any currently running or upcoming activities. Completed activities are moved to the **History** tab.

To install, update, or remove software applications on endpoints, open the Self Service Client application. For more information, see Tanium Community: Help End Users Help Themselves, With Tanium Deploy End User Self Service.

Troubleshooting Deploy

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

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-DDTHH-MM-SS.mmmZ* format.
2. (Optional) On the endpoint, copy the `Tanium\Tanium Client\Tools\SoftwareManagement` folder.
3. (Optional) View status and logs for recent Deploy service jobs.
   a. On the **Support** tab, click **View Job Status**.
   b. In the **Job Detail** window, click **Download Logs** to download a `job-logs.txt` file with more details about recent jobs.

End user notifications are not displayed

End user notifications are supported for Windows endpoints only. If end user notifications are not being displayed on the endpoints:

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 38.

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\python27\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 Package 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**.

No software in the Predefined Package Gallery

After you import Deploy 1.1 or later, you must configure the service account and 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 89 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 82.
   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, Configure service account on page 55 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 89 for assistance.

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.
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.

Contributing factor	Corrective action
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 No software in the Predefined Package Gallery on page 83.

Contributing factor	Corrective action
It takes too look 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.

Uninstall Deploy

> **IMPORTANT:** 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.

Delete Deploy actions

1. Go to **Actions > Scheduled Actions**.
2. Click **Action Groups** and then choose **Tanium Deploy**.
3. Select all of the Deploy actions, click **More**, and choose **Delete Actions**.

Remove deployment artifacts from endpoints

1. Use Interact to target endpoints. To get a list of endpoints that have Deploy tools installed, ask the `Get Deploy - Tools Version from all machines` question.
2. In the results grid, choose an item and click **Deploy Action**.
3. Click **Deployment Package**, choose **Deploy - Remove Tools [*operating system*]**, and select **Remove saved data**.
4. Schedule the deployment to reissue periodically and set an end date. This action removes data from endpoints that come online later.
5. Choose the action group to target with the deployment, preview the deployment, and then click **Deploy Action**.
6. Repeat these steps for each operating system package that is installed.

Remove Deploy from the Tanium Module Server

1. From the Main menu, go to **Administration > Configuration > Solutions**.
2. In the Deploy section, click **Uninstall** and follow the process.
3. Return to the **Tanium 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.
3. Retain the **Deploy - Remove Tools** packages, and select and delete all of the other packages.

(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`

Contact Tanium Support

To contact Tanium Support for help, send an email to support@tanium.com.