Tanium™ Patch User Guide

Version 2.3.7

July 11, 2019

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.

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

Table of contents

Patch overview **8**

Patch scanning options 8

Patch lists and blacklists 12

Superseded patches 12

Microsoft update and servicing details 13

Deployments 13

Maintenance windows 14

Getting started with Patch **15**

Patch requirements **16**

Tanium dependencies 16

Tanium Server and Module Server computer resources 16

Endpoint resource requirements 17

Third-party software 17

Host and network security requirements 17

Security exclusions 17

Internet URLs 18

User role requirements 18

Tanium Server 7.0 18

Tanium Server 7.1 or later 19

Installing Patch **22**

Install Patch solution 22

Set the service account 22

Organize computer groups 23

Add computer groups to Patch action group 23
Initialize Patch 23
Install the Tanium End-User Notifications solution 24
Disable Windows Update restart prompts 24
Upgrade the Patch version 24
What to do next 25
Configuring TDownloader for Linux endpoints 26
Before you begin 26
Configure TDownloader on Tanium™ Appliance 27
Configure TDownloader on Windows 27
Downloading patches in an airgap environment 32
Configure airgap for Windows endpoints 32
Download airgap-downloader utility 32
Generate a list of remote package files 32
Download remote package files 33
Verify the airgap configuration 33
Enforcing scan configurations 35
Offline CAB file 35
Online to Microsoft Windows Update 36
WSUS Scan 36
Configure WSUS Scan 37
Create a scan configuration 37
Scan windows 38
View enforcement status 39
Prioritize scan configurations 40

Edit a scan configuration 40
Remove a scan enforcement 40
Delete a scan configuration 40
Managing patches **42**
Patch list rules 42
Create a patch list 43
Exclude patches with blacklists 43
yum.conf exclusions for Red Hat and CentOS endpoints 44
Create lists from the Patches view 45
Edit a list 45
Check patch visibility 45
Export a list 47
Import a list 47
Delete a list 47
Add a custom Patch field 48
Example CSV 48
Deploying patches **49**
Before you begin 49
Create a deployment to install patches 49
Endpoint restarts 51
Create a deployment to uninstall patches 53
Review deployment summary 55
Add targets to an existing deployment 57
Reissue a deployment 58
Stop a deployment 58

Adjust the deployment retries 59
Create a deployment template 59
Reference: Patch status 59
Deployment status 59
Enforcement status 60
Setting Maintenance Windows 62
Maintenance window options 62
Create a maintenance window 63
Edit a maintenance window 64
Override a maintenance window 65
Delete a maintenance window 65
Patch use cases 66
Example 1: Automatically deploy key 2016 patches 66
Example 2: Create a blacklist that excludes .NET patches 67
Example 3: Stagger patch deployment to a worldwide network 68
Example 4: Address the Wanna Cry vulnerability 68
Troubleshooting Patch 71
Collect a troubleshooting package 71
Configure endpoint logging 71
Patches are not listed in the Patches view 72
Scans are not completed on Linux endpoints 72
Sensors return Could not get results on Linux endpoints 73
Red Hat Linux endpoints stuck in Waiting for Initial Scan status 73
Change the patch visibility aggregation 73
Check and update the Windows Update Agent 74

Uninstall Patch 74

Restore the state of the Patch database 75

Patch overview

Use Patch to manage operating system patching across your enterprise at the speed and scale of Tanium. You can deploy a single patch to a computer group immediately. You can also perform more complex tasks, such as using advanced rule sets and maintenance windows to deliver groups of patches across your environment at specified times.

You can define custom workflows and schedule patches based on rules or exceptions built around patch lists, blacklists, and maintenance windows. For example, you might always apply critical Microsoft patches to all machines except for datacenter servers, or always exclude .NET patches, or install patches during non-working hours.

Patch generates in-depth reports and returns current patch applicability results from every endpoint. For any patch or patch list deployment, the following details are provided:

- The patch details, such as severity, release date, applicable Common Vulnerabilities and Exposures (CVE), files, and links to knowledge base articles.
- The status of the patch, split out by computer group.
- The assigned patch lists or blacklists for the patch.

Patch scanning options

You can choose from several scan methods to determine the installed and missing patches across your network. *Scan configurations* define a scan method, scan frequency, and the computer groups that are being scanned, known as an *enforcement*. One scan configuration is applied to an endpoint. If an endpoint is included in multiple computer groups, the highest priority scan configuration is applied.

Review the following list of scanning options to decide the best method to use for each computer group.

Table 1: Available patch scanning options

Scan method	Platform OS	Updates included	Client impact	Connectivity	Details
Offline CAB file	Windows	• Security Updates • Service Packs	Moderate, during scanning activity	The CAB file is stored locally by the Tanium Client.	• Requires 200+MB download of CAB file. • Does not include routine updates, out of band fixes, hotfixes, and enhancements that are included with WSUS or Online to Microsoft scan methods.

Scan method	Platform OS	Updates included	Client impact	Connectivity	Details
Online to Microsoft	Windows	• Scanning: Critical Updates, Security Updates, Definition Updates, Update Rollups, Service Packs, Tools, Feature Packs, Updates, Upgrades, Drivers • Installing: Critical Updates, Security Updates, Definition Updates, Update Rollups, Service Packs, Tools, Updates, Upgrades	• Moderate, during first scan • Low, subsequent	The Tanium Client must contact Microsoft directly.	• Requires additional network traffic to Microsoft directly. • Feature Pack and Driver updates should be blacklisted for installation.

Scan method	Platform OS	Updates included	Client impact	Connectivity	Details
Windows Server Update Services (WSUS) Scan	Windows	• Scanning: Critical Updates, Security Updates, Definition Updates, Update Rollups, Service Packs, Tools, Feature Packs, Updates, Upgrades, Drivers • Installing: Critical Updates, Security Updates, Definition Updates, Update Rollups, Service Packs, Tools, Updates, Upgrades	Low	The Tanium Client must contact the WSUS server.	• Must deploy and configure one or more WSUS servers. • Updates must be approved in WSUS prior to scanning or deployment. • Feature Pack and Driver updates should be blacklisted for installation.
Repository Scan	• Red Hat • CentOS	All updates in the YUM repositories	Moderate, during scanning activity	The Tanium Client must contact the YUM repositories for scanning as well as patch downloads.	• Must deploy and configure one or more YUM repositories. • Updates must be maintained in the YUM repositories.

Scan method	Platform OS	Updates included	Client impact	Connectivity	Details
Tanium Scan	• Red Hat • CentOS	All updates in the YUM repositories	Moderate, during scanning activity	The Tanium Client stores the repository scanning logic locally.	• Internal or external YUM repositories can be used. • Only the Tanium Server needs connectivity to the YUM repositories.

Note: If you are using Microsoft System Center Configuration Manager (SCCM) with your WSUS server, do not use Tanium for WSUS scanning with the same server.

Patch lists and blacklists

Group patches that can be applied into *patch lists*. Group patches that must be excluded into *blacklists*. These lists can be determined by any detail included in the patch information. For example, you could:

- Create lists based on severity, prioritize the most critical and most recent updates first.
- Focus only on CVE issues.
- Create lists based on the month or a specific release date.

As new patches come out, you can use dynamic rules to automatically assess and populate patches to the appropriate lists. You can iteratively develop these lists by creating new versions. You can deploy any version of the list as needed.

Superseded patches

Each patch includes a column that indicates if the patch has been superseded, or effectively replaced by a newer patch. A patch is marked as superseded when a single endpoint reports that the patch is superseded. Including superseded patches in patch lists can be useful when you want to find or install a specific patch that was superseded. For example, you might need to find or install superseded patches when they are referenced in a security advisory recommendation. Superseded patches are automatically included in blacklists.

Microsoft update and servicing details

In October 2016, Microsoft changed the way they provide software patch updates, based on the operating system of the endpoint. Though these terms are subject to change, it is important to be aware of how they affect your network.

- **Windows 10 and Windows 2016**
  - *Feature Upgrades*: Feature builds are essentially a new build of Windows 10 (for example 1511, 1607, 1703). These upgrades are published every 3-4 months. Currently, Windows 10 build upgrades can be completed with a standard package deployed by Tanium.
  - *2017-XX Cumulative Update*: Released monthly, a cumulative update supersedes any previous cumulative update for Windows 10. Contains all security and non-security fixes for the month and all previous months.
- **Windows 7, 8.1, 2008, 2008R2, 2012, 2012R2**
  - *2017-XX Security Monthly Quality Rollup*: Package is a cumulative update for current and all previous months. Only the current month will be applicable. All previous versions are superseded.
  - *2017-XX Security Only Quality Update*: Security updates for the specified month only. Does not include updates from any previous month. Previous monthly updates will still be applicable and needed.

  Do not deploy both the Security Monthly Quality Rollup and the Security Only Quality Update for the same month at the same time. If both updates are targeted to an endpoint, the Windows Update Agent installs the Security Monthly Quality Rollup, and the Security Only update is ignored. The download size increases without any benefit.

For more information, see Exclude patches with blacklists on page 43 and the Microsoft articles on Simplified Servicing or the Windows Servicing Model.

Deployments

Deployments compile patches, typically from lists, and then distribute Patch packages to the target computers. You can configure deployment options to set when and how patches are installed or uninstalled.

For example, you might want to restart an endpoint after patches are installed to apply the changes. If a patch comes out that would normally be blacklisted but is needed for some reason, you can override the blacklist for that specific deployment rather than making a

new version the blacklist. In urgent situations, you can even override a closed maintenance window.

You can choose whether to restart the endpoint after patch installation, to inform the user about the restart, and to allow the user to postpone the restart.

Maintenance windows

Maintenance windows designate the permitted times that the targeted computer groups are open for patches to be installed or uninstalled. You can have multiple maintenance windows, even with overlapping times. Maintenance windows do not interfere with each other. For a patch deployment to take effect, the deployment and maintenance window times must be met.

Consider establishing a maintenance cycle that keeps your endpoints as up-to-date as possible. You can avoid many security risks with good operational hygiene. Some considerations might include coordinating with the Microsoft Patch Tuesday releases, on weekends, or outside the core work hours for your network.

Getting started with Patch

1. Install the Patch module. See Installing Patch on page 22.
   If you are upgrading, see Upgrade the Patch version on page 24.
2. (Optional) Enable Linux endpoints. Select **RedHat/CentOS Linux** in the **Operating Systems** tab of the Patch Settings and add any custom YUM repositories in the **YUM Repositories** tab of the Patch Settings.
3. Create a scan configuration and add enforcements. See Enforcing scan configurations on page 35.
4. Organize the available patches. See Managing patches on page 42.
5. Install patches on endpoints. See Deploying patches on page 49.
6. Create patch restrictions. See Exclude patches with blacklists on page 43 or Setting Maintenance Windows on page 62.

Patch requirements

Review the requirements before you install and use Patch.

Tanium dependencies

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

Component	Requirement
Platform	7.0.314.6085 or later. Enhanced functionality is available with version 7.0.314.6319 and later. Installing Tanium™ Interact is also suggested. For role-based access control (RBAC), you must have Tanium Platform 7.1.314.3071 or later. To support smart card authentication, including common access cards (CAC), see Tanium Core Platform Deployment Reference Guide: Smart card authentication. Patch 2.3.5 supports Red Hat and CentOS Linux endpoints with Tanium Platform 7.2.314.3235 and later. For more information, see Configuring TDownloader for Linux endpoints on page 26.
Tanium Client	Patch is supported on Windows endpoints. Use Tanium Client 1540 and later. Patch 2.3.5 supports Red Hat and CentOS Linux endpoints with Tanium Client 6.0.314.1554 and later.
Tanium End-User Notifications	1.2.0.004 or later (optional for Windows endpoints). Not supported for Linux endpoints.

Tanium Server and Module Server computer resources

Patch 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. You might need to tune the Tanium Server download bytes and download limit settings (**DownloadBytesPerSecondLimit**) for your environment. Contact your Technical Account Manager (TAM) for details.

Patch downloads and distributes updates regularly. The Tanium Server stores these packages within the `Downloads` directory. Adequate disk space is required on the Tanium

Server. Manual routine cleanup of old patch files is required prior to Tanium Server 7.2. Contact your TAM for details.

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

Endpoint resource requirements

In the Tanium Console Global Settings, set the Tanium Client cache limit (**ClientCacheLimitInMB**) to 2048MB and set the Hot cache (**HotCachePercentage**) to 80%. For more information, see Tanium Platform User Guide: Managing Global Settings.

If VDI is used in your environment, see the Tanium Client Deployment Guide: VDI.

Third-party software

Patch requires that Windows endpoints have Windows Update Agent version 6.1.0022.4 or later installed. Enhanced functionality is available on Windows 7 systems with version 7.6.7601.19161 and later. See Microsoft KB313861. If you are controlling all patch deployments through Tanium, we suggest disabling the Windows Update Agent automatic functions at the domain level.

Host and network security requirements

Specific processes and URLs are needed to run Patch.

Security exclusions

If security software is in use in the environment to monitor and block unknown host system processes, your security administrator must create exclusions to allow the Tanium processes to run without interference.

The Tanium Client uses the Windows Update offline scan file, `Wsusscn2.cab`, to assess computers for installed or missing operating system and application security patches. If your endpoint security solutions scan archive files, refer to the Microsoft KB for information on how to configure those tools to interact appropriately with the `Wsusscn2.cab` file.

Table 2: Patch security exclusions

Target device	Process
Module Server	*<Tanium Module Server>*\services\patch-service\node.exe

Target device	Process
Windows Endpoints	*<Tanium Client>*\Patch\tanium-patch.min.vbs
	<Tanium Client>\Patch\scans\Wsusscn2.cab
	<Tanium Client>\Patch\tools\active-user-sessions.exe
	<Tanium Client>\Patch\tools\TaniumExecWrapper.exe
	<Tanium Client>\Patch\tools\TaniumFileInfo.exe
	<Tanium Client> (exclude from on-access or real-time scans)

Internet URLs

If security software is deployed in the environment to monitor and block unknown URLs, your security administrator must whitelist the following URLs.

- http://download.windowsupdate.com/
- http://go.microsoft.com/fwlink/?linkid=74689

User role requirements

Tanium Server 7.0

Different role types have varying permissions within Patch. Administrators can perform all functions; however, other role types are limited.

Table 3: Tanium 7.0 Patch console role requirements

Permission	Administrator/Content Administrator	Action/Sensor Authors or Action Authors
View workbench	✓	✓
Initialize Patch service	✓	✗
Create, modify, or delete scan configurations and enforce against computer groups	✓	✓
Create, modify, or delete patch lists and blacklists	✓	✓
Create, modify, or delete deployments and target computer groups	✓	✓

Permission	Administrator/Content Administrator	Action/Sensor Authors or Action Authors
Create, modify, or delete maintenance windows and enforce against computer groups	✓	✓

Tanium Server 7.1 or later

For Tanium Platform version 7.1.314.3071 or later, Patch 2.0.9 introduces role-based access control (RBAC) permissions that control access to the Patch workbench. The three predefined roles are Patch Admin, Patch User, and Patch Read Only User.

Table 4: Patch user role permissions for Tanium 7.1.314.3071 or later

Permission	Patch Administrator	Patch User	Patch Read Only User
Show Patch View the Patch workbench	✓[1]	✓[1]	✓[1]
Patch Use API Perform Patch operations using the API	✓[1]	✓[1]	✓[1]
Patch Module Read Read access to the Patch module	✓	✓	✓
Patch Module Write Write access to the Patch module	✓	✓	✗

Permission	Patch Administrator	Patch User	Patch Read Only User
Patch Settings Write Write access to global settings in the Patch module	✓	✗	✗

[1] Denotes a provided permission.

Table 5: Provided Patch Micro Admin and Advanced user role permissions for Tanium 7.1.314.3071 or later

Permission	Role Type	Content Set for Permission	Patch Administrator	Patch User	Patch Read Only User
Read User Group	Micro Admin		✓	✓	✓
Read Computer Group	Micro Admin		✓	✓	✓
Ask Dynamic Questions	Advanced		✓	✓	✓
Read Sensor	Advanced	Base	✓	✓	✓
Read Sensor	Advanced	Reserved	✓	✓	✓
Read Sensor	Advanced	Default	✓	✓	✓
Read Sensor	Advanced	Patch Content Set	✓	✓	✓
Read Action	Advanced	Patch Content Set	✓	✓	✓
Read Package	Advanced	Patch Content Set	✓	✓	✓
Execute Plugin	Advanced	Patch Content Set	✓	✓	✓
Write Package	Advanced	Patch Content Set	✓	✓	✗
Write Saved Question	Advanced	Patch Content Set	✓	✓	✗

Permission	Role Type	Content Set for Permission	Patch Administrator	Patch User	Patch Read Only User
Write Action	Advanced	Patch Content Set	✓	✓	✗
Approve Action	Advanced	Patch Content Set	✓	✓	✗

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

Installing Patch

Install Patch by importing the module, setting the service credentials, and organizing your computer groups.

Install Patch solution

Import Patch from the solutions page.

> **Note:** Installing Patch 2.0 or later disables the Tanium Windows Security Patch content. You do not need both solutions.

1. From the Main menu, click **Tanium Solutions**.
2. Under Patch, click **Import**.
   A progress bar is displayed as the installation package is downloaded.
3. Click **OK**.
   The Import Solution window opens with a list of all the changes and import options.
4. Click **Proceed with Import** and enter your password.
   The Patch installation and configuration process begins.
5. Click **Close**.
6. To confirm the installation, return to the Tanium Solutions page and check the **Installed: *X.X.X.XX*** version for Patch.

   > **Tip:** If you do not see the Patch module in the console, refresh your browser.

Set the service account

For recurring maintenance activities, specify a Tanium user with **Administrator** or **Content Administrator** user role permissions for Tanium Server 7.0 or **Patch Administrator** user role permissions for Tanium Server 7.1.314.3071 or later. Specifying these credentials is a one-time configuration. No other credentials need to be added.

1. From the Patch home page, in the **Configure Patch** section, click the **Configure Service Account** step and click **Configure Service Account**.

> **Note:** If the **Configure Patch** section is not visible in the Patch home page, click **Manage Home Page**, select **Configure Patch**, and click **Save**.

2. Enter the Tanium credentials and click **Save**.

Organize computer groups

One way to apply patches and view deployment results 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
- Endpoint configuration needs, such as VDI machines

For more information, see Tanium Core Platform User Guide: Managing computer groups.

Add computer groups to Patch action group

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

1. From the Patch home page, in the **Configure Patch** section, click the **Select Computer Groups** step and click **Configure Action Group**.

   > **Note:** If the **Configure Patch** section is not visible in the Patch home page, click **Manage Home Page**, select **Configure Patch**, and click **Save**.

2. Select the computer groups that you want to include in the action group. If you select multiple computer groups, choose an operand (AND or OR) to combine the groups.
3. (Optional) In the **All machines currently included in this action group** section, review the included endpoints.

   > **Note:** These results might take a few moments to populate.

4. Click **Save**.

Initialize Patch

Patch installs a set of tools on each endpoint that you have targeted.

1. From the Patch home page, in the **Configure Patch** section, click the **Initialize Endpoints** step and click **Initialize Endpoints** to start the Patch service and begin distributing these tools to your endpoints.

   > **Note:** If the **Configure Patch** section is not visible in the Patch home page, click **Manage Home Page**, select **Configure Patch**, and click **Save**.

2. Enter the Tanium credentials and click **Confirm**.

Install the Tanium End-User Notifications solution

By installing the Tanium End-User Notifications solution, you can create a notification message with your deployment to notify the user that the system is going to restart, and gives the user the option to postpone the restart.

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

To check if your endpoints have the end user notification tools, ask the question: `Get Has End User Notification Tools from all machines with Is Windows = "true"`

Disable Windows Update restart prompts

The Windows Update Agent automatically prompts users to restart their machine when an update is installed from any user or source. The following Local/Group Policies should be configured to allow Tanium End-User Notifications to control endpoint restarts.

1. In the Local Group Policy Editor, go to **Computer Configuration > Administrative Templates > Windows Components > Windows Update**.
2. Enable the **No auto-restart for scheduled Automatic Updates installations** parameter.
3. Disable the **Re-prompt for restart with scheduled installations** parameter.

Upgrade the Patch version

Upgrade Patch to the latest version from the Solutions page.

> **IMPORTANT:** Patch 1.x must be uninstalled before installing Patch 2.x. Uninstalling Patch 1.x includes removing the Patch folder on the Tanium Module Server. Contact your TAM for assistance.

1. From the main menu, click **Tanium Solutions**.
2. Locate Patch and click **Upgrade to *X.X.X.XX***.
3. Click **OK**.
   The Import Solution window opens with a list of all the changes and import options.
4. Click **Proceed with Import** and enter your password.
   The Tanium Patch installation and configuration process begins.
5. To confirm the upgrade, return to the Tanium Solutions page and check the **Installed: *X.X.X.XX*** version for Patch.

   > **Tip:** If the Patch version is not updated, refresh your browser window.

What to do next

See Getting started with Patch on page 15 for more information about using Patch.

Configuring TDownloader for Linux endpoints

To use Patch on Red Hat Linux endpoints, you must configure Tanium Downloader (TDownloader) to use certificate authentication for downloads to the Red Hat Satellite server.

The available scanning techniques include Repo Scan and Tanium Scan. For the Repo Scan technique, you can use all repositories from which an endpoint can pull. For the Tanium Scan technique, you must use Red Hat Content Delivery Network, Red Hat Satellite 6 or later, or custom repositories.

For best results, create separate scan configurations for each major operating system. For more information, see Red Hat Linux endpoints stuck in Waiting for Initial Scan status on page 73.

Before you begin

Ensure that you meet the following prerequesites:

- Tanium Platform 7.2.314.3235 or later.
- Tanium Client 6.0.314.1554 or later.
- Patch 2.3.5 or later.
- YUM version 3.2.29-17.el6 or later.
- Enable the **RedHat/CentOS Linux** option in the **Operating Systems** tab of the Patch Settings.
- In the **Configuration Settings** tab of the Patch Settings, set the **Patch List Applicability Bin Count** value to `10`. For more information about how to fine-tune this setting, consult your TAM.
- (Optional) Add any custom YUM repositories in the **YUM Repositories** tab of the Patch Settings.
- Obtain a valid SSL client certificate and private key and the SSL certificate authority (CA) certificate of the satellite server from the Red Hat, Inc. website. For more information, see Creating a Red Hat certificate for Tanium downloads (login required) and Reference: TDownloader (login required).

Configure TDownloader on Tanium™ Appliance

1. Upload the SSL client private key and client certificate to your Tanium Appliance. Use SFTP with the `tancopy` account and copy the files to the `/incoming` folder.
2. Using the TanOS menu, verify that the Tanium Server can reach cdn.redhat.com or the Red Hat Satellite server by name:
   a. Enter `3` to go to the Tanium Support menu.
   b. Enter `4` to go to the Run Network Diagnostics menu.
   c. Enter `1` to select the Ping Remote System option.
3. On each Tanium Server, add the CA root certificate for the Red Hat Satellite or content delivery network (CDN) server:
   a. Enter `2` to go to the Tanium Operations menu.
   b. Enter `2` to go to the Tanium Configuration Settings menu.
   c. Enter `12` to go to the Control RedHat CA Cert menu.
   d. Enter `2` to select the Install redhat-uep.pem option.
4. On each Tanium Server, add the Red Hat Entitlement client certificate and key:
   a. Enter `2` to go to the Tanium Operations menu.
   b. Enter `2` to go to the Tanium Configuration Settings menu.
   c. Enter `4` to select the Add Tanium Server TDL Auth Cert option.
   d. Enter the URL (https://cdn.redhat.com or the Red Hat Satellite server), client certificate file name, and the SSL client private key file name at each prompt.
   e. At the #Line Content display, enter `R` to return to the previous menu.

For more information, see Tanium Appliance Deployment Guide: Manage authentication certificates for Tanium Patch connections with Red Hat.

Configure TDownloader on Windows

1. Copy the SSL client private key, client certificate, and satellite server certificate to your Tanium Server.
2. Ensure that the Tanium Server can reach cdn.redhat.com or the Red Hat Satellite server by name.
   Example:
   `ping cdn.redhat.com`
3. On each Tanium Server, configure TDownloader to use certificate authentication for downloads to the Red Hat Satellite server.
   Example:
   ```
   cmd-prompt>TDownloader.exe add-auth-cert --url
   ```

`https://cdn.redhat.com --cert C:\client-certificate.pem --key C:\client-key.pem`

where:

- `https://cdn.redhat.com` is the URL prefix for the satellite server download URLs
- `C:\client-certficate.pem` is the client certificate
- `C:\client-key.pem` is the client certificate private key

4. Check the TDownloader config to see that your certificate has been configured.

```
cmd-prompt>TDownloader.exe config list
Keys:
  - Auth:
    - Auth.0:
      - Auth.0.Certificate: -----BEGIN CERTIFICATE-----
MIIFPTCCBCWgAwIBAgIIbY/mIdQbgMowDQYJKoZIhvcNAQEFBQAwgYwxCzAJBgNV
BAYTAlVTMRcwFQYDVQQIDA5Ob3J0aCBDYXJvbGluYTEQMA4GA1UEBwwHUmFsZWln
aDEQMA4GA1UECgwHS2F0ZWxsbzEUMBIGA1UECwwLU29tZU9yZ1VuaXQxKjAoBgNV
BAMMIXJoZWxwYXRjaHNhdGVsbGl0ZTAxLnByb2RxYS5sb2NhbDAeFw0xODA0MjAw
NDAwMDBaFw0xOTA0MjAwMzU5NTlaMEYxGTAXBgNVBAoMEHRhbml1bV9wYXRjaF9k
ZXYxKTAnBgNVBAMTIDBjYjk4NjcyZjBhNTQ0MDJhNzIzYmNjOGI5ODFjYTg3MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtXPySC20fPzMreenmX+4mUhS
s/cdArQZOeeKliCdXI7Q/ZW0ZrhsgmMZTL+BNbZKUp72e0L3GF3yj0wx/8LWRLVC
S9AaZdbXmJRK7B5mwpQaLtfuE93bJIkmBbzKA49jiwFdDE0J6v+wj0NgBZ3hr0NH
V2O1hAwar2xkzz9fCTwyAR6d2I9Dpcfua8nH0ybO5kR8v1Epp70vw9/uMmGM3PCe
YFX81ll3wxStbHj/DznUzQ/vFE0SZxLXh9LyWy9Nq+obLaFeDxJ0DT7iXotwVqWs
Qow/upQ60vuYpAT57JM5tkrP+rKcct+TVVJNS/QmJC3yOwZWf8rIISRH4cb+GQID
AQABo4IB5jCCAeIwEQYJYIZIAYb4QgEBBAQDAgWgMAsGA1UdDwQEAwIEsDCBwQYD
VR0jBIG5MIG2gBRNdbtnITo9NxbcUdarkRIJv464dqGBkqSBjzCBjDELMAkGA1UE
BhMCVVMxFzAVBgNVBAgMDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHDAdSYWxlaWdo
MRAwDgYDVQQKDAdLYXRlbGxvMRQwEgYDVQQLDAtTb211T3JnVW5pdDEqMCgGA1UE
AwwhcmhlbHBhdGNoc2F0ZWxsaXRlMDEucHJvZHFhLmxvY2FsggkAx2ndp2OhmcYw
HQYDVR0OBBYEFHX7IDsUYNAZdI5dBxckm5a8y60aMBMGA1UdJQQMMAoGCCsGAQUF
BwMCMBIGCSsGAQQBkggJBgQFDAMzLjMwFAYJKwYBBAGSCAkIBAcMBUJhc2ljMIGd
BgkrBgEEAZIICQcEgY8EgYx42i2MMQrDMBAE9zFukyYgfyJdHmDO8oIEis7cXYz9
e8ck1UwxjNM2GsbXj1bYsFQP6BpVuzRk7cEeSP8kYYRL3EK1OZ51NrED6f5ASK+f
97RK5DIt3KAO7mHiGIyN4rwGw/wVsVxwAp4aKvUSzZXb1epTaC96MJ25BX5rmucc
vyYlbSe9CpomkcWhADANBgkqhkiG9w0BAQUFAAOCAQEAubxqAqH/IQqIODQwaX9x
NrIuJp3qWIUFjxZ1Vby4lEg2xmwfBtvNKminJBWNwOMZjq40xrEz0C2sxqkr/npv
cbI4MMdQX1rdxMwsntgUZK8ApRR/pPwyxqAoa8IjahVBHNdFoA4+BBjcLcvzA1PB
PReiXo0GS2gQQAb8U7d/jBTG1gm3ZpJFBxv7NBM9tEey3DwzP5LWPnZZmstRrlfx
7sb5J/2zLvWuMG+dMJ5jkgUKTuNdccdBP9PEVrAKiDuoLCl4UqnP0YzMJd+e9Ktx
FC1QCICFUQLhZ/QVAhh8hIw0jSxIcGN+KVJF52BGdzUxvoidfqtMsjc/8NSTRk+T
/g==
-----END CERTIFICATE-----

  - Auth.0.PrivateKey: (protected)
```

```
  - Auth.0.URL: https://rhelpatchsatellite01.prodqa.local
 - LogVerbosityLevel: 41
 - ProxyPassword:
 - ProxyPort:
 - ProxyServer:
 - ProxyType: NONE
 - ProxyUserid:
 - TrustedCertPath: C:\Program Files\Tanium\Tanium
Server\Certs\installedcacert.crt
 - TrustedHostList: localhost,tanium.local,win-2012-r2
```

5. To configure TDownloader to work with the Red Hat CDN, use a text editor to append the PEM-encoded certificate for cdn.redhat.com to the end of the certificate file as referenced by the *TrustedCertPath* value from the previous step (Example: `C:\Program Files\Tanium\Tanium Server\Certs\installedcacert.crt`).
-----BEGIN CERTIFICATE-----

```
-----BEGIN CERTIFICATE-----
MIIG/TCCBOWgAwIBAgIBNzANBgkqhkiG9w0BAQUFADCBsTELMAkGA1UEBhMCVVMx
FzAVBgNVBAgMDk5vcnRoIENhcm9saW5hMRYwFAYDVQQKDA1SZWQgSGF0LCBJbmMu
MRgwFgYDVQQLDA9SZWQgSGF0IE5ldHdvcmsxMTAvBgNVBAMMKFJlZCBIYXQgRW50
aXRsZW1lbnQgT3BlcmF0aW9ucyBBdXRob3JpdHkxJDAiBgkqhkiG9w0BCQEWFWNh
LXN1cHBvcnRAcmVkaGF0LmNvbTAeFw0xMDEwMDQxMzI3NDhaFw0zMDA5MjkxMzI3
NDhaMIGuMQswCQYDVQQGEwJVUzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExFjAU
BgNVBAoMDVJlZCBIYXQsIEluYy4xGDAWBgNVBAsMD1JlZCBIYXQgTmV0d29yazEu
MCwGA1UEAwwlUmVkIEhhdCBFbnRpdGxlbWVudCBQcm9kdWN0IEF1dGhvcml0eTEk
MCIGCSqGSIb3DQEJARYVY2Etc3VwcG9ydEByZWRoYXQuY29tMIICIjANBgkqhkiG
9w0BAQEFAAOCAg8AMIICCgKCAgEA2QurMeAVnCHVsuZNQzciWMdpd4LAVk2eGugN
0cxmBpzoVI8lIsJOmJkpOAuFOQMX9CBr8RuQyg4r1/OH/rfhm6FgGIw8TGKZoWC/
1B9teZqTiM85k6/1GRNxdk6dUK77HVO0PMIKtNBHRxIsXcRzJ1q+u5WPBes9pEVG
nbidTNUkknrSIdynTJcqAI/I0VAsqLqX87XJSzXKvRilE+p/fLHmVTAffl1Cn/Dy
KULxna7ooyrKKnfqeQ5dK8aMr1ASQ1wphWohLjegly9V0amEi+HHWnOL8toxJy8v
WUTUzzAvZ4ZTtTV26xGetZZWEaNyv7YCv2AexjcBQ2x+ejrFJrVNo9jizHS06HK8
UgHVDKhmVcAe2/5yrJCjKDLwg1FJfjKwhzhLYdNVCejpy8CHQndwO0EX1hHv/AfP
RTAmr5qPhHFD+uuIrYrSLUpgMLmWa9dinJcGeKlA1KJvG5emGMM3k64Xr7dJToXo
5loGyZ6lvKPIKLmfeXMRW/4+BqyzwbO1i4aIHAZcSPDFGKWwuvF0iVUYUUVxw0nv
qPZA4roq5+j/YSz0q5XGVgiIt34htlvunLp/ICGYJBR6zEHcB9aZGJdDcJvoYZjw
7Gphw6lFF6Ta4imoyhGECWKjd1ips3opcN+DlU0yCUrcIXVIXAnkTwu5ocOgAkxr
f/6FjqcCAwEAAaOCAR8wggEbMB0GA1UdDgQWBBSW/bscQED/QIStsh8LJsHDam/W
fDCB5QYDVR0jBIHdMIHagBTESXhWRZ0eLGFgw2ZLWAU3LwMie6GBtqSBszCBsDEL
MAkGA1UEBhMCVVMxFzAVBgNVBAgMDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHDAdS
YWxlaWdoMRYwFAYDVQQKDA1SZWQgSGF0LCBJbmMuMRgwFgYDVQQLDA9SZWQgSGF0
IE5ldHdvcmsxHjAcBgNVBAMMFUVudGl0bGVtZW50IE1hc3RlciBDQTEkMCIGCSqG
SIb3DQEJARYVY2Etc3VwcG9ydEByZWRoYXQuY29tggkAkYrPyoUAAAAwEgYDVR0T
AQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQUFAAOCAgEArWBznYWKpY4LqAzhOSop
```

```
t30D2/UlCSr50l33uUCNYD4D4nTr/pyX3AR6P3JcOCz0t22pVCg8D3DZc5VlzY7y
P5RD3KbLxFNJTloclMG0n6aIN7baA4b8zwkduMQvKZnA/YNR5xE7V7J2WJHCEBBB
Z+ZFwGpGsoZpPZP4hHLVke3xHm6A5F5SzP1Ug0T9W80VLK4jtgyGs8l1R7rXiOIt
Nik8317KGq7DU8TI2Rw/9Gc8FKNfUYcVD7uC/MMQXJTRvkADmNLtZM63nhzpg1Hr
hA6U5YcDCBKsPA43/wsPOONYtrAlToD5hJhU+1Rhmwcw3qvWBO3NkdilqGFOTc2K
50PQrqoRTCZFS41nv2WqZFfbvSq4dZRJl8xpB4LAHSspsMrbr9WZHX5fbggf6ixw
S9KDqQbM7asP0FEKBFXJV1rE8P/oSK6yVWQyigTsNcdGR4AUzDsTO9udcwoM2Ed4
XdakVkF+dXm9ZBwv5UBf5ITSyMXL3qlusIOblJVGUQizumoq0LiSnjwbkxh2XHhd
XD/B/qax7FnaNg+TfujR/kk3kF1OpqWx/wC/qPR+zho1+35Al31gZOfNIn/sReoM
tcci9LFHGvijIy4VUDQK8HmGjIxJPrIIe1nB5BkiGyjwn00D5q+BwYVst1C68Rwx
iRZpyzOZmeineJvhrJZ4Tvs=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIHZTCCBU2gAwIBAgIJAJGKz8qFAAAAMA0GCSqGSIb3DQEBBQUAMIGwMQswCQYD
VQQGEwJVUzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcMB1JhbGVp
Z2gxFjAUBgNVBAoMDVJlZCBIYXQsIEluYy4xGDAWBgNVBAsMD1JlZCBIYXQgTmV0
d29yazEeMBwGA1UEAwwVRW50aXRsZW1lbnQgTWFzdGVyIENBMSQwIgYJKoZIhvcN
AQkBFhVjYS1zdXBwb3J0QHJlZGhhdC5jb20wHhcNMTAwMzE4MTEyNDU0WhcNMzAw
MzEzMTEyNDU0WjCBsTELMAkGA1UEBhMCVVMxFzAVBgNVBAgMDk5vcnRoIENhcm9s
aW5hMRYwFAYDVQQKDA1SZWQgSGF0LCBJbmMuMRgwFgYDVQQLDA9SZWQgSGF0IE5l
dHdvcmsxMTAvBgNVBAMMKFJlZCBIYXQgRW50aXRsZW1lbnQgT3BlcmF0aW9ucyBB
dXRob3JpdHkxJDAiBgkqhkiG9w0BCQEWFWNhLXN1cHBvcnRAcmVkaGF0LmNvbTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALsmiohDnNvIpBMZVJR5pbP6
GrE5B4doUmvTeR4XJ5C66uvFTwuGTVigNXAL+0UWf9r2AwxKEPCy65h7fLbyK4W7
/xEZPVsamQYDHpyBwlkPkJ3WhHneqQWC8bKkv8Iqu08V+86biCDDAh6uP0SiAz7a
NGaLEnOe5L9WNfsYyNwrG+2AfiLy/1LUtmmg5dc6Ln7R+uv0PZJ5J2iUbiT6lMz3
v73zAxuEjiDNurZzxzHSSEYzw0W1eO6zM4F26gcOuH2BHemPMjHi+c1OnheaafDE
HQJTNgECz5Xe7WGdZwOyn9a8GtMvm0PAhGVyp7RAWxxfoU1B794cBb66IKKjliJQ
5DKoqyxD9qJbMF8U4Kd1ZIVB0Iy2WEaaqCFMIi3xtlWVUNku5x21ewMmJvwjnWZA
tUeKQUFwIXqSjuOoZDu80H6NQb+4dnRSjWlx/m7HPk75m0zErshpB2HSKUnrs4wR
i7GsWDDcqBus7eLMwUZPvDNVcLQu/2Y4DUHNbJbn7+DwEqi5D0heC+dyY8iS45gp
I/yhVvq/GfKL+dqjaNaE4CorJJA5qJ9f383Ol/aub+aJeBahCBNuVa2daA9Bo3BA
dnL7KkILPFyCcEhQITnu70Qn9sQlwYcRoYF2LWAm9DtLrBT0Y0w7wQHh8vNhwEQ7
k5G87WpwzcC8y6ePR0vFAgMBAAGjggF9MIIBeTAdBgNVHQ4EFgQUxEl4VkWdHixh
YMNmS1gFNy8DInswgeUGA1UdIwSB3TCB2oAUiEumRcRG7I/Wz6b2Gs8mPJDMfxeh
gbakgbMwgbAxCzAJBgNVBAYTAlVTMRcwFQYDVQQIDA5Ob3J0aCBDYXJvbGluYTEQ
MA4GA1UEBwwHUmFsZWlnaDEWMBQGA1UECgwNUmVkIEhhdCwgSW5jLjEYMBYGA1UE
CwwPUmVkIEhhdCBOZXR3b3JrMR4wHAYDVQQDDBVFbnRpdGxlbWVudCBNYXN0ZXIg
Q0ExJDAiBgkqhkiG9w0BCQEWFWNhLXN1cHBvcnRAcmVkaGF0LmNvbYIJAOb+Qigl
yeZeMAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgEGMBEGCWCGSAGG+EIBAQQEAwIB
BjAgBgNVHREEGTAXgRVjYS1zdXBwb3J0QHJlZGhhdC5jb20wIAYDVR0SBBkwF4EV
Y2Etc3VwcG9ydEByZWRoYXQuY29tMA0GCSqGSIb3DQEBBQUAA4ICAQBbTSz+UIXP
AVIT0ZVL1flCHR113aj2j3UBZkaoDkSxtEfa1nqysmN0llpqh4NVBL3anEFYxokL
hQ2PB8mmuD5EuWaNxnXTc4Sr5dsOcjkFiU197lybaJK7w4OzQ2Qg/X/t4+R78cfM
ZK/qHpjuyT3NyHHvCug/WzkvU09pRr2aVHI+fn68u18TRzPJNKvegR4YeA3vsyQW
BgEc8sU7KrAvikFJ3mCTpAk+6SRgbGFLyZE637Qrzy2DDBw0V020dkTkC6YnEsZg
HwZWVmLtCgLlnimx6SRft+6zrXVHWZxod1GT/af7vizpmhrXt/Nu5Se7dpOhPayo
NwYCFNmfZeL4W/foSKNfaizZcc+tiNABRtT+tplfniv/yjr7sBAsFPhJqQB8CfsQ
8BVvKkHtixygyo+EO+NEotZGw3cn+/7soo9B1bWXk3PFSwEr+KwINACFGv2zcGLI
```

```
oeP4iK6DHZImWEV4tgMrQyXatEyPh2axPWU3SjY/fr1Ub5gEt+WpCtyYIN4ObBaN
eL3NPfTj79/VFZ22PhUInmGY/VK/ymvl/dkWyWi8zD8Aq55ofZ33FvQ46dcLp1pV
KWApIVqO27uhL6YxXDFi6n7RXACEIVz6JqDh5fGmOH1F+vfumZKzW78LlVD2QY15
rmCh0i9+AUCiUsNyYdJbSZDPiFPBwlwUoQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIHZDCCBUygAwIBAgIJAOb+QiglyeZeMA0GCSqGSIb3DQEBBQUAMIGwMQswCQYD
VQQGEwJVUzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcMB1JhbGVp
Z2gxFjAUBgNVBAoMDVJlZCBIYXQsIEluYy4xGDAWBgNVBAsMD1JlZCBIYXQgTmV0
d29yazEeMBwGA1UEAwwVRW50aXRsZW1lbnQgTWFzdGVyIENBMSQwIgYJKoZIhvcN
AQkBFhVjYS1zdXBwb3J0QHJlZGhhdC5jb20wHhcNMTAwMzE3MTkwMDQ0WhcNMzAw
MzEyMTkwMDQ0WjCBsDELMAkGA1UEBhMCVVMxFzAVBgNVBAgMDk5vcnRoIENhcm9s
aW5hMRAwDgYDVQQHDAdSYWxlaWdoMRYwFAYDVQQKDA1SZWQgSGF0LCBJbmMuMRgw
FgYDVQQLDA9SZWQgSGF0IE5ldHdvcmsxHjAcBgNVBAMMFUVudGl0bGVtZW50IE1h
c3RlciBDQTEkMCIGCSqGSIb3DQEJARYVY2Etc3VwcG9ydEByZWRoYXQuY29tMIIC
IjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA2Z+mW7OYcBcGxWS+RSKG2GJ2
csMXiGGfEp36vKVsIvypmNS60SkicKENMYREalbdSjrgfXxPJygZWsVWJ5lHPfBV
o3WkFrFHTIXd/R6LxnaHD1m8Cx3GwEeuSlE/ASjc1ePtMnsHH7xqZ9wdl85b1C8O
scgO7fwuM192kvv/veI/BogIqUQugtG6szXpV8dp4ml029LXFoNIy2lfFoa2wKYw
MiUHwtYgAz7TDY63e8qGhd5PoqTv9XKQogo2ze9sF9y/npZjliNy5qf6bFE+24oW
E8pGsp3zqz8h5mvw4v+tfIx5uj7dwjDteFrrWD1tcT7UmNrBDWXjKMG81zchq3h4
etgF0iwMHEuYuixiJWNzKrLNVQbDmcLGNOvyJfq60tM8AUAd72OUQzivBegnWMit
CLcT5viCT1AIkYXt7l5zc/duQWLeAAR2FmpZFylSukknzzeiZpPclRziYTboDYHq
revM97eER1xsfoSYp4mJkBHfdlqMnf3CWPcNgru8NbEPeUGMI6+C0YvknPlqDDtU
ojfl4qNdf6nWL+YNXpR1YGKgWGWgTU6uaG8Sc6qGfAoLHh6oGwbuz102j84OgjAJ
DGv/S86svmZWSqZ5UoJOIEqFYrONcOSgztZ5tU+gP4fwRIkTRbTEWSgudVREOXhs
bfN1YGP7HYvS0OiBKZUCAwEAAaOCAX0wggF5MB0GA1UdDgQWBBSIS6ZFxEbsj9bP
pvYazyY8kMx/FzCB5QYDVR0jBIHdMIHagBSIS6ZFxEbsj9bPpvYazyY8kMx/F6GB
tqSBszCBsDELMAkGA1UEBhMCVVMxFzAVBgNVBAgMDk5vcnRoIENhcm9saW5hMRAw
DgYDVQQHDAdSYWxlaWdoMRYwFAYDVQQKDA1SZWQgSGF0LCBJbmMuMRgwFgYDVQQL
DA9SZWQgSGF0IE5ldHdvcmsxHjAcBgNVBAMMFUVudGl0bGVtZW50IE1hc3RlciBD
QTEkMCIGCSqGSIb3DQEJARYVY2Etc3VwcG9ydEByZWRoYXQuY29tggkA5v5CKCXJ
5l4wDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCAQYwEQYJYIZIAYb4QgEBBAQDAgEG
MCAGA1UdEQQZMBeBFWNhLXN1cHBvcnRAcmVkaGF0LmNvbTAgBgNVHRIEGTAXgRVj
YS1zdXBwb3J0QHJlZGhhdC5jb20wDQYJKoZIhvcNAQEFBQADggIBAJ1hEdNBDTRr
6kI6W6stoogSUwjuiWPDY8DptwGhdpyIfbCoxvBR7F52DlwyXOpCunogfKMRklnE
gH1Wt66RYkgNuJcenKHAhR5xgSLoPCOVF9rDjMunyyBuxjIbctM21R7BswVpsEIE
OpV5nlJ6wkHsrn0/E+Zk5UJdCzM+Fp4hqHtEn/c97nvRspQcpWeDg6oUvaJSZTGM
8yFpzR90X8ZO4rOgpoERukvYutUfJUzZuDyS3LLc6ysamemH93rZXr52zc4B+C9G
Em8zemDgIPaH42ce3C3TdVysiq/yk+ir7pxW8toeavFv75l1UojFSjND+Q2AlNQn
pYkmRznbD5TZ3yDuPFQG2xYKnMPACepGgKZPyErtOIljQKCdgcvb9EqNdZaJFz1+
/iWKYBL077Y0CKwb+HGIDeYdzrYxbEd95YuVU0aStnf2Yii2tLcpQtK9cC2+DXjL
Yf3kQs4xzH4ZejhG9wzv8PGXOS8wHYnfVNA3+fclDEQ1mEBKWHHmenGI6QKZUP8f
g0SQ3PNRnSZu8R+rhABOEuVFIBRlaYijg2Pxe0NgL9FlHsNyRfo6EUrB2QFRKACW
3Mo6pZyDjQt7O8J7l9B9IIURoJ1niwygf7VSJTMl2w3fFleNJlZTGgdXw0V+5g+9
Kg6Ay0rrsi4nw1JHue2GvdjdfVOaWSWC
-----END CERTIFICATE-----
```

Downloading patches in an airgap environment

When your Tanium Server is in an airgap environment, the server cannot download patches from the internet. With Patch 2.3.7, you can configure Patch to install patches from an alternate file location in the Patch Settings for Windows endpoints.

Configure airgap for Windows endpoints

1. From the Patch Settings, click **Airgap Configuration**, and select **Enable Settings for Airgap - Windows**.
2. Provide an **Alternate Patch File Location** where all airgap files are staged.

   Note: To configure a UNC share on your Tanium Server, contact your TAM.
3. Click **Save** and then click **Yes** to confirm your action.
4. From the Main menu, click **Administration > Whitelisted URLs** to verify that the configured alternate Patch file location is listed.

Download airgap-downloader utility

From the **Airgap Configuration** tab of the Patch Settings, click **Download Utility** to download the `airgrap-downloader.exe` utility.

You must run this utility on a Windows computer that can access the internet.

Generate a list of remote package files

From the **Generate Download Manifest** section of the **Airgap Configuration** tab of the Patch Settings, select the **Include CAB File** and **Include MS-CVEs.dat File** options and click **Export Download URLs** to generate a list of files that the Tanium Server requires.

A `urls.txt` file is downloaded to your computer. For example:

```
http://download.windowsupdate.com/microsoftupdate/v6/wsusscan/wsusscn2.cab
https://content.tanium.com/files/hosted_dats/MS-CVEs.dat
```

Note: The **Patch Applicability** filter options apply blacklists to the results.

Download remote package files

Use the `urls.txt` file that you generated from the Tanium Server to download files from a computer that is connected to the internet.

1. Copy the `urls.txt` and `airgap-downloader.exe` files to a computer that is connected to the internet and open a command prompt to that directory.
2. To download the package files from sources contained in `urls.txt`, run:

   ```
   airgap-downloader.exe download_files --no_rename
   ```

   If the `urls.txt` and `airgap-downloader.exe` files are not in the same directory, you must also include the `--urls_source` option.
3. The command downloads the files in the list and generates a `results.zip` archive that contains:
   - The downloaded files
   - A manifest `results.txt`

   Extract the contents of the `results.zip` file to your alternate Patch file location.

Verify the airgap configuration

To verify that airgap was configured correctly, you can confirm the following things:

1. Verify that the Tanium Server has the staged files:
   a. From the Main menu, click **Content > Packages**.
   b. Select the **Patch - External File References - Windows** package and click **Edit**.
   c. In the **Files** section, click **wsusscn2.cab** and verify that the **SHA-256** field has a non-empty hash value.
   d. Click **MS-CVEs.dat** and verify that the **SHA-256** field has a non-empty hash value.
2. Verify that the Windows endpoints can scan against the staged files:
   a. From the Main menu, click **Content > Packages**.
   b. Select the **Patch - Distribute Patch Manifests - Windows** package and click **Edit**.
   c. In the **Files** section, click **required-files-manifest** and then click Download .

d. Open the `required-files-manifest` file and verify that the `<hash>` value for the `wsusscn2.cab` file matches the non-empty hash value in step 1c.

e. Verify that the `<hash>` value for the `MS-CVEs.dat` file matches the non-empty hash value in step 1d.

Enforcing scan configurations

The list of available patches comes from scanning the endpoints in your network. The *scan configuration* determines a scanning technique and frequency. A scan configuration is *enforced* by targeting computer groups.

The available scanning techniques include the offline CAB file (recommended), online Microsoft Windows Update, and Windows Server Update Services (WSUS) Scan.

Offline CAB file

The CAB file is stored locally by the Tanium Client and contains cumulative security and quality patches for all products in the Microsoft Update Catalog, including Windows and Office. On the Patch home page, the latest status of the offline CAB file is available. The active CAB file is the most recent, verified file published by Microsoft. Patch uses only the active CAB file for scan configurations. A rejected CAB is not pushed to a computer group. Patch checks for an updated CAB file every hour. You can click **Update CAB** to force a new download outside of the normal schedule.

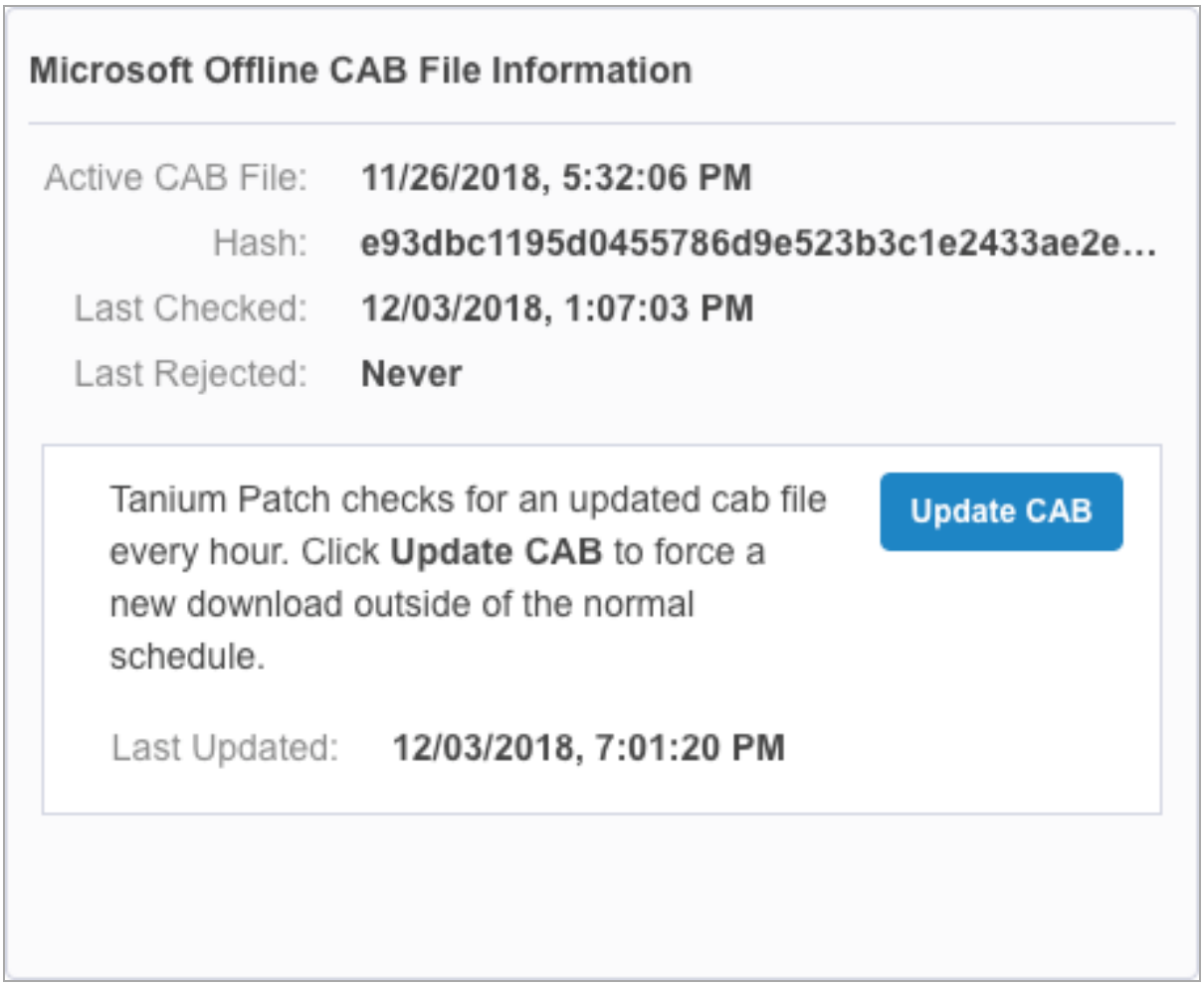


Figure 1: Example CAB file status

Online to Microsoft Windows Update

This option creates additional network traffic between the Tanium Client and Microsoft and is for Windows operating system updates only. The full range of patches are available for the Windows operating system:

- Critical patches
- Cumulative security and quality patches
- Non-security and optional updates

WSUS Scan

Using WSUS servers for patching activities gives the option for the full range of patch types for all products in the Microsoft Update Catalog, including Windows and Office. However,

some additional configuration is required. The Tanium Client must be able to contact the WSUS server, and patches must be approved before they can be downloaded.

The guidelines about how many clients a WSUS server can support are similar to the Microsoft guidelines for SCCM: up to 150,000 clients per WSUS server. See Microsoft Docs: Size and scale numbers for System Center Configuration Manager.

CONFIGURE WSUS SCAN

1. Add the WSUS Server URL to the whitelist.
    a. From the Patch home page, go to Settings.
    b. In the **WSUS Server Configuration** section, enter the URL and click **Submit**.
    c. A regular expression for the URL is generated and added to the whitelist. Click View Whitelisted URLs, or go to **Administration > Whitelisted URLs** to view the entry that was added.
2. On the WSUS server, change the following settings:
    - Set the intranet URL for detecting updates and the statistics server to: `http://<WSUS server URL>:<port>`.
    - We recommend disabling the **Configure Automatic Updates** setting.

Create a scan configuration

You can create multiple scan configurations and add computer group enforcements as needed.

1. In the Patch menu, click **Scan Management**.
2. Click **Create Configuration**, provide a name, and select an operating system.
3. Choose the configuration options.
    a. Select a **Configuration Technique**.
    If you choose Offline CAB File, you can select **Download and scan immediately upon new CAB release** to ensure that the endpoints are scanned whenever a new CAB file is published. Selecting this setting overrides the frequency settings when a new CAB file is detected, but scans still wait for the scan window if configured.
    b. In the Frequency field, enter a number and a time parameter.
    We recommend scanning once a day or longer between scans.
    c. (Optional) Enable **Random Scan Delay** and enter a time to distribute the network activity.
    The default is 120 minutes.

> **Tip:** For VDI environments, set a longer delay to reduce the impact of the scan on the host system.

d. (Optional) Enable **Limit Scan Times** to define the scan window options, such as browser time or local time on the endpoint, how often the window repeats, and override options. For more information, see Scan windows on page 38.

> **Note:** The scan window specifies when a scan can start. If you enabled **Random Scan Delay**, scans can potentially start as late as the specified delay after the end of the scan window. For example, if a scan attempts to start one minute before the end of the scan window, but receives the full random scan delay of 120 minutes, the scan does not start until after that 120 minutes and continues to run until completion, even though the scan window is already closed.

4. Click **Save**.
5. On the scan configuration details page, add one or more computer groups.
   a. Click **Add Computer Group**.

      Enabling the patch applicability results provides a refined aggregation for the specific computer group.

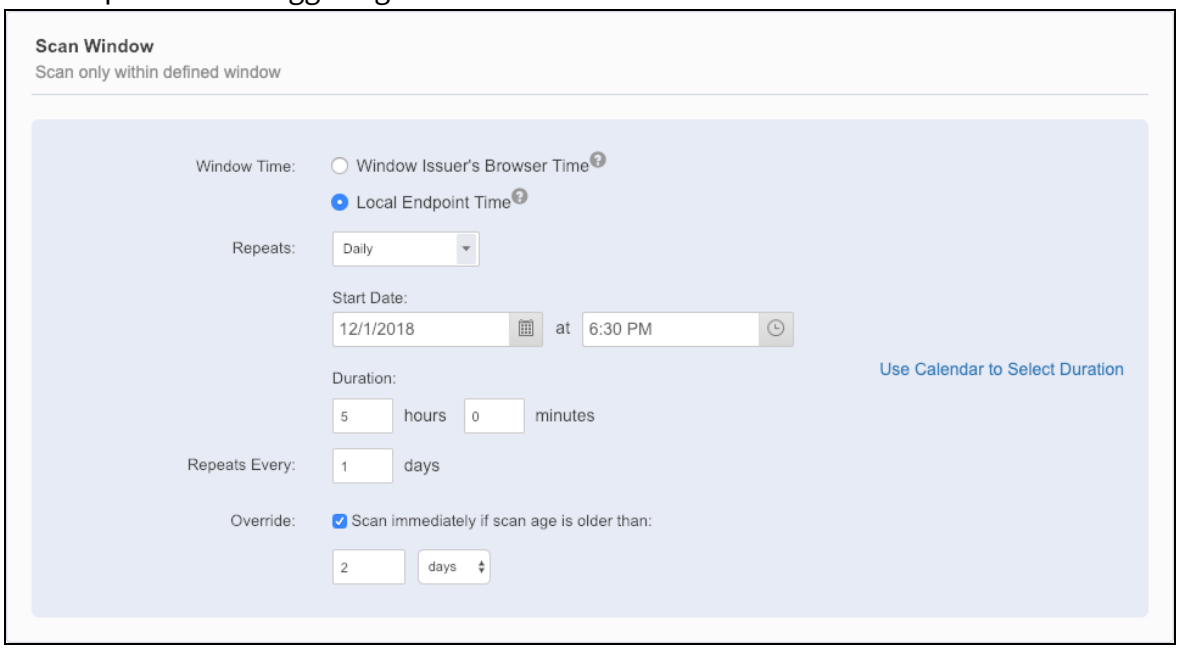
   b. Click **Add** and provide your credentials. Click **Confirm**.

The list of available patches might be displayed within 15-30 minutes. Longer scan delays might result in patches appearing slowly. If no data appears after the scan delay, contact your TAM. If an endpoint cannot be scanned, for example if it is offline, it is scanned at the earliest opportunity.

Scan windows

You can set a scan window to restrict scans to a certain time of day or day of the week. For example, you can create a scan configuration to scan your endpoints daily, but restrict the scans to run during non-business hours, such as from 6:30 PM to 11:30 PM. Additionally, if some of your endpoints are offline during the scan window, you can choose the **Override** option to scan any endpoints that have a scan age older than a specified amount of time, in hours or days.

1. In the **Scan Configuration Options** section, enable **Limit Scan Times**.
2. In the **Scan Window** section, configure your preferences.
   a. Select between your browser time or local time on the endpoint.
   b. Choose whether to repeat the scan window daily or weekly and specify a start date and time and how often the scan window repeats.
   c. (Optional) Enable the **Override** option and specify how many hours or days can elapse before triggering an immediate scan.



View enforcement status

By reviewing a scan configuration, you can see which endpoints in the computer group contain the enforced configuration.

1. In the Patch menu, click **Scan Management**.
2. On the Scan Configurations tab, select a configuration.
3. Expand the computer group to see more details about the scan status.
4. Click Interact to open the question results for each endpoint.
   The Interact results grid shows the endpoint status and the reason, if it is not enforced.

Prioritize scan configurations

You can create multiple scan configurations with multiple computer groups. The order of the configuration decides its priority. If an endpoint is in multiple computer groups with conflicting configurations, only the highest priority configuration is applied to the endpoint.

1. In the Patch menu, click **Scan Management**.
2. On the Scan Configurations tab, click **Prioritize**.
3. Move the Scan Configurations by dragging and dropping or entering a number into the Conflict Resolution Order field and pressing Enter.
4. Click **Save**.

Edit a scan configuration

1. In the Patch menu, click **Scan Management**.
2. On the **Scan Configurations** tab, select a configuration.
3. Click **Edit**.

   Note: You cannot edit a scan configuration if the **Allow Scan Configuration Editing** option is disabled in the Patch settings.
4. Make your changes.
5. Preview the changes.
6. Click **Save**.

Remove a scan enforcement

Removing a computer group from a scan configuration removes the enforcement.

1. In the Patch menu, click **Scan Management**.
2. On the Scan Configurations tab, select a configuration.
3. Delete the computer group.

Delete a scan configuration

After the enforcements are removed, you can delete a scan configuration.

1. In the Patch menu, click **Scan Management**.
2. On the **Scan Configurations** tab, select a configuration.

3. If the scan configuration is enforced against Computer Groups, remove all groups.
4. In the upper right, click **Delete**.
5. Confirm the deletion.

Managing patches

You can manage patches with patch lists and blacklists. *Patch lists* are groups of patches that can be applied on the targeted computer groups. *Blacklists* are groups of patches that are specifically excluded from being downloaded or deployed to the targeted computer groups.

Patch list rules

Although you can manually select patches to include in a patch list, it is more efficient to use rules to dynamically populate lists of patches. As patches are added to the Available Patches list, Tanium assesses those patches for inclusion on a list by comparing them to rules. You can create rules from customized conditions that define which part of the patch description to examine.

By default, superseded patches are not included when you configure a patch list. You can choose to include superseded patches when you create a rule. Consider including superseded patches if you want to install a specific superseded patch or if you want to see installed patches where a patch has been superseded.

Build conditions using one option from each condition field:

Table 6: Rule condition options

Condition	Available options
Column	• Title • Severity • Release Date • Bulletins • KB Articles • CVE
Type	• Contains • Equals • Does Not Contain • Release Date on or After • Release date on or Before
Expression	The search criteria used in the expression.

IMPORTANT: When a rule has more than one condition, the conditions are connected with the AND operand. Patches must meet both conditions to be included. When a list has multiple rules, the rules are connected with the OR operand, so patches that meet either rule are included on the list.

Create a patch list

Sort patches into manageable patch lists for use in deployments. You can add individual patches to the list or populate the list dynamically with rules.

1. In the Patch menu, click **Patch Lists**.
2. Click **Create Patch List**, name the list, and select an operating system.
3. Add patches.

Adding patches dynamically	Add patches manually
a. Click **Add Rule**. b. Name the rule. c. Select **Include superseded patches when applying rules** if you want to include these patches in your patch list. d. Select a **Comparison Column** and **Comparison Type**. e. Type in the expression to search. Searches are not case sensitive.	a. Click **Add Patches Manually**. b. Select the patches that you want. c. (Optional) Click the patch title to see the details in a new browser tab.

   You can get details about the patch, visibility into the results by computer group, and the associated lists.
4. Preview the changes.
5. Click **Create**.

To distribute the patches to endpoints, see Create a deployment to install patches on page 49.

Exclude patches with blacklists

A blacklist is a collection of patches that are prohibited from downloading or deploying to the targeted computer groups. You can add individual patches to the list or populate the list dynamically with rules. Unlike patch lists, you do not need to create a deployment to enforce a blacklist.

Tip: Blacklist patches with the Title containing either "Quality Rollup" or "Security Only" to avoid redundant patch deployments.

1. In the Patch menu, click **Blacklists**.
2. Click **Create Blacklist**, name the list, and select an operating system.
3. Add patches.

Adding patches dynamically	Adding patches manually
a. Click **Add Rule**. b. Name the rule. c. Superseded patches are automatically included in blacklists. d. Select a **Comparison Column** and **Comparison Type**. e. Type in the expression to search against. Searches are case-insensitive.	a. Click **Add Patches Manually**. b. Select the patches that you want. c. (Optional) Click the patch title to see the details in a new browser tab.

   You can get details about the patch, visibility into the results by computer group, and the associated lists.
4. Preview the changes.
5. Click **Create**.
6. On the Blacklist Details page, scroll down and select the targeted computer groups.

The Blacklist is distributed to the selected endpoints, blocking those patches.

Note: If an endpoint is brought online with a patch already installed that is blacklisted, the patch remains until it is uninstalled.

`yum.conf` exclusions for Red Hat and CentOS endpoints

If a Red Hat or CentOS endpoint has excluded packages in the `yum.conf` file, Patch honors those exclusions and will not install them.

Note: Tanium Patch blacklisting occurs on an Advisory basis. Because a Linux Advisory consists of a list of packages that need to be installed on Linux, a non-blacklisted Advisory might not be installed if it includes packages that are associated with a blacklisted Advisory.

Create lists from the Patches view

In addition to creating a list from the Patch Lists or Blacklists page, you can also select individual patches to build lists.

1. In the Patch menu, click **Patches**.
2. Select one or more patches.
3. From the **More** drop-down menu, select the list type.
4. Complete the list.

Edit a list

When a user changes an existing list, the changes become a new version of the list. With some basic changes, such as adding a rule for each new month, you can refine your patch testing and roll up changes without creating a new list.

1. In the Patch menu, click **Patch Lists** or **Blacklists**.
2. Click the list name.
3. Click **Edit**.

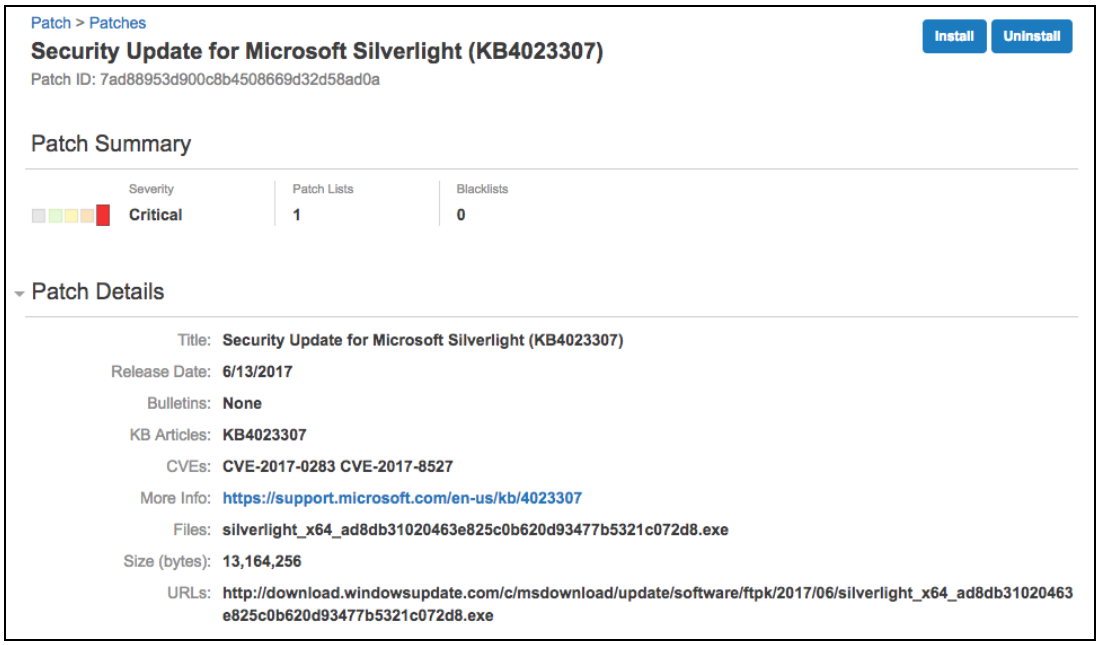
   > **Note:** You cannot edit a blacklist if the **Allow Blacklist Editing** option is disabled in the Patch settings.

4. Make your changes.
5. Preview the changes.
6. Click **Save**.

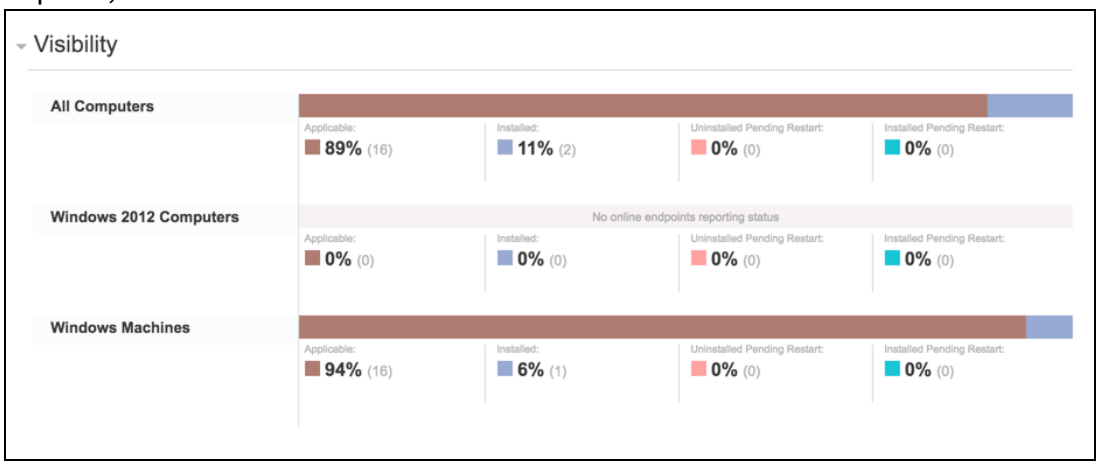
Check patch visibility

You can get details about the patch, the installation results by computer group, and the associated lists.

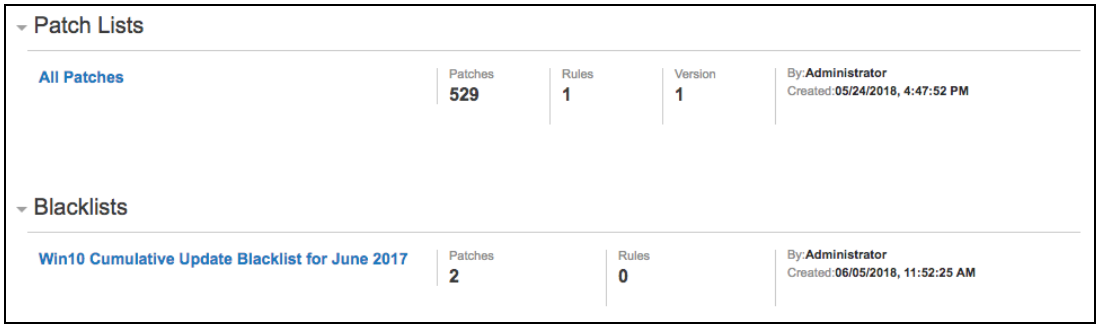
1. In the Patch menu, click **Patches**. To see only patches that are not installed, expand **Filter Results:** and select **Applicable** from the **Patches** drop-down menu.
2. Click the patch name.
3. Expand the section you want to see.
   - **Patch Summary** shows the severity and the associated lists. **Patch Details** has release date, bulletins, KB articles, CVEs, files, size, URLs, and a link to Microsoft support.



- **Visibility** splits out the patch results by computer group. To see results by endpoint, hover over the name and click the Interact icon.



- **Patch Lists** and **Blacklists** are summaries that include the number of patches on the list, rules, version, and creation details.



Export a list

You can facilitate the migration of patch content by exporting lists. The exported file includes rules manually added patches. This is particularly useful in progressive deployment models where patches must be moved from a testing environment to a production environment.

1. In the Patch menu, click **Patch Lists** or **Blacklists**.
2. Click the list name.
3. (Optional) Select the version.
4. Click Export .

The JSON file is available in your downloads folder. The file name is the list identifier, the actual list name appears after import.

Import a list

You can import an exported list into a new environment. The import contains the latest version of the list and the version is set to 1 in the new environment.

> **Note:** You cannot import a list with the same name as an existing list.

1. In the Patch menu, click **Patch Lists** or **Blacklists**.

   > **IMPORTANT:** Take care to only import the list as the right type.

2. Click Import .
3. Browse to the list JSON file.
4. Click **Import**.

Delete a list

Deleting a list does not delete patches, it only deletes the assembled list and any previous versions.

> **Note:** Remove computer group enforcements before deleting a blacklist.

1. In the Patch menu, click **Patch Lists** or **Blacklists**.
2. Select the list name.

3. Click **Delete**.
4. On the confirmation window, click **Delete**.

Add a custom Patch field

You can add a custom field to your patches based on a mapping that you provide in a CSV file. You might use this custom field to override the severity of a patch.

1. From the Patch home page, click Settings and then click **Custom Field**.
2. Click **Choose File** and add the CSV file.
3. The Custom Column shows up in your patch list views.

Example CSV

The following example maps the Vendor KB value to a new custom value.

```
KB,IAVM
KB829438,1234-A-0016
KB822362,1234-A-0016
kb828037,1234-A-0017
```

Deploying patches

Use deployments to install or uninstall patches on a set of target computers. Deployments can run once, or be ongoing to maintain operational hygiene for computers that come online after being offline.

Before you begin

- Organize the available patches into lists. See Create a patch list on page 43.
- If you want to notify the end users of your endpoints about the restarts that occur after patch installations, install the Tanium End-User Notification solution. See Install the Tanium End-User Notifications solution on page 24 and Endpoint restarts on page 51.

Create a deployment to install patches

Deployments download and install or uninstall patches on target computers. You can create a single deployment or set up ongoing deployments to ensure that offline endpoints are patched when they come online.

1. In the Patch menu, go to **Deployments > Installs**and click **New**.

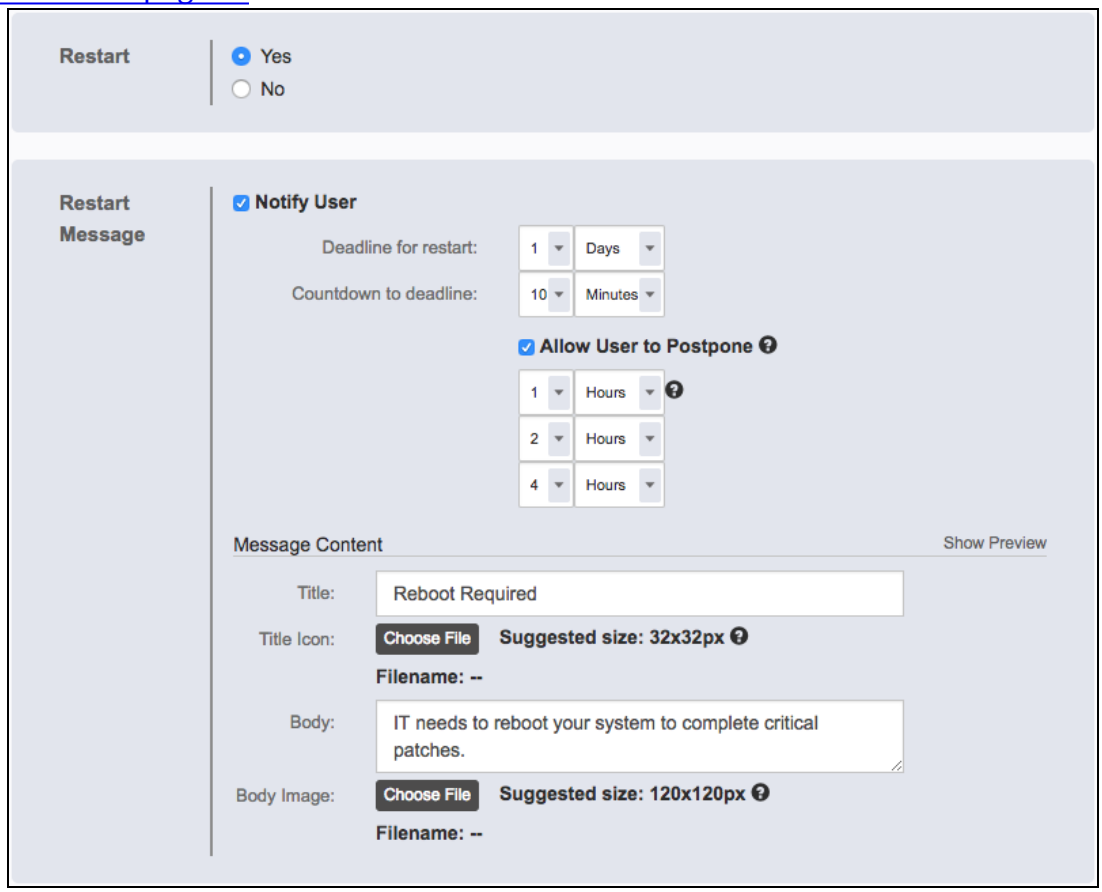
   Tip: You can also create a deployment from the Patches view. Select a group of patches and click **Install**.

2. Name the deployment and select an operating system.
3. Select deployment options.
   a. Designate the deployment times and repetition pattern.
      You can choose from your browser time or local time on the endpoint.
   b. Choose whether you want to base this deployment on a deployment template. To create a new deployment template based on this template, select **Create Deployment Template**. For more information, see Create a deployment template on page 59.
   c. 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.
   d. If you want the endpoints to download the patch content before the installation time, select **Download immediately**.

e. To minimize concurrent CPU utilization and disk input/output, select **Distribute over time** and indicate the time.

f. If you want to ignore patching restrictions, select **Override Blacklists** or **Override Maintenance Windows**.

g. Select whether to restart the endpoint. For more information, see Endpoint restarts on page 51.



h. If you enabled endpoint restarts, you can enable end user notifications about the restarts. Select **Notify User**. You can then configure settings that allow the user to postpone the restart. You also must configure the **Message Content** that informs the user about the restart. To preview the window that displays the message and postponement options, click **Show Preview**.

4. Add one or more patch lists, including version, or add patches manually.
5. Add targets.

   Select any or all of the following targeting methods. Click **Add Target**, and complete the fields as needed:

- **By Computer Group** provides a drop-down list of all filter-based computer groups. These groups can be included or excluded from patch applicability results, as needed.

  > **Note:** Computer group targeting is not available for manually created groups.

- **By Targeting Question** filters on all endpoints with a specific set of criteria and within the limiting groups selected from the drop-down menu of available groups. For example, you can type `Computer Name containing win` to target all Windows endpoints within those groups. The deployment is applied to all endpoints that meet the criteria. Individual rows cannot be selected. If you define multiple limiting groups, they are evaluated with an OR operator.
- **By Computer Names** uses the exact name, such as the FQDN, registered with Tanium. Typed in manually, separated by commas, or uploaded as a CSV file, targeting should be limited to 100 names or less to reduce the impact on the All Computers group.

6. Preview the changes.
7. Click **Deploy**.

To change the number of retries for each phase of a deployment, see Adjust the deployment retries on page 59.

Endpoint restarts

Patch can trigger a restart of any 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.
- 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:

  Deadline for restart

  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.

  Countdown to deadline

Specify the amount of time in minutes 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.

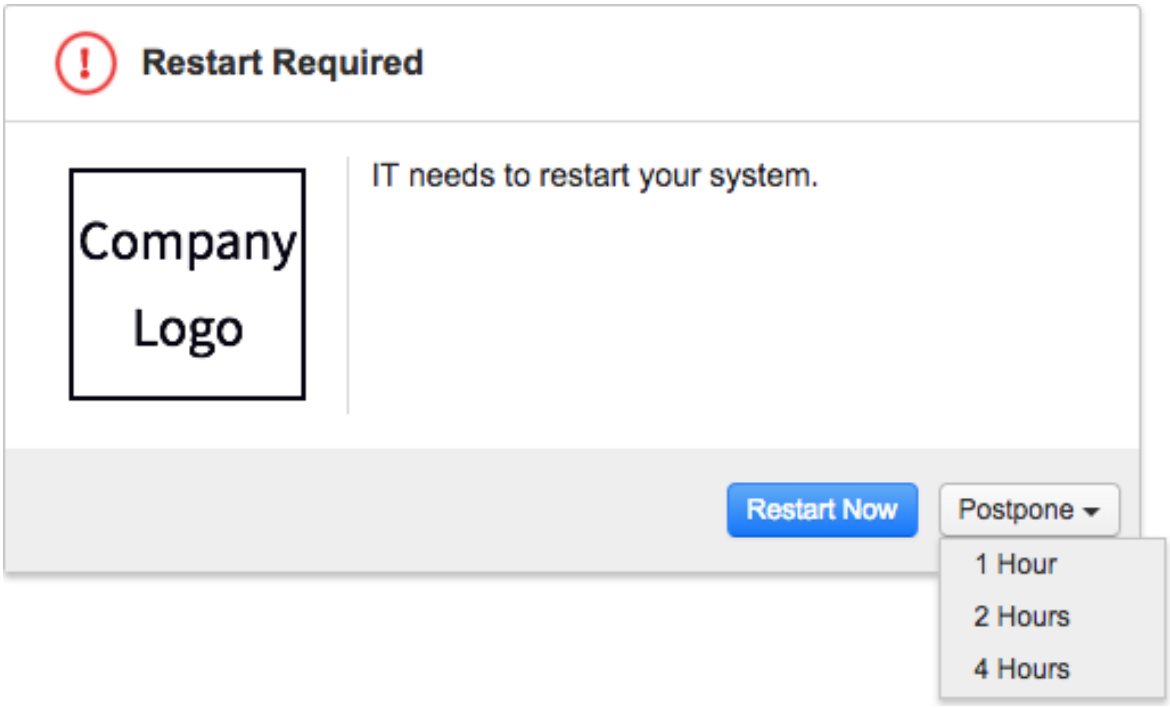
User Postponement Options

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

Message Content

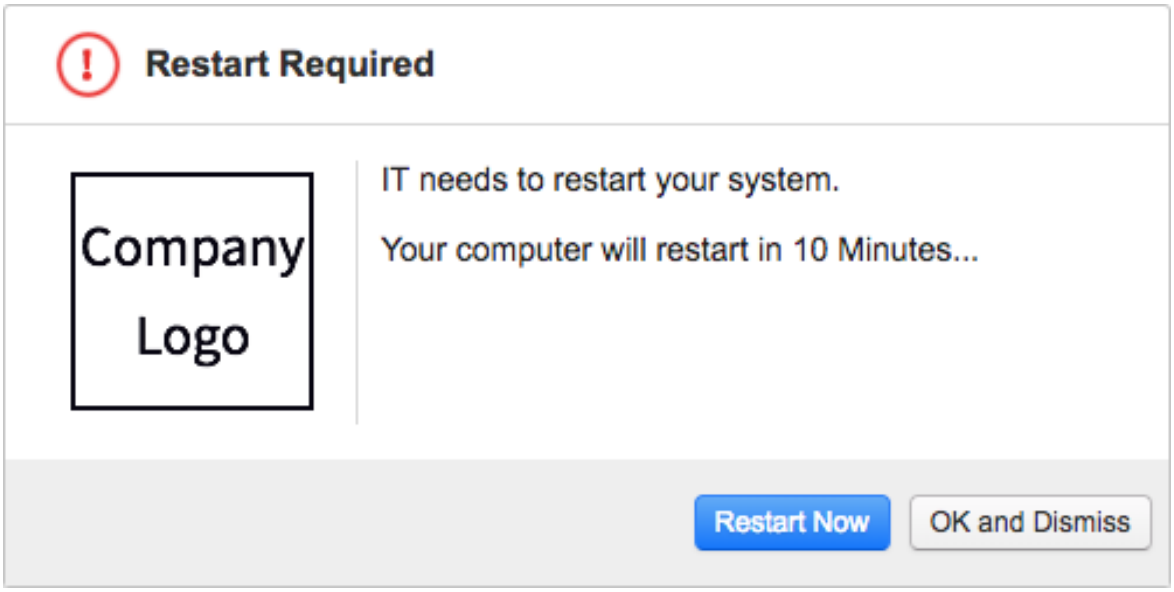
Specify the title and body of the notification message. Upload optional icon and body images for branding to avoid confusing users and to limit support calls. Click **Show Preview** to preview the notifications.

This message is configurable, and might look like the following example:



After the deadline for restart passes, the user gets a message that they cannot

postpone:



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

IMPORTANT: If your deployment is configured for a notification, but the client does NOT have the End User Notifications Tools installed, the endpoint will install the updates, but will NOT restart. You will see a status message in the Patch workbench about the missing tools.

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

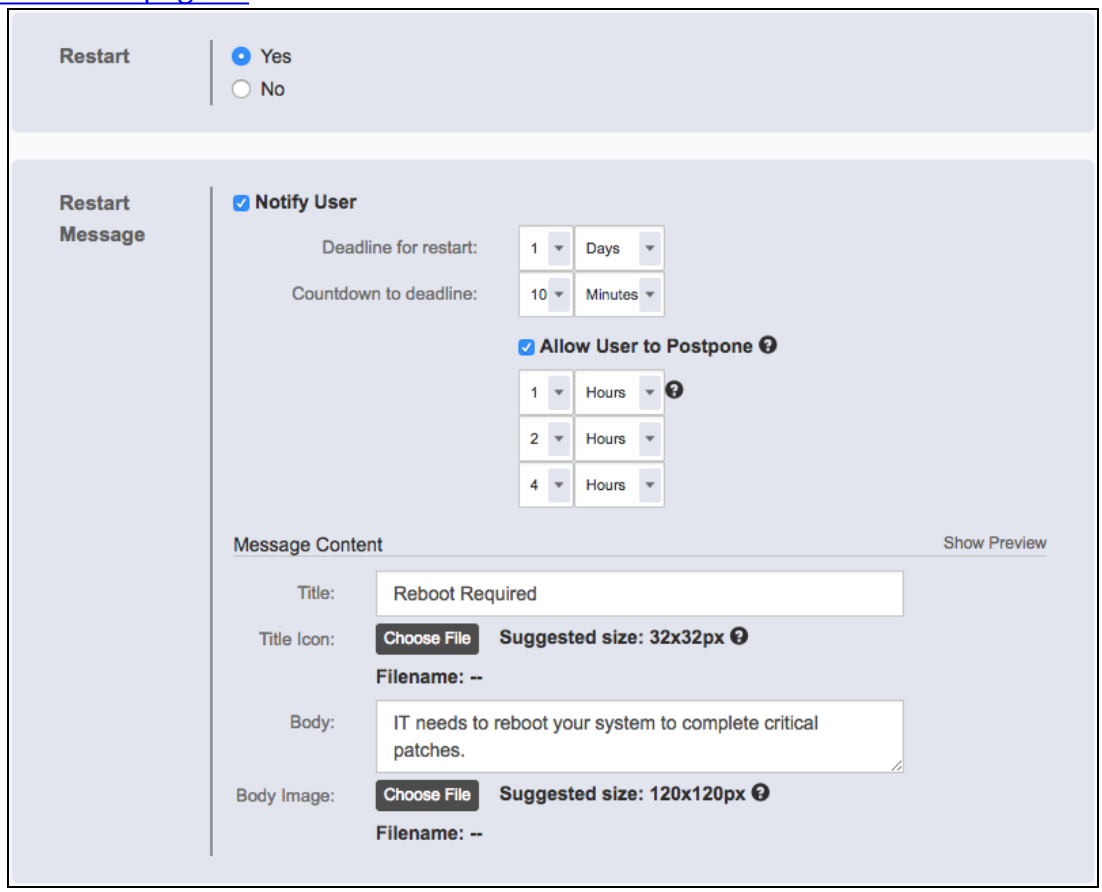
Create a deployment to uninstall patches

You can uninstall any patch deployment that was started from Tanium Patch.

1. In the Patch menu, go to **Deployments > Uninstalls** and click **New**.
2. Name the deployment and select an operating system.

3. Select the deployment options.
    a. Designate the deployment times.

       You can choose from your browser time or local time on the endpoint.
    b. Choose whether you want to base this deployment on a deployment template. To create a new deployment template based on this template, select **Create Deployment Template**. For more information, see Create a deployment template on page 59.
    c. To minimize concurrent CPU utilization and disk input/output, select **Distribute over time** and indicate the time.
    d. If you want to ignore patching restrictions, select **Override Maintenance Windows**.
    e. Select whether the endpoint must restart. For more information, see Endpoint restarts on page 51.



    f. If you enabled endpoint restarts, you can enable end user notifications about the restarts. Select **Notify User**. You can then configure settings that allow the user to postpone the restart. You also must configure the **Message Content**

that informs the user about the restart. To preview the window that displays the message and postponement options, click **Show Preview**.

4. Add one or more patches.

   > **Note:** The applicability count in the grid is for endpoints that do not have the patch installed.

5. Add targets.

   Select any or all of the following targeting methods. Click **Add Target**, and complete the fields as needed:

   - **By Computer Group** provides a drop-down list of all filter-based computer groups. These groups can be included or excluded from patch applicability results, as needed.

     > **Note:** Computer group targeting is not available for manually created groups.

   - **By Targeting Question** filters on all endpoints with a specific set of criteria and within the limiting groups selected from the drop-down menu of available groups. For example, you can type `Computer Name containing win` to target all Windows endpoints within those groups. The deployment is applied to all endpoints that meet the criteria. Individual rows cannot be selected. If you define multiple limiting groups, they are evaluated with an OR operator.
   - **By Computer Names** uses the exact name, such as the FQDN, registered with Tanium. Typed in manually, separated by commas, or uploaded as a CSV file, targeting should be limited to 100 names or less to reduce the impact on the All Computers group.

6. Preview the changes.
7. Click **Deploy**.

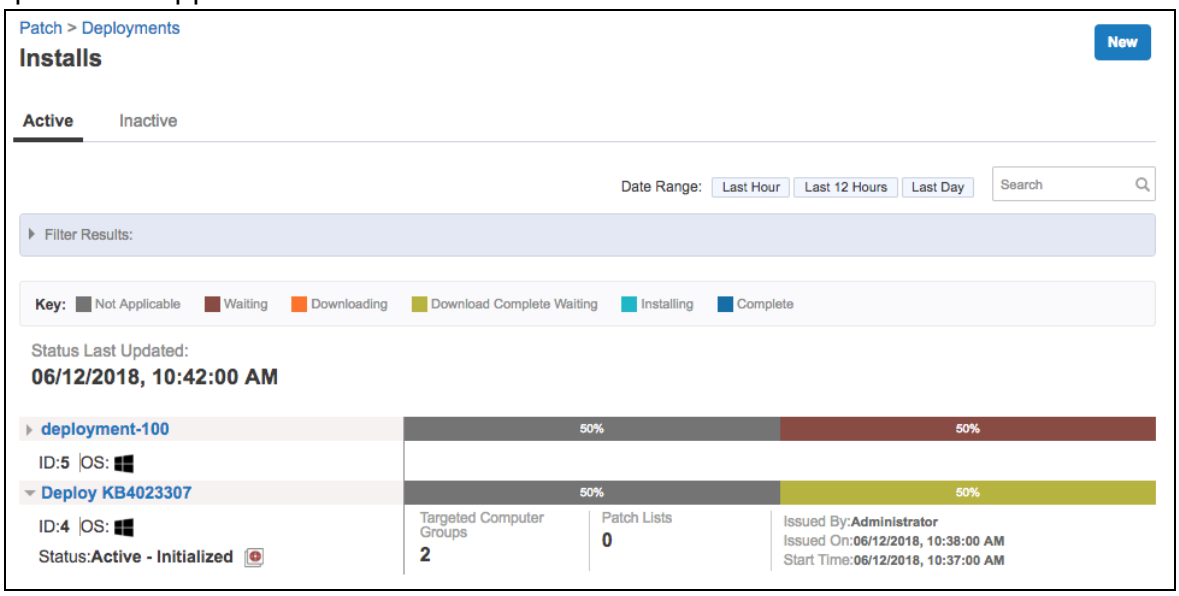
Review deployment summary

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

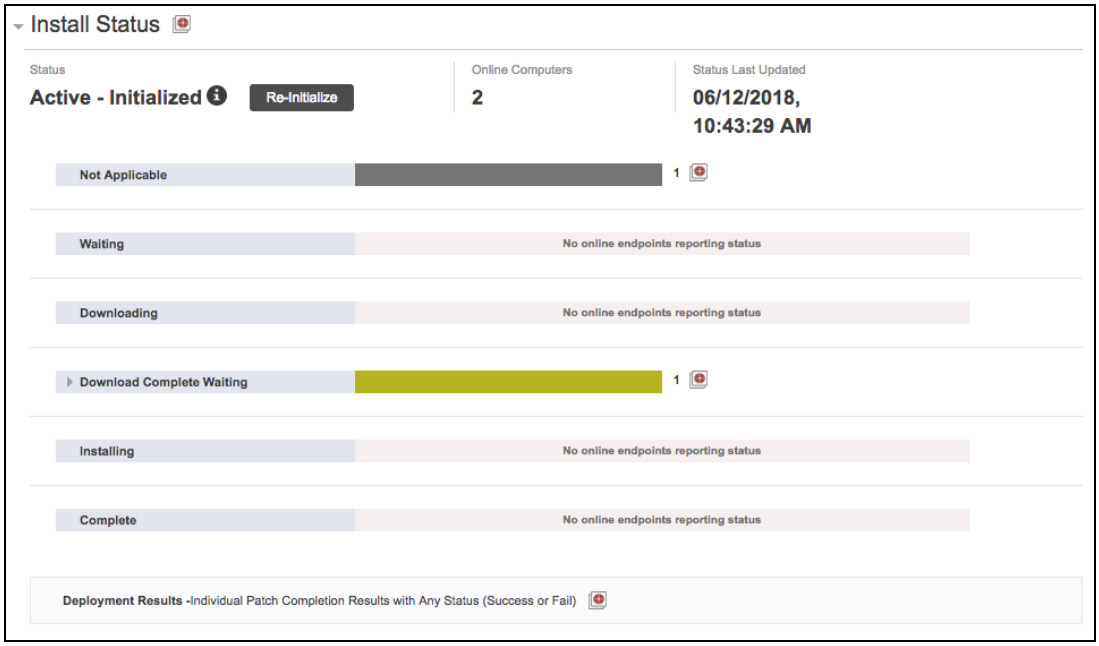
1. In the Patch menu, click **Deployments**.
2. Select **Installs** or **Uninstalls**.

3. Select either the **Active** or **Inactive** tab.

   Expand the sections to see summary information about the deployment, such as the number of targets, lists, issue details. For inactive deployments, it includes either expired or stopped.



4. Click the deployment name.
5. Expand the section you want to see.
   - **Install Summary** shows the OS, list count, number of patches, and number of targeted computer groups.
   - **Install Results** has the install status, number of online endpoints, and the date and time of the last status update.



The results are split out by status, expanding a status provides more information and the Interact icon to see the results by endpoint.

- **Error Messages** include the patch list or blacklist number, a brief description, the error number, the count of affected machines, and the Interact icon to drill down.

  If no list number is provided, it indicates a general issue.
- **Deployment Details** provides all the configuration information.
- **Targeted Computer Groups** lists the targeted computer groups for the deployment.

Add targets to an existing deployment

You can add more targets to a deployment. For example, you can limit patch testing to a select computer group and then roll it out to more groups after it has been validated. All other deployment options remain the same and deployment results from the previous Install deployments are preserved.

1. From the Patch menu, click **Deployments**.
2. Select **Installs** or **Uninstalls**.
3. Click the deployment name.
4. Under the Install Summary, click **Add**.
5. From the drop-down menu, select a computer group.
6. Click **Add**.

Reissue a deployment

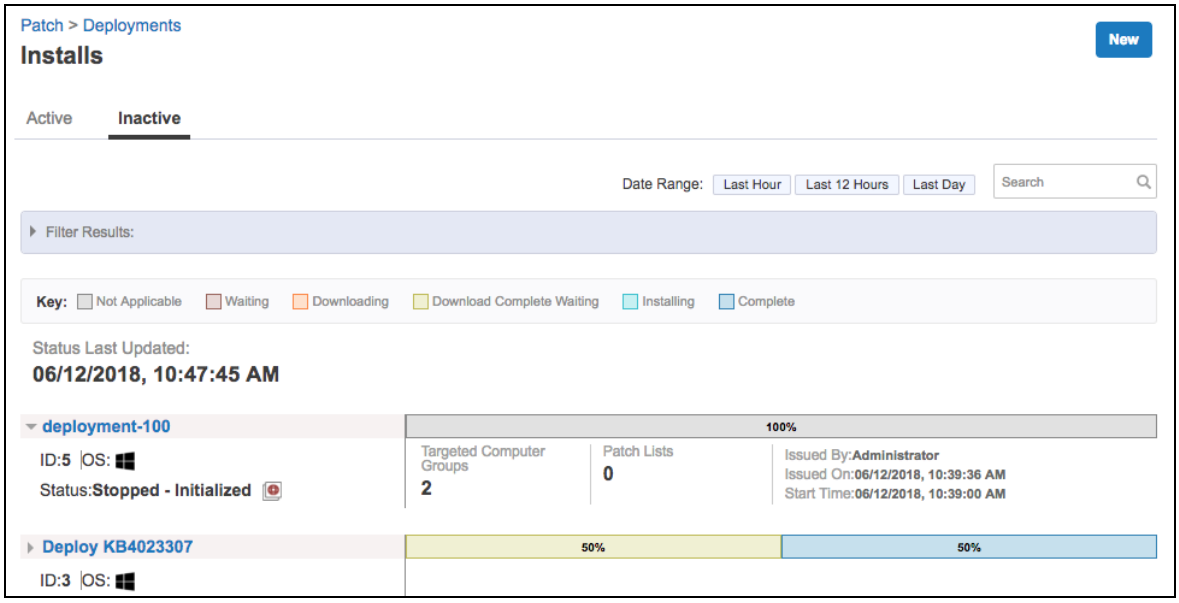
You can restart a stopped deployment or reissue a one-time deployment. Reissuing a deployment creates a new deployment with the same configuration and targets.

1. From the Patch menu, click **Deployments**.
2. On the Active tab, click the deployment name.
3. Click **Reissue**.
4. (Optional) Make any necessary changes.
5. Preview the changes.
6. Click **Deploy**.

Stop a deployment

You can stop a patch deployment. Stopping changes the deployment end time to now. It does not remove patches that have already completed installation.

1. In the Patch menu, click **Deployments**.
2. On the **Active** tab, click the deployment name.
3. Click **Stop**.
4. Go to the **Inactive** tab and click the deployment name to verify the status.



Adjust the deployment retries

You can change how many times Patch attempts each stage of a deployment. For example, with the default of five times, Patch tries to download the patches five times, install five times, and so on.

1. From the Patch home page, click Settings .
2. From the **Retry Limit** drop-down menu, select the number of retries.
   The default is five.
3. In the **Reset Frequency** field, type in the number of hours.
4. Click **Save**.

Create a deployment template

You can create an install or uninstall deployment template. This template saves 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 Patch menu, click **Deployment Templates**.
2. Click either **Install Template** or **Uninstall Template**.
3. Click **Create Template**, name the deployment template, and select an operating system.
4. Select deployment options. These options are the same as the options you can configure in an individual deployment.
5. Click **Save**.
6. You can use this template when you create a deployment.

Reference: Patch status

Deployment status

The following is a list of all possible deployment status groups and the sub-statuses. If there has been more than one attempt, the status might be appended with `- Retry #`, for example `Downloading - Retry 2`.

Status group	Sub-status
Waiting	• Waiting for Deployment Configuration File • Waiting for Deployment Start Time • Waiting for Maintenance Window • Waiting for Scan Configuration File
Downloading	• Downloading • Downloading - Retry • Download Complete, Waiting for Deployment Start Time • Download Complete, Waiting for Maintenance Window Configuration File • Download Complete, Waiting for Blacklist Configuration File • Download Complete, Waiting for Maintenance Window • Download Complete, Awaiting User Acceptance (this includes user-postponed restarts)
Installing	• Pre-Install Random Delay • Pre-Install Scan • Installing • Pending Restart, Waiting for Maintenance Window • Pending Restart, Waiting for Maintenance Window Configuration File • Pending Restart, Awaiting User Acceptance [this includes user has postponed] • Pending Restart, Missing End-User Notification Tools • Pending Restart, End-User Notification Unsupported • Post-Install Scan
Complete	• Complete, All Patches Applied / Complete, All Patches Removed • Complete, Some Patches Applied / Complete, Some Patches Removed (if you have exhausted your retries) • Error, No Patches Applied / Error, No Patches Removed • Error, Install Aborted / Error, Uninstall Aborted • Error, Deployment Ended Before Any Action Was Taken

Enforcement status

Status group	Sub-status
Blacklists and maintenance windows	• Enforced • Unenforced

Status group	Sub-status
Scan configurations	• Unenforced • Waiting For Initial Scan • Complete, Waiting For Next Scan • Downloading • Scanning

Setting Maintenance Windows

Maintenance windows control when patches can be applied to a computer group. A maintenance window is separate from the deployment start and end time. After a maintenance window is applied to a computer, that endpoint does not install patches or restart to complete patch installation, unless it is currently in an open maintenance window. To install a patch, the maintenance window must be open during the configured deployment time.

> **Note:** A maintenance window is different from a scan window. For more information about limiting scan activity to a designated scan window, see Scan windows on page 38.

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 patch 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

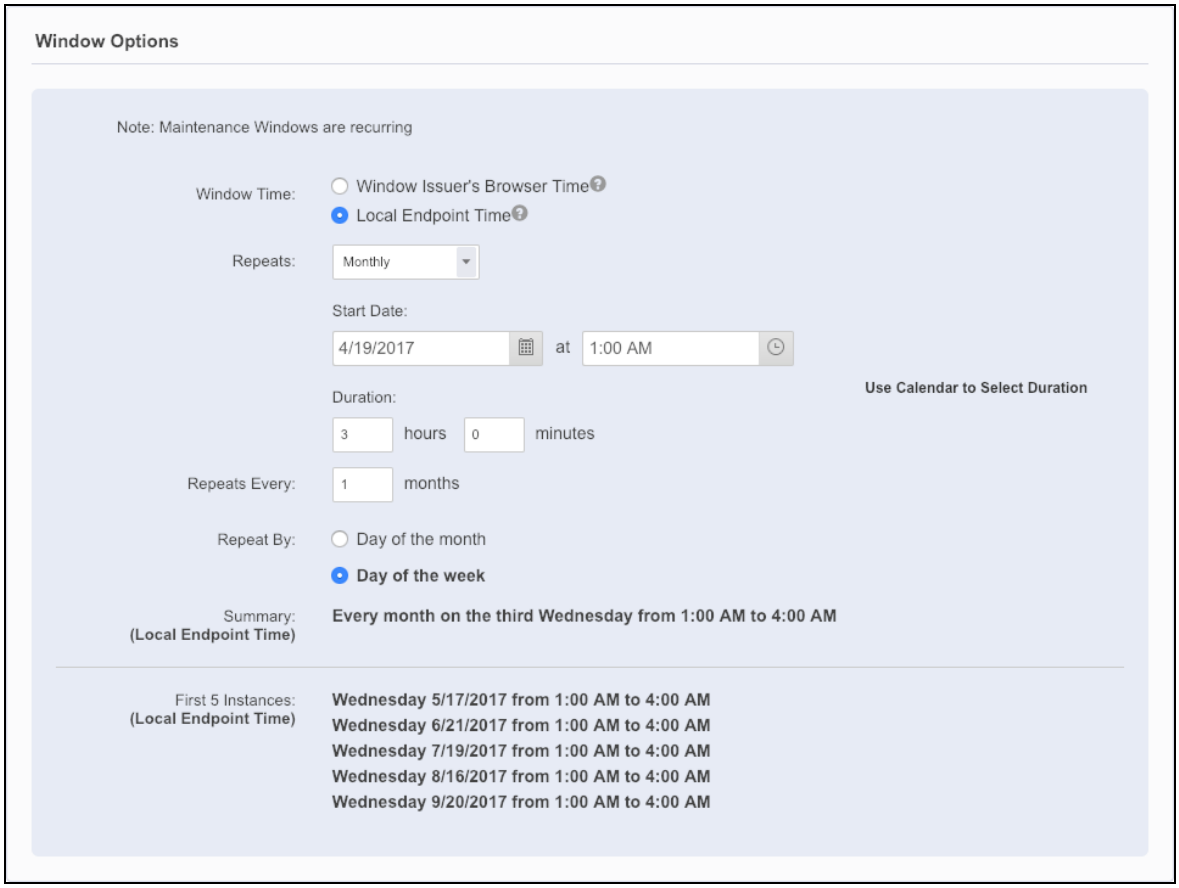
IMPORTANT: If a maintenance window does not repeat and it is the only one enforced against a computer group, patches cannot be applied after the window closes.

Create a maintenance window

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

1. In the Patch menu, click **Maintenance Windows**.
2. Click **Create Window**.
3. Name the window and select an operating system.
4. Choose from your browser time or local time on the endpoint.
5. Configure the window repetition.
    a. Select the repetition time frame.
    b. Set additional options, such as day of the week, day of the month, and how often the window repeats.

For example, to account for Patch Tuesday, you could use these settings for the Wednesday a week after patch updates are typically released by Microsoft.



6. 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.

7. Click **Create**.
8. Add one or more target computer groups.

Edit a maintenance window

1. In the Patch menu, click **Maintenance Windows**.
2. Select a window.

3. Click **Edit**.

   > **Note:** You cannot edit a maintenance window if the **Allow Maintenance Window Editing** option is disabled in the Patch settings.

4. Make your changes.
5. Preview the changes.
6. Click **Save**.

Override a maintenance window

You can apply a patch outside of a maintenance window by configuring the **Override Maintenance Windows** option during a patch deployment. For more information, see Deploying patches on page 49. Note that if you also choose to restart the endpoint in the deployment options, the endpoint restarts immediately after the patch is installed.

Delete a maintenance window

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

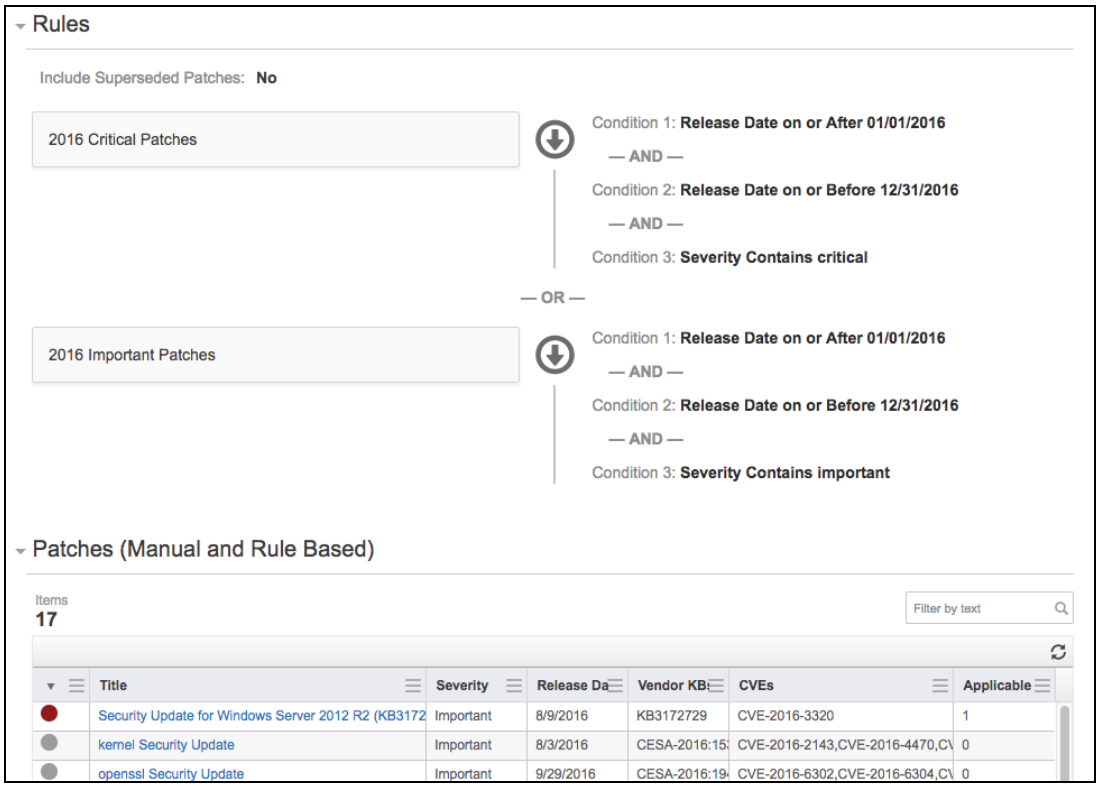
1. In the Patch menu, click **Maintenance Windows**.
2. Select a window.
3. If the window is enforced against computer groups, remove all groups.
4. In the upper right, click **Delete**.
5. Confirm the deletion.

Patch use cases

Example 1: Automatically deploy key 2016 patches

You can create a patch list that identifies all important and critical 2016 patches. A patch list like this is useful for targeting groups of endpoints even if you have already achieved a high level of patch compliance. Many organizations want newly added endpoints in an enterprise network to automatically receive patches. This helps achieve patch security compliance automatically and avoids compliance issues caused by out-of-date endpoints that appear on the network between patch audit reporting cycles.

1. Create a patch list with these settings:
    a. In the Rules section, create two rules with these conditions:
        - 2016 Critical Patches conditions
            - **Release Date**, **On or After**, `01/01/2016`
            - **Release Date**, **On or Before**, `12/31/2016`
            - **Severity**, **Contains**, `critical`
        - 2016 Important Patches conditions
            - **Release Date**, **On or After**, `01/01/2016`
            - **Release Date**, **On or Before**, `12/31/2016`
            - **Severity**, **Contains**, `important`



b. Target the applicable computer groups.

2. Install the patches with an ongoing deployment using the Patch List.

Any patches matching rule 1 or 2 are applied to the targeted computer groups. A catch-all patch list for previously released important and critical patches ensures that if a machine is brought online, even after a period of inactivity, that the policy is automatically applied.

For detailed steps, see Create a patch list on page 43 and Create a deployment to install patches on page 49.

Example 2: Create a blacklist that excludes .NET patches

Assume you have several servers in a computer group of application servers that run business critical applications. Since .NET patches can change the underlying framework of an endpoint, you want to make sure these servers do not receive a patch that could adversely affect the running applications.

Create a blacklist for .NET patches with these settings:

1. Create a rule with the conditions of **Patch Title**, **Contains**, `.NET`.
2. Target the computer group that contains the application servers.

For detailed steps, see Exclude patches with blacklists on page 43.

Example 3: Stagger patch deployment to a worldwide network

Assume that you have a network that spans multiple time zones and you can only patch endpoints during certain times to avoid interfering with core work hours.

1. If you want to monitor the results by time zone, create a computer group for each time zone.

   For example, you can use the question: `Time Zone containing "EST"` to create a filter-based computer group.
2. Create one maintenance window. Set it to Tanium Client local time, such as 1-4 A.M. and how often it should repeat.
3. Add the computer groups you want to target.
4. Create a deployment to install the patches and target the same computer groups.

The endpoints install the patches at the designated times when employees are not working. The deployment results are split out by time zone to get a global view of the installation success.

For detailed steps, see Tanium Core Platform User Guide: Managing computer groups, Create a maintenance window on page 63, and Create a deployment to install patches on page 49.

Example 4: Address the Wanna Cry vulnerability

As one of the known leverage points of the Wanna Cry (wcry) ransomware, the Microsoft SMBv1 legacy protocol vulnerability was addressed in the Microsoft Security Bulletin MS17-010. Typically, a recent scan with the latest CAB file should indicate the need for any additional patches. You can use Patch to verify which endpoints are missing these critical patches by creating a patch list and deploying it where needed.

1. (Optional) To get a count of affected endpoints in Interact, ask `Get Online from all machines with Applicable Patches matching "(.*4012598.*|.*4012212.*|.*4012215.*|.*4012213.*|.*4012216.*|.*4012214.*|.*4012217.*|.*4012606.*|.*4013198.*|.*4013429.*)"`.

   This question provides a list of endpoints that are vulnerable to the MS17-010 Security Bulletin.
2. If installation is needed, create a Patch list with one rule for each KB number using the conditions **KB Articles**, **Contains**, and these KB numbers as the expression:

OS version	Description	Patches to check
• Windows 10 • Windows 2016	Windows 10 and Windows 2016 use the latest cumulative update process. Deploying the March 2017 or later cumulative update should apply all necessary patches.	Windows 10 • KB4012606 • KB4013198 • KB4013429
		Windows 2016 - KB4013429
• Windows 7 • Windows 8.1 • Windows 2008 • Windows 2008R2 • Windows 2012 • Windows 2012R2	There are two methods available to update vulnerable systems. • **Method 1:** Deploy the March 2017 Security Only Quality Updates • **Method 2:** Deploy the March 2017 (or later) Security Monthly Quality Rollup	Windows Server 2008R2, Windows 7 • Method 1 – KB4012212 • Method 2 – KB4012215
		Windows Server 2012R2, Windows 8.1 • Method 1 – KB4012213 • Method 2 – KB4012216
		Windows 2012 • Method 1 – KB4012214 • Method 2 – KB4012217
		Windows Server 2008 SP2 - KB4012598 (Method 1 only)
• Windows XP • Windows 2003	Contact your TAM for assistance.	

Note: These must be individual rules so that they use the OR operand. We recommend using computer groups divided by operating system.

3. (Optional) Review the applicability counts for each computer group.
4. Install the patch lists with a deployment that includes restarting the endpoints.

   Tip: Consider making this an ongoing deployment to address endpoints that are currently offline.

5. When the deployment is done, go to the **Deployments > Installs** page and select your deployment.

6. Review the deployment status, expanding any section to display the count by sub-status.
7. If you need to drill down further, you can click the Interact icon to see the results by computer name.

For more information on using other Tanium Modules to mitigate WannaCry, see the Tanium Tech Blog: “WannaCry” / “wcry” Ransomware Outbreak: How Tanium Can Help.

Troubleshooting Patch

If Patch is not performing as expected, you might need to do some troubleshooting or change settings. You can also contact your TAM for assistance.

Collect a troubleshooting package

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

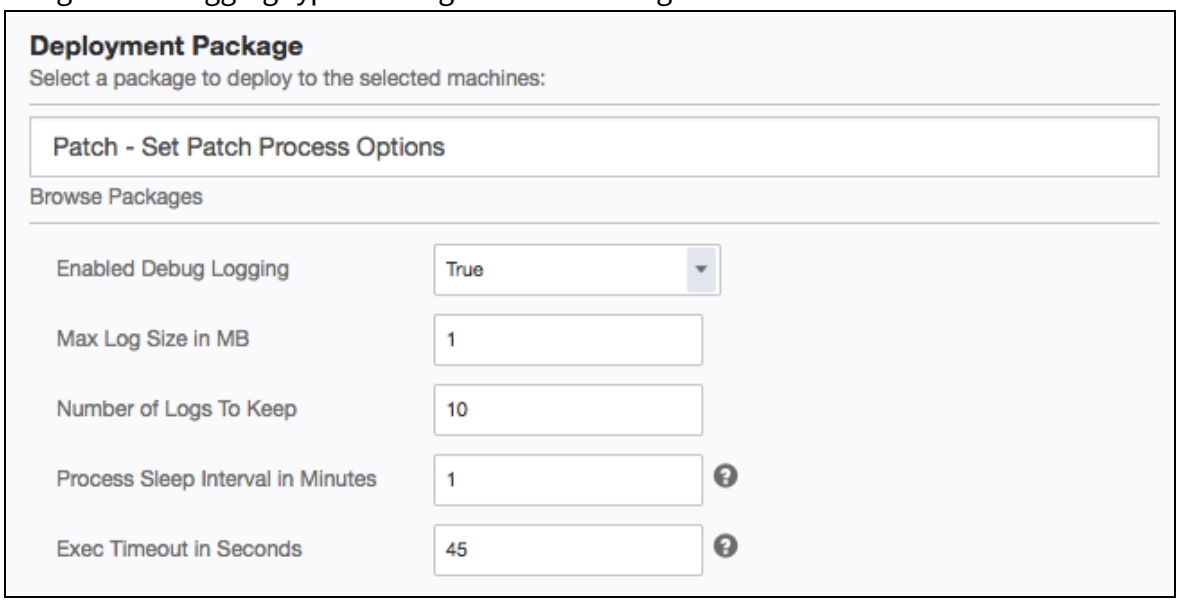
1. Get the Patch log.
   a. On the Patch home page, click Help.
   b. Click **Collect Troubleshooting Package**.

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

Configure endpoint logging

Distribute the **Patch - Set Patch Process Options** package to your endpoints to change the default logging type and log rotation settings.

1. Target the systems on which you want to configure logging.
2. Click **Deploy Action**. Select the **Patch - Set Patch Process Options** package.
3. Configure the logging type and log rotation settings.



By default, a new log is created when the log size reaches 1 MB. For example, you might have `patch0.log`, `patch1.log`, `patch2.log`, and so on, up to 10 log files.

Patches are not listed in the Patches view

If you are having difficulty getting patches to appear:

1. Verify that the **Patch - Is Process Running** sensor returns `Yes` for your endpoints.
2. Check the scheduled actions for Patch.
   a. From the Main menu, click **Actions > Scheduled Actions**.
   b. In the Action Groups pane, click **Patch**.
   c. Review the issue details of the **Patch - Ensure Patch Process** and **Patch - Distribute Deployment # (*name*)** actions.
3. Check the endpoint log at `\Tanium Client\Patch\patch`*x*`.log`.
4. For offline CAB file scan configurations, check that a CAB file is available at `\Tanium Client\Patch\Scans\Wsusscn2.cab`.
5. For WSUS or Microsoft Online scan configurations, check the `c:\Windows\WindowsUpdate.log` for details.
6. In the Scan Configuration, change the **Random Scan Delay** setting.

Scans are not completed on Linux endpoints

Patch 2.3.5 supports Red Hat and CentOS Linux endpoints. If you are having difficulty getting scans to run on Linux endpoints:

1. Verify that the **RedHat/CentOS Linux Support** option is enabled in the **Operating Systems** tab of the Patch Settings ⚙.
2. Verify that the **Patch - Is Process Running** sensor returns `Yes` for your Linux endpoints.
3. Verify that `repomd.xml` file can be reached by appending `/repodata/repomd.xml` to the configured **baseurl** value.
4. Check the endpoint log at `/opt/Tanium/TaniumClient/Tools/Patch/logs/scan-process.log` for errors.

Sensors return `Could not get results` on Linux endpoints

If your sensors return `Could not get results` on Linux endpoints, the Patch tools might not be installed on your Linux endpoints.

1. Verify that the **RedHat/CentOS Linux Support** option is enabled in the **Operating Systems** tab of the Patch Settings ⚙.
2. If the Patch tools are not installed on your Linux endpoints, the **Patch - Tools Version** sensor returns:
   ```
   Not Installed
   Linux Package Required
   ```
3. To install the Patch tools on your Linux endpoints, Initialize Patch on page 23.

Red Hat Linux endpoints stuck in `Waiting for Initial Scan` status

If you configure a scan that includes both **Red Hat Enterprise Linux 6 Server (RPMs)** and **Red Hat Enterprise Linux 7 Server (RPMs)** repositories, your targeted endpoints might appear to be stuck in the `Waiting for Initial Scan` status.

1. Verify that each major operating system is configured in separate scan configurations.
2. Target Linux endpoints by major operating systems.

Change the patch visibility aggregation

When a configuration scan is enforced against a computer group, a saved question is sent to the endpoints to check if a patch is applicable. This returns as an aggregate count in the Patch Visibility section. If you need to reduce the load on the Tanium Service or Client, you can limit which computer groups are included in the aggregation. Patch actions are still performed on all targeted endpoints; however, the applicability counts only include the selected computer groups.

1. On the Patch home page, click Settings ⚙.
2. From the **Computer Groups for Patch Visibility** grid, select the computer groups. The All Computers group is targeted by default, resulting in a single saved question that is necessary for Patch to function. Each additional computer group creates an additional saved question.

3. Click **Save**.

> **Note:** Only users with the administrator role can make changes to Patch settings.

> **Note:** Patch actions are still performed on all targeted endpoints; however, the applicability saved questions only include the selected computer groups.

Check and update the Windows Update Agent

You can use Tanium to check which Windows Update Agent versions are installed on your Windows endpoints.

1. In Interact, ask the `Get File Version["C:\Windows\System32\wuaueng.dll"] from all machines` question.
2. Update any below 6.1.0022.4. See the Microsoft article Updating the Windows Update Agent.

Uninstall Patch

If you need to uninstall Patch, first clean up the Patch artifacts on the endpoint and then uninstall Patch from the server.

1. Clean up patch artifacts from the endpoints.
   a. Use Interact to target endpoints. To get a list of endpoints that have Patch, you can ask the `Patch - Is Process Running` question.
   b. Click **Deploy Action**. Choose the **Patch - Clean Up Patch 2 Processes and Files** package.
   c. Check the status of the action on the **Actions > Action History** page.
2. Remove the Patch solution from the Tanium Module Server. From the Main menu, click **Tanium Solutions**.
   a. In the Patch section, click **Uninstall** and follow the process.
   b. Click **Proceed with Uninstall**.
   c. The uninstaller disables any actions and reissuing saved questions.
   d. Return to the Tanium Solutions page and verify that the **Import** button is available for Patch.
   If the Patch module has not updated in the console, refresh your browser.

Restore the state of the Patch database

You can import the `patch.db` file to restore the Patch configuration.

1. Stop the Patch service on the Tanium Module Server.
2. Copy your `patch.db` file into the `c:\Program Files\Tanium\Tanium Module Server\services\patch-service\` directory, replacing the existing file.
3. Restart the Patch service.
4. In the Tanium Console, refresh the Patch workbench.
5. Reset the service credentials. Click **Set your service account** and enter your user name and password.
6. Any existing data, including patch lists, deployments, and associated patches and actions are displayed in the Patch workbench.

   Note: If a deployment scheduled action is missing, you might need to wait up to 5 minutes for it to show up.