# Tanium™ Patch User Guide

Version 2.0.9

November 07, 2017

# Table of contents


**Patch overview** ..... **7**

Patch scanning options ..... 7

Patch lists and blacklists ..... 9

Superseded patches ..... 9

Microsoft update and servicing details ..... 9

Deployments ..... 10

Maintenance windows ..... 10

**Getting started with Patch** ..... **12**

**Patch requirements** ..... **13**

Tanium dependencies ..... 13

Tanium Server and Module Server computer resources ..... 13

Endpoint resource requirements ..... 13

Third-party software ..... 14

Host and network security requirements ..... 14

Security exclusions ..... 14

Internet URLs ..... 14

Console role requirements ..... 14

Tanium Server 7.0 ..... 14

Tanium Server 7.1 ..... 15

**Installing Patch** ..... **16**

Install Patch solution ..... 16

Set the service credentials ..... 16

Organize computer groups ..... 17

Add computer groups to Patch action group ..... 17
Upgrade the Patch version ..... 17
**Enforcing scan configurations ..... 19**
Offline CAB file ..... 19
Online to Microsoft Windows Update ..... 19
WSUS Scan ..... 19
Configure WSUS Scan ..... 20
Create a scan configuration ..... 20
View enforcement status ..... 21
Prioritize scan configurations ..... 21
Remove a scan enforcement ..... 22
Delete a scan configuration ..... 22
**Managing patches ..... 23**
Patch list rules ..... 23
Create a patch list ..... 24
Exclude patches with blacklists ..... 24
Create lists from the Patches view ..... 25
Edit a list ..... 26
Check patch visibility ..... 26
Export a list ..... 28
Import a list ..... 28
Delete a list ..... 28
**Deploying patches ..... 30**
Create a deployment to install patches ..... 30
Create a deployment to uninstall patches ..... 31

Create deployments from the Patches view ..... 33
Review deployment summary ..... 33
Add targets to an existing deployment ..... 34
Reissue a deployment ..... 35
Stop a deployment ..... 35
Adjust the deployment retries ..... 36
Reference: Patch deployment status ..... 36
**Setting maintenance windows ..... 38**
Maintenance window options ..... 38
Create a maintenance window ..... 38
Override a maintenance window ..... 40
Delete a maintenance window ..... 41
**Patch use cases ..... 42**
Example 1: Automatically deploy key 2016 patches ..... 42
Example 2: Create a blacklist that excludes .NET patches ..... 43
Example 3: Stagger patch deployment to a worldwide network ..... 44
Example 4: Address the Wanna Cry vulnerability ..... 44
**Troubleshooting Patch ..... 47**
Collect a troubleshooting package ..... 47
Configure endpoint logging ..... 47
Change the endpoint status report settings ..... 48
Patches are not listed in the Patches view ..... 48
Change the patch visibility aggregation ..... 49
Check and update the Windows Update Agent ..... 49
Uninstall Patch ..... 50

Restore the state of the Patch database ..... 50

# Patch overview

Use Patch to manage Windows 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.

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.

You can also 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 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 | Updates included | Client impact | Connectivity | Details |
|---|---|---|---|---|
| Offline CAB file | • Critical security patches<br>• Cumulative security and quality patches | Moderate, during scanning activity | The CAB file is stored locally by the Tanium Client. | • Requires 200+MB download of CAB file.<br>• Does not include routine updates, out of band fixes, hotfixes, and enhancements that are included with WSUS or Online to Microsoft scan methods. |
| Online to Microsoft | • Critical security patches<br>• Critical routine patches<br>• Cumulative security and quality patches<br>• Non-security and optional updates | • Moderate, during first scan<br>• Low, subsequent | The Tanium Client must contact Microsoft directly. | • Typically not allowed by company policy.<br>• Additional network traffic to Microsoft. |
| Windows Server Update Services (WSUS) Scan | • Critical security patches<br>• Critical routine patches<br>• Cumulative security and quality patches<br>• Non-security and optional updates | Low | The Tanium Client must contact the WSUS server. | • Must deploy and configure one or more WSUS servers.<br>• Updates must be approved in WSUS prior to scanning or deployment. |

**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 24 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.

## 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 16.
   If you are upgrading, see Upgrade the Patch version on page 17.
2. Create a scan configuration and add enforcements. See Enforcing scan configurations on page 19.
3. Organize the available patches. See Managing patches on page 23.
4. Install patches on endpoints. See Deploying patches on page 30.
5. Create patch restrictions. See Exclude patches with blacklists on page 24 or Setting maintenance windows on page 38.

# 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 | 6.5.314.4380 or later<br><br>Enhanced functionality is available with version 7.0.314.6319 and later. As part of this, we recommend installing Tanium Interact™ (Interact).<br><br>For role-based access control (RBAC), you must have Tanium Platform 7.1.314.3037 or later.<br><br>To support smart card authentication, including common access cards (CAC), see Tanium Core Platform Installation Guide: Smart card authentication. |
| Tanium Client | Patch is supported on Windows endpoints. We recommend using the Tanium Client 1540 and later. |

## Tanium Server and Module Server computer resources

Patch is installed and runs as a service on the Module Server host computer. The impact on Module Server is minimal and depends on usage. For more information, see Tanium Core Platform Installation Guide: Host computer sizing. 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.

## 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 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.

| Target device | Process |
|---|---|
| Module Server | `node.exe`<br>or<br>`"<Tanium Module Server directory>\services\patch\node.exe" service.js` |
| Endpoint computers | `tanium-Patch.min.vbs`<br>`wsusscn2.cab` |

### 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

## Console role requirements

### Tanium Server 7.0

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

**Table 2: Tanium 7.0 Patch Console Role Requirements**

| Privilege | 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 | ✅ | ✅ |
| Create, modify, or delete maintenance windows and enforce against computer groups | ✅ | ✅ |

## Tanium Server 7.1

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 3: Tanium 7.1 Patch User Role Privileges**

| Privilege | Patch Administrator | Patch User | Patch Read Only User |
|---|---|---|---|
| Patch Module Read | ✅ | ✅ | ✅ |
| Patch Module Write | ✅ | ✅ | ❌ |
| Patch Settings Write | ✅ | ❌ | ❌ |

# 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 credentials

For recurring maintenance activities, specify a Tanium user with administrator or content administrator permissions. Specifying these credentials is a one-time configuration. No other credentials need to be added.

1. From the Patch home page, under the Required Setup Steps, click the **Service Credential** link.
2. Enter the Tanium credentials and click **Initialize**.

## 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, click **Review the targeting or change it**.
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**.

## 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.

# 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 only. 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.

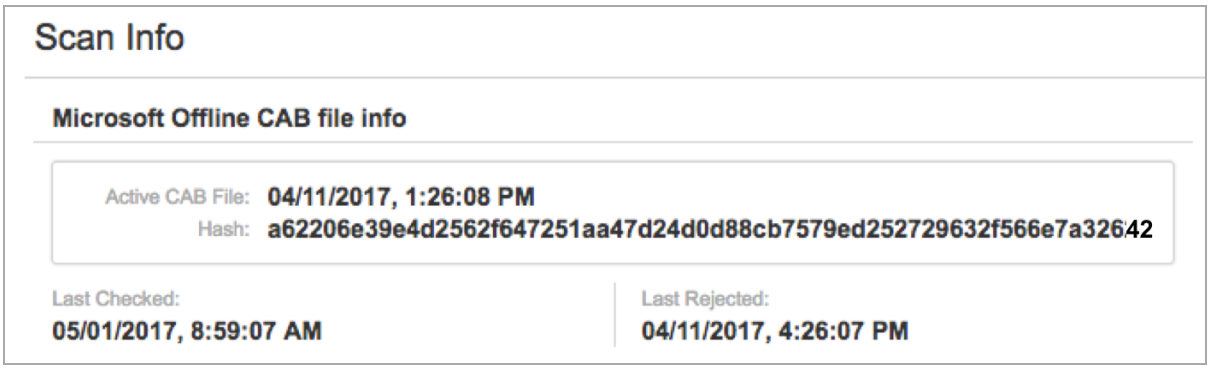



**Figure 1: Example CAB file status**

## Online to Microsoft Windows Update

Although this option creates additional network traffic between the Tanium Client and Microsoft, the full range of patches are available:

- 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, but requires additional changes. The Tanium Client must be able to contact the WSUS

server, and patches must be approved before they can be downloaded.

#### CONFIGURE WSUS SCAN

1. In the Tanium Console, add the WSUS Server URL to the whitelist as a regular expression.
    a. From the main menu, click **Administration > Whitelisted URLs**. Click **New URL Expression**.
    b. Enter the URL in the format:
    `http:\/\/wsusservername\.domain\.com\:port\/.*`.
    c. Enable the **Treat the above text as a regular expression** setting.
    d. Clear **Check for changes after setting** check box, disabling the setting. After you save the whitelist, this value displays as 999 days.
    e. (Tanium Server 7.1 and later) Use the default values for the **Expiration**. The default value is 7 days.
    f. Save your changes.
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**.
3. Choose the configuration options.
    a. Select a **Configuration Technique**.
    If you chose Offline CAB File, you can select **Scan upon new CAB file** to ensure that the endpoints are scanned whenever a CAB file is published. Selecting this setting overrides the frequency settings.
    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, we recommend a longer delay to reduce the impact of the scan on the host system.

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.

## 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**.

## 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 4: Rule condition options**

| Condition | Available options |
|---|---|
| Column | • Title<br>• Severity<br>• Release Date<br>• Bulletins<br>• KB Articles<br>• CVE |
| Type | • Contains<br>• Equals<br>• Does Not Contain<br>• Release Date on or After<br>• 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**.
3. Name the list.
4. Add patches.

| Adding patches dynamically | Add patches manually |
|---|---|
| a. Click **Add Rule**<br>b. Name the rule.<br>c. Select **Include superseded patches when applying rules** if you want to include these patches in your patch list.<br>d. Select a **Comparison Column** and **Comparison Type**.<br>e. Type in the expression to search. Searches are not case sensitive. | a. Click **Add Patches Manually**<br>b. Select the patches that you want.<br>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.
5. Preview the changes.
6. Click **Create**.

To distribute the patches to endpoints, see Create a deployment to install patches on page 30.

## 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:** We recommend blacklisting 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**.
3. Name the list.
4. Add patches.

| Adding patches dynamically | Adding patches manually |
| --- | --- |
| a. Click **Add Rule**<br>b. Name the rule.<br>c. Superseded patches are automatically included in blacklists.<br>d. Select a **Comparison Column** and **Comparison Type**.<br>e. Type in the expression to search against. Searches are case-insensitive. | a. Click **Add Patches Manually**<br>b. Select the patches that you want.<br>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.
5. Preview the changes.
6. Click **Create**.
7. 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.

## 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

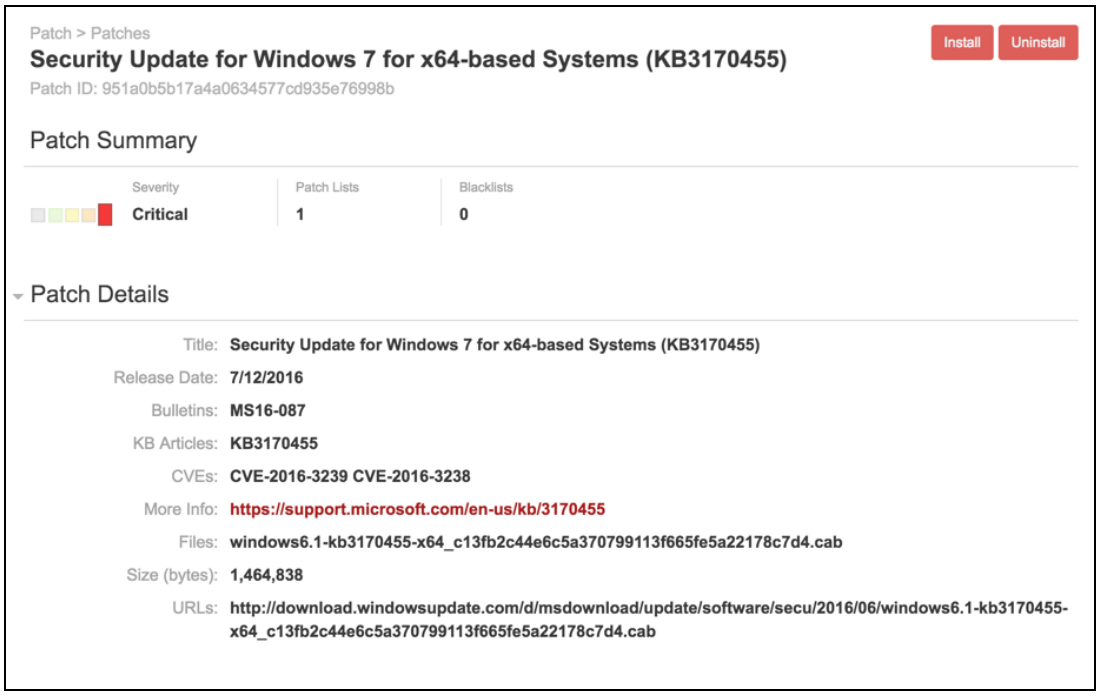
When a user changes an existing list, the changes become a new version of the list. With some basic changes, such as adding a rule for each new month, you can refine your patch testing and roll up changes without creating a new list.

1. In the Patch menu, click **Patch Lists** or **Blacklists**.
2. Click the list name.
3. Click **Edit**.
4. Make your changes.
5. Preview the changes.
6. Click **Save**.

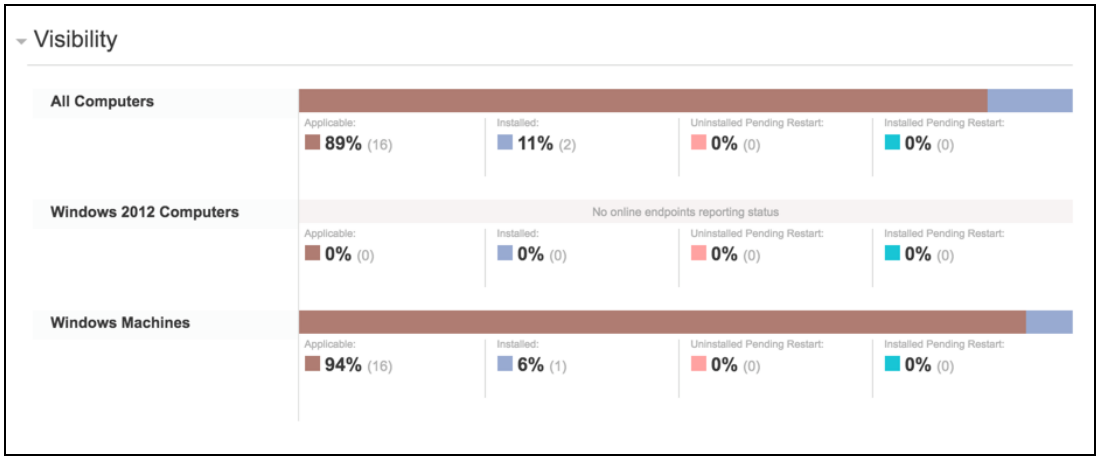
## Check patch visibility

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

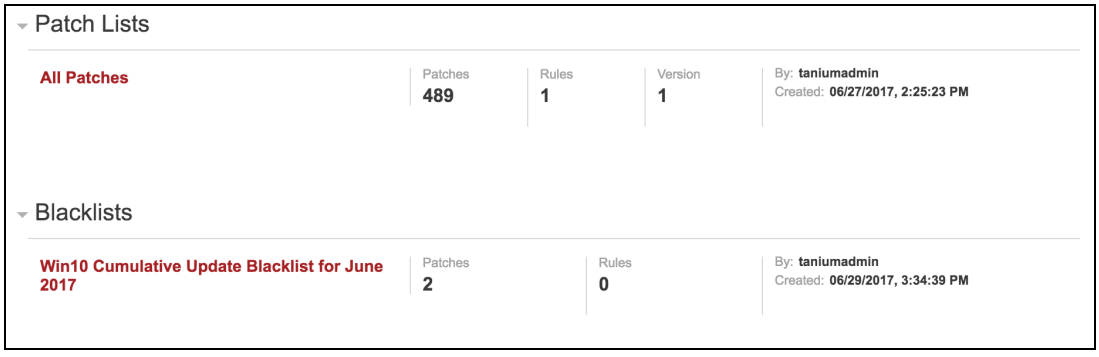
1. In the Patch menu, click **Patches**. To see only patches that are not installed, click **Applicable**.
2. Click the patch name.
3. Expand the section you want to see.
    - **Patch Summary** shows the severity and the associated lists. **Patch Details** has release date, bulletins, KB articles, CVEs, 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 a progressive deployment models where patches must be moved from a testing 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**.

# Deploying patches

After organizing the available patches into lists, deploy the lists to the target endpoints. These deployments can install or uninstall patches. Deployments can run once, or be ongoing to maintain operational hygiene for computers that come online after being offline.

## Create a deployment to install patches

With deployments, you can download and install patches to target computer groups. Create a single deployment or set up ongoing deployments to ensure that offline endpoints are addressed when the come online.

1. In the Patch menu, go to **Deployments > Installs**.
2. Click **New** and name the deployment.
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. If you want the endpoints to download the patch content before the installation time, select **Download immediately**.
    c. To reduce the network load, select **Distribute over time** and indicate the time.
    d. If you want to ignore patching restrictions, select **Override Blacklists** or **Override Maintenance Windows**.
    e. Select whether the endpoint must restart.

    > **IMPORTANT:** The end user of the endpoint does not receive any notification about restarts.

    > **IMPORTANT:** If you select the **Override Maintenance Windows** option and choose to restart the endpoint, the patch is applied immediately, but the endpoint does not restart until the maintenance window begins.
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. Use for single deployments only.

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

> **Tip:** If you want to reboot separately, you can create a deployment without patches that includes the restart setting.

To change the number of retries for each phase of a deployment, see Troubleshooting Patch on page 47 for more information.

## 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**.
2. Click **New**.
3. Name the deployment.

4. Select the deployment options you need.
    a. Designate the deployment times.
    You can choose from your browser time or local time on the endpoint.
    b. To reduce the network load, select **Distribute over time** and the time.
    c. If you want to ignore patching restrictions, select **Override Maintenance Windows**.
    d. Select whether the endpoint must restart.

    > **IMPORTANT:** There is no end user notification for restarts.

5. Add one or more patches.

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

6. 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.
    - **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. Use for single deployments only.
7. Preview the changes.
8. Click **Deploy**.

## Create deployments from the Patches view

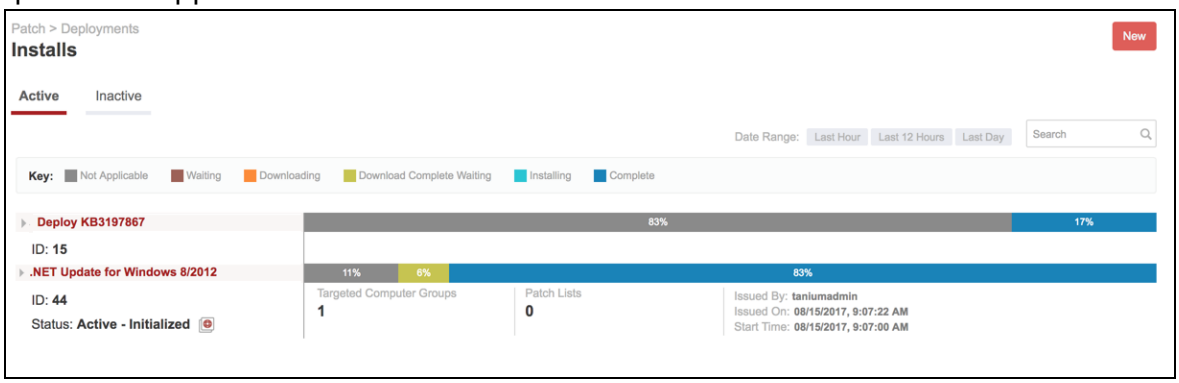
In addition to deploying patches from the Deployments page, you can also select individual patches to build them.

1. In the Patch menu, click **Patches**.
2. Select one or more patches.
3. Select **Install** or **Uninstall**.
4. Complete the deployment.

## 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.
   - **Summary** shows the list count, number of patches, and number of targeted Computer Groups.

- **Install Status** has the install status, number of online endpoints.


  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.
- **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.

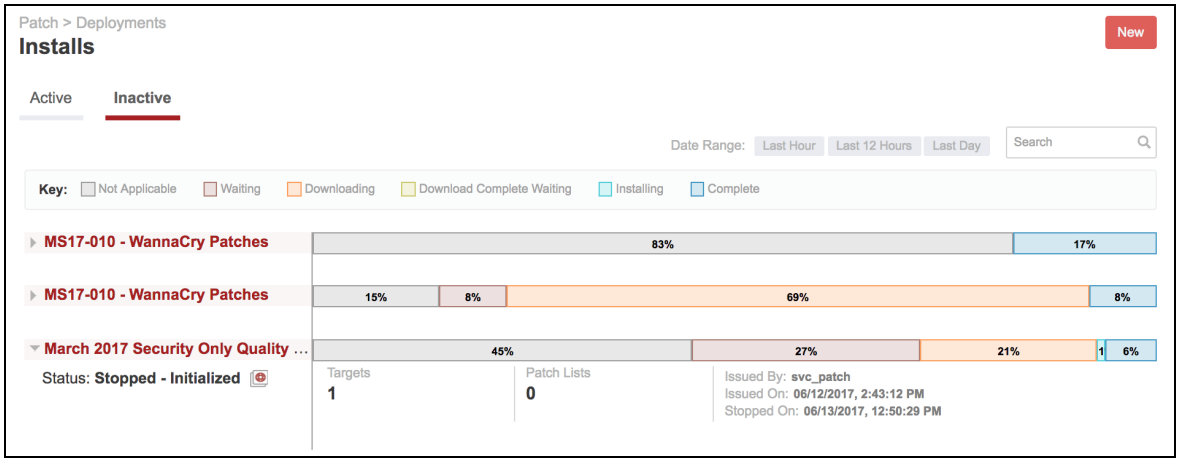
1. From the Patch menu, click **Deployments**.
2. On the Active tab, click the deployment name.
3. Click **Reissue**.
4. (Optional) Make any necessary changes.
5. Preview the changes.
6. Click **Deploy**.

## 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, etc.

1. On the 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**.

## Reference: Patch 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 Start Time<br>• Waiting for Maintenance Window |

| Status group | Sub-status |
| --- | --- |
| Downloading | • Downloading<br>• Downloading<br>• Download Complete Waiting<br>• Download Complete, Waiting for Deployment Start Time<br>• Download Complete, Waiting for Maintenance Window |
| Installing | • Pre-Install Scan<br>• Installing<br>• Pending Restart<br>• Post-Install Scan |
| Complete | • Complete, All Patches Applied / Removed<br>• Complete, Some Patches Applied / Removed<br>• Error, No Patches Applied / Removed<br>• Error, Install / Uninstall Aborted |

# 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. To install a patch, the maintenance window must be open and it must be during the configured the deployment time.

## 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

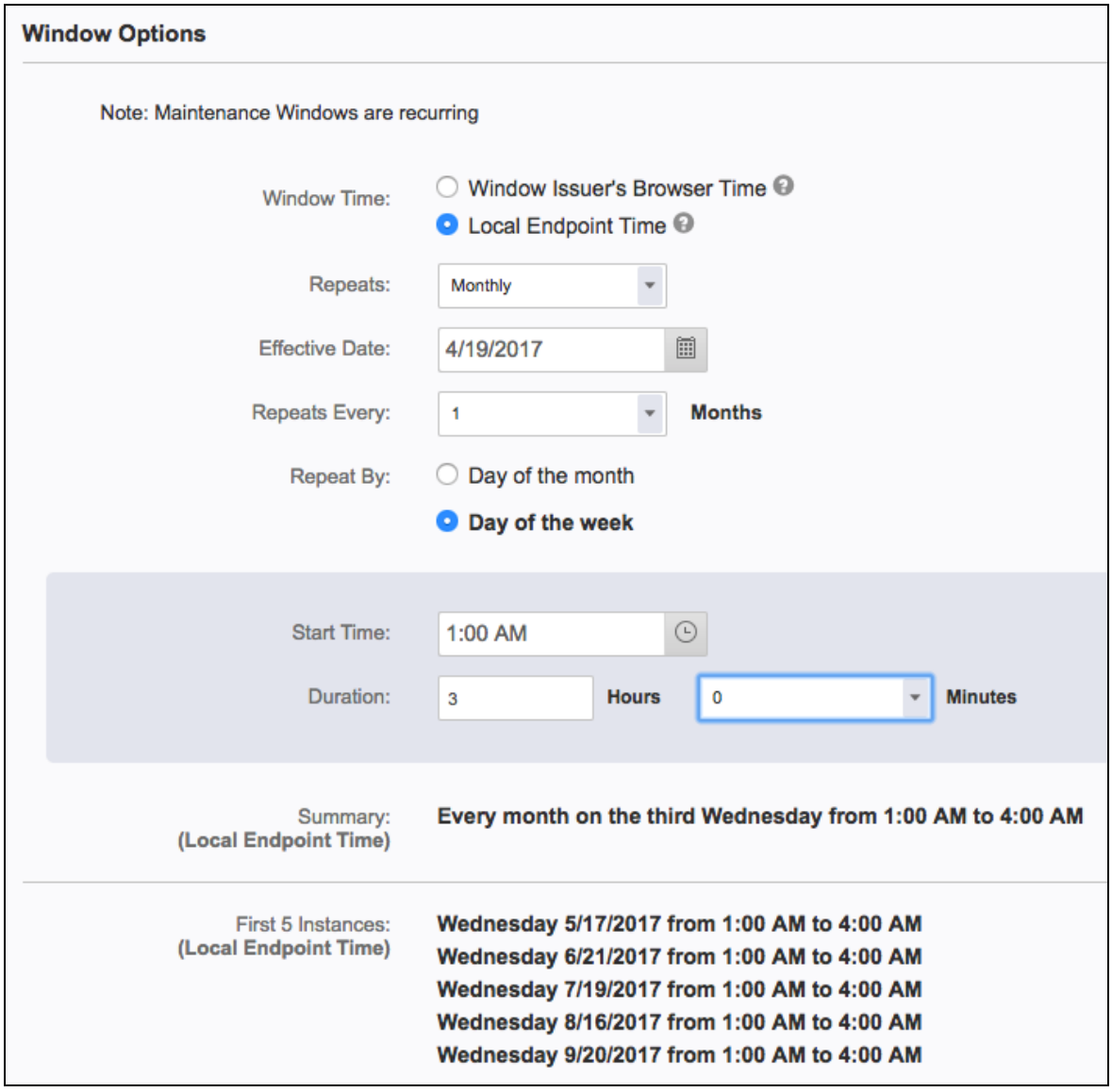
patches during periods of low network activity or outside of core working hours.

1. In the Patch menu, click **Maintenance Windows**.
2. Click **Create Window**.
3. Name the window.
4. Choose from your browser time or local time on the endpoint.
5. Use the date and time pickers to set the start and end time of the window.
6. Configure the window repetition.
    a. Select the repetition time frame.

    > **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.

    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.




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

## Override a maintenance window

You can apply a patch during a maintenance window by configuring the **Override Maintenance Windows** option during a patch deployment. For more information, see Deploying patches on page 30. Note that if you also choose to restart the endpoint in the deployment options, the endpoint does not restart until the maintenance window begins.

## Delete a maintenance window

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

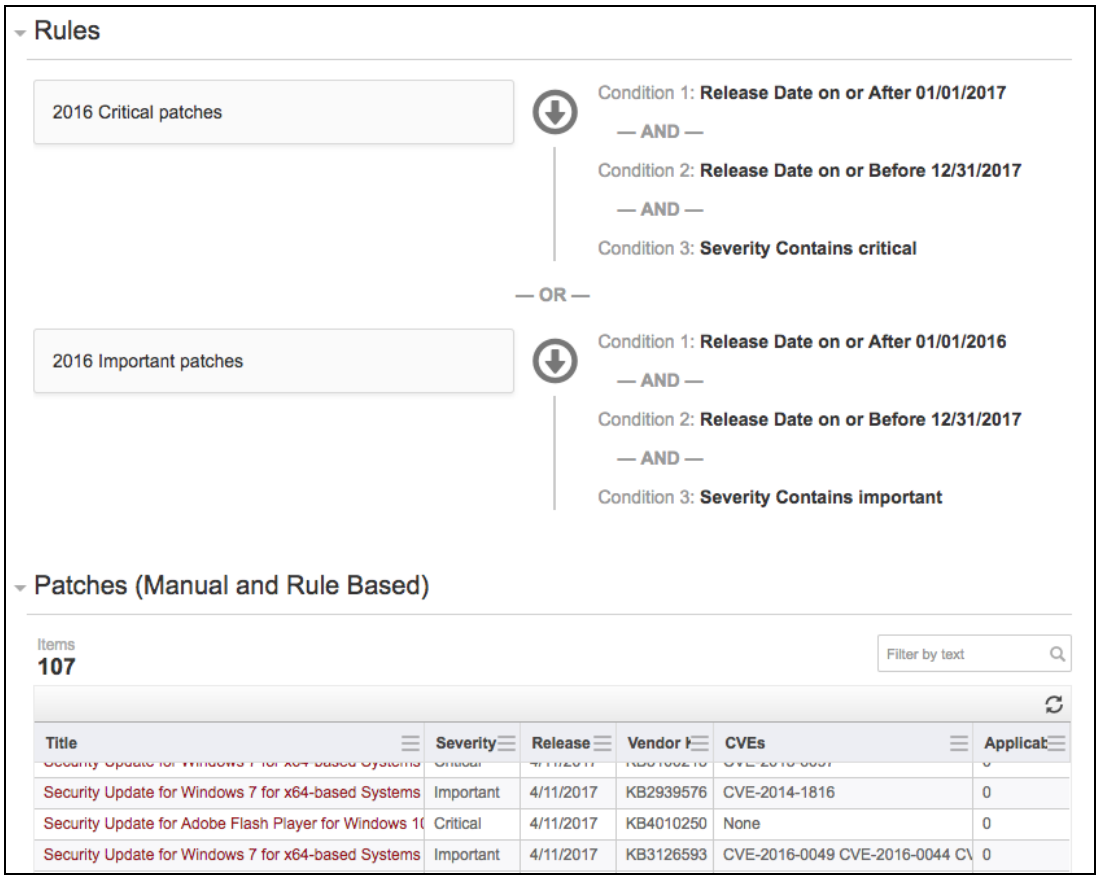
1. In the Patch menu, click **Maintenance Windows**.
2. Select a window.
3. If the window is enforced against computer groups, remove all groups.
4. In the upper right, click **Delete**.
5. Confirm the deletion.

# 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:
        - Rule A conditions
            - **Release Date**, **On or After**, `01/01/2016`
            - **Release Date**, **On or Before**, `12/31/2016`
            - **Patch Severity**, **Contains**, `critical`.
        - Rule B conditions
            - **Release Date**, **On or After**, `01/01/2016`
            - **Release Date**, **On or Before**, `12/31/2016`
            - **Patch 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 and Create a deployment to install patches.

## 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 a Blacklist.

## 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, and Create a deployment to install patches.

## 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<br>• 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<br>• KB4012606<br>• KB4013198<br>• KB4013429 |
| | | Windows 2016 - KB4013429 |
| • Windows 7<br>• Windows 8.1<br>• Windows 2008<br>• Windows 2008R2<br>• Windows 2012<br>• Windows 2012R2 | There are two methods available to update vulnerable systems.<br>• **Method 1:** Deploy the March 2017 Security Only Quality Updates<br>• **Method 2:** Deploy the March 2017 (or later) Security Monthly Quality Rollup | Windows Server 2008R2, Windows 7<br>• Method 1 – KB4012212<br>• Method 2 – KB4012215 |
| | | Windows Server 2012R2, Windows 8.1<br>• Method 1 – KB4012213<br>• Method 2 – KB4012216 |
| | | Windows 2012<br>• Method 1 – KB4012214<br>• Method 2 – KB4012217 |
| | | Windows Server 2008 SP2 - KB4012598 (Method 1 only) |
| • Windows XP<br>• 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.

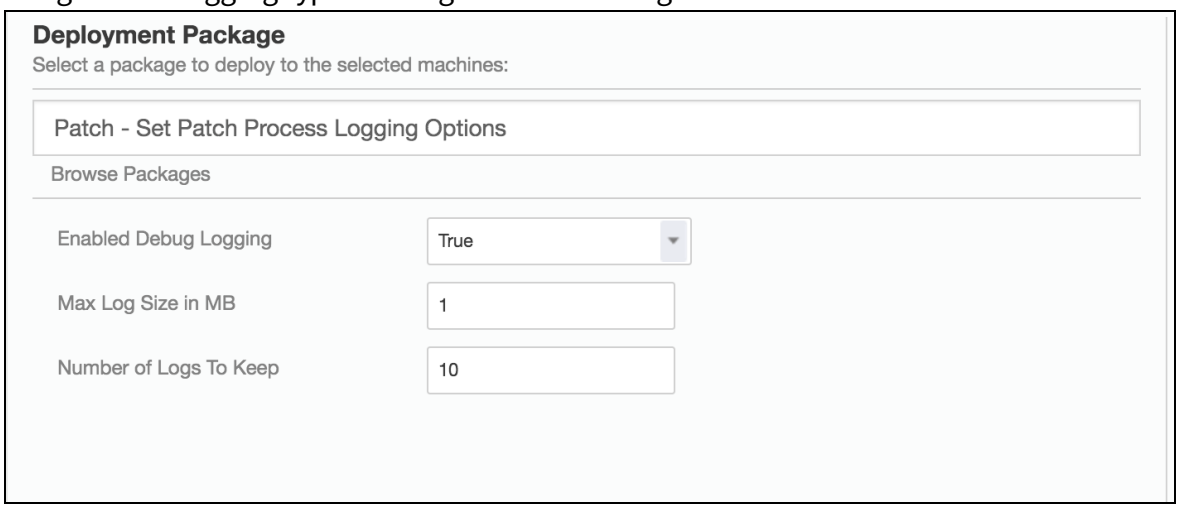
1. Get the Patch log.
   a. On the home page, click **Help**.
   b. Click **Collect Troubleshooting Package**.

   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 **Set Patch Process Logging 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 **Set Patch Process Logging 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.

## Change the endpoint status report settings

If you are troubleshooting or testing and need to capture up-to-date information, you can increase how often the endpoints are polled for their status.

> **CAUTION:** Do not use this setting in a normal production environment. This setting can affect the performance of the servers if used for long periods.

1. On the Patch home page, click **Settings**  .
2. Select the **Checking Profile** value.
   - **Production**: The saved question cache expiration is normal and the endpoints are polled every 10 minutes.
   - **Aggressive**: The cache expiration is short and the endpoints are polled every 10 seconds.
3. Click **Save**.

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

## 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 is running on your endpoints.
2. Check the scheduled actions for Patch.
   a. From the main menu, go to **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\patchx.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.

## 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 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 WUA Version from all machines` saved 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` saved 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\` 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.