**BigFix Labs** Patch Channels

Version 1.0

Aug 24, 2021

A picture containing clock

Description automatically generated

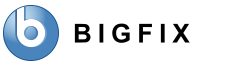
 

Table of Contents

[Document Control 3](#_Toc81467267)

[Overview 4](#_Toc81467268)

[Initial Dashboard Setup 5](#_Toc81467269)

[Channel Setup 7](#_Toc81467270)

[Sequencing and Custom Steps 8](#_Toc81467271)

[Action Setup 10](#_Toc81467272)

[New Patches vs Past Relevant Patches 10](#_Toc81467273)

[One time action setup 11](#_Toc81467274)

[Recurring action setup 11](#_Toc81467275)

[Monthly Process 12](#_Toc81467276)

[Fixlet Channel Report 12](#_Toc81467277)

[Admin Considerations 13](#_Toc81467278)

[BESAdmin Settings with Pop-ups 13](#_Toc81467279)

[Channel JSON 13](#_Toc81467280)

[Max Number of Actions 13](#_Toc81467281)

# Document Control

| **Version** | **Author** | **Date** | **Comments** |
| --- | --- | --- | --- |
| 1.0 | Marjan Radanovic | 08-24-21 |  |
|  |  |  |  |

# Overview

Patch Channels solution is a slightly different approach to patching within BigFix. It is similar conceptually to creating monthly baselines and then pushing them out to groups of machines, but this solution operates automatically and without creating new content (I.e. baselines). As such it is more efficient and requires less operator effort. It preforms these operations by relying on two key concepts:

* Patch channels
* Maintenance window

Patch channel is a user-defined collection of Fixlet metadata that uniquely describes a set of patches. Let us take a simple example of creating a .NET channel by including “.NET” and excluding “Superseded” from the Fixlet name. If we set a setting PatchChannels = “.NET” on a subset of machines, those systems could get the “.NET” patches applied to them automatically, monthly, and within their maintenance window.

Maintenance window is the second key component. Patch channel concept revolves around issuing content to all systems “subscribed” to the channel and having those systems apply the patches whenever they are in their maintenance window. This keeps the action footprint, and therefore load on the environment, low.

Patch Channel actions can be issued on demand, or monthly using an orchestrator script. Actions can also be filtered based on the content source release date, which gives you an opportunity to filter past content from monthly patch content, as well as ability to push out all monthly content (and not just relevant one) which can be advantageous in specific circumstances.

Patch channels are extremely powerful, and once set up, require minimal amount of work to upkeep but they are not for everyone. If you are pushing out every patch available to all computers in your environment at any time, this might not be the solution for you. However, if you find yourself creating unique baselines for different computer groups, and fine tuning those baselines every month, patch channels might save you a lot time and alleviate load on your environment and your process.

# Initial Dashboard Setup

Patch Channel initial setup involves two steps:

* Copying over any Channel JSON you might have set up in a DEV environment
* Creating and importing initial set of helper tasks, analyses, and properties

For a first-time setup you might not have a channel JSON to paste into the text area field (consider starting from one in the [Admin Considerations](#_Channel_JSON) below).

Graphical user interface, table

Description automatically generated

Clicking on the “Complete Setup” button will create and import all the necessary helper content. You will have to be an admin operator to do this, and this content will go into your ActionSite. This is a requirement, as it is the easiest way to make sure that everyone has access to the content created. Content created will be the following:

#### PatchChannelsTAG property

This is a property used to determine computer channel subscription. It reads the value of PatchChannelsTAG setting on the BigFix Agent. This could be an integration point in case these values are stored in an external data source (like a CMDB).

#### Computer Channel assignment tasks

There are 3 tasks that assist with assigning channels to computers (or “subscribing computers to channels”):

* Patch Channels: Assign Channels To Systems
* Patch Channels: Exclusion From Automation
* Patch Channels: Remove Exclusion From Automation

Computers can be assigned a channel but excluded from automation if channel assignment is used for reporting purposes only. Computers excluded from automation will NOT RUN any of the Patch Channel actions.

#### RHEL multiple package installation helper tasks

These tasks are used to assure multiple package installation process on RHEL 6, 7, and 8. Tasks are:

* Patch Channels: Multiple-Package Baseline Installation - RHEL 8
* Patch Channels: Multiple-Package Baseline Installation - RHEL 6,7
* Patch Channels: Import RPM-GPG-KEY-redhat-release - RHEL 6,7,8
* Patch Channels: Enable the Multiple-Package Baseline Installation feature - RHEL 6,7,8
* Patch Channels: Cleanup - RHEL 6,7,8

#### Reboot Helper task

Task is named “Patch Channels: Restart” and it is used to set up reboots anywhere inside the channel (at the beginning, end or somewhere in the middle). It applies only to systems that are pending a restart.

*Orchestrator Helpers*

* Patch Channels: Install Python 3.9 (Orchestrator setup)
* Patch Channels: Orchestrator Profile Analysis

Monthly automation is performed by a designated orchestrator. Task is used as an orchestrator setup and analysis is used for orchestrator monitoring.

# Channel Setup

Patch channel is the concept that differentiates this solution from all other approaches to patching within BigFix. As stated above, channel is a collection of Fixlet metadata that uniquely describes a set of patches. That metadata can include Fixlet site name, name, category, and CPE value as seen in the image below. Each field can contain multiple values and values within a field are used in disjunction (combined with a logical OR). Fields are then combined in conjunction (combined with a logical AND).

#### Graphical user interface, text, application Description automatically generated

In the example on the left we have a .NET channel.

Fixlet sites can be any of the following: Enterprise Security (this is Patches for Windows), Updates for Windows Applications or ESU Patching Add-on for Windows 2008.

CPE values have to include “cpe:2.3:a:Microsoft:.net\_framework:” or “a:Microsoft:.net\_framework:”.

CPE value match has no exclusions.

Fixlet name cannot include “preview of” or “preview for”.

Category cannot include any of the following: “Undo Workaround”, “Workaround”, “Uninstall”, “Unspecified”, “Setting”, “Microsoft Unsupported”, “Audit”, “Service Packs”.

#### Site Names

This category should include names of all sites that could contain Fixlets for this channel. Names should be complete (not partial) and should not be site “display names”, but site names as site display names are not necessarily unique. In majority of situations these two are the same expect for one important exception. “Patches for Windows” is a site display name. Site name for this site is “Enterprise Security”. Site Name category is case sensitive.

#### CPE include and CPE exclude

These two categories refer to the Common Platform Enumeration (CPE) signature – revision 2.3. CPE is a structured naming scheme for IT products and a lot of BigFix Fixlets have a CPE tag inside of them (you can find these easily in the Fixlet Channels Report tab). Matches for both inclusion and exclusion are done assuming partial values. For example CPE include value of “cpe:2.3:a:Microsoft:.net\_framework:” will match any CPE value that includes that particular string (“cpe:2.3:a:Microsoft:.net\_framework:4.5::::” as well as “cpe:2.3:a:Microsoft:.net\_framework:2.5::::”). These categories are not case sensitive.

#### Name include and Name exclude

These two categories, similarly to CPE categories preform a partial match and do not accept any wildcards. Name inclusion of “.NET” will include any Fixlet with “.NET” in its name. Name exclusion of “preview of” and “preview for” will exclude all Fixlets with any of those two strings in their name. Name exclusion category is **case sensitive** while name inclusion is not, in order to provide absolute flexibility with string matching on Fixlet name.

#### Category include and Category exclude

These two categories (just like the site name field) preform a full match on the value in the Fixlet Category field. These fields are vendor provided and usually strictly defined so doing a complete match is preferable. These two categories are not case sensitive.

#### Include Tag and Exclude Tag

These two categories are present strictly for situations where all other ways to classify a specific Fixlet fail. These tags are always going to be of the form #<channel name> and #no-<channel name> respectively. They can be added inside a Fixlet comment field. Exclusion tag takes precedence over the inclusion tag and can also be used in emergency situations when testing reveals that a specific patch causes unwanted side effects (breaking an application or similar). We do not expect you would have to use these more than a couple of times a year. Special tag (#redlisted) can be used to exclude a Fixlet from all channels.

## Sequencing and Custom Steps

Sometimes Fixlets within a specific channel need to be executed in order. Common example of this occurs when patching Windows operating systems, where we prefer to execute content in the following order:

* Servicing stack patches
* Reboot (if needed)
* Other content
* Another Reboot (if needed)

This can be accomplished by creating a custom sequence for the channel as pictured below

Graphical user interface, application

Description automatically generated

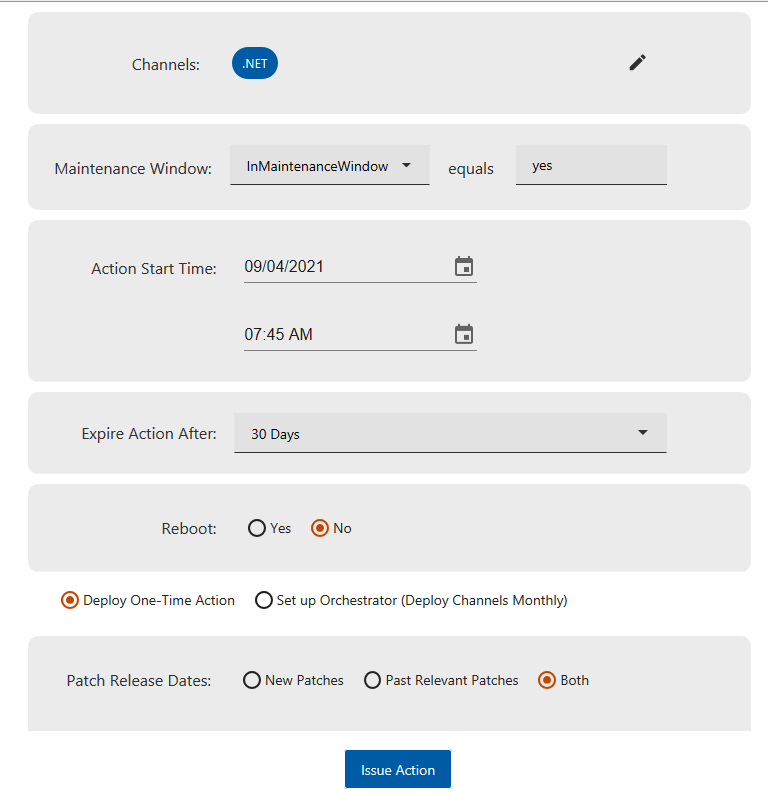
In addition to custom sequencing, you can also add arbitrary custom tasks to execute prior to and after the content within the channel. This can come in handy for systems that have to run a script prior to, or after patching (for example bringing an application down).

# Action Setup

Patch channel actions are issued from the Action Setup Tab by clicking on the “Issue PatchChannels Action” button. During this process, you will be able to choose channels to issue actions on, maintenance window constraint, action start/end time as well as post action reboot.

This reboot will be added to the end of the multiple action group from each channel and apply to all systems that belong to the channel.

For a more nuanced reboot approach, we recommend using the reboot task as part of an individual channel sequencing.



## New Patches vs Past Relevant Patches

Some organizations like to separate monthly patching from bringing systems up to date with old patches, i.e. “catch-up” patching. This selection allows operators to treat these two patch time frames differently and filter their content based on patch issue date.

For environments where this does not matter, we suggest just sending out past relevant patches and adjusting the time frame appropriately.

“New Patch” pushes can also include content that is not relevant on any system in the environment. This can come in handy when issuing patches right after they get released and before they get evaluated and reported on by the whole environment. This is not an option for past relevant content as this would result in thousands of unnecessary actions.

Selecting the option for “Both” will issue two multiple action groups, one for the new patches and one for the past relevant ones.

## One time action setup

One time action setup will issue actions immediately for the specified channel(s) with the constraints specified. These actions will show up in the action list for every channel, including the ones that might not have any Fixlets that satisfy the time criteria. These actions will be empty and apply to no computers but will be there for reporting purposes.

Channels with component count greater than the “max number of actions” threshold will not get issued. Popup with actions not issued will be served to the used and this error will be recorded in the database.

## Recurring action setup

Recurring action setup will issue a single action to an orchestration endpoint. This action will be a policy action that will get executed on a predetermined periodic basis. This policy action will in turn issue channel actions with predetermined characteristics (just like a one-time setup would).

**NOTE:** For this process to complete successfully, it is important for the orchestration endpoint to have a clear path to the root server, a valid user/password, and a web reports server running.

# Monthly Process

Patch Channels solution is designed to be an iterative process. On initial implementation, you will have some ideas around what channels you should have in your environment and how these channels can be defined. Once you provide these definitions, review the Fixlet Channel report tab, and examine if your definition is accurately including Fixlets for the current month. If not, try to add additional criteria to your channels until you have a good match. You can also reach out to our [**forum**](https://forum.bigfix.com/c/bigfix-labs)with questions on the best way of doing this. Do not use tagging as a default method for adding Fixlets to channels, as this will prove to be more effort than it is worth every month.

## Fixlet Channel Report

This report is designed to give a console operator view into Fixlet metadata as well as current channel matches on a per Fixlet basis. CPE field might prove to be the most useful when trying to define a channel accurately. Be careful to add the correct string to the match that is not too inclusive but not to specific either (“cpe:2.3:a:Microsoft:.net\_framework” is a good example).

Graphical user interface, text, application

Description automatically generated with medium confidence

Search through the Fixlets in this report to ensure you have matched everything appropriately. You can export the table to csv as well by clicking the icon above the table on the left, to further analyze the data in any other tool of choice.

# Admin Considerations

Patch Channels solution is a complex, but immensely powerful solution. Channel definitions are shared among all users so consider limiting access to only people that are required.

## BESAdmin Settings with Pop-ups

There are a few Advanced Option settings in BESAdmin.exe that cause pop-ups in the BigFix console during action issuing. These settings can cause a dashboard crash while issuing actions, due to a specific “bug” inside the React library related to a state change with an alert() dialog. We recommend either disabling these settings or “popping out” the dashboard into its own window and closing it if the crash occurs.

## Channel JSON

Setting up channels initially can be somewhat laborious so please consider the JSON string below as a good initial step. You can add these channels directly to your environment by clicking on the settings icon in the top right and pasting the string below directly into the text area.

## Max Number of Actions

This value represents the limit to number of actions that will get issued as part of a single multiple action group. This limit can be used as a measuring stick for channels that are “too big”. Channels are a way to tailor specific patch content to computers and if you find yourself having a channel that encompasses “all Fixlets from a site”, channel approach might not be suited for your environment.