Customer Exercise Guide

# SOFY BIGFIX

Document Version 1.7

# Table of Contents

# Introduction

**HCL Solution Factory and BigFix –** This guide is designed to walk you through demonstration scenarios using BigFix in the HCL Solution Factory (SoFy).

**Please Note:** The images in this document are provided to aid you in the creation and use of your HCL SoFy BigFix Solution. They are representations of the screens you will see, but the images in this document may vary slightly from what you see in SoFy. For example, you may see a different Helm Chart version than the one in the documentation. This is to be expected, as the documentation is not updated every time there is a new Helm Chart release.

**You may be familiar with BigFix** – It is commonly known as a systems and security management product which allows my customers to reduce cost, risk, and complexity of managing cloud, server, desktop, laptop, point-of-sale, and other endpoints – all using a single, intelligent agent – all through a single port – offering a complete view of their environment. This enables you to **find more**, **fix more** and **do more** than competing solutions in the marketplace.

**As it relates to the HCL Solution Factory (SoFy)** –SoFy is a HUGE investment in innovation for HCL Software. SoFy is the Cloud Native Solution Factory for HCL Software. This provides access to 50 containerized products which are the HCL Software Crown Jewels, 2,000+ REST API Endpoints and access to customized integrated demos. This will allow you to Deploy your enterprise software in minutes on any cloud. Amazing Talent. This is the realization of the dream of allowing customers like you to simply deploy and maintain enterprise software products at scale in minutes into dynamic public, private and public clouds.

*Using BigFix will help your organization keep your endpoints continuously patched and compliant using one singular agent across multiple operating systems. With BigFix, you will be able to deliver patches in an efficient, automated process to reduce patching cycles from days to minutes.*

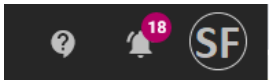
Are you ready to gain some efficiency with BigFix? Let's get started!

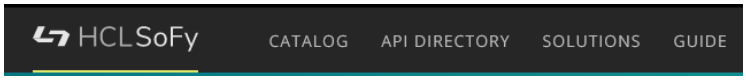
# Accessing SoFy

To access SoFy, navigate to [https://hclsofy.com](https://hclsofy.com) and click the “LOGIN” link in the upper right-hand corner (click “REQUEST ACCESS” if you do not have access)

While on this page, familiarize yourself with the SoFy site contents across the top of the screen:


LINKS ON TOP-RIGHT 


- Contact us – use this link to open a support ticket or provide feedback about HCL SoFy.
- Notifications – contains information about solutions you build and deploy. You can view and dismiss notifications from this side bar.
- Profile – contains information about your HCL SoFy profile.

LINKS ON TOP-LEFT 

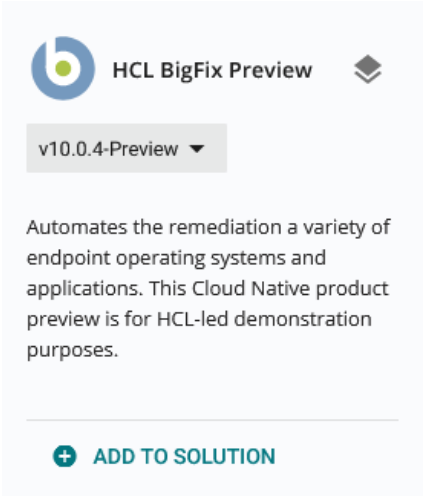

- HCL SoFy link – returns you to the HCL SoFy home page.
- Catalog – the Catalog lists the software components that can be added to Solutions within HCL SoFy. The Catalog Items are designed to work together to demonstrate an HCL software solution.
- API Directory – lists the Application Programming Interfaces (APIs) available with HCL SoFy.
- Solutions – This page shows the solutions you have currently deployed in SoFy, as well as their version and description. The solution name provides a hyperlink to the individual solution page.
- Guide – use this link to view a tutorial about HCL SoFy. There is a 3-minute video tutorial on this page that will give you a tour of HCL SoFy.

# Solution Setup and Prerequisites

*Following the instructions in Accessing SoFy, navigate to https://hclsofy.com, log in, and build your SOFY instance.*

## Creating a Solution

From the menu bar at the top of the page, click on "CATALOG."
Type "bigfix" in the box under the "Explore the HCL Software Catalog" heading and click "SEARCH."
You will see results for BigFix:

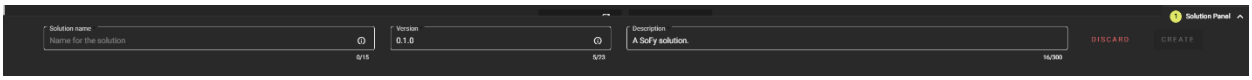



NOTE: There is a grey box under the title of the catalog item that contains a drop-down list of versions. The latest available version may not correspond with the version in the image on the right, but the latest version is the one that appears in the grey box by default, and this is the version you should choose. **Make sure you choose the latest version of each catalog item unless you have a specific reason to choose an earlier version.**

Click "ADD TO SOLUTION" on each result from #3 above to add them to your BigFix demonstration environment. At the time of writing this document, there are two catalog results when searching for "bigfix" and both are required for the demos.

NOTE: If you add the wrong catalog item to your solution you can remove it by clicking on the grey circle at the bottom of the catalog item, next to "ADDED TO SOLUTION" (it turns red when you hover over it)

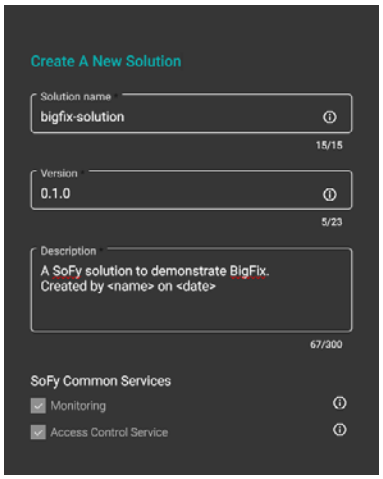
After you click "ADD TO SOLUTION" for your catalog items, you will see a black bar at the bottom of the page. It will look like this:



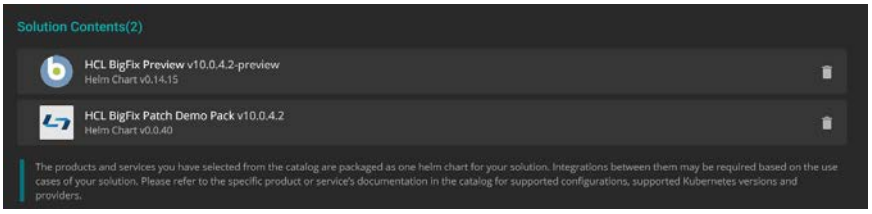

Click on the 

icon at the bottom right of the screen to expand the Solution Panel.
There are two sections in the Solution Panel:

a. Create a New Solution
   - Solution Name – required. The name should reflect the purpose behind the build.
     Here are some solution name rules:
     - Name is limited to 15 characters.
     - First character must be a letter.
     - Name must be all lowercase.
     - No spaces are allowed in the name.
     - The hyphen (-) is the only special character allowed; if used, must be followed by a letter.
   - Version – optional.
   - Description – optional but encouraged. Give the solution a description to differentiate it from other solutions.



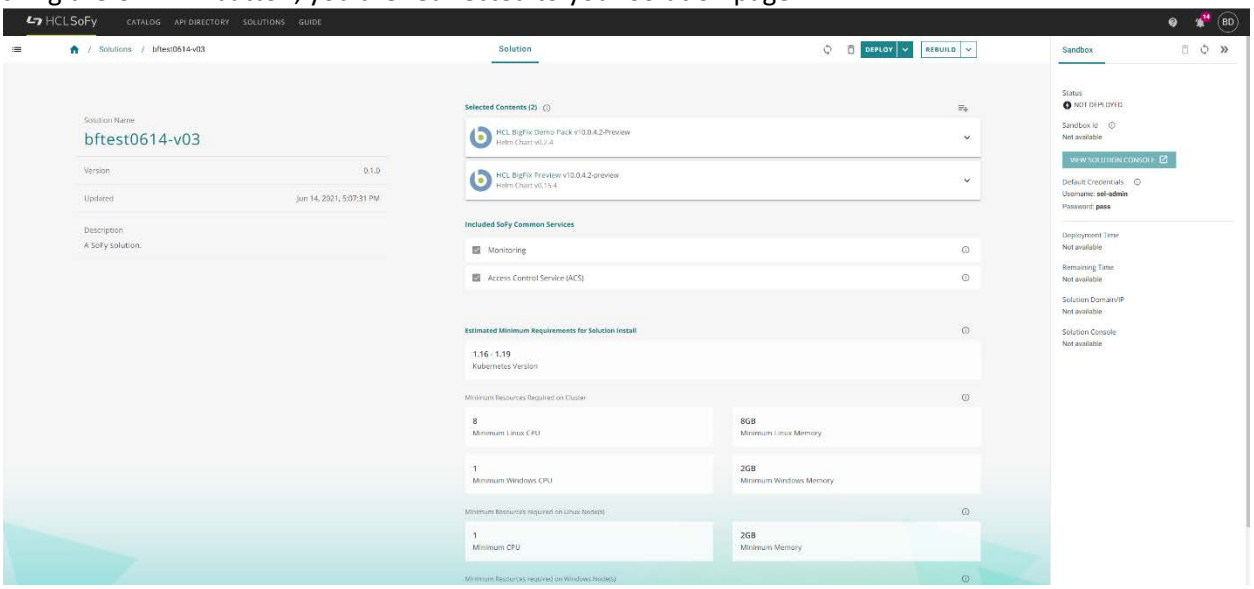
Solution Contents. This section shows what catalog items have been added to the solution. You can remove items from the solution by clicking on the grey trash can to the right of the name (turns red when you hover over it).




Once you have entered the required information, the CREATE button (below the Solution Contents section) becomes available. Click this button to create your solution.

NOTE: for best results, build the solution using the Chrome browser. Other browsers may produce errors during the build process.

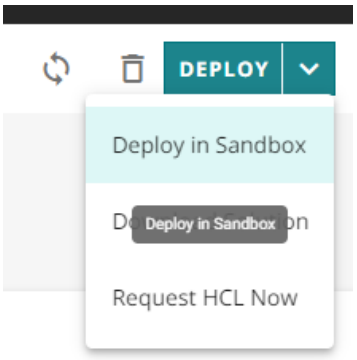
After clicking the CREATE button, you are redirected to your Solution page:




This page contains information about your new solution.

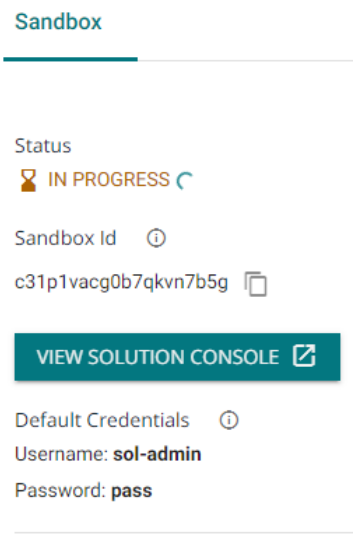
## Deploying a Solution

2. At the top of the screen, click the DEPLOY button, and choose “Deploy Sandbox” from the dropdown list.




in

Once the deployment process starts, you will see the following information in the “Sandbox” panel on the right:
The Status will show “IN PROGRESS” while the solution builds in the Solution Sandbox

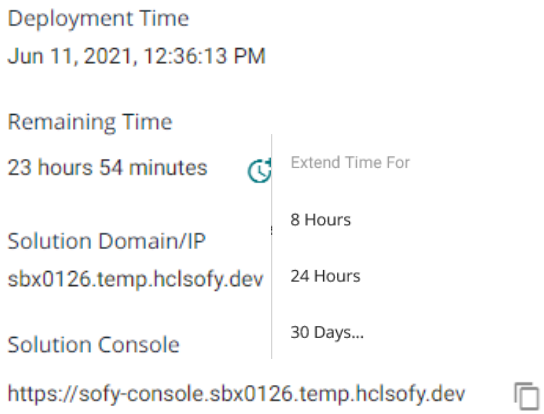


## Extending Deployment Time

1. While we are waiting for the solution console to become available, we will extend the solution deployment time.

Click on “Extend time”. You have the following options:

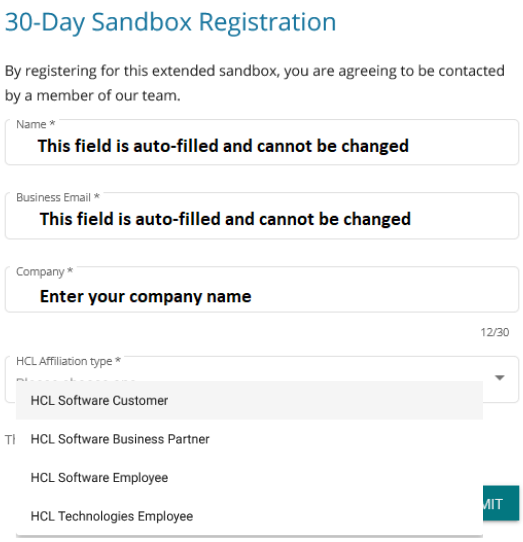
- 8 Hours
- 24 Hours
- 30 Days



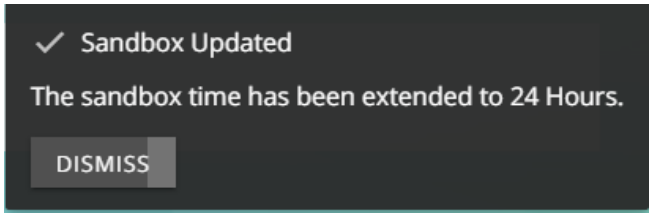

If you choose 30 days, you will be prompted to provide some additional information:

- Company: Provide your company Name
- HCL Affiliation type: The available choices are
  - HCL Software Customer
  - HCL Software Business Partner
  - HCL Software Employee
  - HCL Technologies Employee

**If you are unsure, choose HCL Software Customer**




Click “Submit” and you will see the same “Sandbox Updated” with the new time listed (in this case, 24 hours).



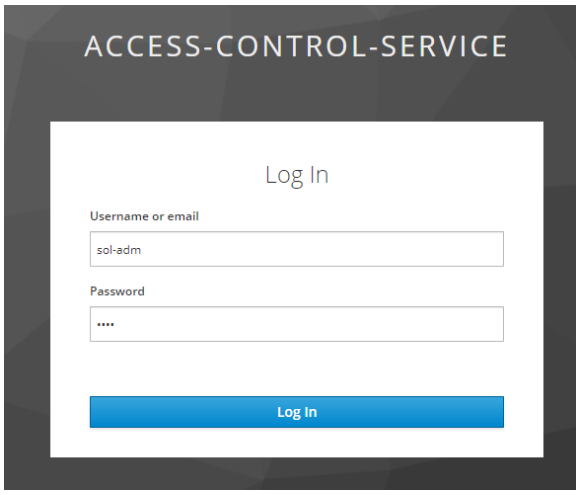

NOTE: Extending the time does not **add** this amount of time to the Remaining Time (e.g., clicking Extend Time -> 8 Hours or 24 Hours does not add 8 or 24 hours to the remaining time) – it sets the Remaining Time to the option you choose.

The solution deployment is now in progress. The 

button is not available until the solution sandbox build is underway. Once the build starts, you can click the Solution Console button and login.

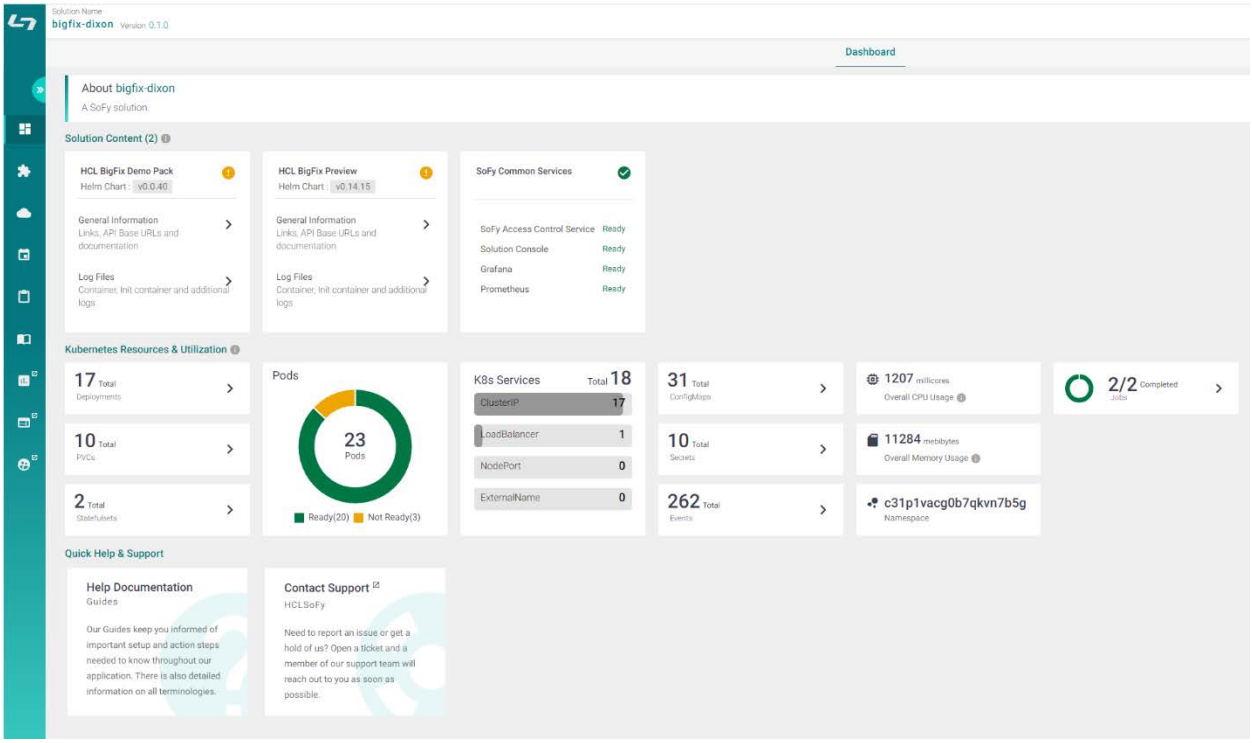
# HCL BigFix SoFy Solution Login

1. Open the solution console using the credentials provided on the Solution page. The Default Credentials are listed on the right-side of the screen, just below the VIEW SOLUTION CONSOLE button.




NOTE: The Solution Console opens in a new tab by default, so if you did not make note of the credentials, you can return to Solution Dashboard without having to use your browser's back button

When you log in, the screen you see is the HCL SoFy Solution Console. The Solution Console provides a simplified administration experience for your solution. If the solution is running in the SoFy Sandbox, a link to the Solution Console is displayed in the Solution Details view.




NOTE: Your screen will have the same content as the preceding image but may differ slightly in numbers and results – like Pods that are ready/not ready. Please be patient as all components of the demo solution build to completion.

## Dashboard Familiarization

You can take this time to tour the SoFy dashboard. Next to the Solution Name (the name you gave your solution in step seven of the previous section) you will see two sideways chevrons, or a “double greater than” symbol:  click on this to expand the left side-pane. You will see that the view you are currently seeing is the Dashboard, as evidenced by the name being in a darker highlight in the list on the left side-pane, and the title at the top center of the page.

The Dashboard shows you an overview of your Solution Content, Kubernetes Resources, and Events.

### Solution Content

The next item below the Dashboard is Solution Content, which provides details on your products/services in your solution. Clicking on the cards will provide you with more detailed information. Here, details of the services such as name, health status, links, API base URLs, API Documentation links and more can be accessed via the product card. Logs related with the services can also be accessed from here.

When you click on the green or red dot (Health icon) of the card, a pop-up window will display all pods associated with that service. If one of the container states is not healthy in any of the pods associated with the service, the health of the service is considered as unhealthy and is represented with a red circle. If it is healthy, it is represented as with a green circle.

### Kubernetes Resources

Below Solution Content you will see Kubernetes Resources, which gives you information on Deployments, ConfigMaps, Pods, Secrets, Services, and other information.

### Guides

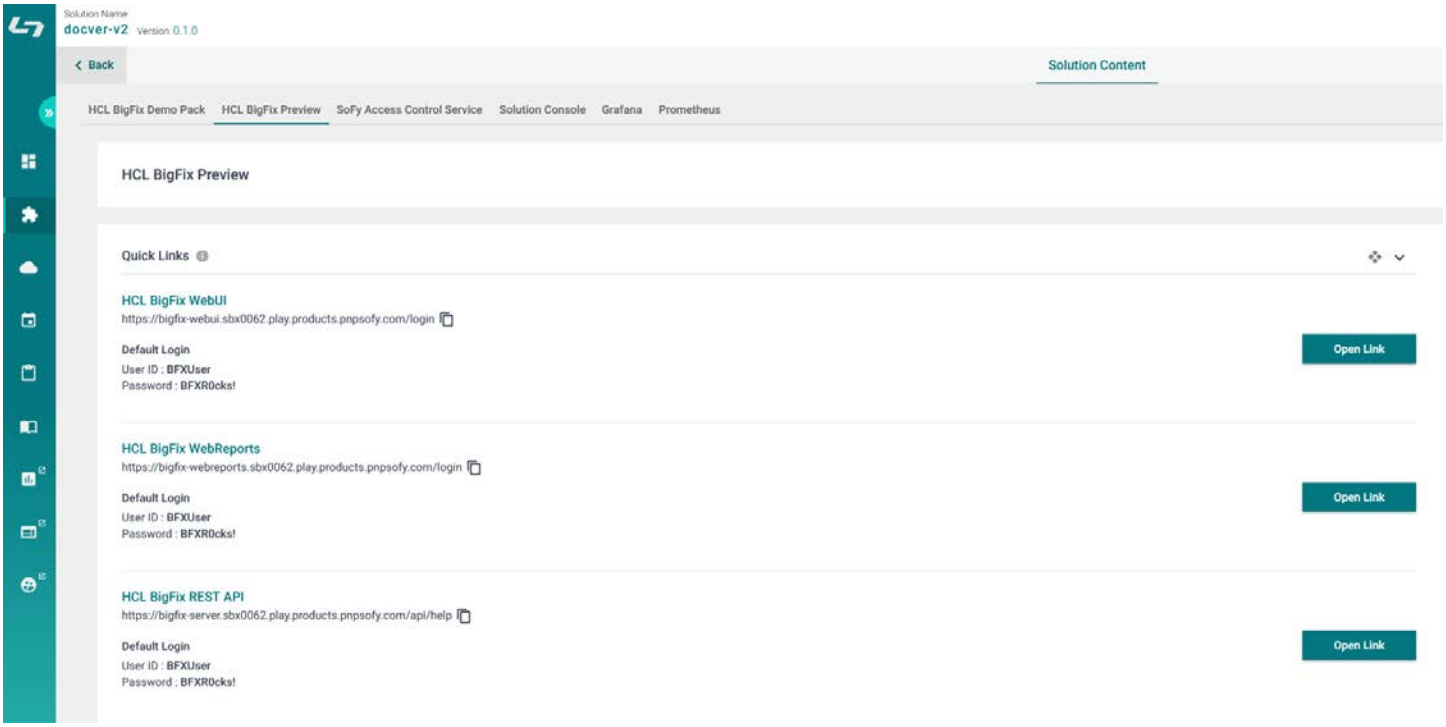
For more information about the contents of the Solution Console, click on the 

link, the sixth in the list on the left side-pane.

You can click on the double chevron (now a “double less than” symbol) to collapse the left side-pane.

# Using the BigFix Solution in SoFy

1. Click on “HCL BigFix Preview” -> “General Information” – then click on the Appropriate Open Link button. Use the User ID and Password provided with the link. For purposes of these exercises, we will be starting with the HCL BigFix WebUI, which is the top item.




If you will be using this solution for an extended period, copy the URL, and/or bookmark the site.

# BigFix Patching Scenario

## Executive Summary

BigFix Patch provides an automated, simplified patching process that is administered from a single console.

Built on BigFix technology, this software gives you unified, near real-time visibility and enforcement to deploy and manage patches to all your endpoints, wherever they may be. This software can help you reduce business risk, control costs, and enhance security.

BigFix Patch:

- Automatically manages patches to hundreds of thousands of endpoints for multiple operating systems and applications, regardless of location, connection type or status.
- Applies only the correct patches to the correct endpoint.
- Gives you greater visibility into patch compliance with flexible, near real-time monitoring and reporting.
- Provides near real-time visibility and control from a single management console.
- Can help reduce security risk by streamlining remediation cycles from weeks to hours.

PLEASE NOTE: This is the first version of BigFix on HCL SoFy, and it is intended to demonstrate the effectiveness of patching endpoints using BigFix. The Web User Interface used during this exercise is the actual BigFix interface. However, because the interface is used in a containerized operating system, some of the functionality in areas other than patch is limited. We will add functionality with each subsequent release of BigFix on HCL SoFy

## Scenario

You are a retail customer with establishments where you serve your own customers. You have a central datacenter at your corporate office, regional distribution centers, and retail stores. These locations may or may not have dedicated connections (VPN or otherwise).

The patch process for your company has been established to support the business, and your job is to enforce the process to protect the business interests. You must patch your endpoints, regardless of location, on a schedule that does not interfere with retail business hours. You must be able to select patches based on severity and operating system, and you must be able to deploy patches on different schedules with different procedures based on location, function, or operating system. Finally, you must have the ability to perform all functions without the aid of a local operator.

The endpoints in your environment are managed different ways depending on their location and purpose. For purposes of this scenario, the endpoints are distributed as follows:

- Windows devices represent the point-of-sale devices (POS) in your retail stores
    - These devices must be patched weekly between 10:00pm today, and 1:00am tomorrow*
    - These devices must be rebooted automatically at the end of the patch cycle.
- Ubuntu devices represent other devices in your retail stores
    - These devices must be patched weekly between 11:00pm today and 1:00am tomorrow*
- Red Hat devices represent devices in your datacenter and your regional distribution centers
    - These devices must be patched monthly, between 10:00pm today and 12:30am tomorrow*
    - These devices should not be scheduled to reboot at the end of the patch cycle
    - These devices can be patched out of band (outside the normal patch window)

*For purposes of this exercise, we assume “today” and “tomorrow” are the pre-set days for your maintenance window, rather than defining a specific day/date that you would have to wait for to use this scenario script.

Note: this demonstration scenario and the script below is provided as a means of familiarizing you with how BigFix works. Even if your business does not line up with the retail model, most businesses have endpoints in more than one location, and must apply patches on varying schedules with varying requirements. Once you are familiar with the solution, feel free to exercise it using different scenarios, or use your own patching scenario.

# Windows Patch Walk-thru Script: Weekly Patch Cycle

1. To perform the demo, navigate to https://hclsofy.com to create an environment, or to the WebUI URL you bookmarked previously.

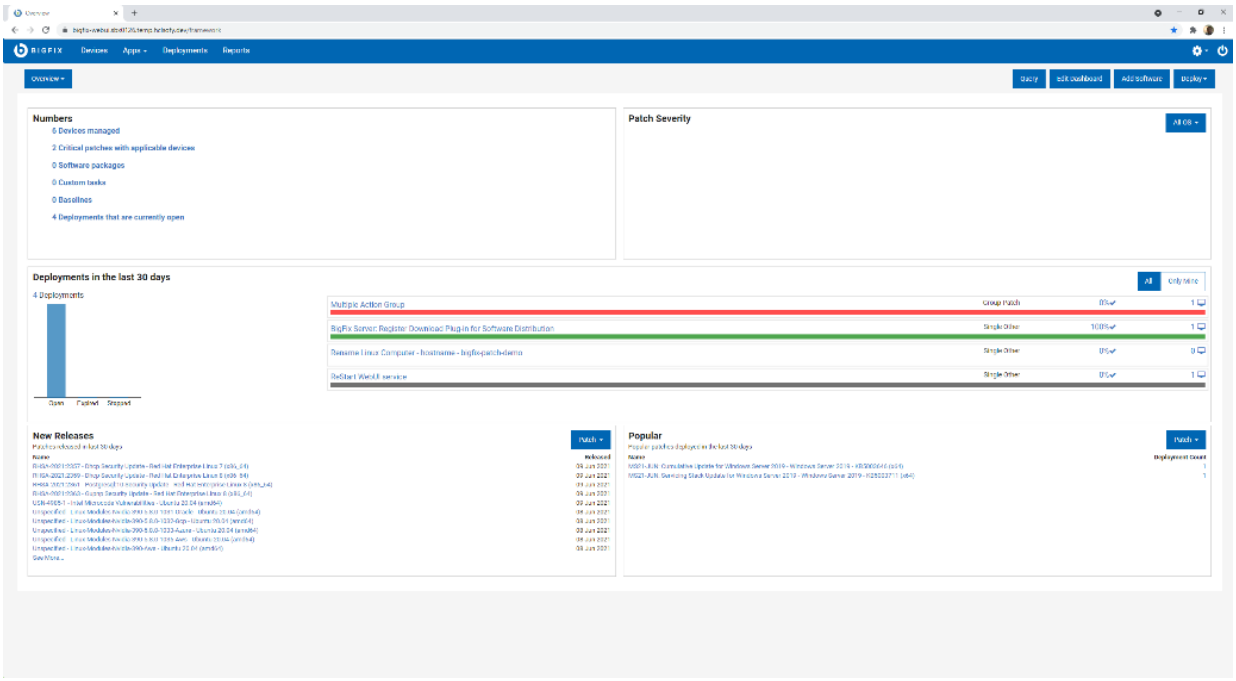
NOTE: SoFy Solutions do not last forever; they have a maximum life of 24 hours at any given time. If you wait more than 24 hours without extending, the solution will expire, and you will have to create another one (see Extending Deployment Time for more information).

In this scenario we are going to apply Windows patches using BigFix. We will apply some filters to look at Critical Patches for Windows, and we will focus on patches that are relevant in our environment right now. As we walk through this demonstration, feel free to work with the filters to see what choices you have, and how the selections change by applying and removing filters.
We will first log into the WebUI.

a. This URL is located on the Solution Content -> HCL BigFix Preview -> General Information -> Open Link Button to the right of "HCL BigFix WebUI
b. Use the User ID and Password located on this page to log into the WebUI.

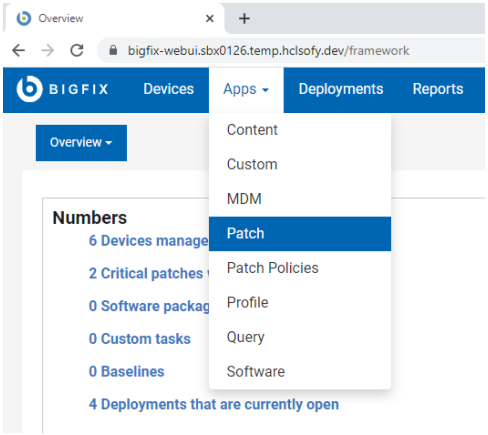

IMPORTANT: The username and the password are both case sensitive!

The first page you will see in the BigFix WebUI is the Overview Dashboard.

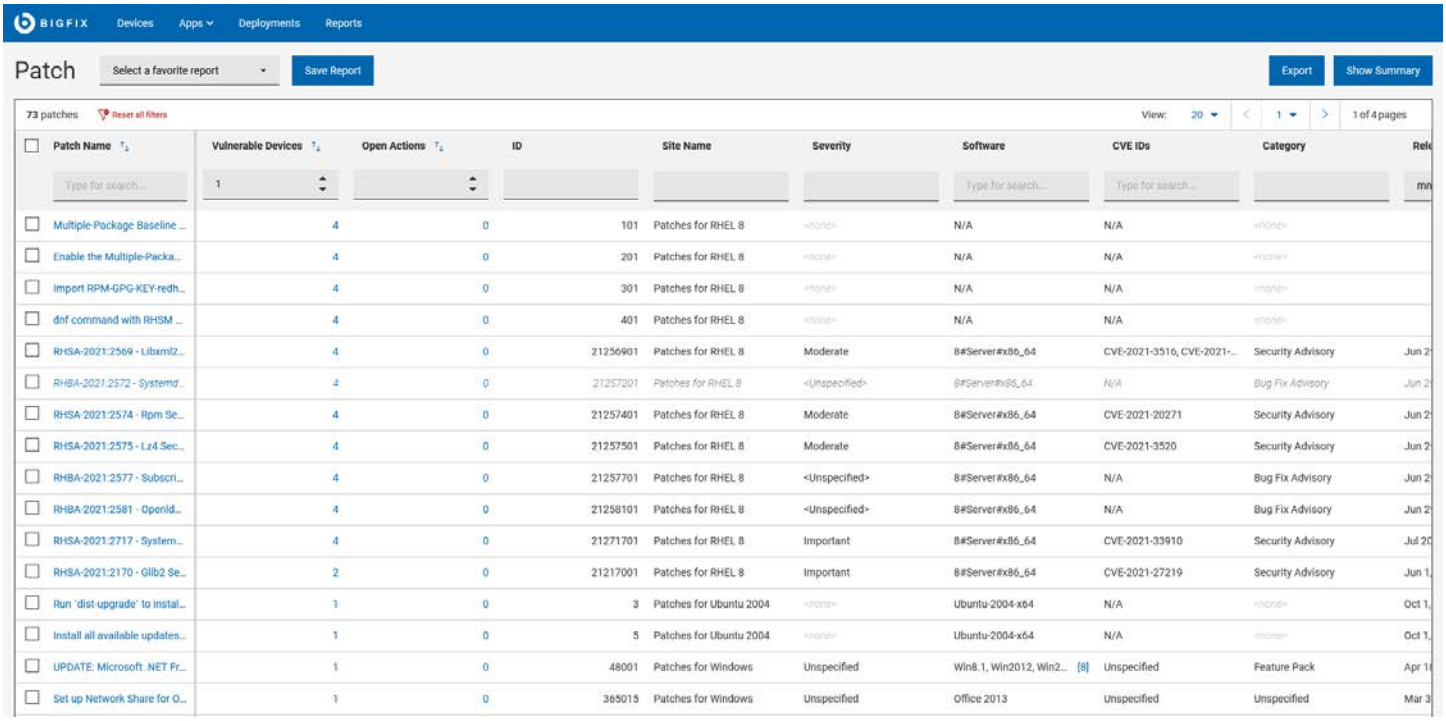



Take a minute to look around and see what information is available on this page. This is your "at-a-glance" information center for managing your infrastructure. This is data available to you without having to initiate an endpoint scan or run a report against a database. These tiles are customizable as well – you can re-arrange them or gather different data than what is currently visible.

From the WebUI Overview Dashboard, Click Apps -> Patch.




On this page we see at a glance, the patches that are applicable in our environment right now. The BigFix Agent has already evaluated this current content and determined that it is applicable to the device on which it is running. Again, we did not have to initiate a scan or run a report – the agent already knows.




The first column lists the Patch Name. Next to this column we see Vulnerable Devices. There is an entry in the grey box at the top of the column which means a filter has been applied, in this case, to only show patches that are applicable to at least one device in our environment right now. If we turn the filter off by clicking on the “down” triangle to the right of the number “1”, we can see all patch content available in BigFix right now.

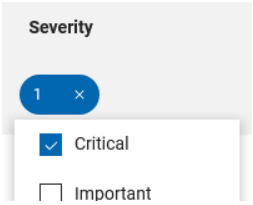
Go ahead and turn off this filter to see more content. You will notice the number of patches in the top left corner increases when you do.

We will turn this filter back on in a minute during the patching process.

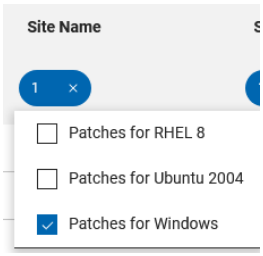
 

We will set up some filters to look for Patches of a Critical Severity on Windows endpoints only and are applicable to endpoints in our environment right now. The process is below but see if you can apply these filters by looking at the WebUI page. They are pretty intuitive.

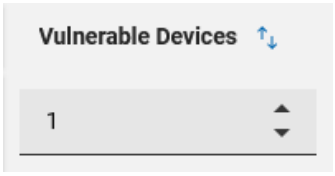
c. Apply a filter to see only Critical patches
   - Click the grey box in the "Severity" column
   - Check the box next to "Critical"
   - Note the number one (1) in the blue oval in the header. This means we have applied a filter to this column
   - Click anywhere on the page to collapse the "picker"




d. Apply a filter to see only Windows patches
   - Click in the grey box in the "Site Name" column
   - Check the box next to "Patches for Windows"
   - As with patch severity above, note the number one (1) in the blue oval in the header. This means we have applied a filter to this column
   - Click anywhere on the page to collapse the "picker"

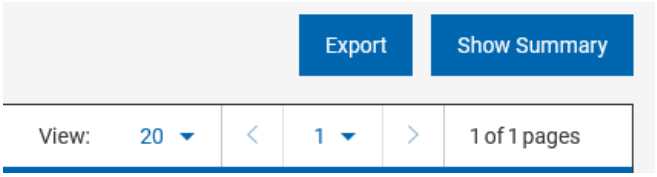



e. Apply a filter to see currently applicable patches
   - Remember that we turned this filter off in step 6.
   - Click the "up" triangle in the grey box in the "Vulnerable Devices" column
   - Note the "1" in the grey box

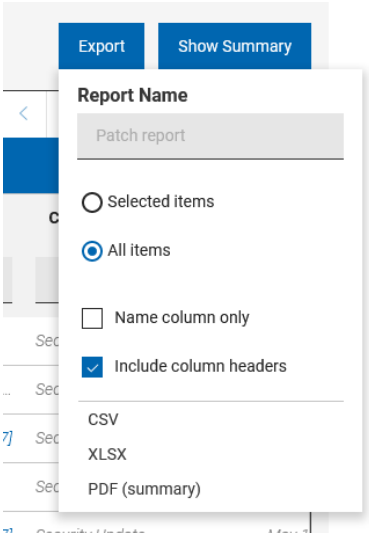



Also note that the list of patches has decreased

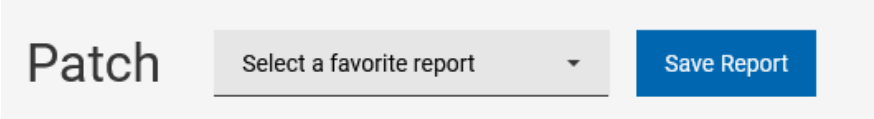
We also have the option to export this information to a file.



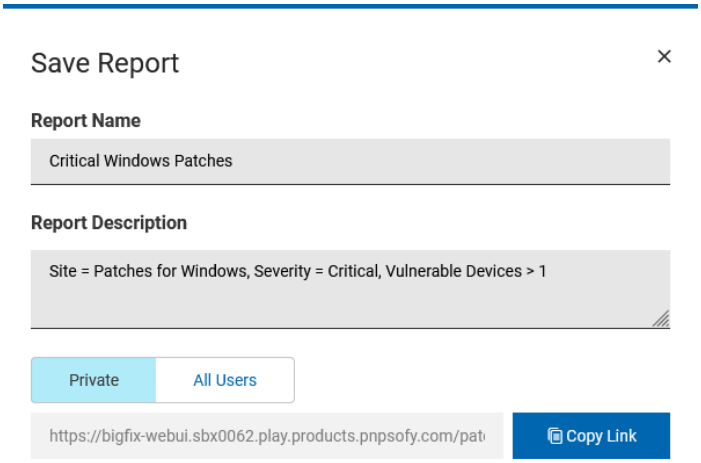

f. Click on the "Export" button at the top right
g. Give the report a name
h. Specify whether you would like to export all items or the items you have selected (if you have selected any items yet)
i. Specify the type of file you would like to save the report as (CSV, Excel, or PDF)
j. Choose to open or save the report



We can also save this current filter as a Report for later use.

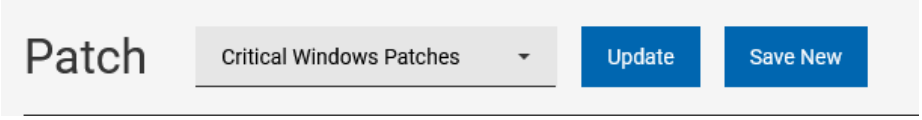



k. Click on the blue “Save Report” button and enter information about the report
l. Provide a meaningful name
m. Provide a description for the Report
n. You can make the report Private (available only to you) or you can make it available to All Users.
o. You also see the report URL, which you can bookmark for later, or share with others.



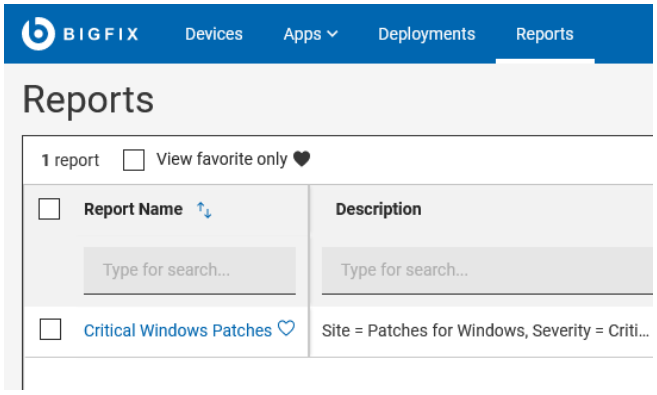

Note: the URL is a link to the report in this BigFix environment, and anyone you share the report with must have access to this environment.

Feel free to explore the other filters to see what other criteria are available. If you make any changes to the filters, you will see the header change from “Save Report” to “Update/Save New”

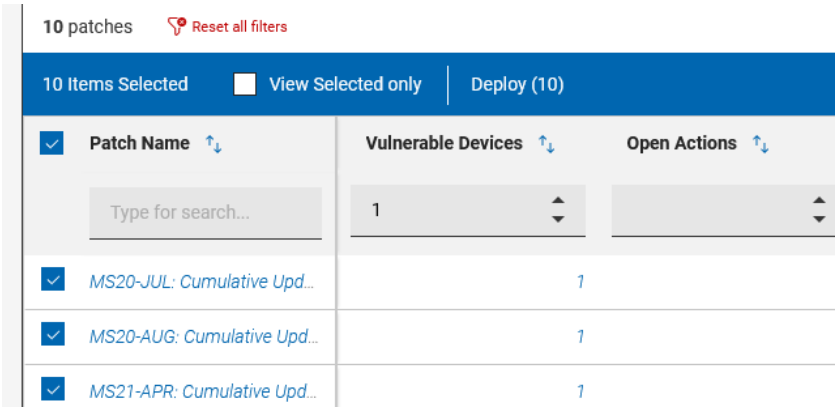



If you click “Update” you will overwrite the existing report with the new filters. If you click “Save New” you will be prompted to enter details about a new report

You can also return to the original report by clicking “Reports” in the menu bar at the top, and selecting your report from the list



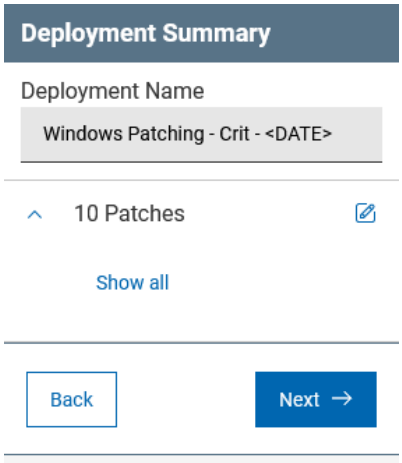
Now we are going to decide which of these patches to deploy. Based on our filters, these are all the Windows Critical patches that are applicable to devices in our environment right now.
If we want to deploy all of them, we simply check the box at the top of the “Patch Name” column and click “Deploy”. The number of selected patches appears next to “Deploy”




NOTE: The number of applicable patches in this guide may differ from what you see in your view.

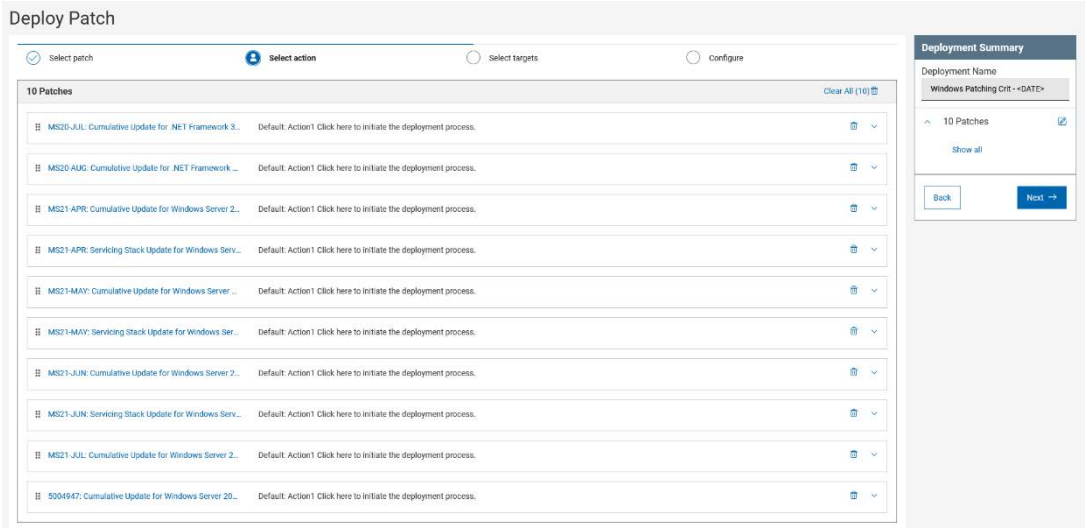
The sidebar on the right of the page lists the Deployment Summary

p. This deployment name is “Multiple Action Group” by default, because we are deploying multiple patches, or taking multiple actions with BigFix.
q. Enter a meaningful name in the grey Deployment Name box. This allows us to tell this deployment apart from other deployments.
r. If we wish to change the patches being deployed we can click on the “paper and pencil” icon to the right of the number of patches

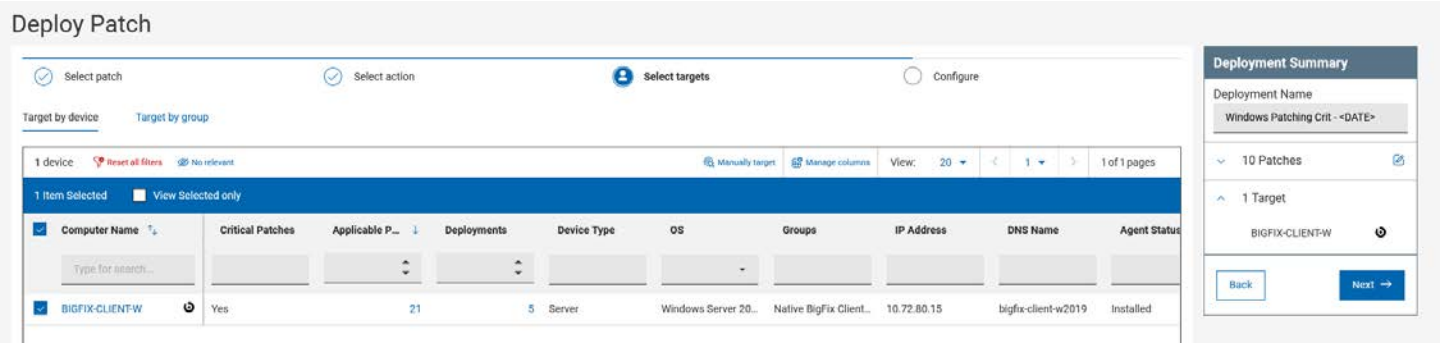



Click “Next” to continue the deployment process

**Select Action**. In this step of the patch deployment, we ensure that the correct Action is selected for each patch. Many patch Fixlets contain what is call a “Default Action” meaning this action is selected by default. In the case of a patch, the default action is to deploy the patch. Sometimes however, there is no default action, because there is more than one viable option for a patch deployment. On this screen, we make sure each patch has an action selected, default or otherwise. We can also remove patches from the list by clicking on the blue trash can icon on the right.




Click “Next” to continue the deployment process.
**Select Targets**. In this step of the patch deployment, we choose what endpoints to deploy these patches to. The endpoints with applicable patches will show up in the list. Check the box(es) next to the applicable device(s), or check the box next to “Computer Name” to select all devices
Click “Next” to continue the deployment process




NOTE: In this tutorial, the number of endpoints is one, but yours may be different.

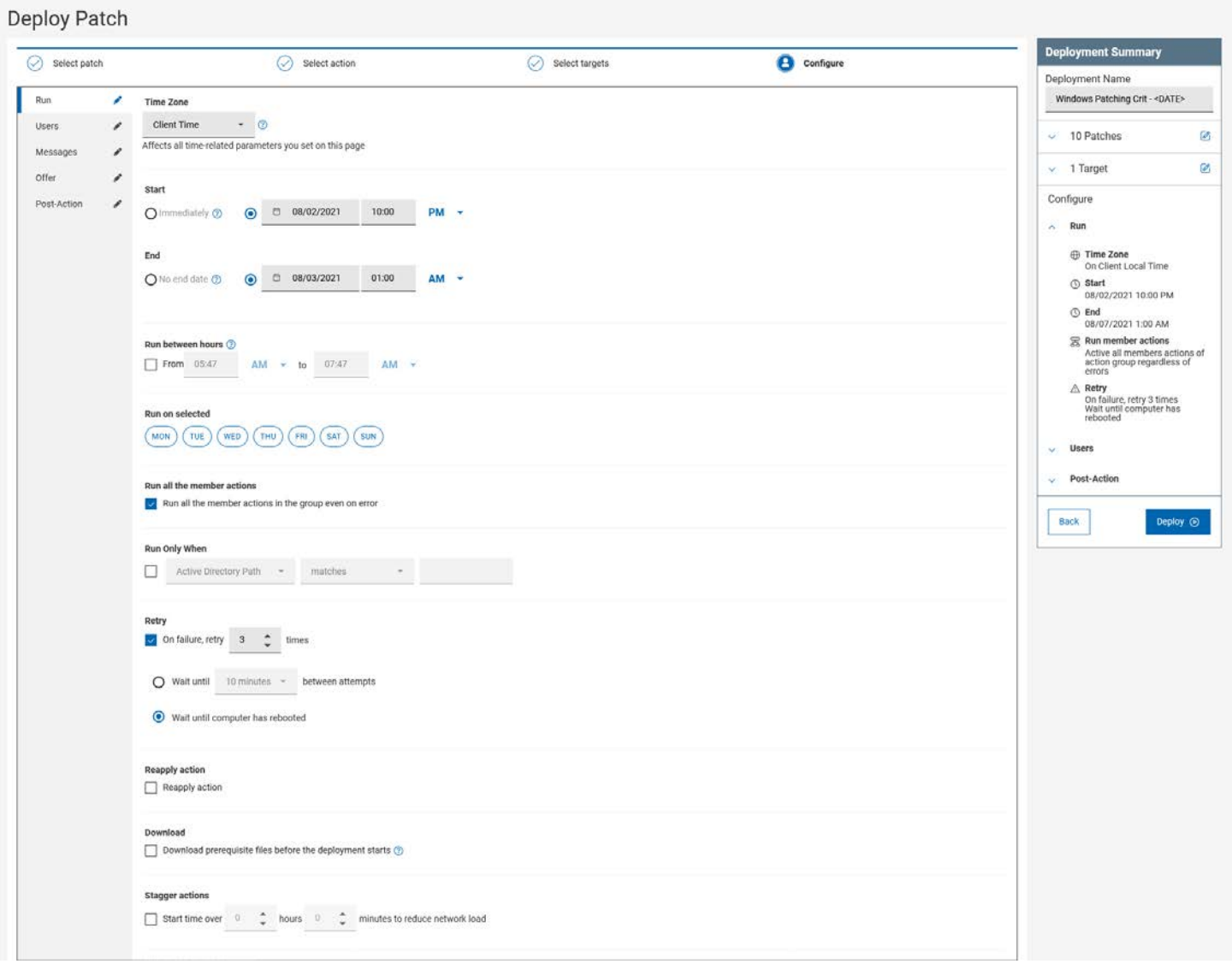
**Configure**. In this step we will specify how and when these patches are to be deployed, how and if the end user will interact, and actions to take after the patches have been deployed. There are five screens, and we will go through each one setting behavior and constraints that correspond to our scenario.

Instructions for each page in the **Configure** step follow, along with settings for each. We will make settings adjustments according to our scenario.

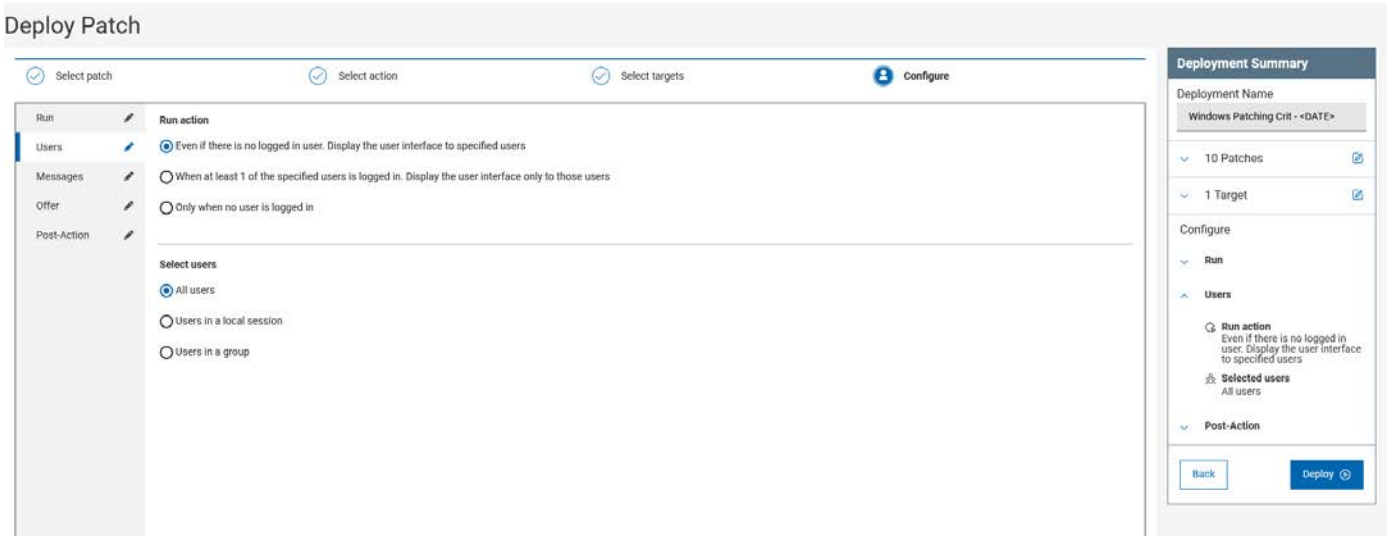
Note: If you wish to exercise more settings than just the one in our exercise, click the paper and pencil icon next to the number of patches on the right and de-select some of the patches from this deployment. This will allow you to perform additional patch deployments and explore other deployment options.

**Configure Options: Run** This page specifies schedule information for deploying patches. Make the following settings on this page:

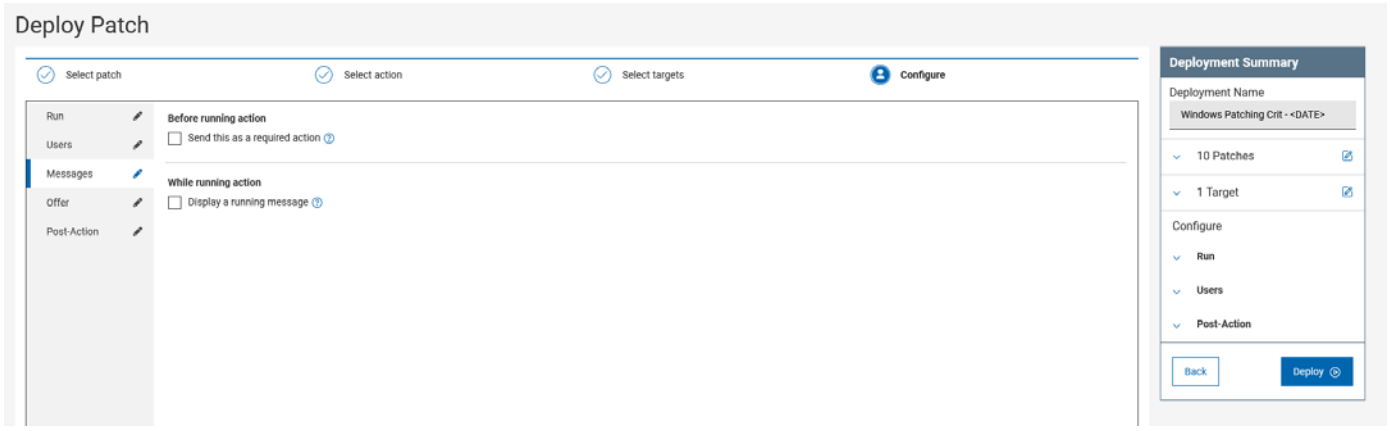
- Start: Use today's date and the time of 10:00pm
- End: Use tomorrow's date and the time of 1:00am
- Retry: Check this box to retry failed patches during the patch window. Click the radio button for "Wait until computer has rebooted"



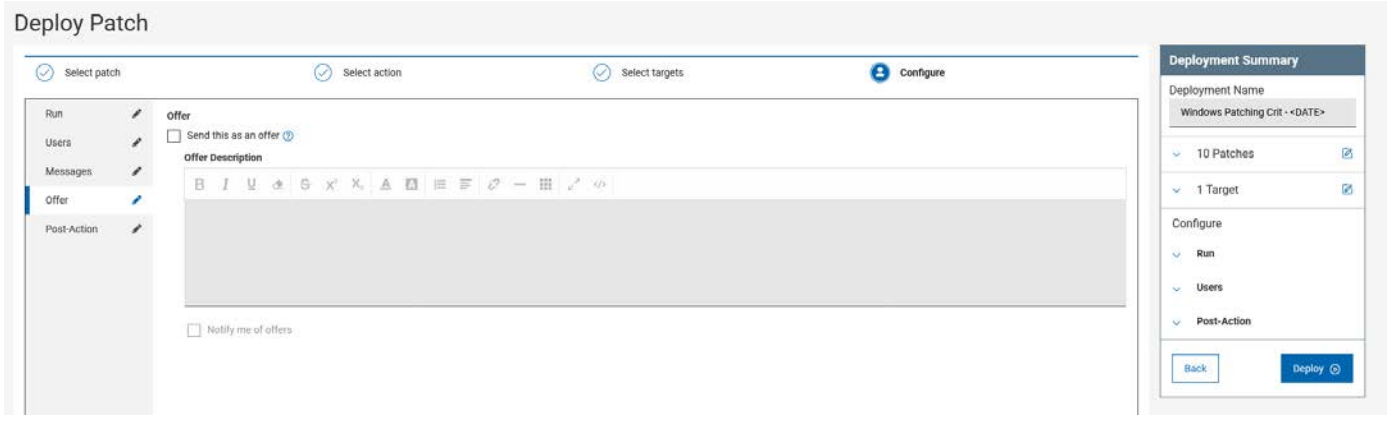
**Configure Options: Users**. This page specifies how the patch deployment behaves according to logged-in users. In our scenario the retail establishments are closed which means that no users are logged in. We will not make any settings changes on this page.




**Configure Options: Messages**. This page allows us to display information about a pending and/or running action for end-users. We will not be using messages, as no users will be logged in.

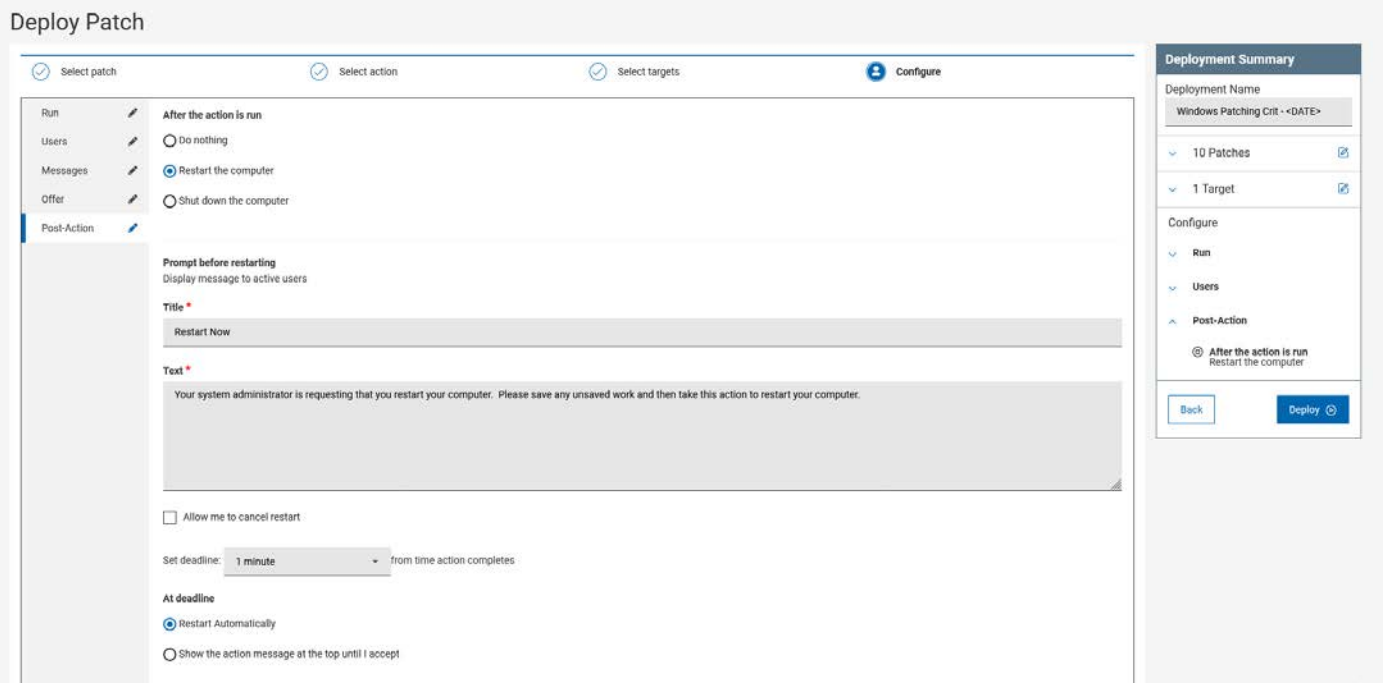



**Configure Options: Offers.** This page allows logged-on users to run the patch deployments outside of the "Run" window. We will not be using Offers, as no users will be logged in.

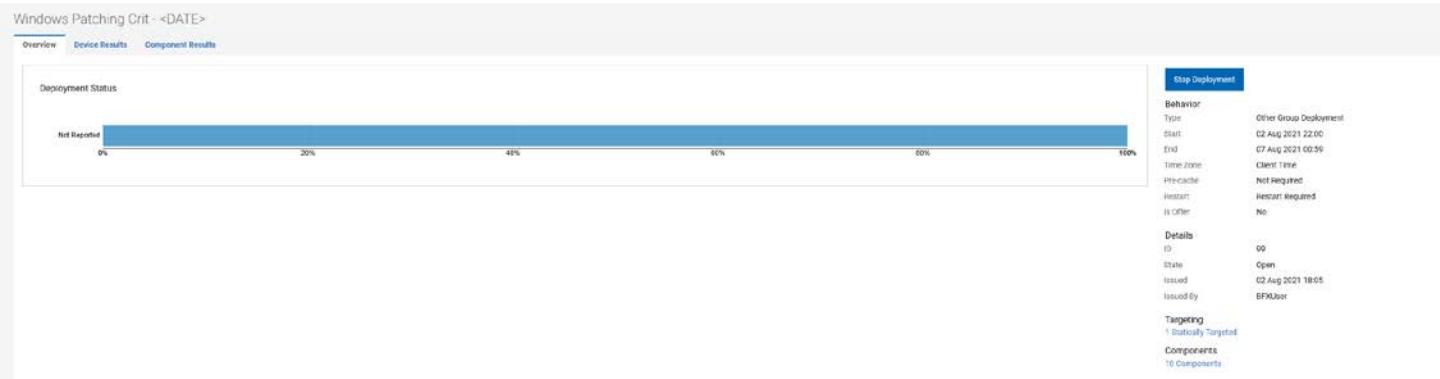


**Configure Options: Post Action**. This page allows us to restart or shut down endpoints after patching.

s. We will reboot the endpoints after the patch cycle, so select the “Restart the computer” radio button
t. We will accept the default Title and Text under “Prompt before restarting”
u. Leave the “Allow me to cancel restart” unchecked. “Me” is the end-user, not the administrator
v. Set the Deadline for 1 minute from time action completes
w. Accept the “Restart Automatically” default radio button in the “At Deadline” section.

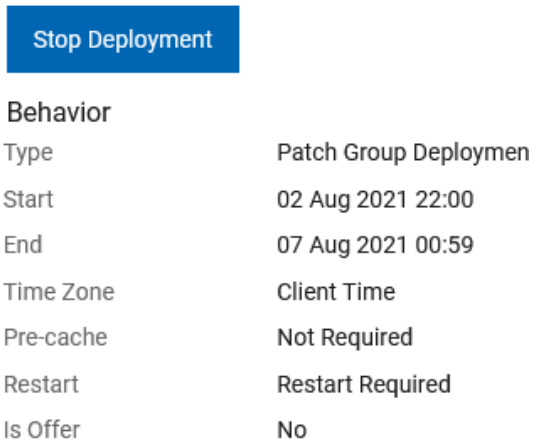



Verify your selections as necessary. When you are satisfied with the selections, click the blue “Deploy” button in the right sidebar.
You may now watch the deployment progress in the Deployment window

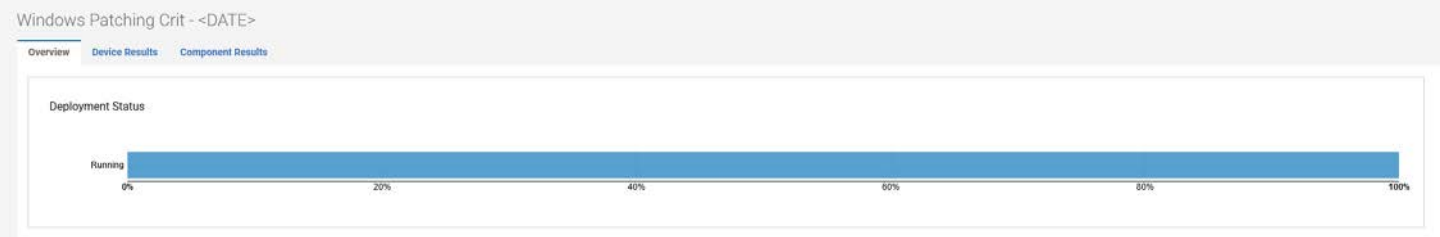


There is some useful information on this page:

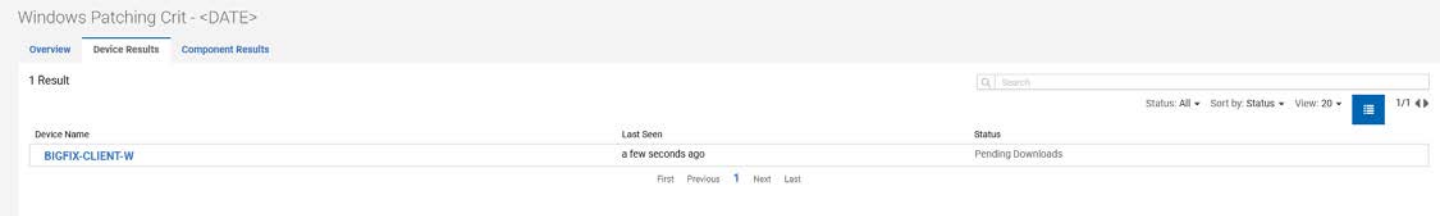
x. Stop Deployment button. You can click on this button on the right to stop the deployment. Any currently running patch installations will continue to run, but subsequent patches will not install.



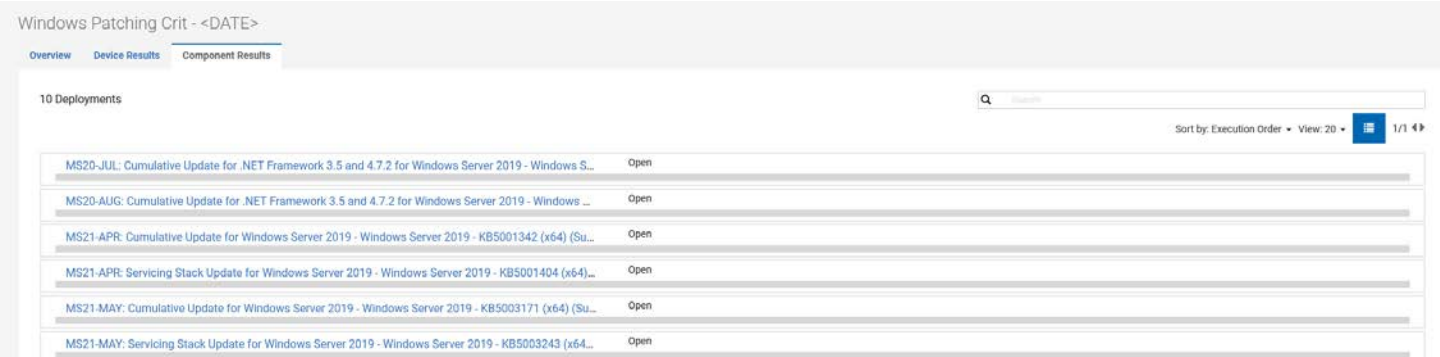

y. Overview tab. Shows the progress of the deployment.




z. Device Results tab. Gives an overview of the devices in the deployment and their current status.




aa. Component Results tab. Gives the status of each component/patch in the deployment

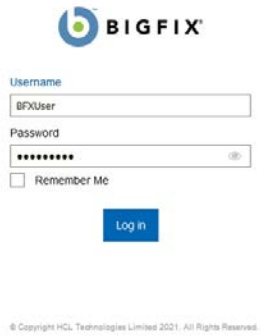


2. To perform the demo, navigate to https://hclsofy.com to create an environment, or to the WebUI URL you bookmarked previously.

NOTE: SoFy Solutions do not last forever; they have a maximum life of 24 hours at any given time. If you wait more than 24 hours without extending, the solution will expire, and you will have to create another one (see Extending Deployment Time for more information).

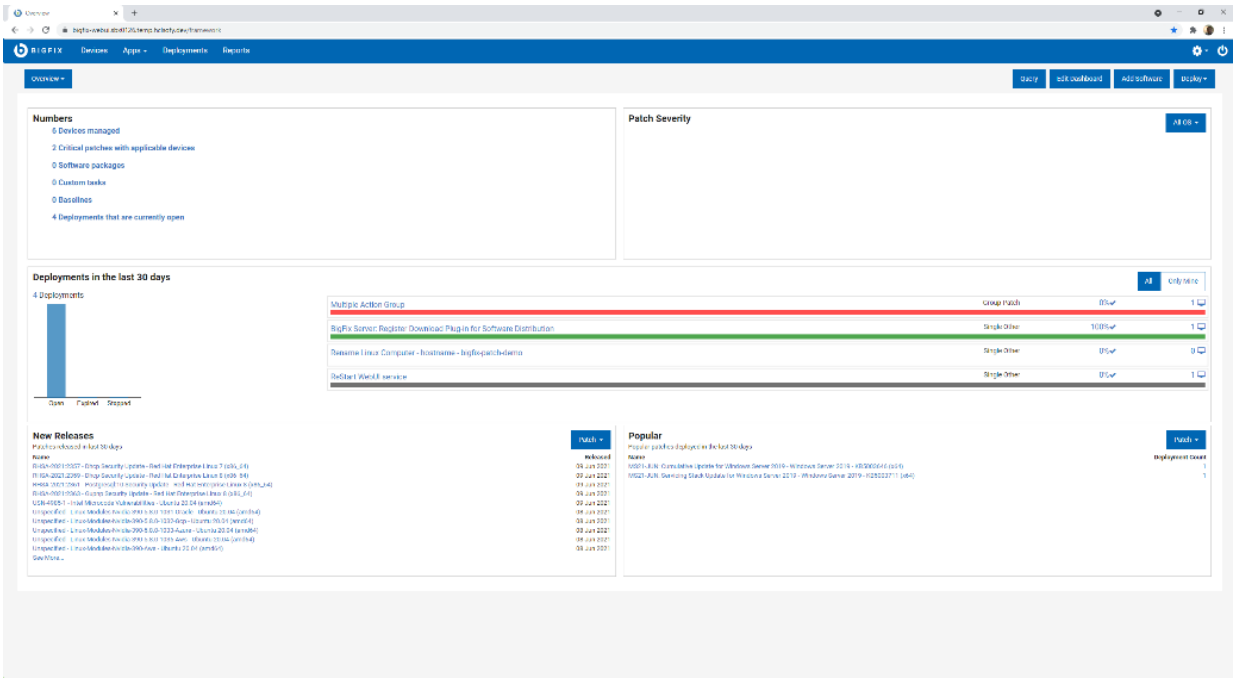
3. In this scenario we are going to apply Red Hat Linux patches using BigFix. We will apply some filters to look at Critical and Important Patches for Red Hat, and we will focus on patches that are relevant in our environment right now. As we walk through this demonstration, feel free to work with the filters to see what choices you have, and how the selections change by applying and removing filters.
4. We will first log into the WebUI.
    a. This URL is located on the Solution Content -> HCL BigFix Preview -> General Information -> Open Link Button to the right of "HCL BigFix WebUI
    b. Use the User ID and Password located on this page to log into the WebUI.




IMPORTANT: The username and the password are both case sensitive!

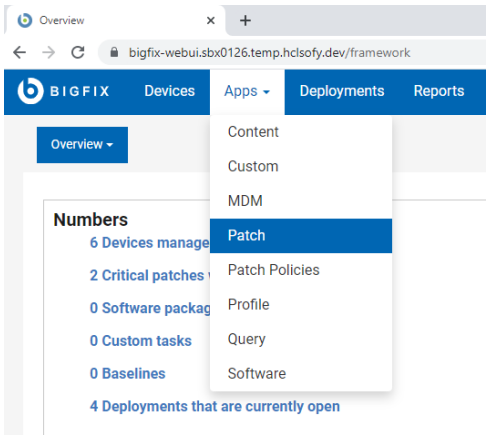
.

5. The first page you will see in the BigFix WebUI is the Overview Dashboard.

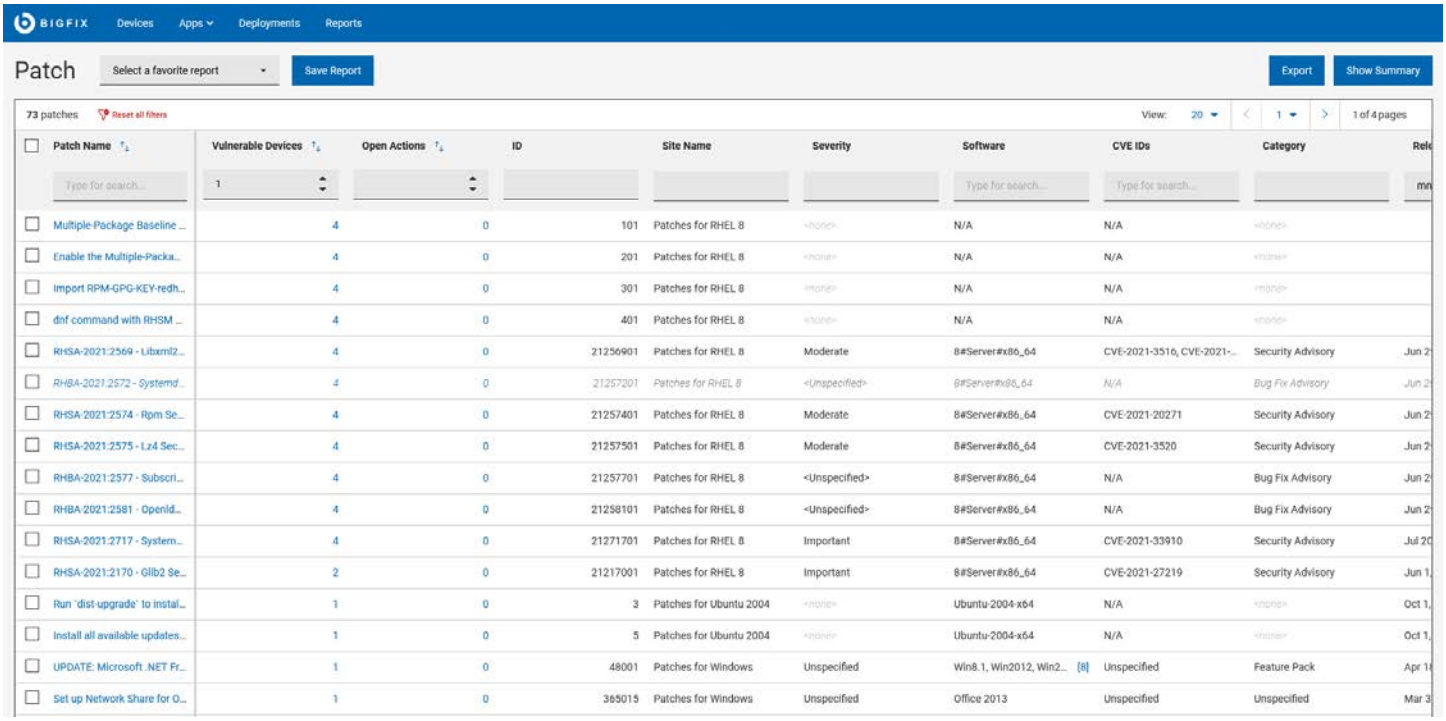



Take a minute to look around and see what information is available on this page. This is your "at-a-glance" information center for managing your infrastructure. This is data available to you without having to initiate an endpoint scan or run a report against a database. These tiles are customizable as well – you can re-arrange them or gather different data than what is currently visible.

6. From the WebUI Overview Dashboard, Click Apps -> Patch.




On this page we see at a glance, the patches that are applicable in our environment right now. The BigFix Agent has already evaluated this current content and determined that it is applicable to the device on which it is running. Again, we did not have to initiate a scan or run a report – the agent already knows.




The first column lists the Patch Name. Next to this column we see Vulnerable Devices. There is an entry in the grey box at the top of the column which means a filter has been applied, in this case, to only show patches that are applicable to at least one device in our environment right now. If we turn the filter off by clicking on the "down" triangle to the right of the number "1", we can see all patch content available in BigFix right now.

7. Go ahead and turn off this filter to see more content. You will notice the number of patches in the top left corner increases when you do.

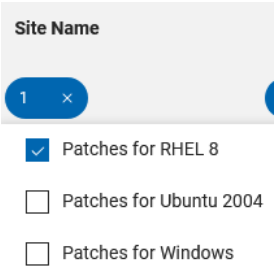
   We will turn this filter back on in a minute during the patching process.

8. We will set up some filters to look at Red Hat endpoints only for Patches of a Critical and Important Severity and are applicable to endpoints in our environment right now. The process is below but see if you can apply these filters by looking at the WebUI page. They are pretty intuitive.

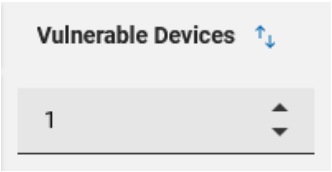
   PLEASE NOTE: the order of our filtering is changed for this exercise. In this exercise we are filtering by operating system first. This is purely for the purposes of the following exercise, "Out-of-Band Patching Scenario." The reason for filtering operating system first is to ensure we do not select all available patches for this exercise, so we have patches available for the next exercise.

   a. Apply a filter to see only Critical and Important patches
      - Click the grey box in the "Severity" column
      - Check the boxes next to "Critical" and "Important"
      - Note the number two (2) in the blue oval in the header. This means we have applied a filter to this column
      - Click anywhere on the page to collapse the "picker"


   b. Apply a filter to see only Red Hat patches
      - Click in the grey box in the "Site Name" column
      - Check the box next to "Patches for RHEL8"
      - As with patch severity above, note the number one (1) in the blue oval in the header. This means we have applied a filter to this column
      - Click anywhere on the page to collapse the "picker"

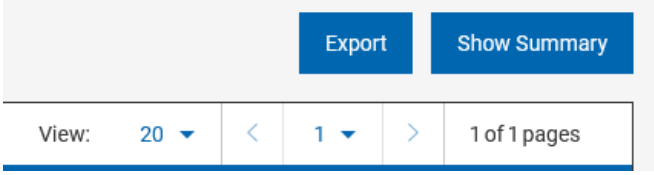



   c. Apply a filter to see currently applicable patches
      - Remember that we turned this filter off in step 6.
      - Click the "up" triangle in the grey box in the "Vulnerable Devices" column
      - Note the "1" in the grey box

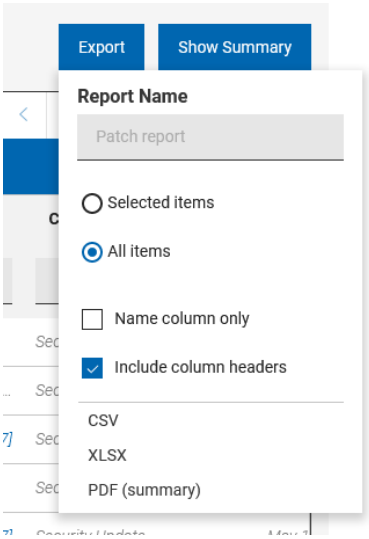



   Also note that the list of patches has decreased

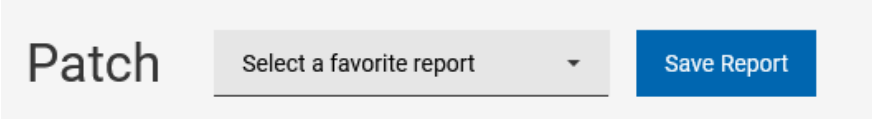
9. We also have the option to export this information to a file.



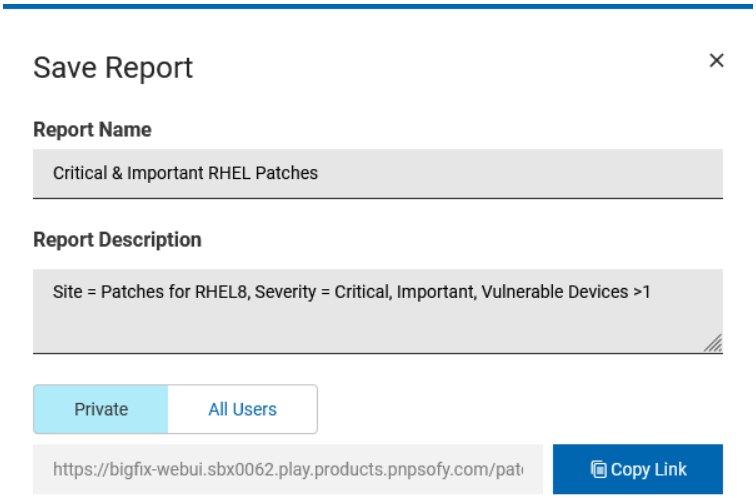

   a. Click on the "Export" button at the top right
   b. Give the report a name
   c. Specify whether you would like to export all items or the items you have selected (if you have selected any items yet)
   d. Specify the type of file you would like to save the report as (CSV, Excel, or PDF)
   e. Choose to open or save the report



10. We can also save this current filter as a Report for later use.

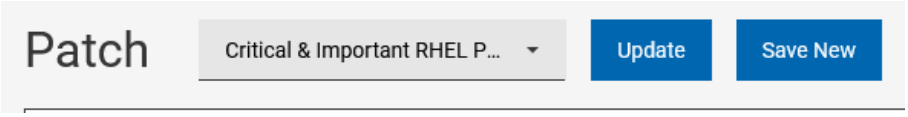



a. Click on the blue “Save Report” button and enter information about the report
b. Provide a meaningful name
c. Provide a description for the Report
d. You can make the report Private (available only to you) or you can make it available to All Users.
e. You also see the report URL, which you can bookmark for later, or share with others.



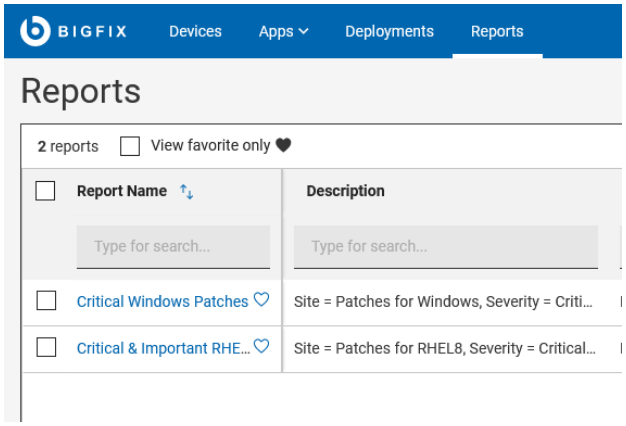

Note: the URL is a link to the report in this BigFix environment, and anyone you share the report with must have access to this environment.

Feel free to explore the other filters to see what other criteria are available. If you make any changes to the filters, you will see the header change from “Save Report” to “Update/Save New”

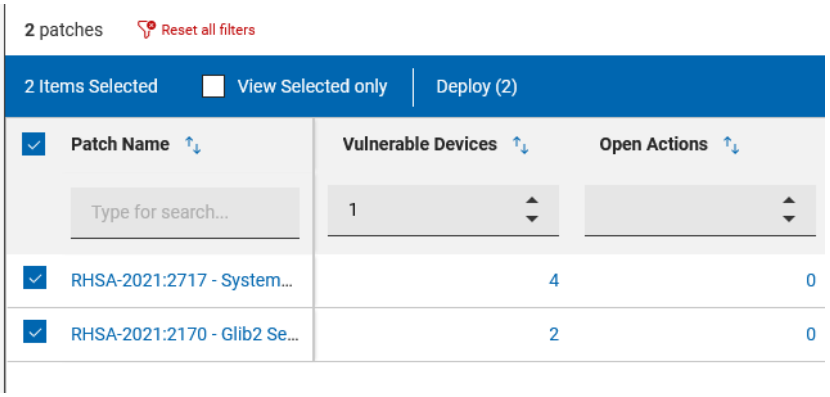



If you click “Update” you will overwrite the existing report with the new filters. If you click “Save New” you will be prompted to enter details about a new report

You can also return to the original report by clicking “Reports” in the menu bar at the top, and selecting your report from the list



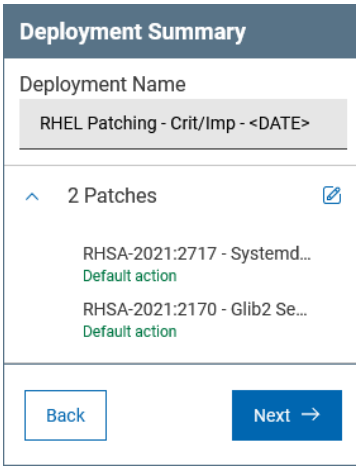
11. Now we are going to decide which of these patches to deploy. Based on our filters, these are all the Red Hat Critical and Important patches that are applicable to devices in our environment right now.
12. If we want to deploy all of them, we simply check the box at the top of the “Patch Name” column and click “Deploy”. The number of selected patches appears next to “Deploy”




NOTE: In this tutorial, the number of applicable patches is two, but yours may be different.

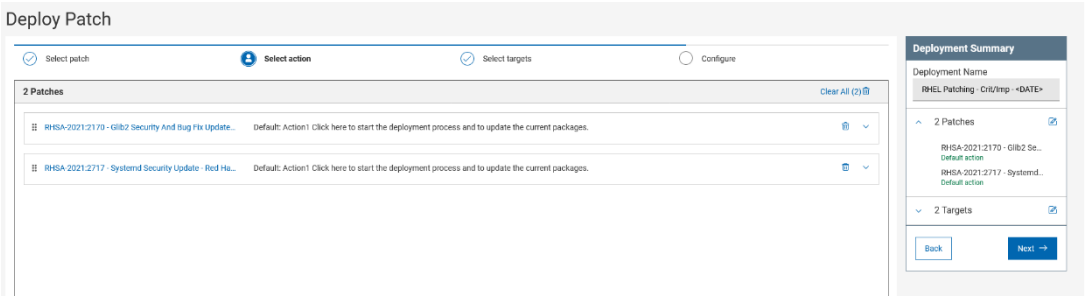
PLEASE MAKE SURE YOU HAVE AT LEAST ONE PATCH OTHER THAN THE ONES YOU HAVE SELECTED FOR THE NEXT EXERCISE. The patch for the next excersise does not have to be Critical or Important, but if all you have available are Critical and Import patches, de-select one of them for use in the next exercise

13. The sidebar on the right of the page lists the Deployment Summary
    a. This deployment name is “Multiple Action Group” by default, because we are deploying multiple patches, or taking multiple actions with BigFix.
    b. Enter a meaningful name in the grey Deployment Name box. This allows us to tell this deployment apart from other deployments.
    c. If we wish to change the patches being deployed we can click on the “paper and pencil” icon to the right of the number of patches

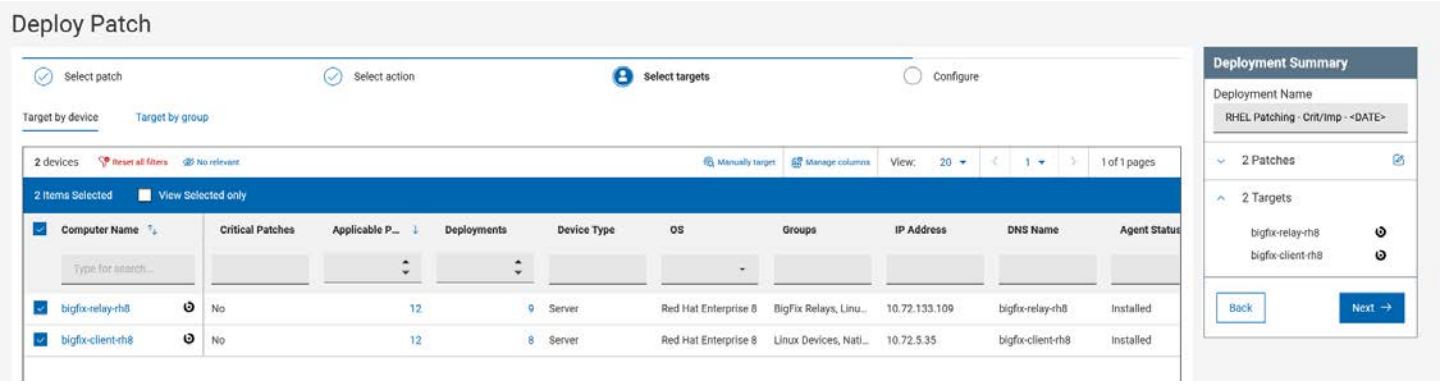



14. Click “Next” to continue the deployment process

15. **Select Action**. In this step of the patch deployment, we ensure that the correct Action is selected for each patch. Many patch Fixlets contain what is call a “Default Action” meaning this action is selected by default. In the case of a patch, the default action is to deploy the patch. Sometimes however, there is no default action, because there is more than one viable option for a patch deployment. On this screen, we make sure each patch has an action selected, default or otherwise. We can also remove patches from the list by clicking on the blue trash can icon on the right.




16. Click “Next” to continue the deployment process.
17. **Select Targets**. In this step of the patch deployment, we choose what endpoints to deploy these patches to. The endpoints with applicable patches will show up in the list.
18. Check the box(es) next to the applicable device(s), or check the box next to “Computer Name” to select all devices
19. Click “Next” to continue the deployment process




NOTE: In this tutorial, the number of endpoints is one, but yours may be different.

20. **Configure**. In this step we will specify how and when these patches are to be deployed, how and if the end user will interact, and actions to take after the patches have been deployed. There are five screens, and we will go through each one setting behavior and constraints that correspond to our scenario.

    Instructions for each page in the **Configure** step follow, along with settings for each. We will make settings adjustments according to our scenario.

Note: If you wish to exercise more settings than just the one in our exercise, click the paper and pencil icon next to the number of patches on the right and de-select some of the patches from this deployment. This will allow you to deploy the other patches to explore other deployment options

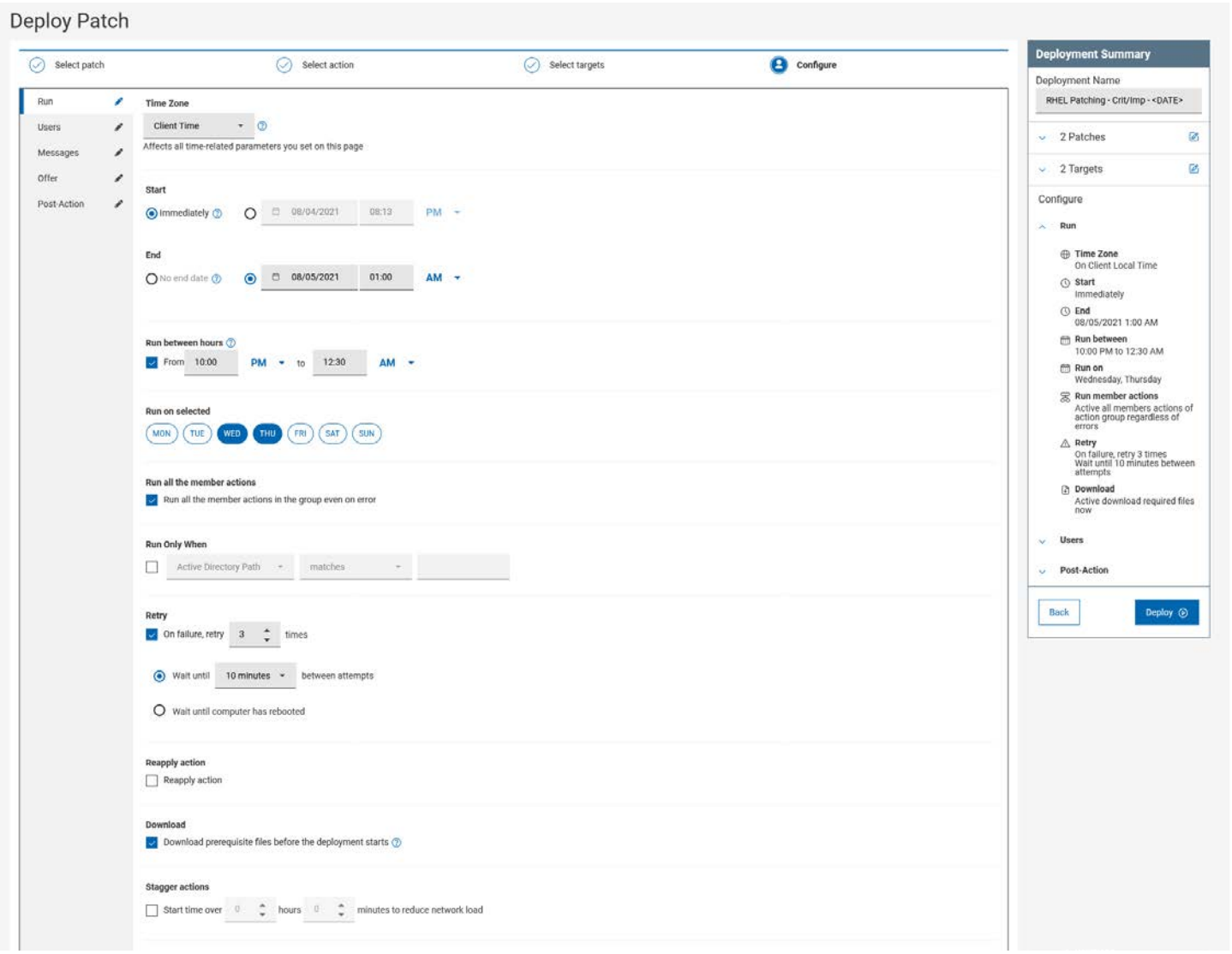
**Configure Options: Run** This page specifies schedule information for deploying patches. Make the following settings on this page:

Our settings for this patch deployment will be a little different, just to show you different options for scheduling deployments. Last time, we used a defined start and end day and time. This time, we will use a window of time on specific days. The result will be the same, it's just another way of getting there!

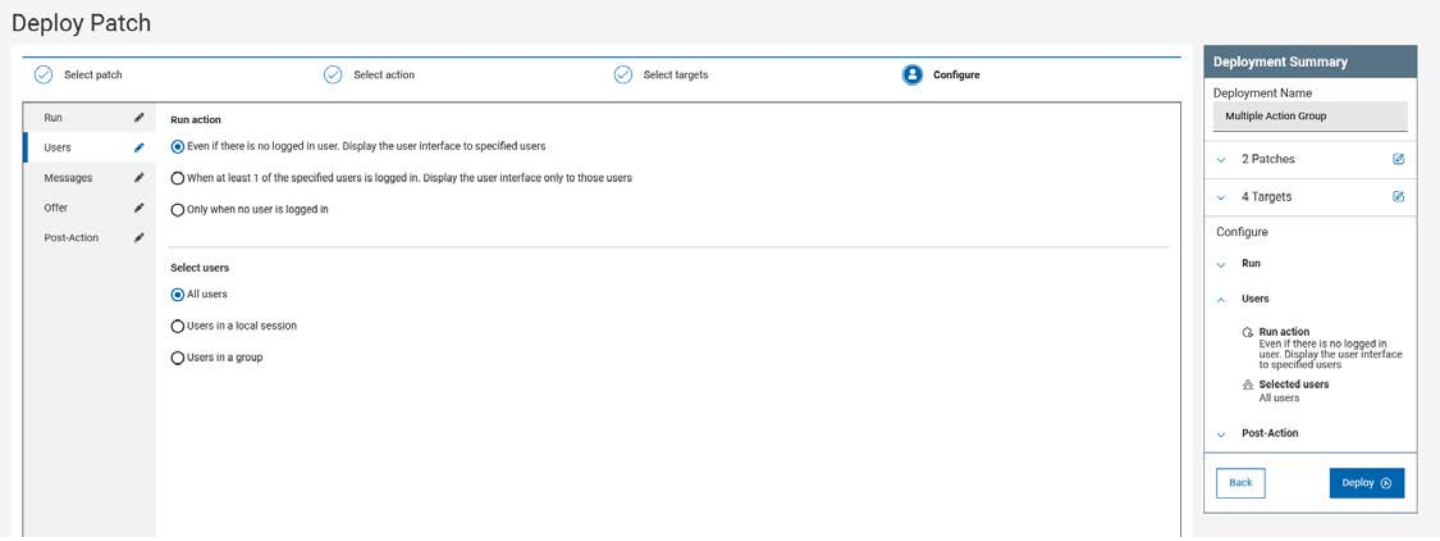
- Start: Leave this set at "Immediately"
- End: Change the date to tomorrow, and the time to 1:00am
- Check the "Run between hours" checkbox, and enter 10:00pm to 12:30am
- Run on selected: Select the days of the week corresponding to today and tomorrow
- Retry: Check this box to retry failed patches during the patch window. Accept the default "Wait until 10 minutes between attempts"
- Download. Check the box to download prerequisite files. This ensures that at 10:00pm, we are patching and not just starting to download patch content.

Note the "End" time of 1:00am. This time could have been anything between 12:31am tomorrow (the end of our window) and 9:59pm tomorrow night – because if we had made it later than that, the "Run between hours" would have applied tomorrow. That's why we had to change the end day to tomorrow

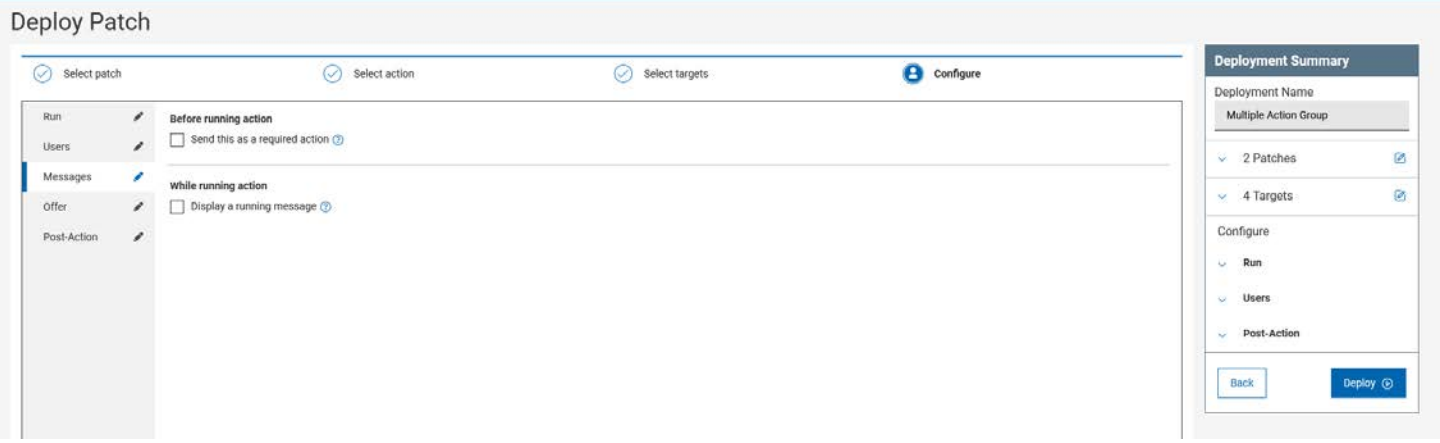
The screen image of these settings is on the next page.



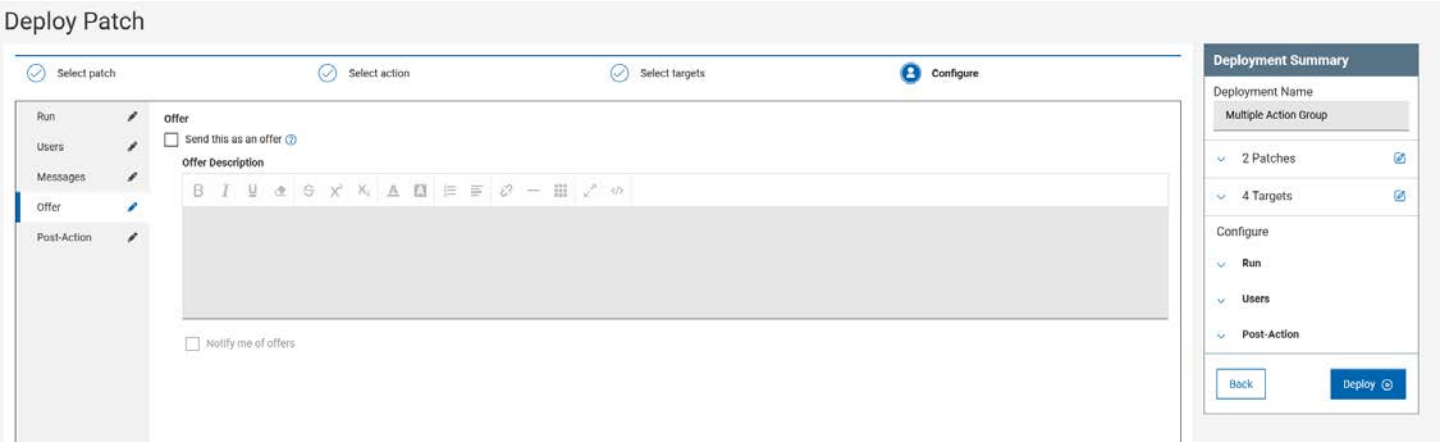
**Configure Options: Users**. This page specifies how the patch deployment behaves according to logged-in users. In our after-hours scenario it doesn't matter if users are logged in or not. We will not make any settings changes on this page.




**Configure Options: Messages**. This page allows us to display information about a pending and/or running action for end-users. We will not be using messages, as no users will be logged in.

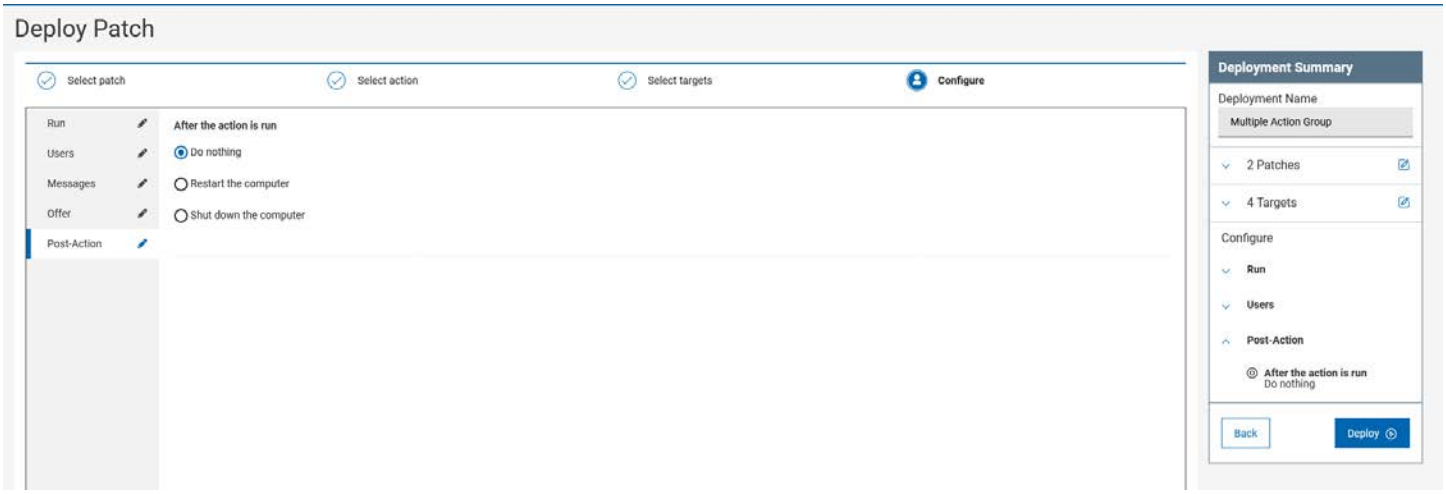



**Configure Options: Offers.** This page allows logged-on users to run the patch deployments outside of the "Run" window. We will not be using Offers, as no users will be logged in.

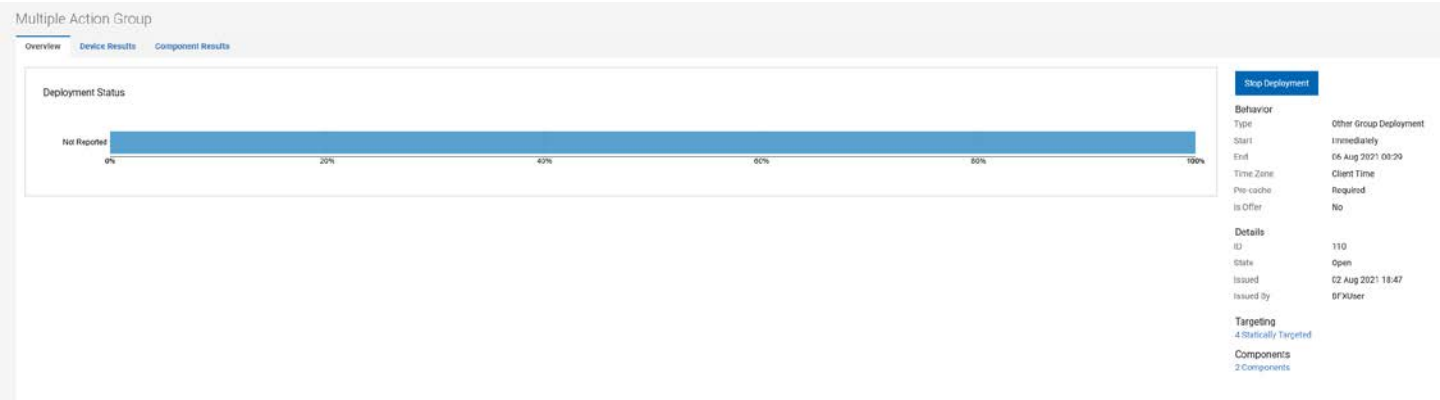



**Configure Options: Post Action**. This page allows us to restart or shut down endpoints after patching.

a. We will not reboot our servers during this window.
b. Leave the default “Do nothing” radio button selected.



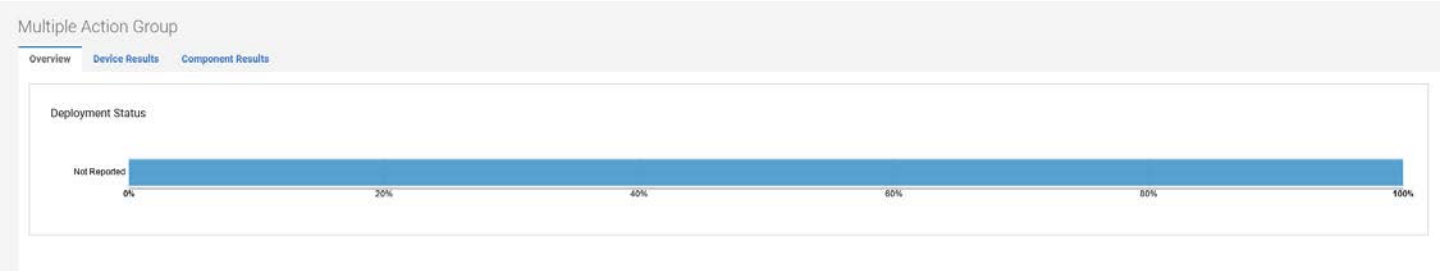

21. Verify your selections as necessary. When you are satisfied with the selections, click the blue “Deploy” button in the right sidebar.
22. You may now watch the deployment progress in the Deployment window



There is some useful information on this page:

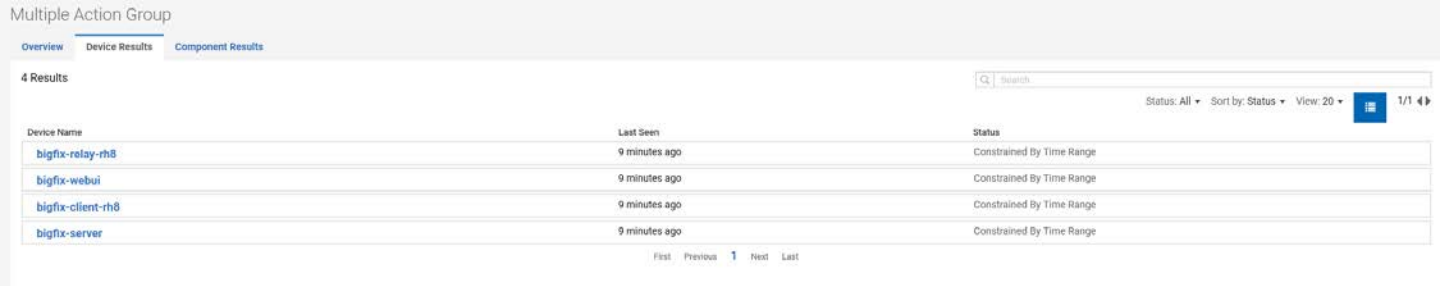
a. Stop Deployment. You can click on this button on the right to stop the deployment. Any currently running patch installations will continue to run, but subsequent patches will not install.


b. Overview tab. Shows the progress of the deployment.

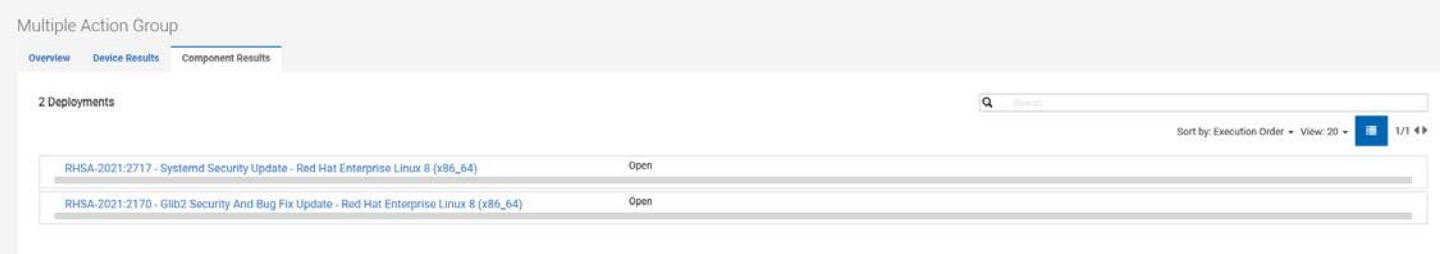



c. Device Results tab. Gives an overview of the devices in the deployment and their current status.

Note: When we click on the Device Results" tab, we may see messages such as "Constrained by distribution time" or "Constrained by distribution date." This has to do with the fact that the patch distribution is scheduled in the future. It is expected, not an error.




d. Component Results tab. Gives the status of each component/patch in the deployment

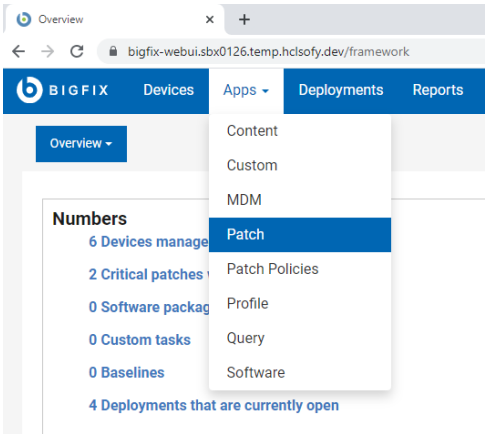


# Red Hat Patch Walk-thru Script: Out-of-Band Patching Scenario

We are already logged into the WebUI and are already familiar with the layout.

Sometimes there are patches that must be applied outside of normal maintenance windows, or “out of band”

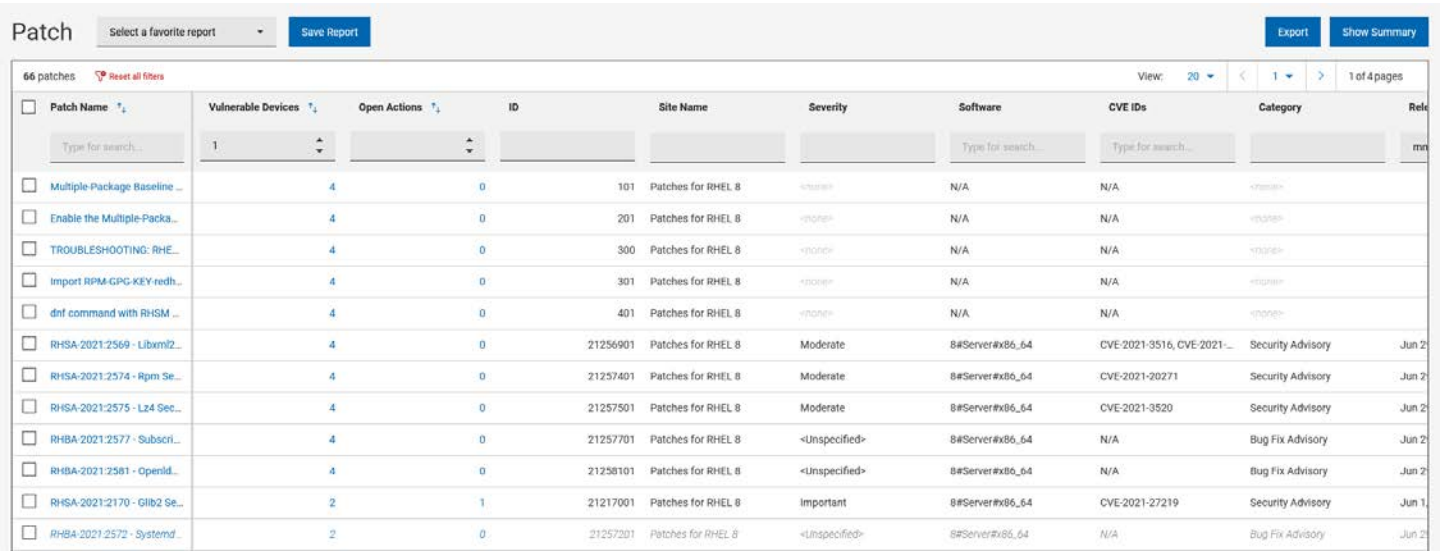
23. From the WebUI Overview Dashboard, Click Apps -> Patch.




Because this is an out-of-band patch scenario, our approach might be different. For instance, we might know the name of the patch we want to deploy, or we might know the name of the server that needs the patch.

24. Let us look for the patch by name first.

On this page we see, at a glance, the patches that are applicable in our environment right now. The BigFix Agent has already evaluated this current content and determined that it is applicable to the device on which it is running. Again, we did not have to initiate a scan or run a report – the agent already knows.



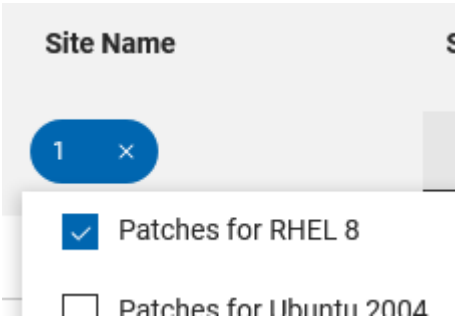

| Patch Name | Vulnerable Devices | Open Actions | ID | Site Name | Severity | Software | CVE IDs | Category |
|---|---|---|---|---|---|---|---|---|
| Multiple-Package Baseline ... | 4 | 0 | 101 | Patches for RHEL 8 | <none> | N/A | N/A | <none> |
| Enable the Multiple-Packa... | 4 | 0 | 201 | Patches for RHEL 8 | <none> | N/A | N/A | <none> |
| TROUBLESHOOTING: RHE... | 4 | 0 | 300 | Patches for RHEL 8 | <none> | N/A | N/A | <none> |
| Import RPM-GPG-KEY-redh... | 4 | 0 | 301 | Patches for RHEL 8 | <none> | N/A | N/A | <none> |
| dnf command with RHSM ... | 4 | 0 | 401 | Patches for RHEL 8 | <none> | N/A | N/A | <none> |
| RHSA-2021:2569 - Libxml2... | 4 | 0 | 21256901 | Patches for RHEL 8 | Moderate | 8#Server#x86_64 | CVE-2021-3516, CVE-2021-... | Security Advisory |
| RHSA-2021:2574 - Rpm Se... | 4 | 0 | 21257401 | Patches for RHEL 8 | Moderate | 8#Server#x86_64 | CVE-2021-20271 | Security Advisory |
| RHSA-2021:2575 - Lz4 Sec... | 4 | 0 | 21257501 | Patches for RHEL 8 | Moderate | 8#Server#x86_64 | CVE-2021-3520 | Security Advisory |
| RHBA-2021:2577 - Subscri... | 4 | 0 | 21257701 | Patches for RHEL 8 | <Unspecified> | 8#Server#x86_64 | N/A | Bug Fix Advisory |
| RHBA-2021:2581 - Openld... | 4 | 0 | 21258101 | Patches for RHEL 8 | <Unspecified> | 8#Server#x86_64 | N/A | Bug Fix Advisory |
| RHSA-2021:2170 - Glib2 Se... | 2 | 1 | 21217001 | Patches for RHEL 8 | Important | 8#Server#x86_64 | CVE-2021-27219 | Security Advisory |
| RHBA-2021:2572 - Systemd ... | 2 | 0 | 21257201 | Patches for RHEL 8 | <Unspecified> | 8#Server#x86_64 | N/A | Bug Fix Advisory |

The first column lists the Patch Name. Next to this column we see Vulnerable Devices. There is an entry in the grey box at the top of the column which means a filter has been applied, in this case, to only show patches that are applicable to at least one device in our environment right now. Because we are dealing with an applicable patch, we will leave this filter on.

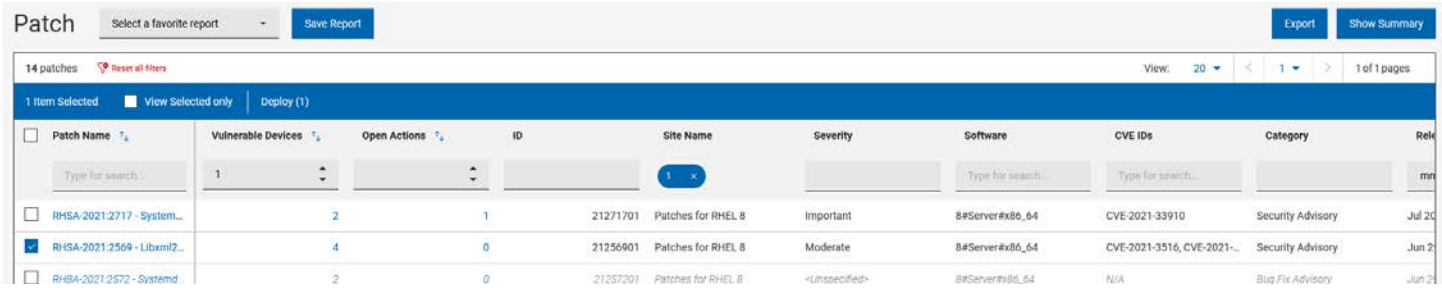
25. We have a patch that shows as Relevant at the time of writing this tutorial, but your results will be different. From this window, apply a filter, similar to the last exercise, to look for Patches for Red Hat endpoints only. The process is below but see if you can apply these filters by looking at the WebUI page. They are pretty intuitive.

    Red Hat Endpoints:

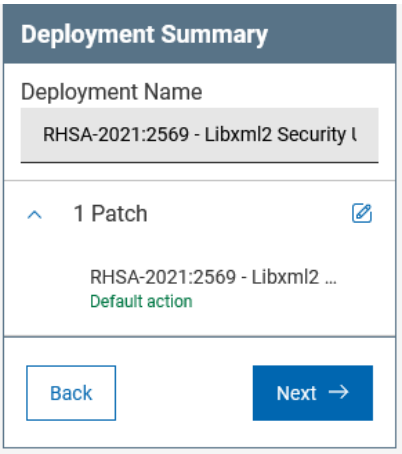
    - Expand **Operating System**
    - Check the box next to "Red Hat Enterprise Linux".




26. Now we are going to decide which of these patches to deploy as an "out of band" patch. Obviously if this were a real production environment, we would already have this information. For our demonstration, we will choose one patch from the list that we did not deploy in the previous example (note: your content may be different from what is displayed in the image below):

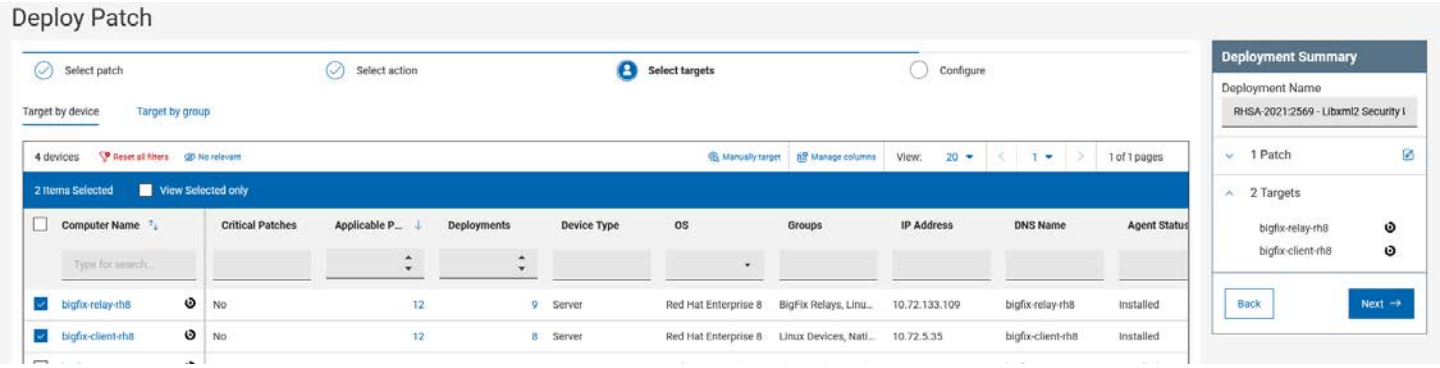



27. Click "Deploy" to deploy this patch
28. The sidebar on the right of the page lists the Deployment Summary
    a. This deployment name is the same as the patch we are deploying, since it is a single patch.
    b. We can edit the name, maybe add "OOB" to the name, or leave the name as-is.

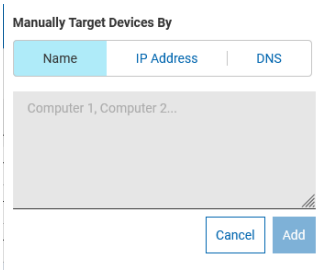



29. Click "Next" to continue the deployment process
30. **Select Targets**. In this step of the patch deployment, we choose what endpoints to deploy these patches to. The endpoints with applicable patches will show up in the list.
31. Check the box(es) next to the applicable device(s), or check the box next to "Computer Name" to select all devices

32. Click “Next” to continue the deployment process




NOTE: We could also choose to “Manually Target Devices” by clicking on the words “Manually target”. In the resulting box we could enter the device name. This is especially useful if you have the name(s) of the device(s) already and a lot of devices in the list. We can target by name, IP Address, or DNS Name. This makes sense in our example, because we might receive instructions to distribute “Patch123” to “EndpointABC” and is this case we could enter the name rather than search the list.




33. **Configure**. In this step we will specify how and when these patches are to be deployed, how and if the end user will interact, and actions to take after the patches have been deployed. There are five screens, and we will go through each one setting behavior and constraints that correspond to our scenario.

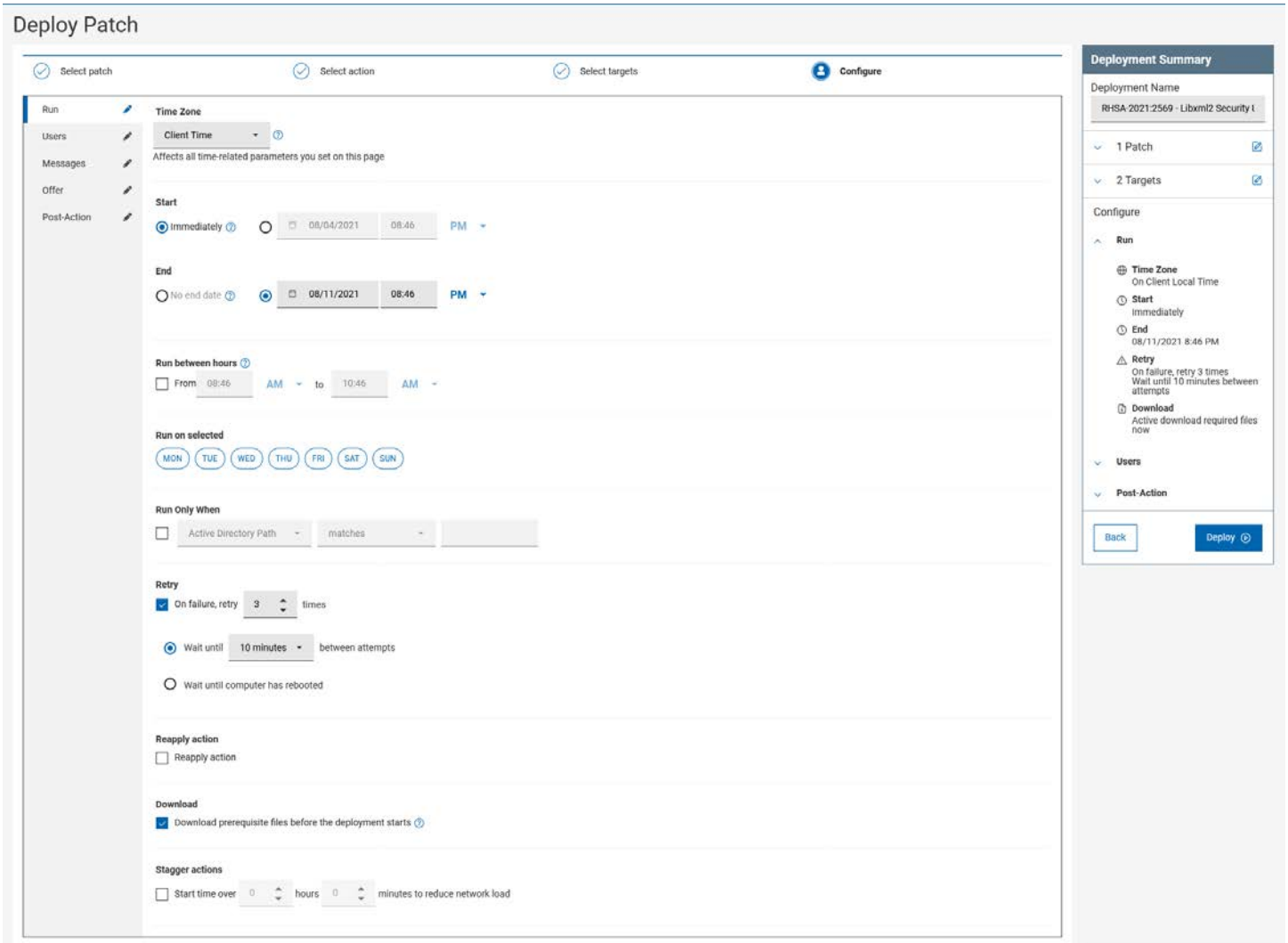
    Instructions for each page in the **Configure** step follow, along with settings for each. We will make settings adjustments according to our scenario.

Note: If you wish to exercise more settings than just the one in our exercise, click the paper and pencil icon next to the number of patches on the right and de-select some of the patches from this deployment. This will allow you to perform additional patch deployments and explore other deployment options.

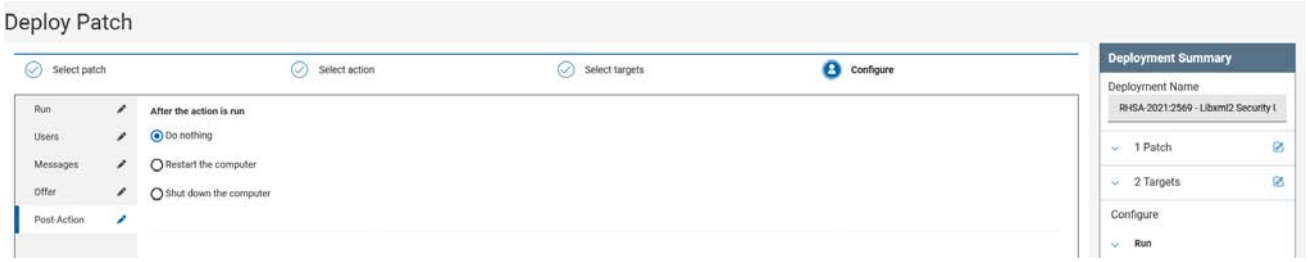
 

**Configure Options: Run** This page specifies schedule information for deploying patches. Make the following settings on this page:

a. Start: Use the default of “Immediately”
b. End: Use the end date of a week from today
c. Retry: Check this box to retry failed patches during the patch window, and accept the other defaults
d. Download: Check this box to download the required files now in case there is a delay in starting the patching.




e. The only other setting we will make is to restart the computer after patching. You will set this on the **Configure: Post Action** page:

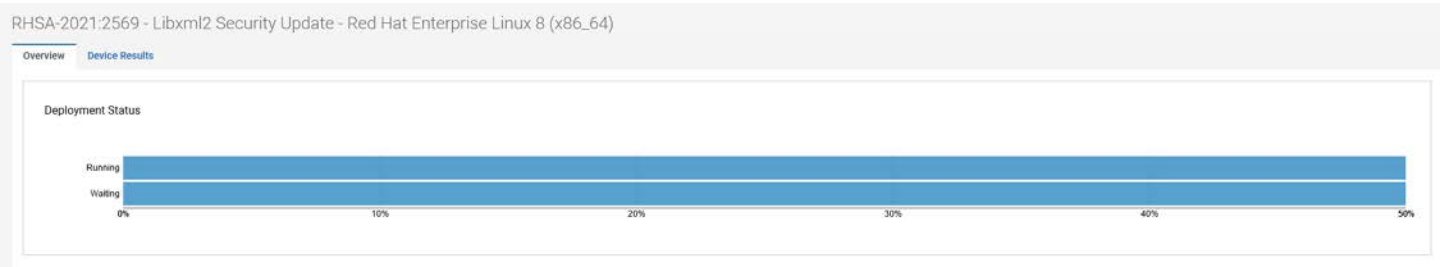


34. Verify your selections as necessary. When you are satisfied with the selections, click the blue “Deploy” button in the right sidebar.
35. You may now watch the deployment progress in the Deployment window


There is some useful information on this page:

a. Stop Deployment button. You can click on this button on the right to stop the deployment.


b. Overview tab. Shows the progress of the deployment.




c. Device Results tab. Gives an overview of the devices in the deployment and their current status.


d. There is no “Component Results” tab, as this deployment is only one component

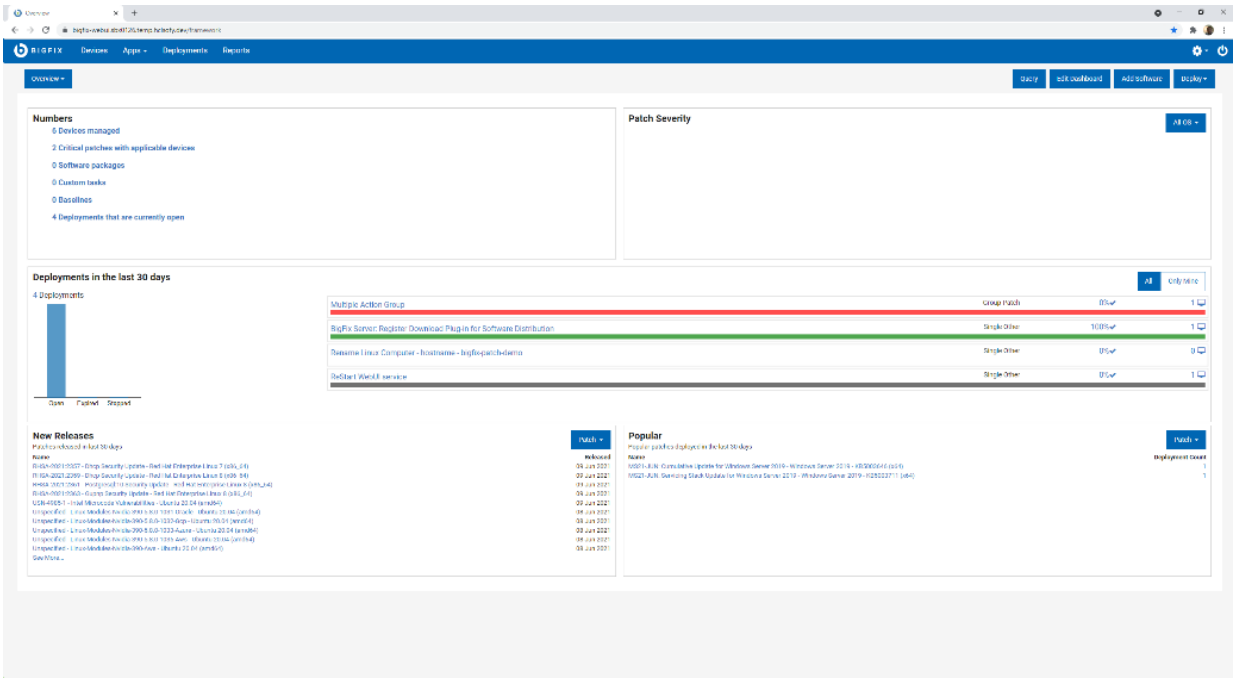
36. To perform the demo, navigate to https://hclsofy.com to create an environment, or to the WebUI URL you bookmarked previously.

NOTE: SoFy Solutions do not last forever; they have a maximum life of 24 hours at any given time. If you wait more than 24 hours without extending, the solution will expire, and you will have to create another one (see Extending Deployment Time for more information).

37. In this scenario we are going to apply Ubuntu patches using BigFix. We will apply some filters to look at Patches for Ubuntu, and we will focus on patches that are relevant in our environment right now. As we walk through this demonstration, feel free to work with the filters to see what choices you have, and how the selections change by applying and removing filters.
38. We will first log into the WebUI.
    a. This URL is located on the Solution Content -> HCL BigFix Preview -> General Information -> Open Link Button to the right of "HCL BigFix WebUI
    b. Use the User ID and Password located on this page to log into the WebUI.

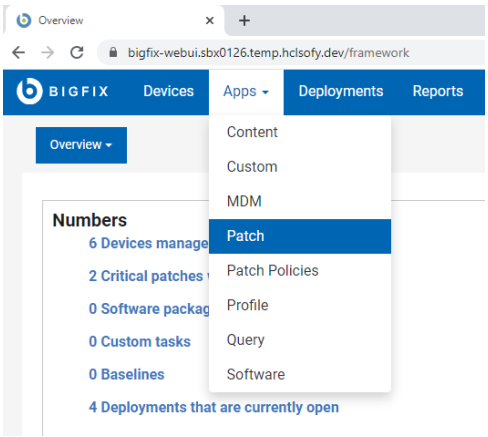

IMPORTANT: The username and the password are both case sensitive!

39. The first page you will see in the BigFix WebUI is the Overview Dashboard.

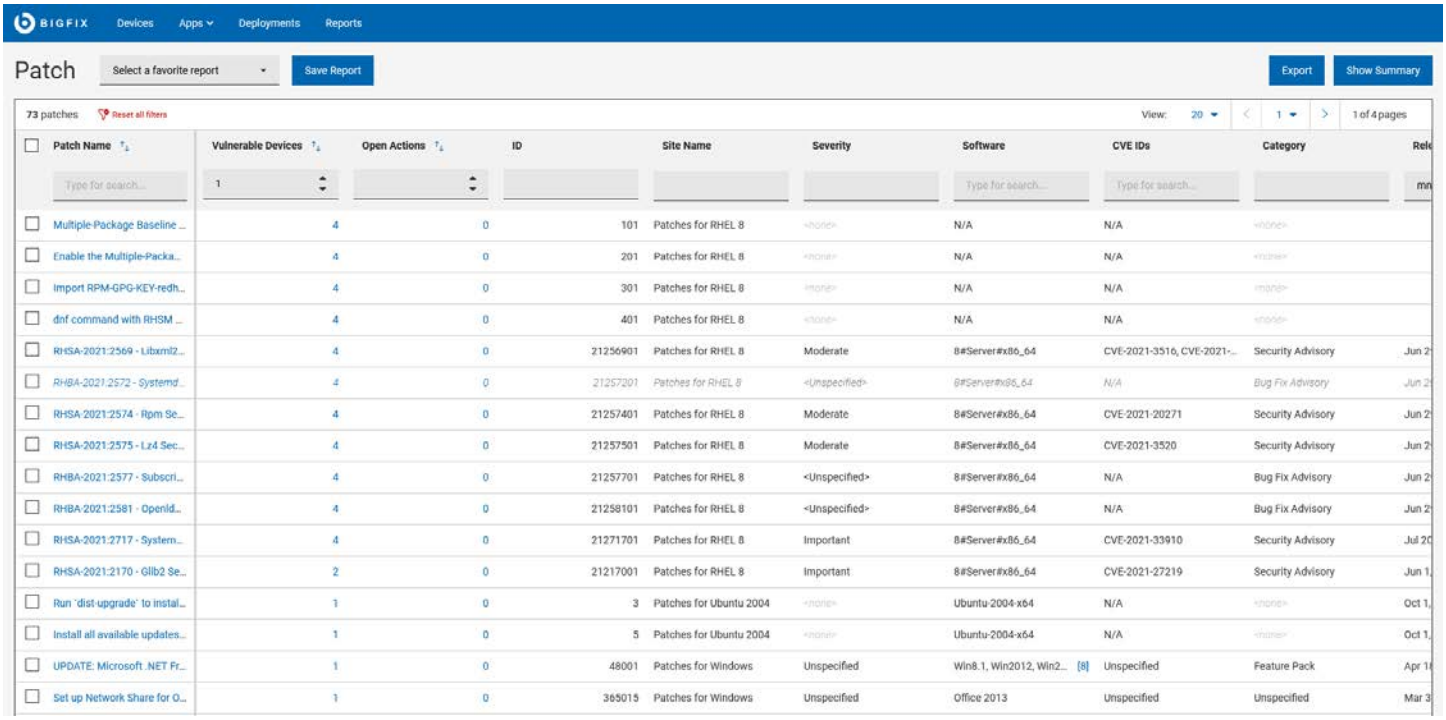



Take a minute to look around and see what information is available on this page. This is your "at-a-glance" information center for managing your infrastructure. This is data available to you without having to initiate an endpoint scan or run a report against a database. These tiles are customizable as well – you can re-arrange them or gather different data than what is currently visible.

40. From the WebUI Overview Dashboard, Click Apps -> Patch.




On this page we see, at a glance, the patches that are applicable in our environment right now. The BigFix Agent has already evaluated this current content and determined that it is applicable to the device on which it is running. Again, we did not have to initiate a scan or run a report – the agent already knows.



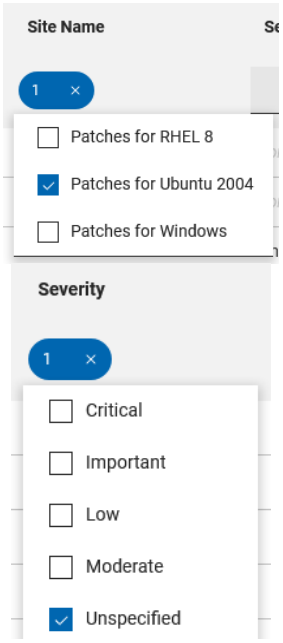

The first column lists the Patch Name. Next to this column we see Vulnerable Devices. There is an entry in the grey box at the top of the column which means a filter has been applied, in this case, to only show patches that are applicable to at least one device in our environment right now. If we turn the filter off by clicking on the "down" triangle to the right of the number "1", we can see all patch content available in BigFix right now.

41. Go ahead and turn off this filter to see more content. You will notice the number of patches in the top left corner increases when you do.

    We will turn this filter back on in a minute during the patching process.

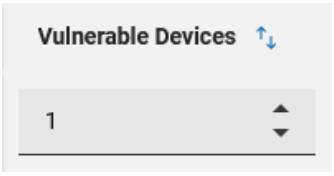
42. We will set up some filters to look for Patches of a Critical Severity on Windows endpoints only and are applicable to endpoints in our environment right now. The process is below but see if you can apply these filters by looking at the WebUI page. They are pretty intuitive.

a. Apply a filter to see only Ubuntu patches
   - Click in the grey box in the "Site Name" column
   - Check the box next to "Patches for Ubuntu <version>"
   - As with patch severity above, note the number one (1) in the blue oval in the header. This means we have applied a filter to this column
   - Click anywhere on the page to collapse the "picker"



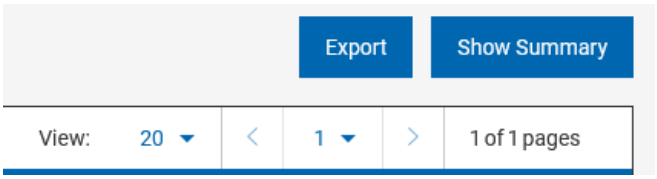

b. Apply a filter to see only Critical patches
   - Click the grey box in the "Severity" column
   - Check the box next to "Critical"
   - Note the number one (1) in the blue oval in the header. This means we have applied a filter to this column
   - Click anywhere on the page to collapse the "picker"

c. Apply a filter to see currently applicable patches
   - Remember that we turned this filter off in step 6.
   - Click the "up" triangle in the grey box in the "Vulnerable Devices" column
   - Note the "1" in the grey box

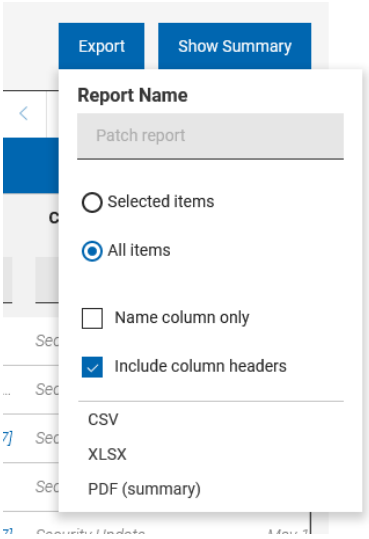



Also note that the list of patches has decreased

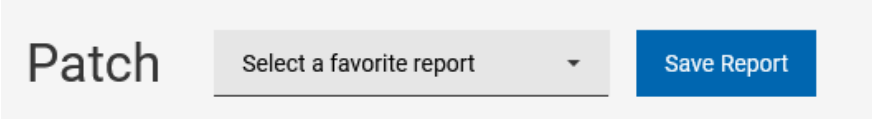
43. We also have the option to export this information to a file.



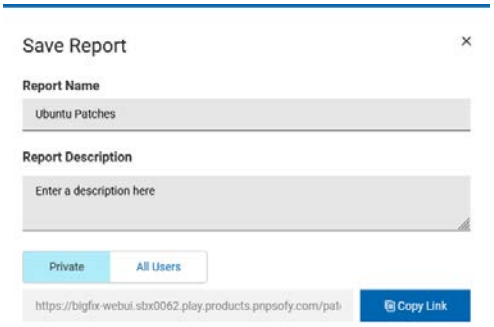

a. Click on the "Export" button at the top right
b. Give the report a name
c. Specify whether you would like to export all items or the items you have selected (if you have selected any items yet)
d. Specify the type of file you would like to save the report as (CSV, Excel, or PDF)
e. Choose to open or save the report



44. We can also save this current filter as a Report for later use.

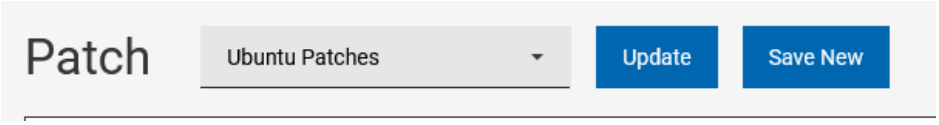



a. Click on the blue “Save Report” button and enter information about the report
b. Provide a meaningful name
c. Provide a description for the Report
d. You can make the report Private (available only to you) or you can make it available to All Users.
e. You also see the report URL, which you can bookmark for later, or share with others.



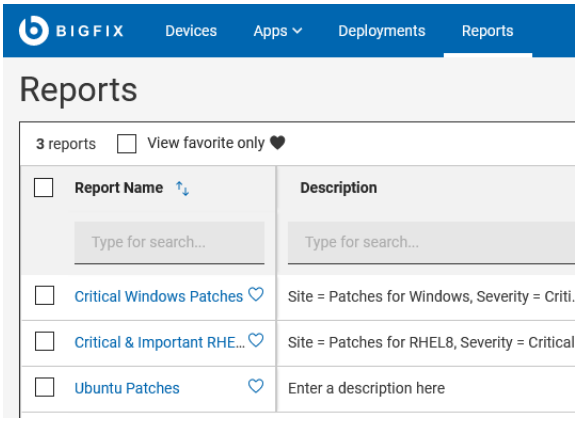

Note: the URL is a link to the report in this BigFix environment, and anyone you share the report with must have access to this environment.

Feel free to explore the other filters to see what other criteria are available. If you make any changes to the filters, you will see the header change from “Save Report” to “Update/Save New”



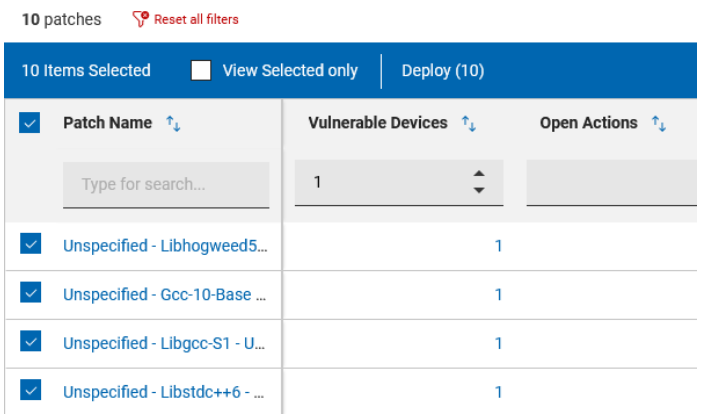

If you click “Update” you will overwrite the existing report with the new filters. If you click “Save New” you will be prompted to enter details about a new report

You can also return to the original report by clicking “Reports” in the menu bar at the top, and selecting your report from the list



45. Now we are going to decide which of these patches to deploy. Based on our filters, these are all the "Unspecified" Ubuntu patches that are applicable to devices in our environment right now.
46. If we want to deploy all of them, we simply check the box at the top of the "Patch Name" column and click "Deploy". The number of selected patches appears next to "Deploy"

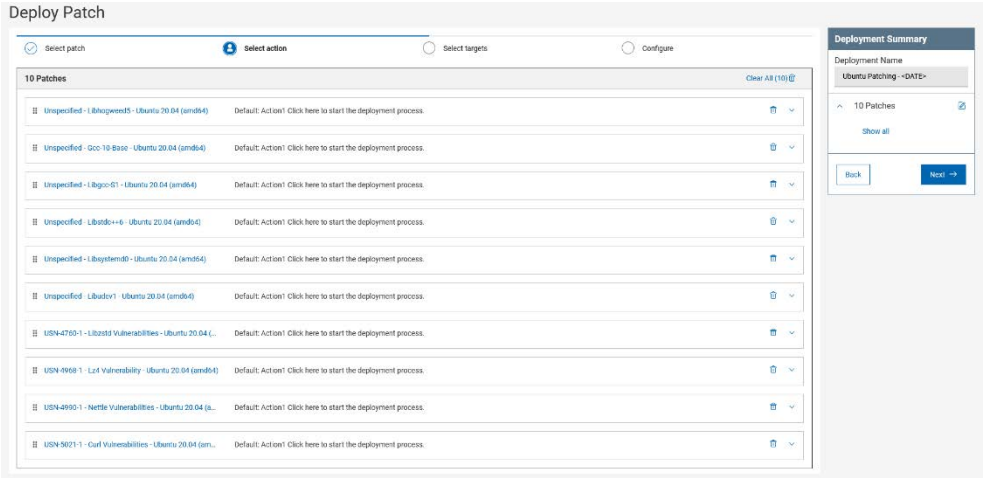
NOTE: The number of applicable patches in this guide may differ from what you see in your view.




47. The sidebar on the right of the page lists the Deployment Summary
    a. This deployment name is "Multiple Action Group" by default, because we are deploying multiple patches, or taking multiple actions with BigFix.
    b. Enter a meaningful name in the grey Deployment Name box. This allows us to tell this deployment apart from other deployments.
    c. If we wish to change the patches being deployed we can click on the "paper and pencil" icon to the right of the number of patches

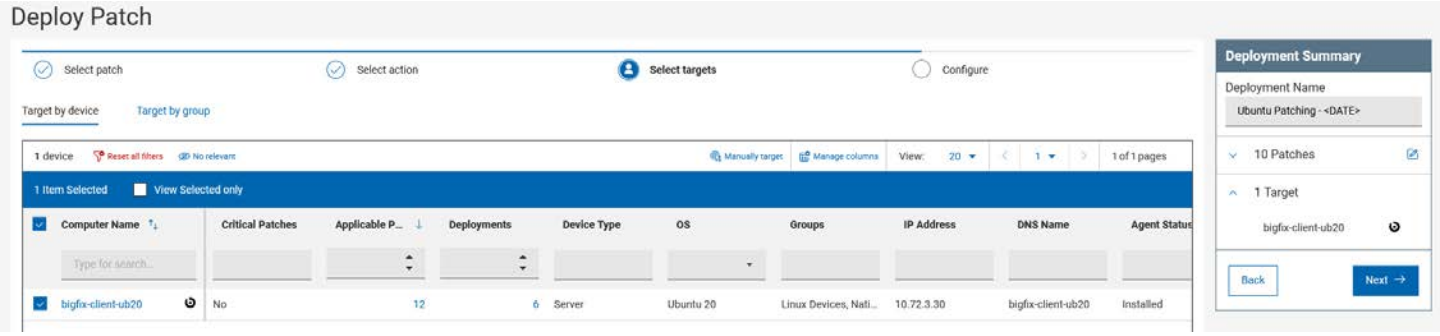

48. Click "Next" to continue the deployment process

49. **Select Action**. In this step of the patch deployment, we ensure that the correct Action is selected for each patch. Many patch Fixlets contain what is call a "Default Action" meaning this action is selected by default. In the case of a patch, the default action is to deploy the patch. Sometimes however, there is no default action, because there is more than one viable option for a patch deployment. On this screen, we make sure each patch has an action selected, default or otherwise. We can also remove patches from the list by clicking on the blue trash can icon on the right.




50. Click "Next" to continue the deployment process.

51. **Select Targets**. In this step of the patch deployment, we choose what endpoints to deploy these patches to. The endpoints with applicable patches will show up in the list.
52. Check the box(es) next to the applicable device(s), or check the box next to "Computer Name" to select all devices
53. Click "Next" to continue the deployment process




NOTE: In this tutorial, the number of endpoints is one, but yours may be different.

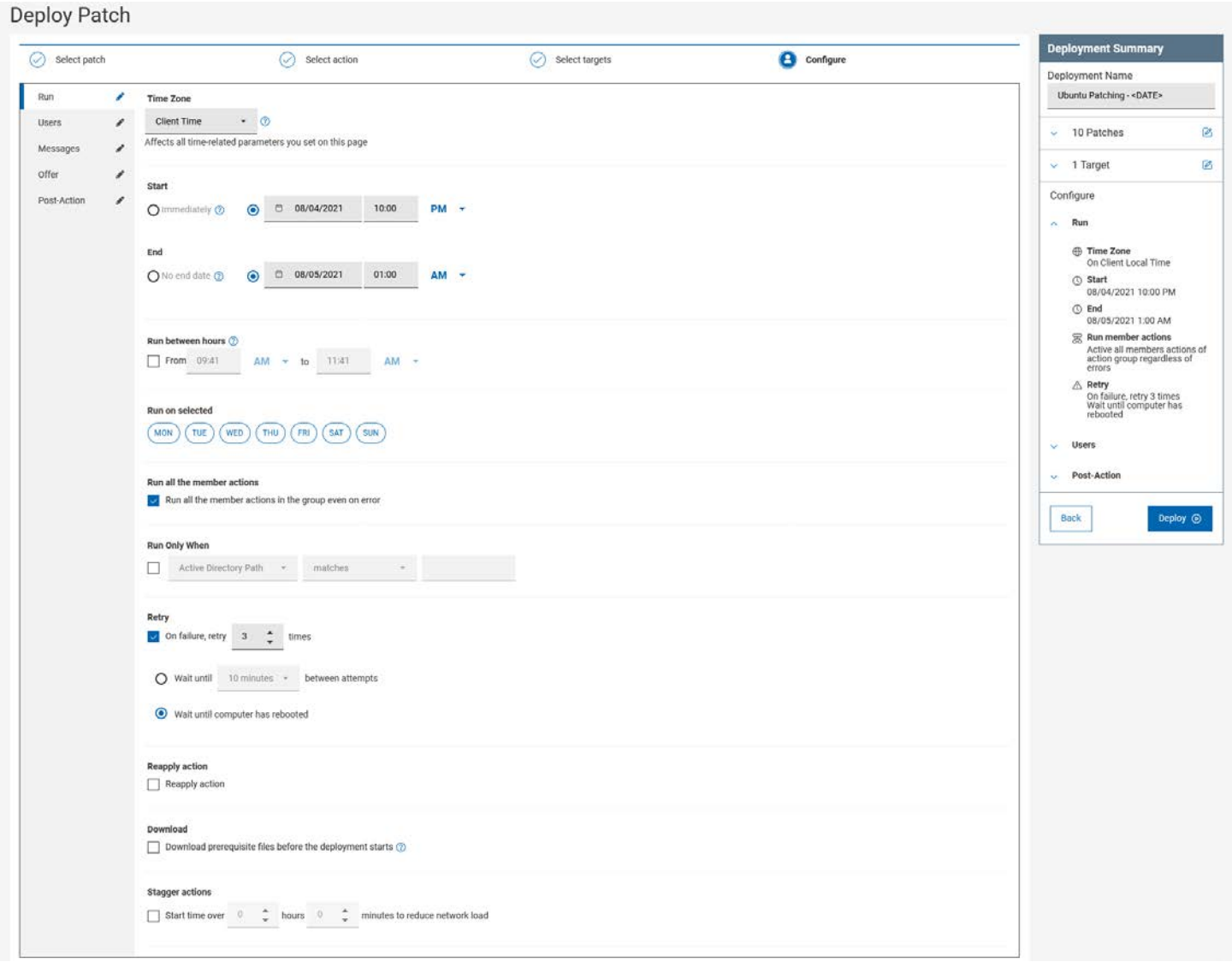
54. **Configure**. In this step we will specify how and when these patches are to be deployed, how and if the end user will interact, and actions to take after the patches have been deployed. There are five screens, and we will go through each one setting behavior and constraints that correspond to our scenario.

    Instructions for each page in the **Configure** step follow, along with settings for each. We will make settings adjustments according to our scenario.

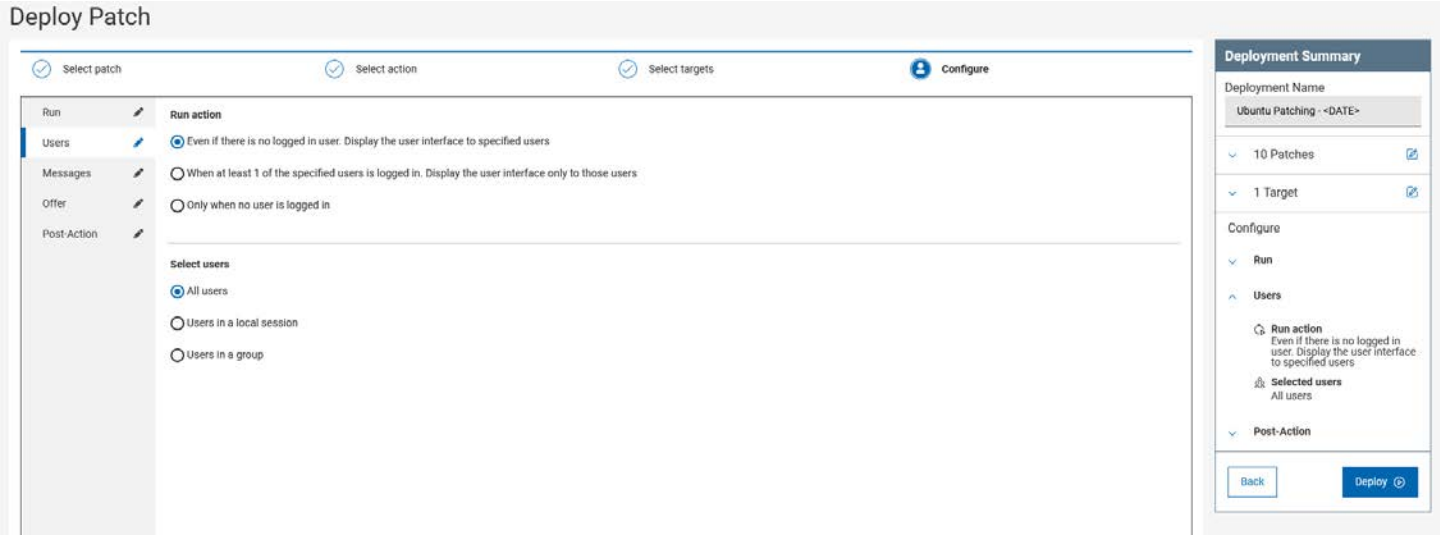
Note: If you wish to exercise more settings than just the one in our exercise, click the paper and pencil icon next to the number of patches on the right and de-select some of the patches from this deployment. This will allow you to perform additional patch deployments and explore other deployment options.

**Configure Options: Run** This page specifies schedule information for deploying patches. Make the following settings on this page:

- Start: Use today's date and the time of 10:00pm
- End: Use tomorrow's date and the time of 1:00am
- Retry: Check this box to retry failed patches during the patch window. Click the radio button for "Wait until computer has rebooted"

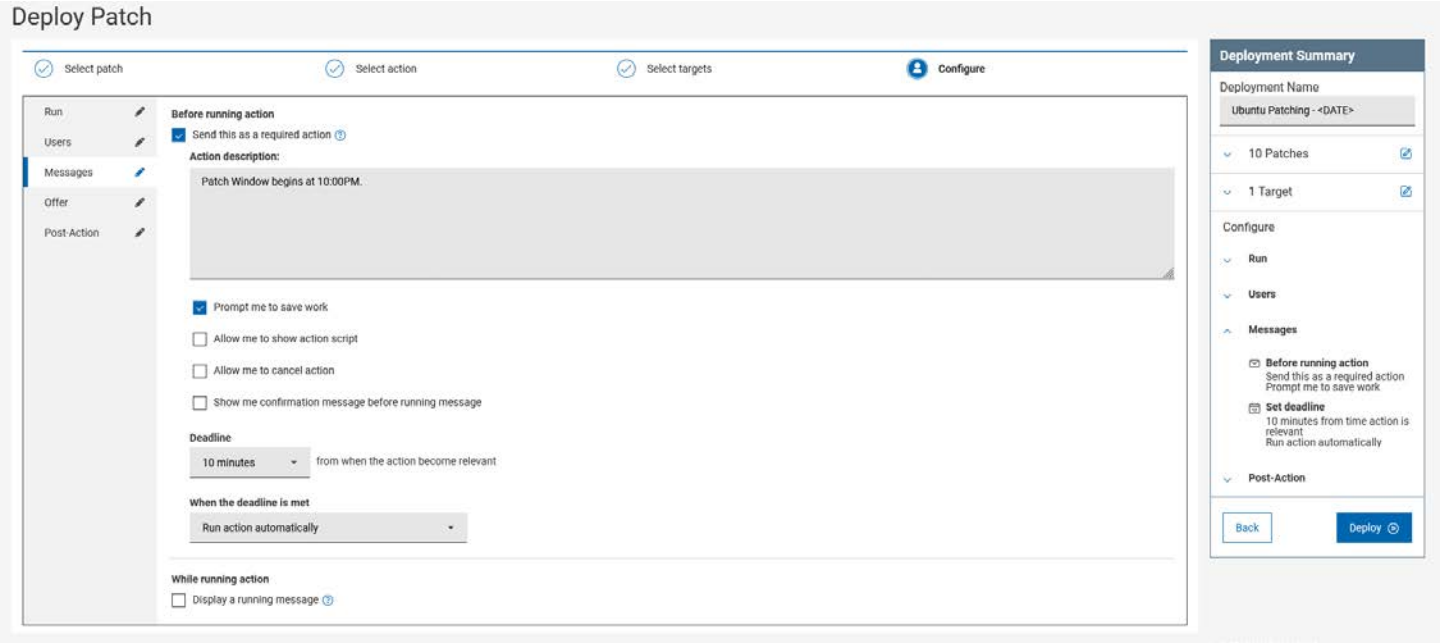


**Configure Options: Users**. This page specifies how the patch deployment behaves according to logged-in users. In our scenario the retail establishments are closed which means that no users are logged in. We will not make any settings changes on this page.



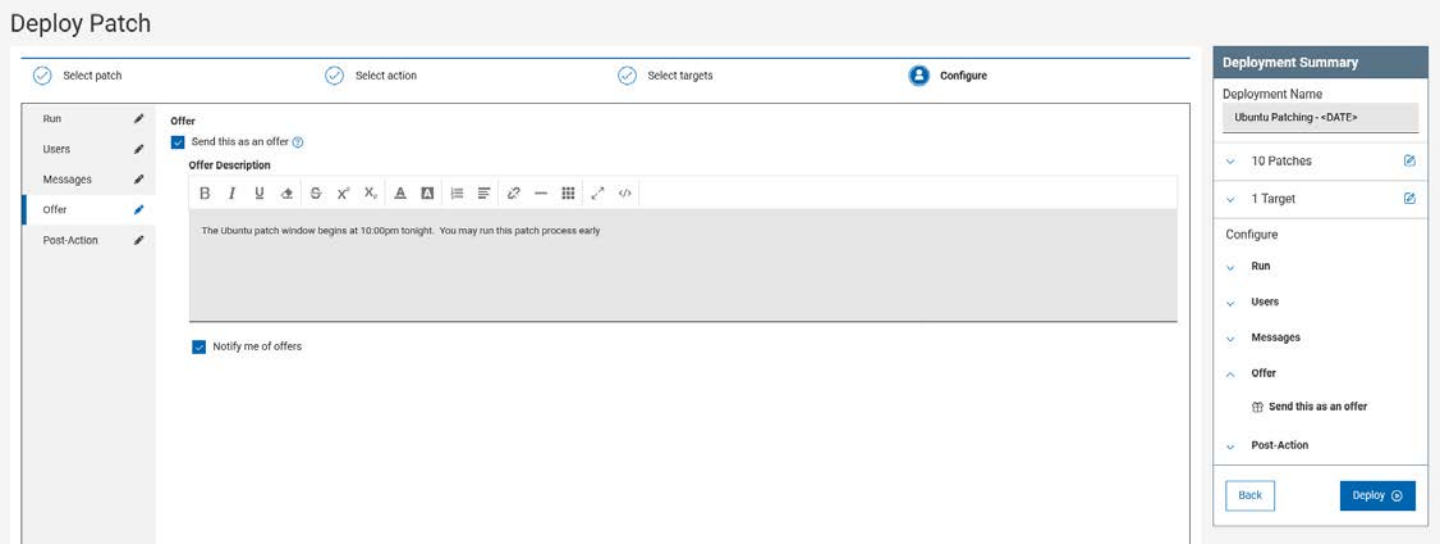

**Configure Options: Messages**. This page allows us to display information about a pending and/or running action for end-users. Depending on the week and month, there may be people working late, and logged into one of these systems. We will send a notice that the patch process is about to start.

- Before running action: Check the box to send this as a required action
- Action description: Enter a description in the grey box



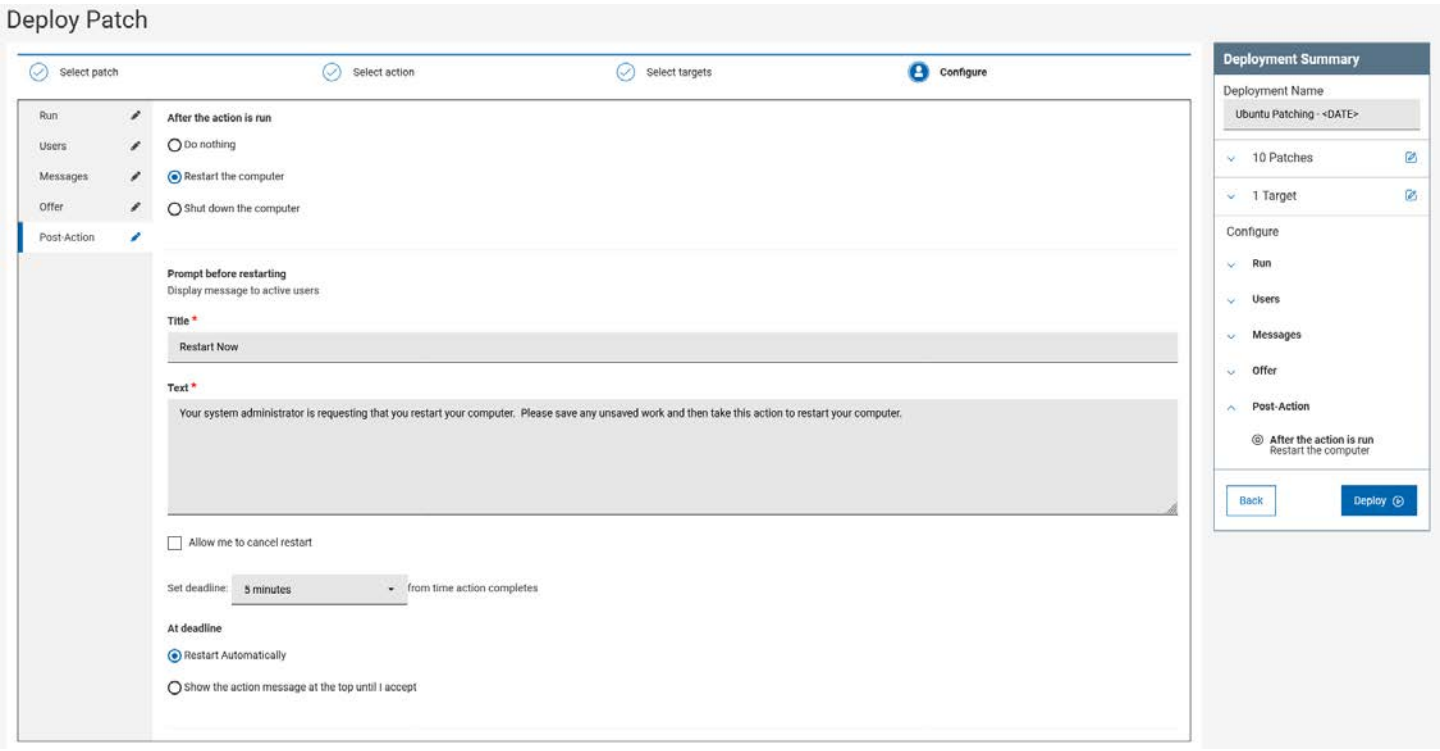
**Configure Options: Offers.** This page allows logged-on users to run the patch deployments outside of the “Run” window. We will allow these users to kick off the patch process early if they choose.

- Offer: Check the box to send as an offer
- Offer Description: Enter a description in the grey box
- Check the box to notify the logged-on user about this offer



**Configure Options: Post Action**. This page allows us to restart or shut down endpoints after patching.

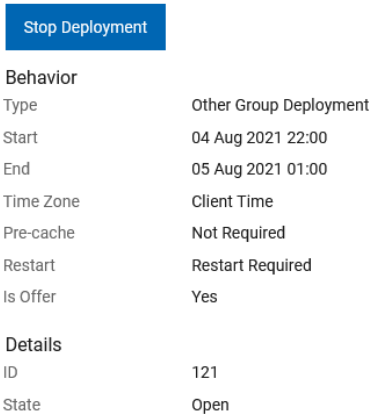
a. We will reboot the endpoints after the patch cycle, so select the “Restart the computer” radio button
b. We will accept the default Title and Text under “Prompt before restarting”
c. Leave the “Allow me to cancel restart” unchecked. “Me” is the end-user, not the administrator
d. Set the Deadline for 5 minutes from time action completes
e. Accept the “Restart Automatically” default radio button in the “At Deadline” section.



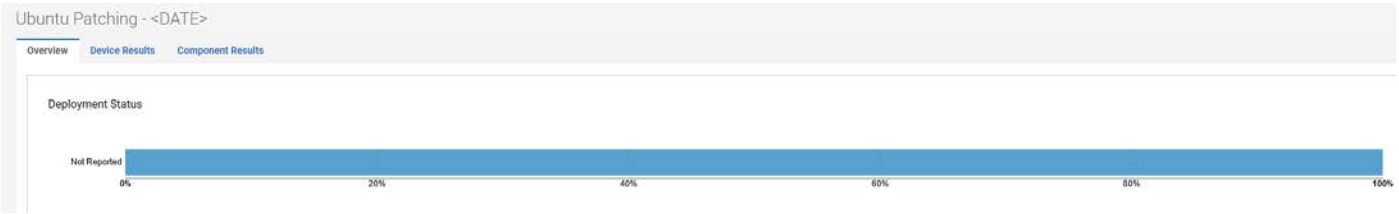

55. Verify your selections as necessary. When you are satisfied with the selections, click the blue “Deploy” button in the right sidebar.
56. You may now watch the deployment progress in the Deployment window

There is some useful information on this page:

a. Stop Deployment button. You can click on this button on the right to stop the deployment. Any currently running patch installations will continue to run, but subsequent patches will not install.

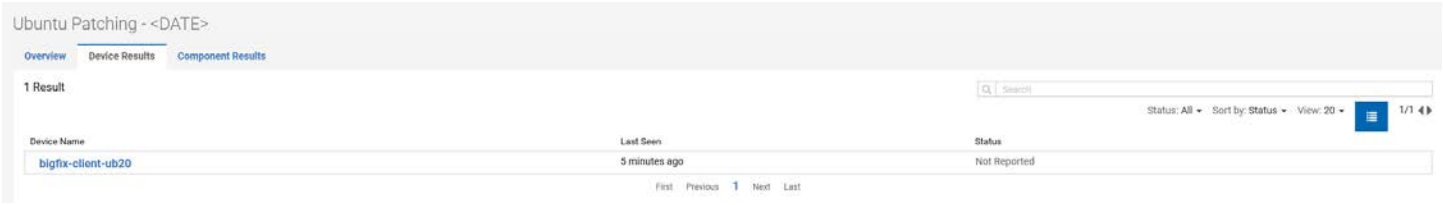



b. Overview tab. Shows the progress of the deployment.

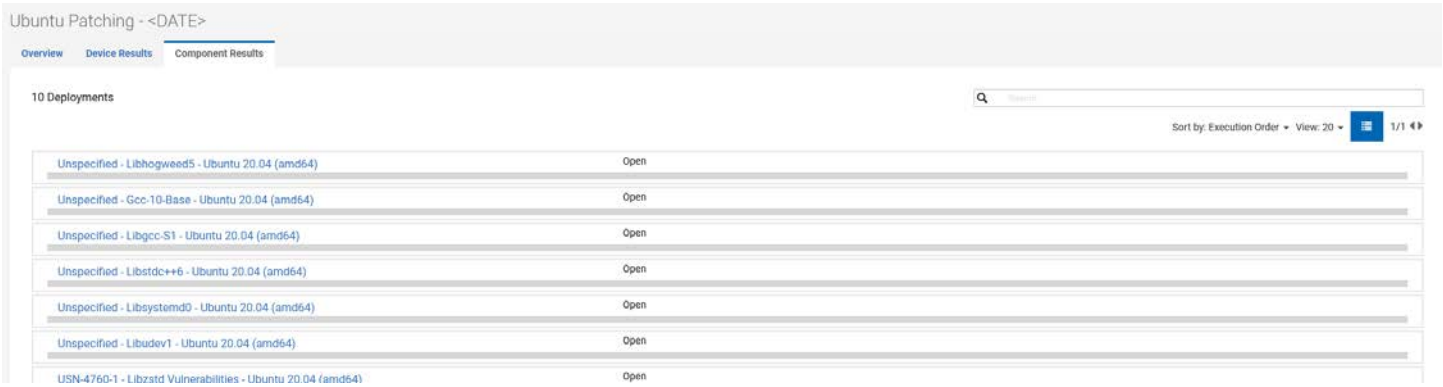



c. Device Results tab. Gives an overview of the devices in the deployment and their current status.

Note: When you click on the Device Results" tab, you may see messages such as "Constrained by distribution time" or "Constrained by distribution date." This has to do with the fact that the patch distribution is scheduled in the future. It is expected, not an error.




d. Component Results tab. Gives the status of each component/patch in the deployment



# BigFix Patching Scenario – Using Patch Policies

## Executive Summary

A Patch Policy is a set of criteria that defines a patch list; that is, a collection of Fixlets that meet the patching criteria of a specific set of endpoints.

Patch Policies enable you to enforce your organization's patching cycles and security guidelines, to ensure continuous security and compliance for your organization. With Patch Policies, you can create patching schedules for different groups of machines and assign different deployment behaviors to each. You can also set patch timing, frequency and duration, pre-caching and retry behavior, stagger start times, bypass errors, and notify device owners when a restart is pending.

BigFix Patch Policies:

- Enable you to choose what content is available for your patch process
- Allow you to update content on a schedule, so you always have the latest content if the vendor makes a change
- Allow you to create different schedules for patching endpoints
- Can be completely automated end-to-end, or policies and schedules can be enabled and disabled as needed

Here are some examples of a Patch Policy:

Distribute all critical and important patches to all Windows 10 workstations beginning the Friday after the second Tuesday of the month and keeping the content available until the last day of the month.

Another example of a Patch Policy is to test all Critical Windows Server patches by distributing them to a group of test servers at 10:00pm on the second Tuesday of the month, and based on the successful outcome, distributing the same patches to a group of DEV servers at 10:00pm on the Wednesday after the second Tuesday of the month, and distributing the same patches (as long as successful) to the production servers on the Friday after the second Tuesday, between 10:00pm and 11:59pm

Another example is the requirement to patch the platform (operating system) of a group of production database servers, but not the application (MS SQL) running on those servers, and to perform this patch process the Saturday after the second Tuesday, between 10:00pm and 11:59pm.

Patch Policies can be used in three ways:

Fully Automated Patching. You can set a Patch Policy to check for applicable patches on a specified interval. You can then enable a patching schedule that automatically delivers this patch content to the endpoints you specify. This method takes advantage of the automation within BigFix to apply a "Set it and forget it" methodology to patching endpoints.

Semi-Automated Patching. You can set a Patch Policy as indicated above and set up multiple schedules for the endpoints you want to patch (test, dev, prod), and suspend the schedules so the endpoints are not patched until the patch content has been tested in your environment.

Scheduled and/or exception patching. You build a patch policy with schedules that dictate when different groups of endpoints get patched, and endpoints and/or endpoint groups are added or removed to the schedules as needed

## Scenario

You are a retail customer with establishments where you serve your own customers. You have a central datacenter at your corporate office, regional distribution centers, and retail stores.

The endpoints in your environment are managed different ways depending on their location and purpose. For purposes of this scenario, the endpoints are distributed as follows:

- Windows devices represent the point-of-sale devices (POS) in your retail stores
- Ubuntu devices represent other devices in your retail stores
- Red Hat devices represent devices in your datacenter and your regional distribution centers

The patch process for your company has been established to support the business, and your job is to enforce the process to protect the business interests. You must patch your endpoints, regardless of location, on a schedule that does not interfere with retail business hours. You must be able to select patches based on severity and operating system, and you must be able to deploy patches on different schedules with different procedures based on location, function, or operating system. Finally, you must have the ability to perform all functions without the aid of a local operator.

Note: this demonstration scenario and the script below is provided as a means of familiarizing you with how BigFix works. Even if your business does not line up with the retail model, most businesses have endpoints in more than one location, and must apply patches on varying schedules with varying requirements. Once you are familiar with the solution, feel free to exercise it using different scenarios, or use your own patching scenario.

# Windows Patch Policies Walk-thru Script: Weekly Patch Cycle

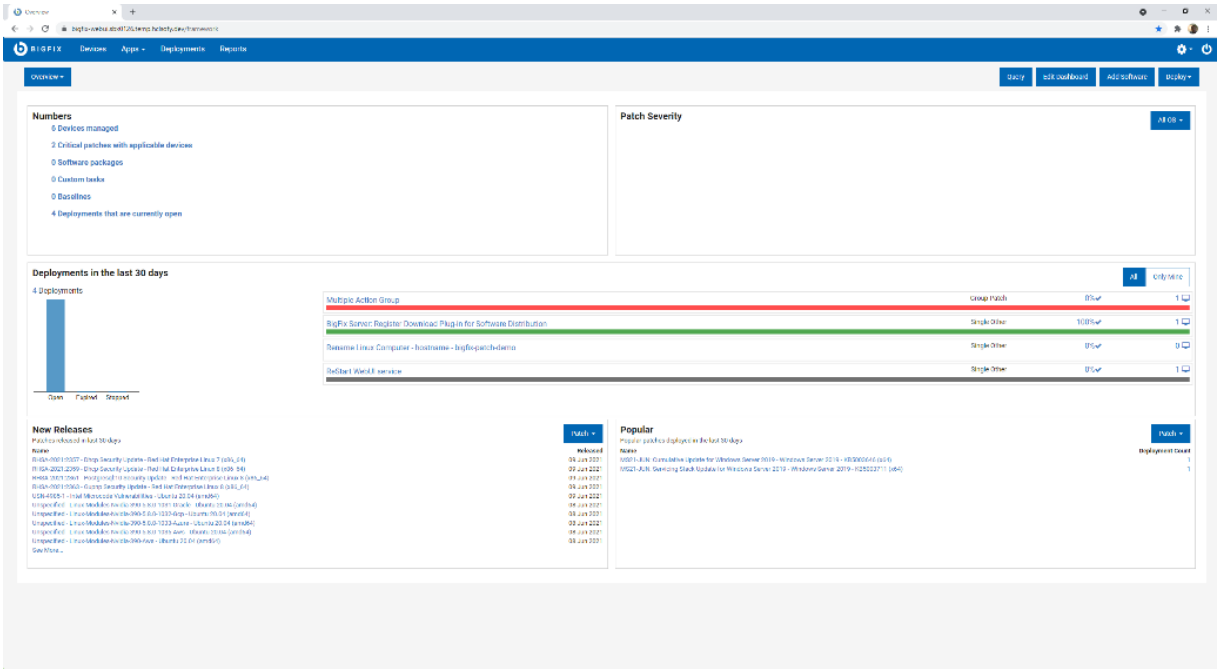
57. To perform the demo, navigate to https://hclsofy.com to create an environment, or to the WebUI URL you bookmarked previously.

NOTE: SoFy Solutions do not last forever; they have a maximum life of 24 hours at any given time. If you wait more than 24 hours without extending, the solution will expire, and you will have to create another one (see Extending Deployment Time for more information).

58. In this scenario we are going to apply Windows patches using BigFix. We will apply some filters to look at Critical Patches for Windows, and we will focus on patches that are relevant in our environment right now. As we walk through this demonstration, feel free to work with the filters to see what choices you have, and how the selections change by applying and removing filters.
59. We will first log into the WebUI.
    a. This URL is located on the Solution Content -> HCL BigFix Preview -> General Information -> Open Link Button to the right of "HCL BigFix WebUI
    b. Use the User ID and Password located on this page to log into the WebUI.

    IMPORTANT: The username and the password are both case sensitive!

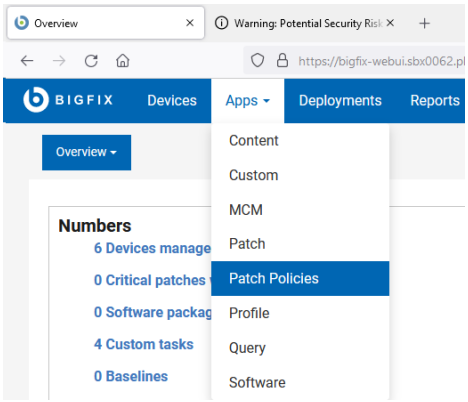

60. The first page you will see in the BigFix WebUI is the Overview Dashboard.




Take a minute to look around and see what information is available on this page. This is your "at-a-glance" information center for managing your infrastructure. This is data available to you without having to initiate an endpoint scan or run a report against a database. These tiles are customizable as well – you can re-arrange them or gather different data than what is currently visible.

## Creating a Patch Policy #1

61. From the WebUI Overview Dashboard, Click Apps -> Patch Policies.




62. This is where we create different policies for the content we want to deploy. Since there are no existing Patch Policies, we will need to create one. Click the “Add Policy” button in the top right corner


63. Enter the following information to create the Patch Policy:
    a. Policy Name: Red Hat Patch Policy
    b. Site: Demo
    c. Description: Enter a meaningful description, that will be useful after you have created multiple policies
    d. Include Content: External Content
    e. Operating Systems: Red Hat Enterprise Linux
    f. Severity: Critical & Important
    g. Category: Bug Fix & Security
    h. Type: OS Updates
    i. Include Patches for: Red Hat Enterprise 7 & Red Hat Enterprise 8
    j. Auto-refresh: Click the “Enable” button and change the time to 5:00am
    k. Change the Timezone to (GMT-5:00) Eastern Time (US and Canada).

    A screen image follows to reference the appropriate settings

**Patch List Criteria**

Policy Name *
Red Hat Patch Policy

Site *
Demo

Description (optional)
External content
Red Hat Enterprise Linux 7 & 8
Bug Fix & Security
OS Updates
Auto-refreshes monthly, 1 day after the 2nd Tuesday at 5am Eastern Time

Include Content *
- [ ] Custom content
- [x] External content

**Include External Content**

Operating System *
- ○ CentOS
- ○ Oracle Linux
- ◉ Red Hat Enterprise Linux
- ○ SUSE Linux Enterprise
- ○ Ubuntu
- ○ Windows

Severity *
- [x] Critical
- [x] Important
- [ ] Moderate
- [ ] Low
- [ ] Unspecified

Category *
- [x] Bug Fix
- [ ] Enhancement
- [ ] Mandatory
- [ ] Optional
- [ ] Recommended
- [x] Security
- [ ] Service Pack

Type *
- [x] OS Updates
- [ ] OS Application Updates
- [ ] 3rd Party Updates

Include Patches for:
- [ ] Red Hat Enterprise 5
- [ ] Red Hat Enterprise 6
- [x] Red Hat Enterprise 7
- [x] Red Hat Enterprise 8

**Exclude Content**

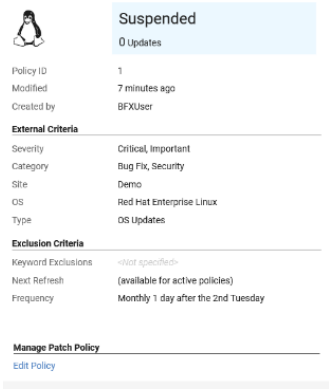
Exclude from this policy any patch whose title contains one of these keywords:
Enter keywords

**Auto-refresh** Disable

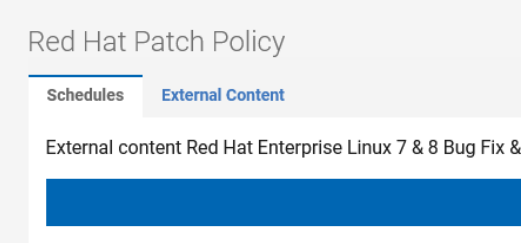
This policy refreshes Monthly
1 Day after the 2nd Wednesday
At 05 : 00 AM
Timezone: (GMT-05:00) Eastern Time (US and Canada)

64. Click “Save” to save the policy

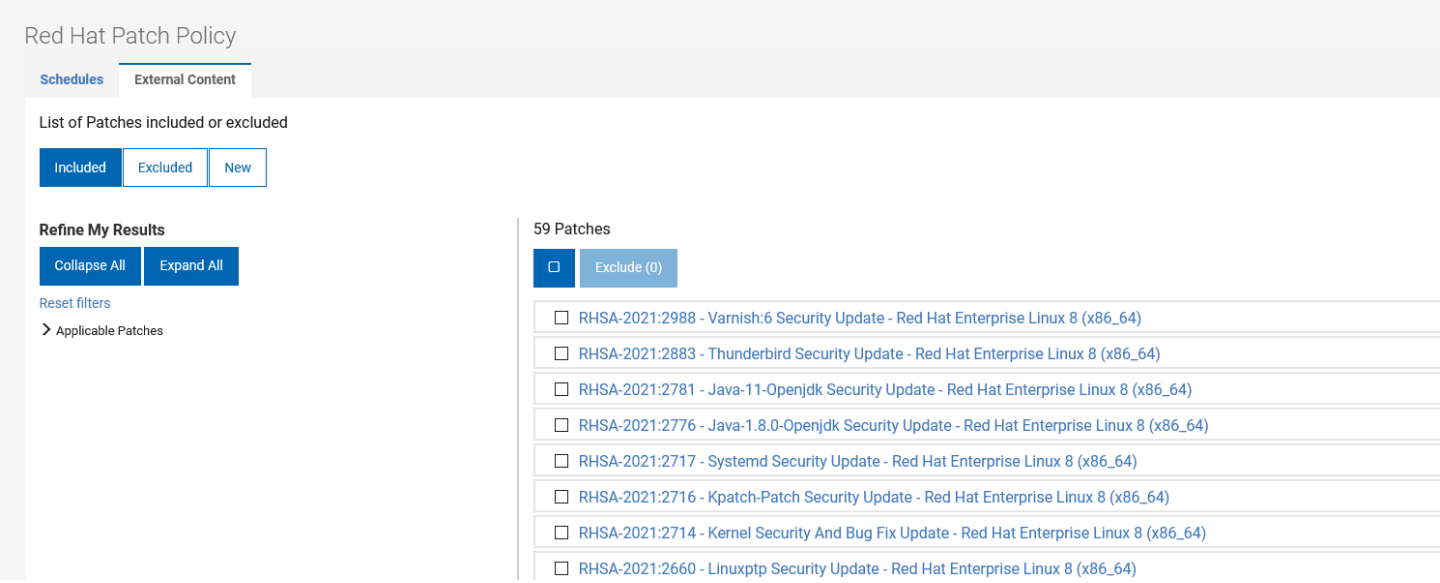
65. The right pane displays the new policy details. The Patch Policy state is **Suspended** when created, and the **Activate** button is not available until at least one schedule is added



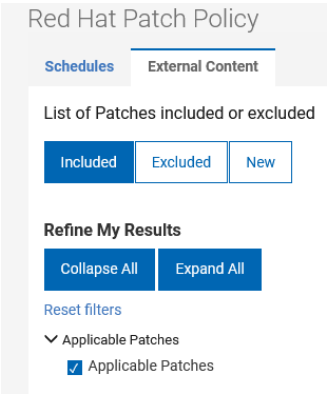
66. Click on the “External Content” tab to view the patches included in this policy



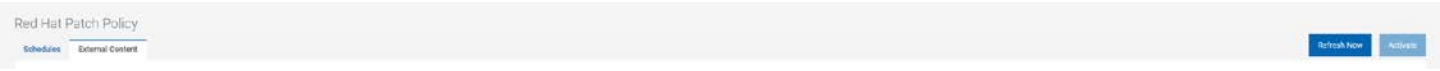

67. The screen displays the list of patches included in the policy




68. Under “Refine My Results” click the “Expand All” button
69. Check the box next to “Applicable Patches”
70. Notice the list of patches decreases in number. This allows you to control the patches included in your patch deployment.
71. We will leave the box un-checked for this exercise, so un-check the box

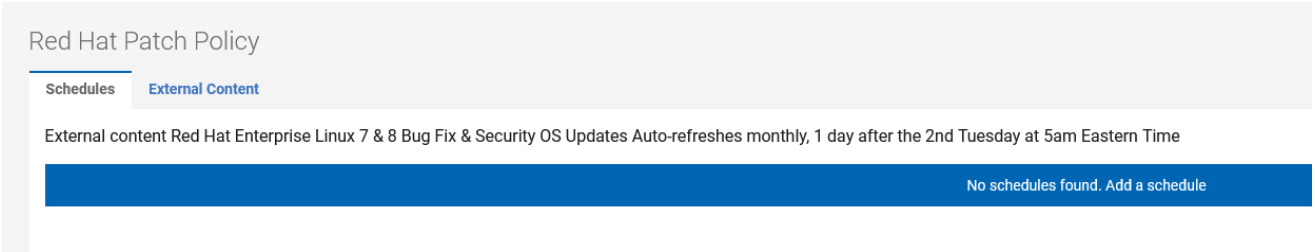



72. The “Refresh Now” button refreshes the applicable patch list, overriding the schedule we set when we created the policy
73. The “Activate” button is not available until we add a schedule to this policy

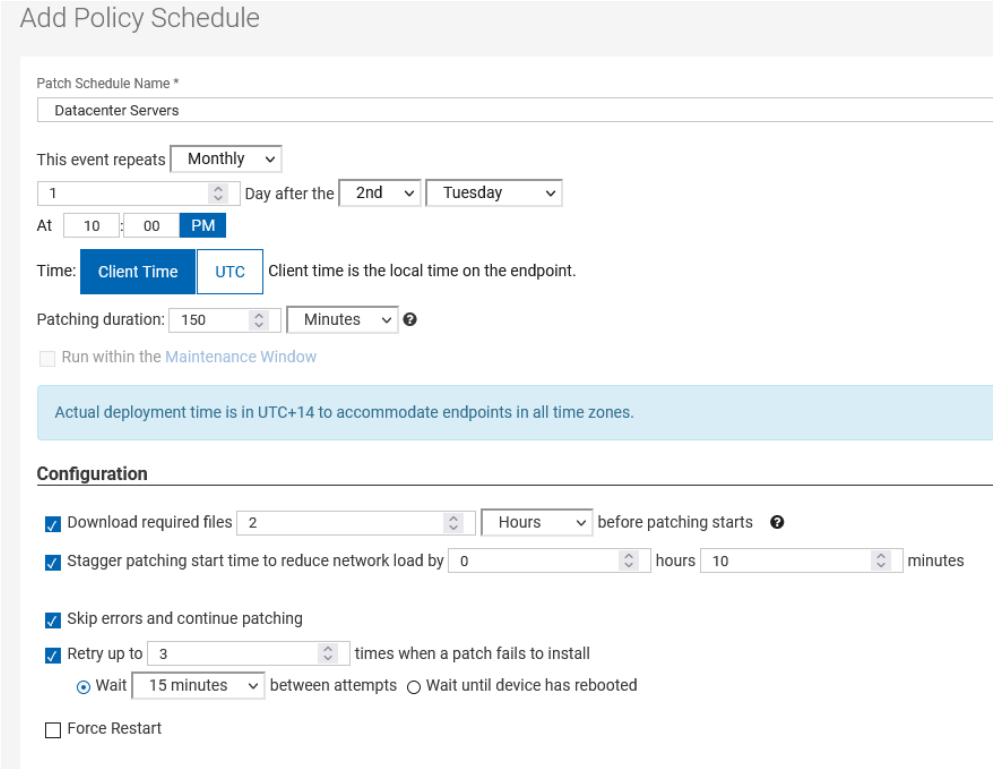


## Adding a Schedule to a Patch Policy

74. Click on the “Schedules” tab to return to the previous window and click the blue bar to add a schedule.



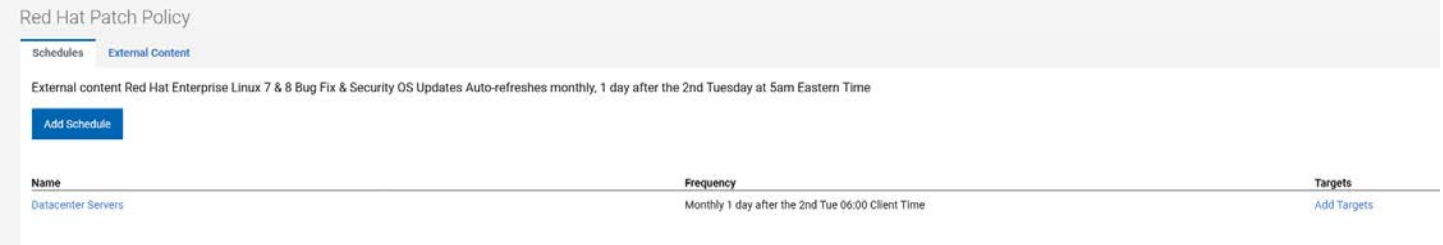

75. We will use the same schedule as the Red Hat Patch Exercise.
    a. Patch Schedule a Name: Datacenter Servers
    b. This event repeats: Monthly (no change)
    c. No change to “1 Day after the 2nd Tuesday”
    d. At: The servers in the datacenter are patched at 10pm, so change the time to 10:00 PM
    e. Time: No change, use “Client Time”
    f. Patching Duration: 150 Minutes (the window is 2 ½ hours, so we have to define the duration in minutes)
    g. Check “Download required files” and change the time to 2 Hours
    h. Change “Stagger patching start time…” to 0 hours 10 minutes
    i. Leave “Skip errors and continue patching” checked
    j. Change the “Retry” to 15 minutes between attempts
    k. Leave “Force restart” unchecked




76. Click “Save” in the upper right corner to save the schedule

## Adding Targets to a Patch Policy Schedule

77. Click the “Add Targets” hyperlink under the “Targets” heading on the right



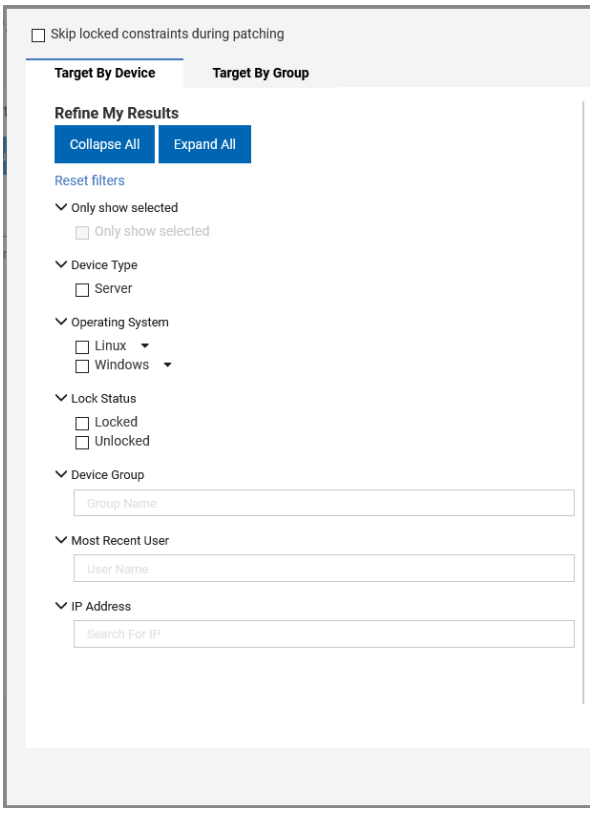

78. Click the blue “Expand All” button and take a look at the available filters. These are the different ways we can select the target endpoints for this patch policy schedule.

    We can also target by computer group. Click the “Target By Group” tab to see the available computer groups.

    We will select our target devices using the filters.

    a. Click on the “Target By Device” tab
    b. Expand “Operating System”
    c. Expand “Linux”
    d. Check the box next to “Red Hat Enterprise Linux”
    e. Select the devices on the right that correspond to the filter on the left

79. Click “OK” in the bottom right corner

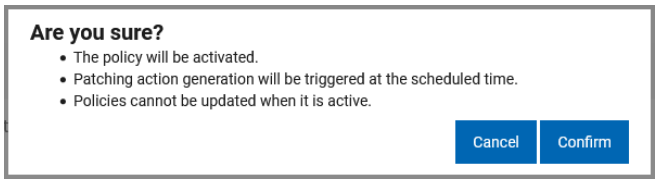



NOTE: You can also select the devices on the right without using the filters on the left. <u>If you use the filters however, you must remember to select the endpoints, otherwise no endpoints will be added to the schedule</u>

## Activating a Patch Policy

We have now created a Patch Policy, a scheduled patch deployment, and added target devices to the schedule, but the policy is not active

80. Click the blue “Activate” button in the top right to activate the Patch Policy.
81. Confirm the subsequent message

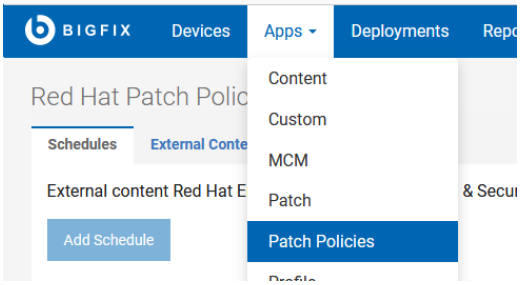



82. Review the policy, schedule, and target devices to ensure the settings are correct.
    a. If you need to make a change to the schedule or the policy, you must first suspend the policy
    b. You may make changes to the targeted endpoints (add or remove) without suspending the policy

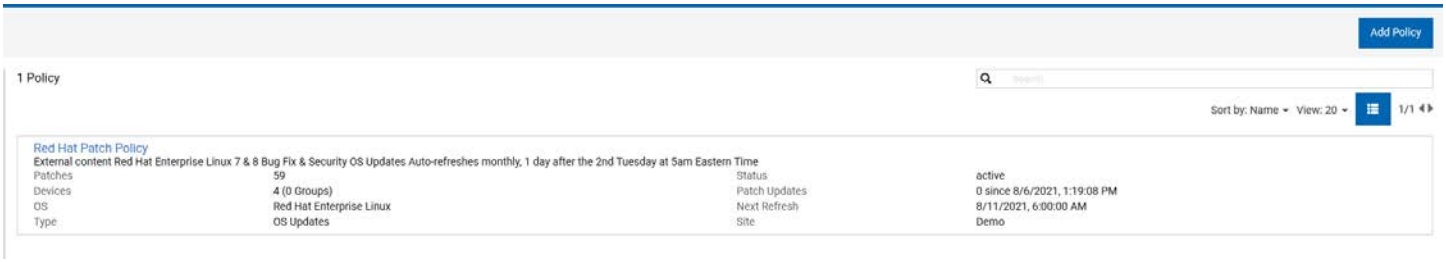
## Creating a Patch Policy #2

We are going to create another policy for the retail endpoints.

83. Click Apps -> Patch Policies on the WebUI menu bar.




84. Notice the policy we just created, and the information provided
85. Click the “Add Policy” button in the top right corner




86. Enter the following information to create the new Patch Policy:
    a. Policy Name: Retail Servers Patch Policy
    b. Site: Demo
    c. Description: Enter a meaningful description, that will be useful after you have created multiple policies
    d. Include Content: External Content
    e. Operating Systems: Windows
    f. Severity: Critical
    g. Category: Security
    h. Type: OS Updates
    i. Include Patches for: Click the “Show More” link and check the box next to “Windows Server 2019”
    j. Auto-refresh: Click the “Enable” button
    k. Change “This policy refreshes” to “Weekly”
    l. Change the “On” day to “Wednesday”
    m. Change the time to 5:00am
    n. Change the Timezone to (GMT-5:00) Eastern Time (US and Canada).

A screen image follows to reference the appropriate settings

**Patch List Criteria**

Policy Name *
Retail Servers Patch Policy

Site *
Demo

Description (optional)
Windows Critical Patch policy
OS Security updates
Windows Server 2019

Include Content *
- [ ] Custom content
- [x] External content

**Include External Content**

Operating System *
- ○ CentOS
- ○ Oracle Linux
- ○ Red Hat Enterprise Linux
- ○ SUSE Linux Enterprise
- ○ Ubuntu
- ◉ Windows

Severity *
- [x] Critical
- [ ] Important
- [ ] Moderate
- [ ] Low
- [ ] Unspecified

Category *
- [ ] Bug Fix
- [ ] Enhancement
- [ ] Mandatory
- [ ] Optional
- [ ] Recommended
- [x] Security
- [ ] Service Pack

Type *
- [x] OS Updates
- [ ] OS Application Updates
- [ ] 3rd Party Updates

Include Patches for:
- [ ] Windows 10
- [ ] Windows 7
- [ ] Windows 8
- [ ] Windows 8.1
- [ ] Windows Server 2003
- [ ] Windows Server 2008
- [x] Windows Server 2019

Show More

**Exclude Content**

Exclude from this policy any patch whose title contains one of these keywords:
Enter keywords

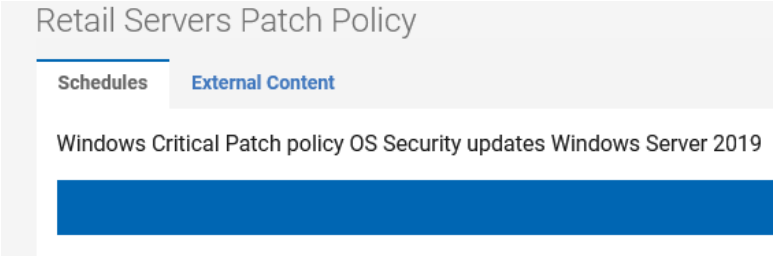
**Auto-refresh** Disable

This policy refreshes Weekly
On Wednesday
At 05 : 00 AM
Timezone: (GMT-05:00) Eastern Time (US and Canada)

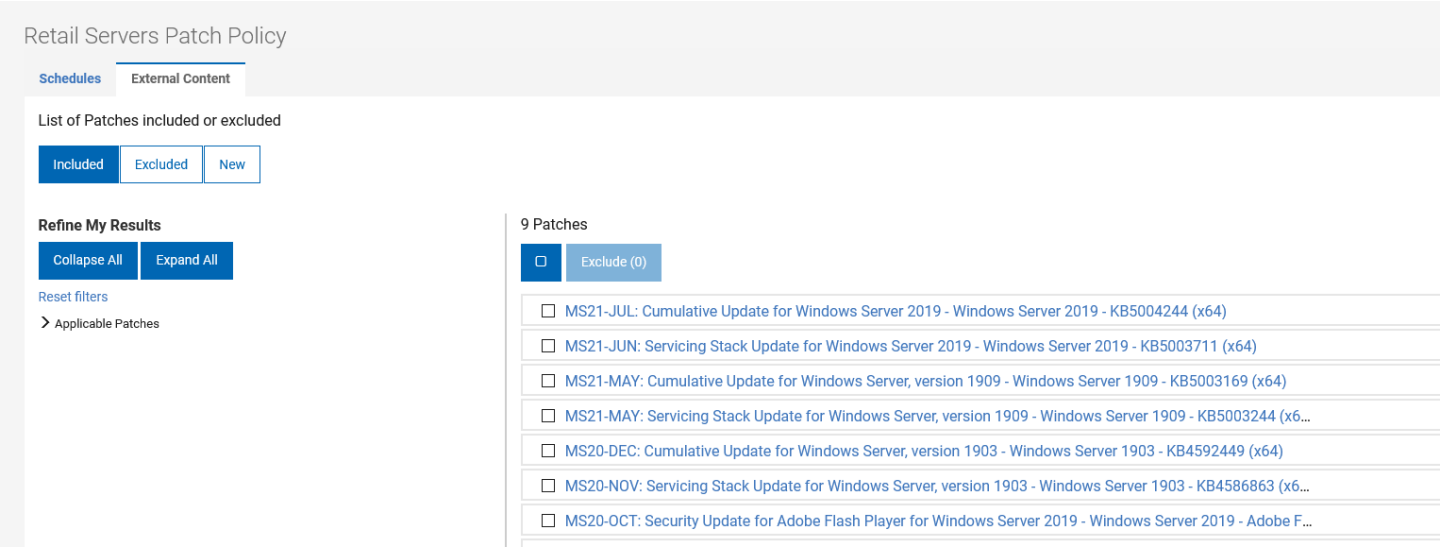
87. Click “Save” to save the policy

88. The right pane displays the new policy details. The Patch Policy state is **Suspended** when created, and the **Activate** button is not available until at least one schedule is added

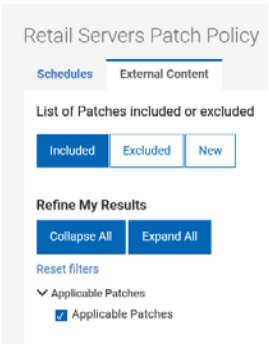
89. Click on the “External Content” tab to view the patches included in this policy



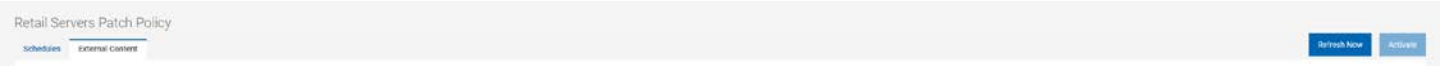

90. The screen displays the list of patches included in the policy




91. Under “Refine My Results” click the “Expand All” button
92. Check the box next to “Applicable Patches”
93. Notice the list of patches decreases in number. This allows you to control the patches included in your patch deployment.
94. We will leave the box un-checked for this exercise, so un-check the box

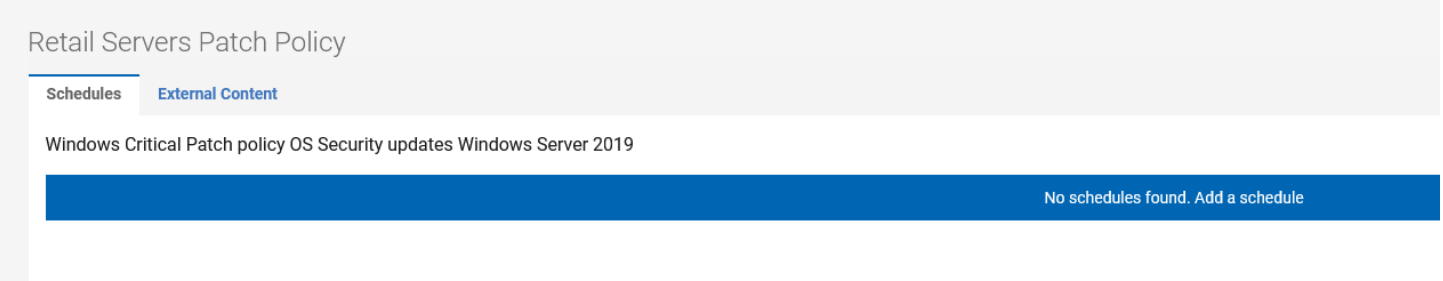



95. The “Refresh Now” button refreshes the applicable patch list, overriding the schedule we set when we created the policy
96. The “Activate” button is not available until we add a schedule to this policy

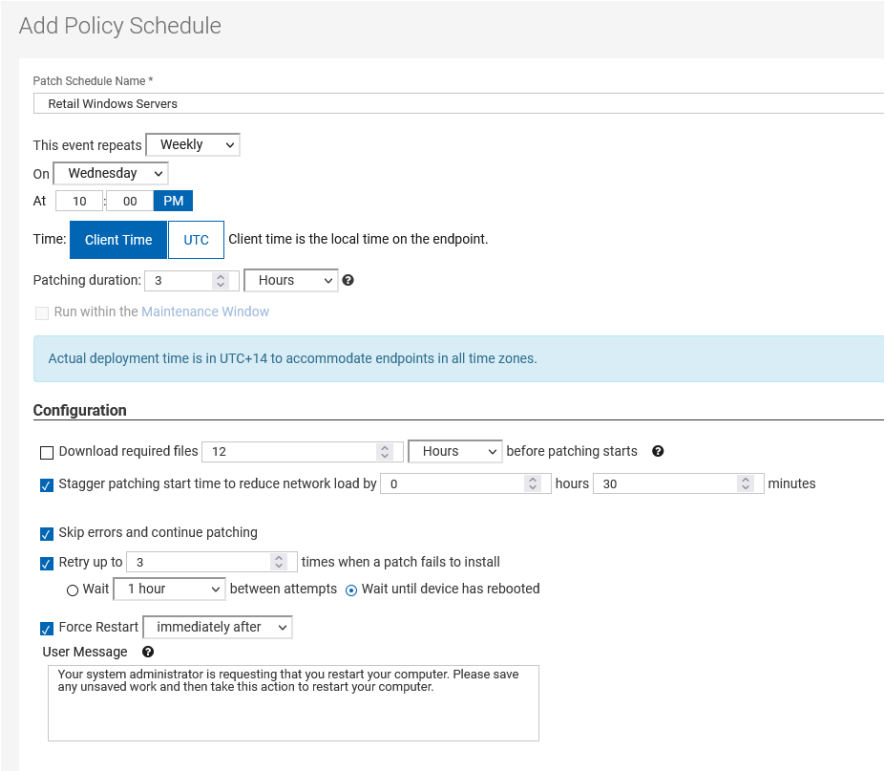


## Adding a Schedule to a Patch Policy

1. Click on the “Schedules” tab to return to the previous window and click the blue bar to add a schedule.



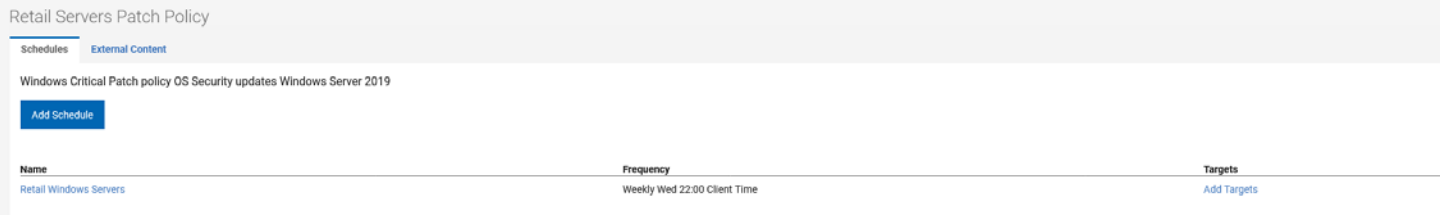

2. Click the blue bar to add a schedule. We will use the same schedule as the Windows Patch Exercise.
    a. Patch Schedule a Name: Retail Windows Servers
    b. This event repeats: Weekly
    c. On: The day corresponding to *today* (if you are doing this exercise on Wednesday, choose “Wednesday”)
    d. At: The servers in the datacenter are patched at 10pm, so change the time to 10:00PM
    e. Time: No change, use “Client Time”
    f. Patching Duration: 150 Minutes (we could use hours, but the window is 2 ½ hours, so we will use minutes)
    g. Check “Download required files” and change the time to 2 Hours
    h. Change “Stagger patching start time…” to 0 hours 10 minutes
    i. Leave “Skip errors and continue patching” checked
    j. Change the “Retry” to 15 minutes between attempts
    k. Leave “Force restart” unchecked




3. Click “Save” in the upper right corner

## Adding Targets to a Patch Policy Schedule

1. Click the “Add Targets” hyperlink under the “Targets” heading on the right

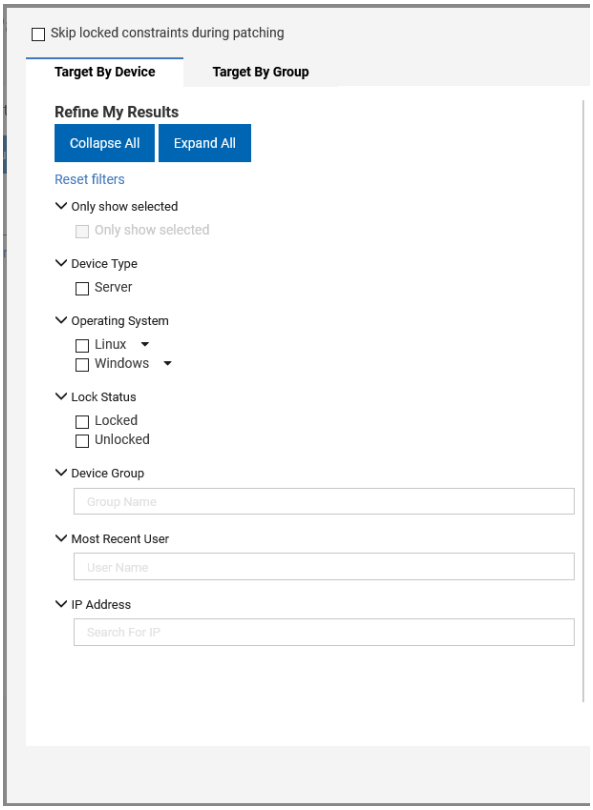



2. Click the blue “Expand All” button and take a look at the available filters. These are the different ways we can select the target endpoints for this patch policy schedule.

   We can also target by computer group. Click the “Target By Group” tab to see the available computer groups.

   We will select our target devices using the filters.

   a. Click on the “Target By Device” tab
   b. Expand “Operating System”
   c. Check the box next to “Windows”
      We could expand “Windows” but there is no need in the exercise, because the only Windows computer is Server 2019
   d. Select the devices on the right that correspond to the filter on the left

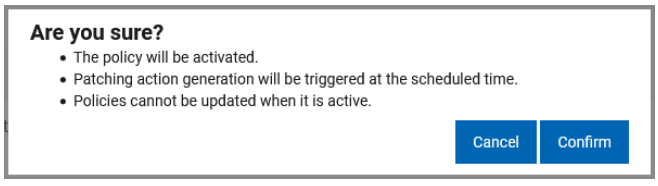



3. Click “OK” in the bottom right corner

NOTE: You can also select the devices on the right without using the filters on the left. <u>If you use the filters however, you must remember to select the endpoints, otherwise no endpoints will be added to the schedule</u>

We have now created a Patch Policy, a scheduled patch deployment, and added target devices to the schedule, but the policy is not active

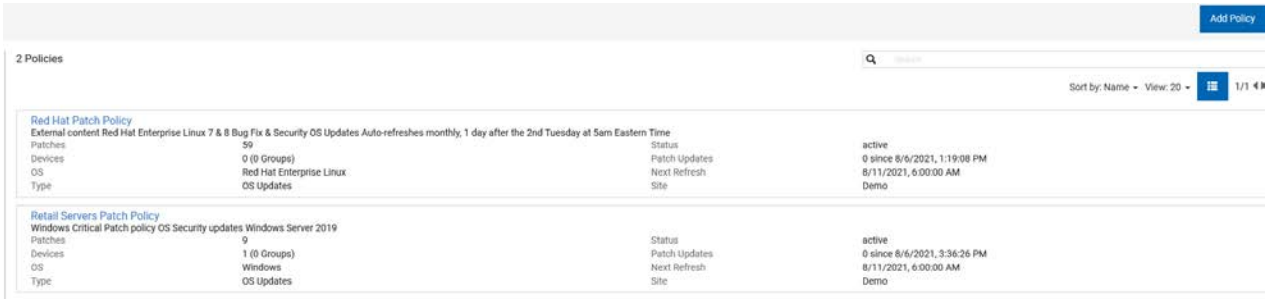
4. Click the blue “Activate” button in the top right to activate the Patch Policy.
5. Confirm the subsequent message




6. Review the policy, schedule, and target devices to ensure the settings are correct.
   a. If you need to make a change to the schedule or the policy, you must first suspend the policy
   b. You may make changes to the targeted endpoints (add or remove) without suspending the policy

## Creating a Patch Policy #3

1. We are going to repeat the Patch Policy creation, the Policy Schedule creation, and adding targets for the Ubuntu store server.
2. Click Apps -> Patch Policies on the WebUI menu bar., and click the “Add Policy” button in the top right corner




3. Enter the following information to create the new Patch Policy:
    a. Policy Name: Retail Ubuntu Servers Patch Policy
    b. Site: Demo
    c. Description: Enter a meaningful description, that will be useful after you have created multiple policies
    d. Include Content: External Content
    e. Operating Systems: Ubuntu
    f. Severity: Unspecified
    g. Category: Security
    h. Type: OS Updates
    i. Include Patches for: check the box next to “Ubuntu 20.04”
    j. Auto-refresh: Click the “Enable” button
    k. Change “This policy refreshes” to “Weekly”
    l. Change the “On” day to “Wednesday”
    m. Change the time to 5:00am
    n. Change the Timezone to (GMT-5:00) Eastern Time (US and Canada).

    A screen image follows to reference the appropriate settings

**Patch List Criteria**

Policy Name *

Retail Ubuntu Servers Patch Policy

Site *

Demo

Description (optional)

Ubuntu
Unspecified
Security
OS Updates
Ubuntu 20.04

Include Content *

- [ ] Custom content
- [x] External content

**Include External Content**

Operating System *

- ○ CentOS
- ○ Oracle Linux
- ○ Red Hat Enterprise Linux
- ○ SUSE Linux Enterprise
- ◉ Ubuntu
- ○ Windows

Category *

- [ ] Bug Fix
- [ ] Enhancement
- [ ] Mandatory
- [ ] Optional
- [ ] Recommended
- [x] Security
- [ ] Service Pack

Include Patches for:

- [ ] Ubuntu 14.04
- [ ] Ubuntu 16.04
- [ ] Ubuntu 18.04
- [x] Ubuntu 20.04

Severity *

- [ ] Critical
- [ ] Important
- [ ] Moderate
- [ ] Low
- [x] Unspecified

Type *

- [x] OS Updates
- [ ] OS Application Updates
- [ ] 3rd Party Updates

**Exclude Content**

Exclude from this policy any patch whose title contains one of these keywords:

Enter keywords

**Auto-refresh** Disable

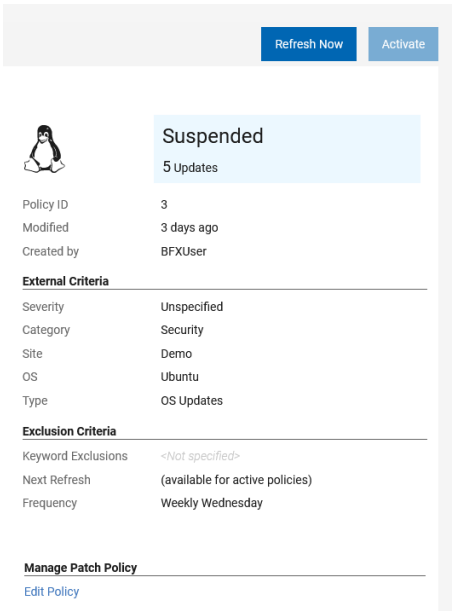
This policy refreshes Weekly

On Wednesday

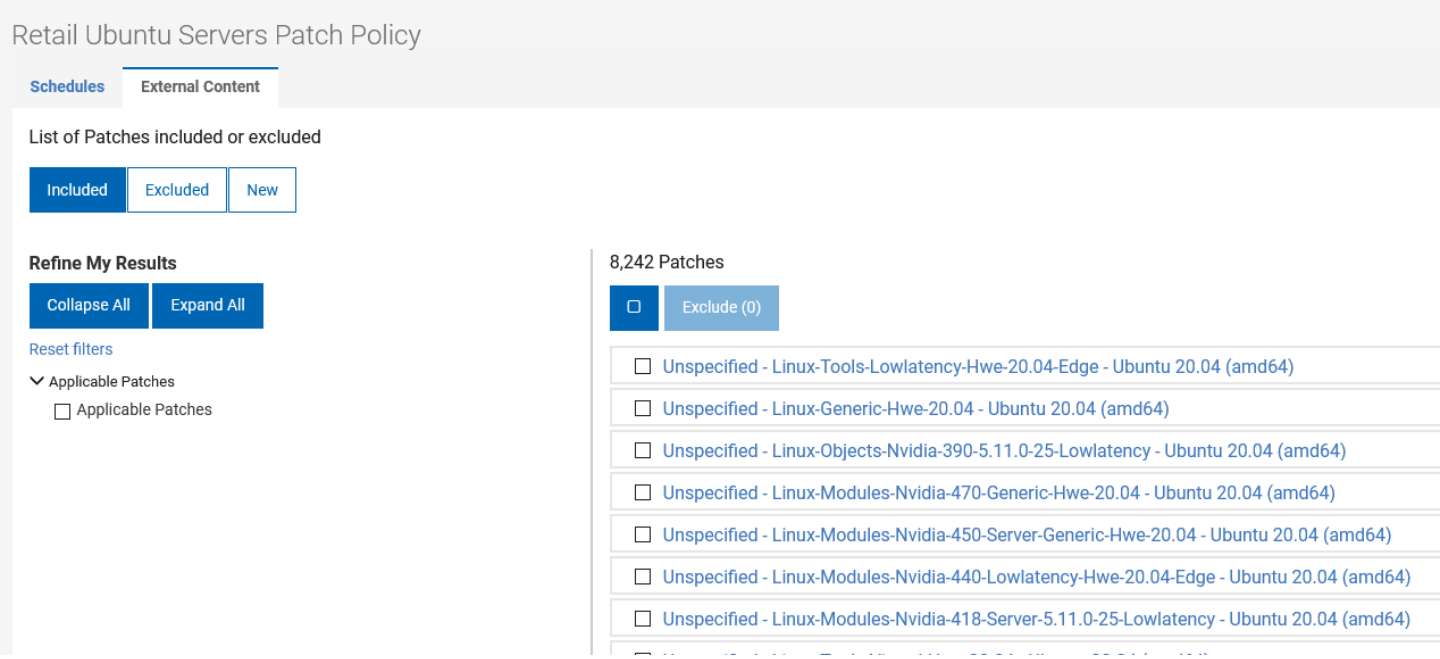
At 05 : 00 AM

Timezone: (GMT-05:00) Eastern Time (US and Canada)

4. Click “Save” to save the policy
5. The right pane displays the new policy details. The Patch Policy state is **Suspended** when created, and the **Activate** button is not available until at least one schedule is added



6. Click on the “External Content” tab to view the patches included in this policy



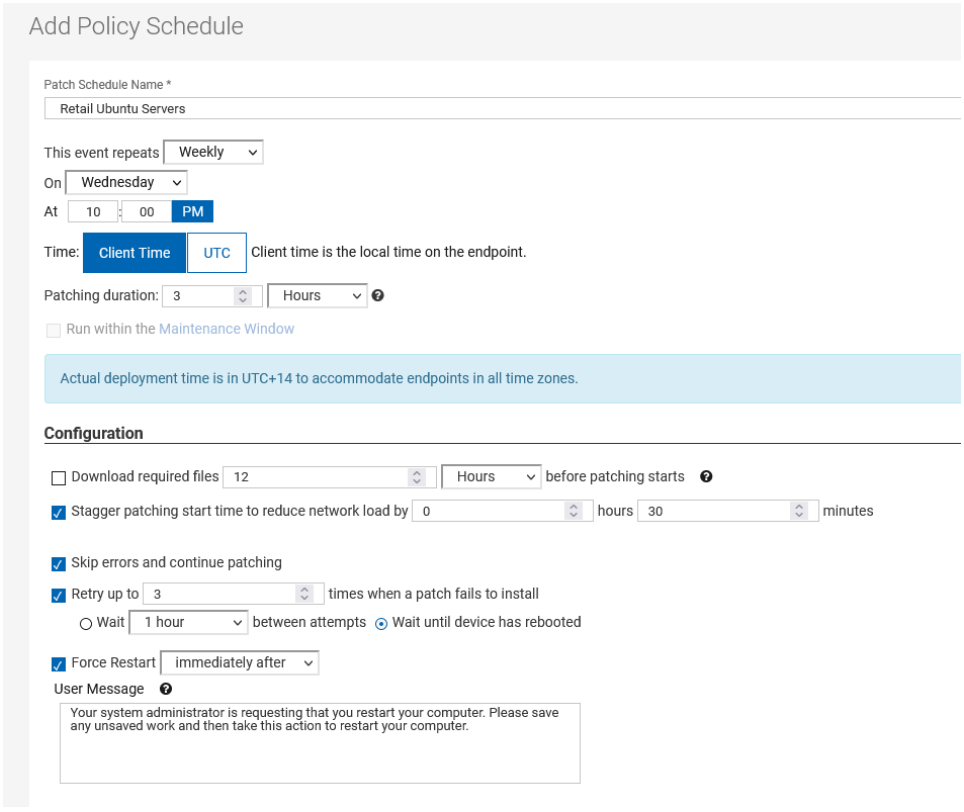

7. If we wanted to exclude any of the available patches, we would check the box next to the patch and click the blue “Exclude” button
8. The “Refresh Now” button at the top right refreshes the applicable patch list, overriding the schedule we set when we created the policy

## Adding a Schedule to a Patch Policy

9. Click on the “Schedules” tab to return to the previous window and click the blue bar to add a schedule.


10. Click the blue bar to add a schedule. We will use the same schedule as the Ubuntu Patch Exercise.
    a. Patch Schedule a Name: Retail Ubuntu Servers
    b. This event repeats: Weekly
    c. On: The day corresponding to *today* (if you are doing this exercise on Wednesday, choose “Wednesday”)
    d. At: The servers in the datacenter are patched at 10pm, so change the time to 10:00PM
    e. Time: No change, use “Client Time”
    f. Patching Duration: 150 Minutes (we could use hours, but the window is 2 ½ hours, so we will use minutes)
    g. Check “Download required files” and change the time to 2 Hours
    h. Change “Stagger patching start time…” to 0 hours 10 minutes
    i. Leave “Skip errors and continue patching” checked
    j. Change the “Retry” to 15 minutes between attempts
    k. Leave “Force restart” unchecked




11. Click “OK” in the upper right corner

## Adding Targets to a Patch Policy Schedule

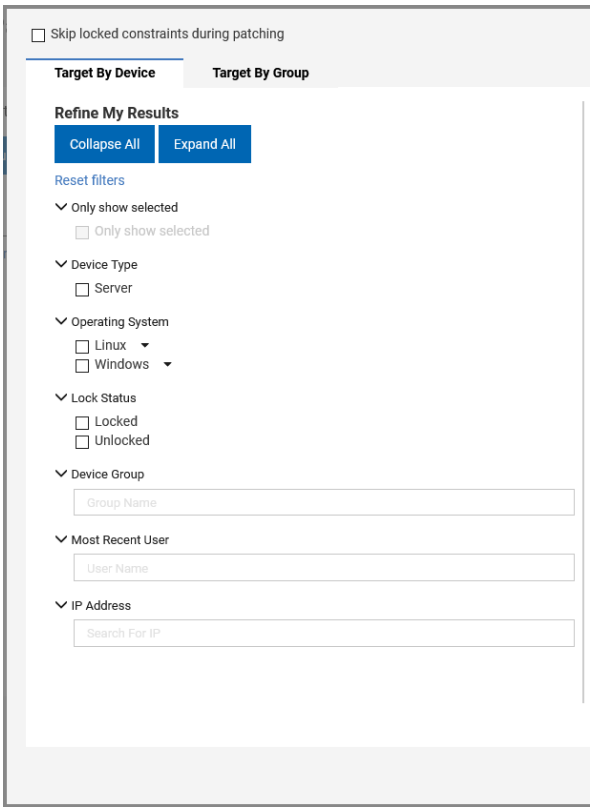
1. Click the “Add Targets” hyperlink under the “Targets” heading on the right


2. Click the blue “Expand All” button and take a look at the available filters. These are the different ways we can select the target endpoints for this patch policy schedule.

   We can also target by computer group. Click the “Target By Group” tab to see the available computer groups.

   We will select our target devices using the filters.

   a. Click on the “Target By Device” tab
   b. Expand “Operating System”
   c. Expand “Linux”
      Check the box next to “Ubuntu”
   d. Select the devices on the right that correspond to the filter on the left

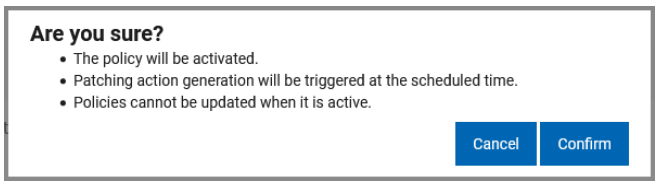



3. Click “OK” in the bottom right corner

NOTE: You can also select the devices on the right without using the filters on the left. <u>If you use the filters however, you must remember to select the endpoints, otherwise no endpoints will be added to the schedule</u>

We have now created a Patch Policy, a scheduled patch deployment, and added target devices to the schedule, but the policy is not active

4. Click the blue “Activate” button in the top right to activate the Patch Policy.
5. Confirm the subsequent message




6. Review the policy, schedule, and target devices to ensure the settings are correct.
   a. If you need to make a change to the schedule or the policy, you must first suspend the policy
   b. You may make changes to the targeted endpoints (add or remove) without suspending the policy

# BigFix Reporting (Reporting within the WebUI)

## Executive Summary

WebUI Reports allow you to quickly create and save custom reports to obtain more specific information about devices, patches, and deployments of endpoints. WebUI Reports are like bookmarking a page so you can view it later. All of your WebUI Reports are viewable by clicking the Reports button on the menu bar at the top of the page.

## Scenarios

Here are some scenarios when you may find WebUI Reporting useful:

- A patch administrator wants to track all critical and important patches that are applicable to all endpoints, regardless of operating system.
- A workstation management administrator wants a quick way to view deployments of patches and software, to keep track of deployment progress.
- The IT operations manager wants to view summary information about the team's tasks and export this information for later use.

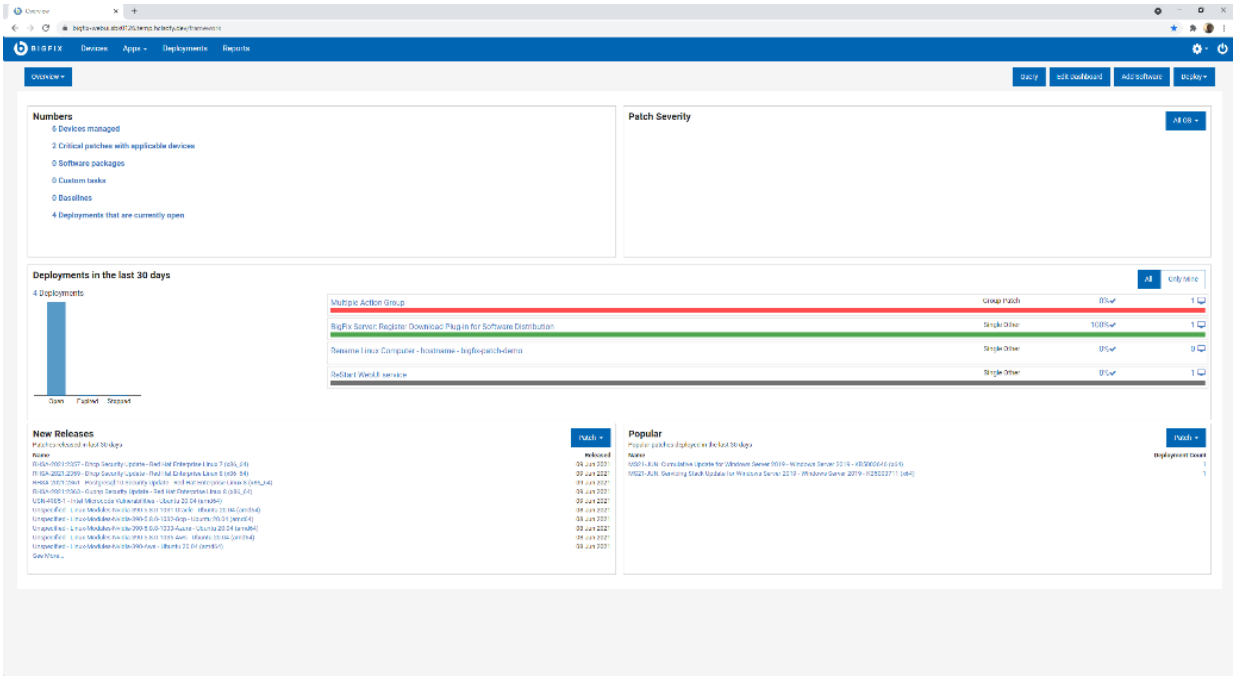
If you completed the patch exercises, you may have already created some reports. We will create some more here, to demonstrate the ease of use of BigFix Reporting

# BigFix Reports: Patch Compliance

7. We will first log into the WebUI.
    a. This URL is located on the Solution Content -> HCL BigFix Preview -> General Information -> Open Link Button to the right of “HCL BigFix WebUI
    b. Use the User ID and Password located on this page to log into the WebUI.

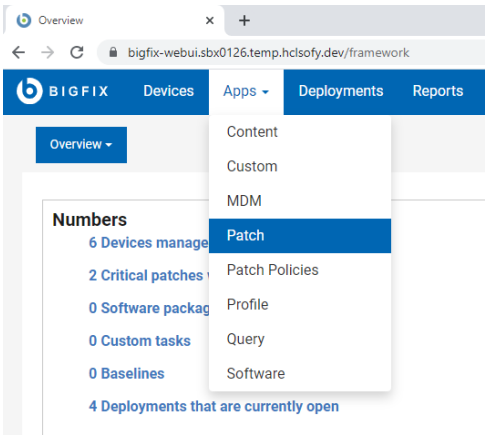

IMPORTANT: The username and the password are both case sensitive!

8. The first page you will see in the BigFix WebUI is the Overview Dashboard.

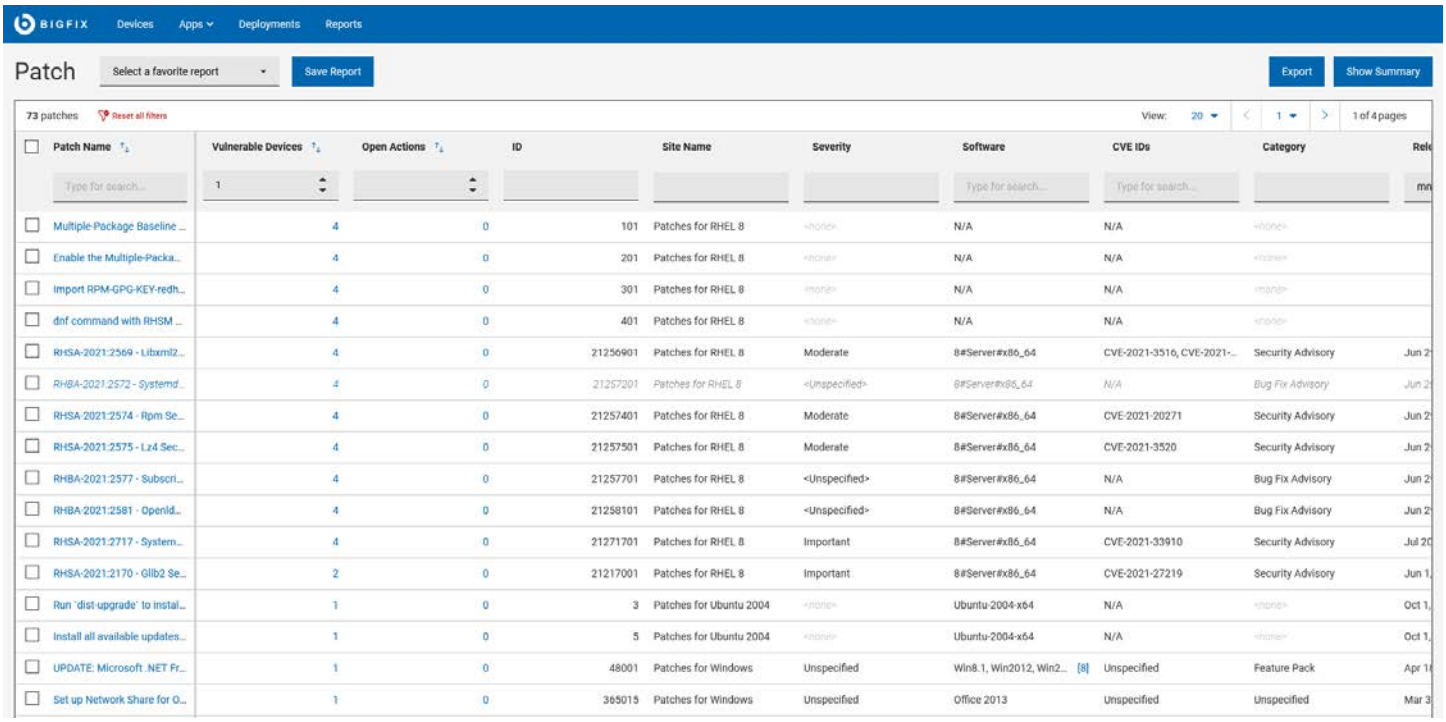



Take a minute to look around and see what information is available on this page. This is your “at-a-glance” information center for managing your infrastructure. This is data available to you without having to initiate an endpoint scan or run a report against a database. These tiles are customizable as well – you can re-arrange them or gather different data than what is currently visible.

9. From the WebUI Overview Dashboard, Click Apps -> Patch.




On this page we see at a glance, the patches that are applicable in our environment right now. The BigFix Agent has already evaluated this current content and determined that it is applicable to the device on which it is running. Again, we did not have to initiate a scan or run a report – the agent already knows.

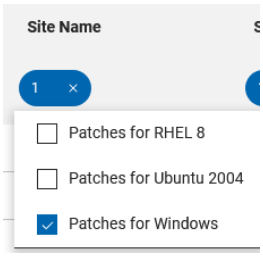



The first column lists the Patch Name. Next to this column we see Vulnerable Devices. There is an entry in the grey box at the top of the column which means a filter has been applied, in this case, to only show patches that are applicable to at least one device in our environment right now. If we turn the filter off by clicking on the “down” triangle to the right of the number “1”, we can see all patch content available in BigFix right now.

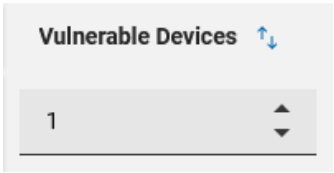
10. Go ahead and turn off this filter to see more content. You will notice the number of patches in the top left corner increases when you do.
11. We will set up some filters to look for Windows Critical and Important patches that are applicable to endpoints in our environment right now. The process is below but see if you can apply these filters by looking at the WebUI page. They are pretty intuitive.

a. Apply a filter to see only Critical and Important patches
   - Click the grey box in the “Severity” column
   - Check the boxes next to “Critical” and “Important”
   - Note the number two (2) in the blue oval in the header. This means we have applied a filter to this column
   - Click anywhere on the page to collapse the “picker”


b. Apply a filter to see only Windows patches
   - Click in the grey box in the “Site Name” column
   - Check the box next to “Patches for Windows”
   - As with patch severity above, note the number one (1) in the blue oval in the header. This means we have applied a filter to this column
   - Click anywhere on the page to collapse the “picker”

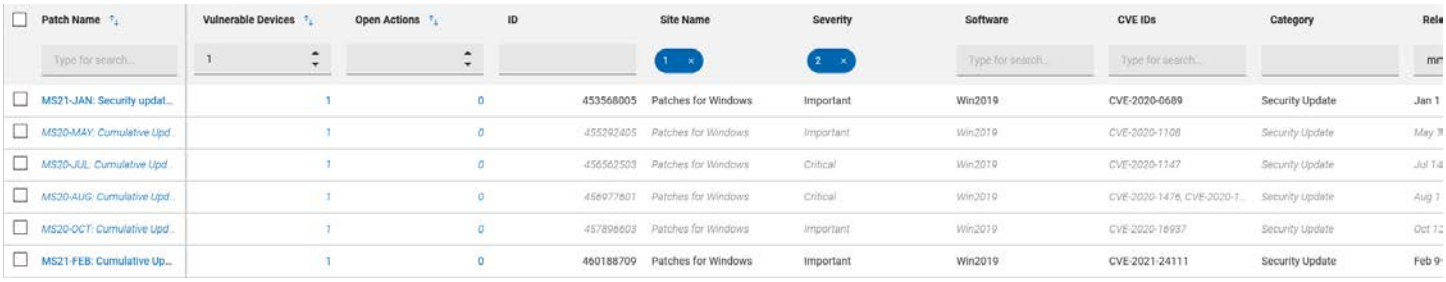



c. Apply a filter to see currently applicable patches
   - Remember that we turned this filter off in step 6.
   - Click the “up” triangle in the grey box in the “Vulnerable Devices” column
   - Note the “1” in the grey box



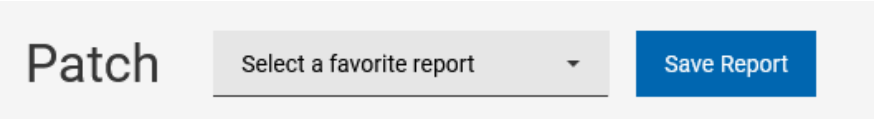

Also note that the list of patches has decreased

12. Notice that the list contains some patches in black text and some in gray italics text. The patches in italics have been superseded by another patch, like a cumulative rollup. The vulnerability that the patch addresses still exists however, which is why the patch shows up in the list as “applicable” to one of the devices in our environment.

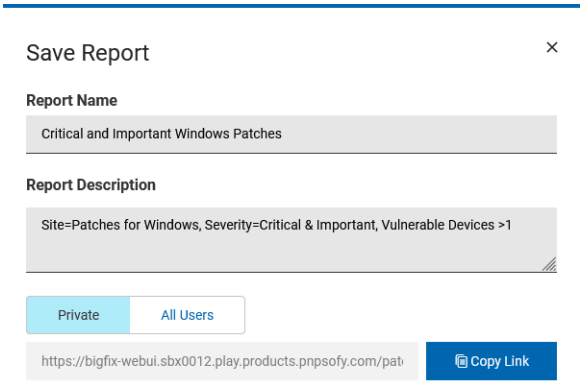


| Patch Name | Vulnerable Devices | Open Actions | ID | Site Name | Severity | Software | CVE IDs | Category | Rele |
|---|---|---|---|---|---|---|---|---|---|
| MS21-JAN: Security updat... | 1 | 0 | 453568005 | Patches for Windows | Important | Win2019 | CVE-2020-0689 | Security Update | Jan 1 |
| MS20-MAY: Cumulative Upd... | 1 | 0 | 455292405 | Patches for Windows | Important | Win2019 | CVE-2020-1108 | Security Update | May 1 |
| MS20-JUL: Cumulative Upd... | 1 | 0 | 456562503 | Patches for Windows | Critical | Win2019 | CVE-2020-1147 | Security Update | Jul 14 |
| MS20-AUG: Cumulative Upd... | 1 | 0 | 456977601 | Patches for Windows | Critical | Win2019 | CVE-2020-1476, CVE-2020-1... | Security Update | Aug 1 |
| MS20-OCT: Cumulative Upd... | 1 | 0 | 457896603 | Patches for Windows | Important | Win2019 | CVE-2020-16937 | Security Update | Oct 12 |
| MS21-FEB: Cumulative Up... | 1 | 0 | 460188709 | Patches for Windows | Important | Win2019 | CVE-2021-24111 | Security Update | Feb 9 |

13. We will now save this filtered list as a report so we can reuse the filter later. Click on the blue “Save Report” button

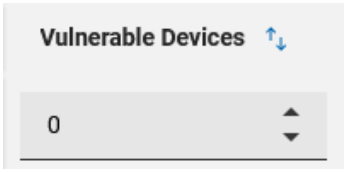



a. Enter information about the report
b. Provide a meaningful name, to distinguish it from other reports
c. Provide a description for the Report. The description will help others understand the reason for the report
d. You can make the report Private (available only to you) or you can make it available to All Users.
e. You also see the report URL, which you can bookmark for later, or share with others.

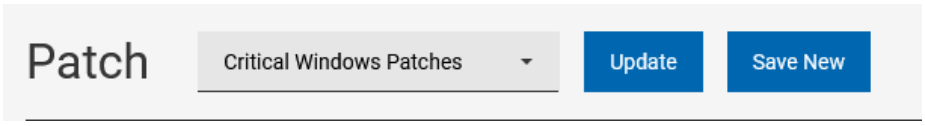


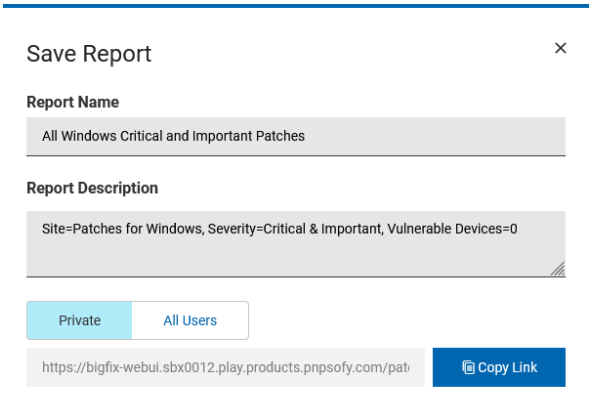

Note: the URL is a link to the report in this BigFix environment, and anyone you share the report with must have access to this environment.

14. We are going to create another report while we are on this page, a report that shows all Windows Critical and Important Patches, whether they are applicable to devices in our environment or not. The reason for creating this report is that we want to use it for patch deployments, and we may include patches that are not relevant now but may become relevant during the patch deployment, or at a later point.
15. Click the bottom black triangle under “Vulnerable Devices” to remove the filter.

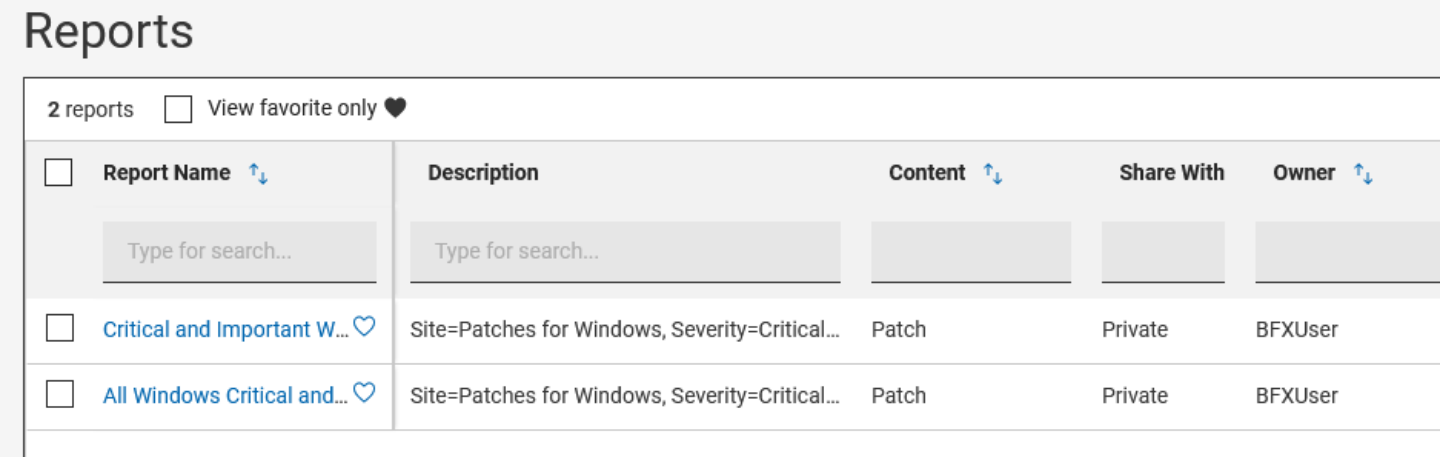



16. You will notice several things change on the page:
    a. The number of patches increased
    b. The “Save Report” button was replaced with “Update” and “Save New” buttons. The “Update” button overwrites the report we just created with the new filters. The “Save New” button saves a new report with the new filters.
17. Click on the “Save New” button and provide a name and a description, like we did before.



18. One you have saved the reports, they are listed in the Reports section of the WebUI, and you can return to them by clicking “Reports” in the menu bar at the top and selecting your report from the list.

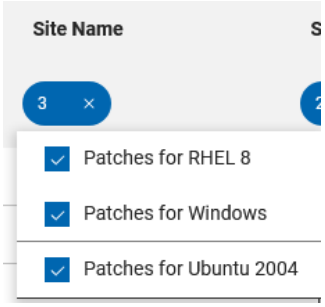



Keep in mind that the filters in the report govern what information the report returns but does not save the *results* of the report. In other words, if you run one of these reports today and use it to patch your environment, the results will be different if you run the same report tomorrow.

## Editing a Report

Remember that our first report was to keep track of critical and important patches for *all* operating systems, not just Windows.

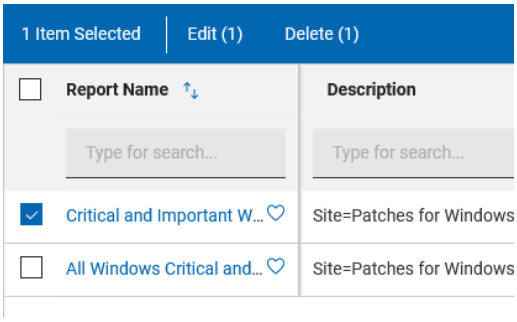
19. Click on “Reports” in the WebUI menu bar
20. Click on the blue oval under “Site Name” and add the other operating system(s) patch site(s).
21. Click “Update” to update the existing report filters
22. Now we need to change the name and the description of the report, to reflect what the report is for




23. Click on “Reports” in the WebUI menu bar
24. Check the box next to the report you wish to edit
25. Click “Edit” in the blue report header bar

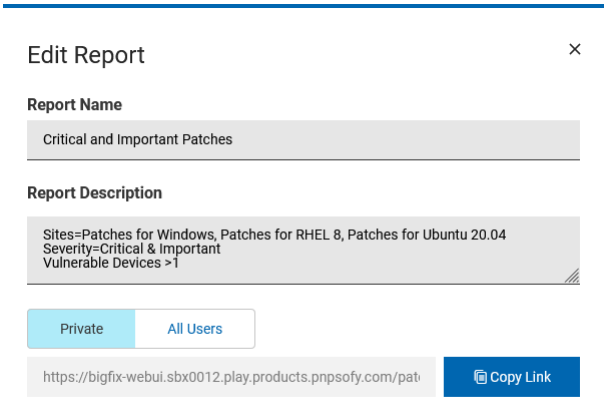
NOTE: If you select multiple reports to edit at the same time, you can only edit the availability of the report: Private or All Users.

NOTE: You can also delete reports from this page



26. Make changes, as appropriate, to the Report Name and the Report Description
27. Click “Save” at the bottom right of the page

NOTE: When you edit the report, the URL does not change

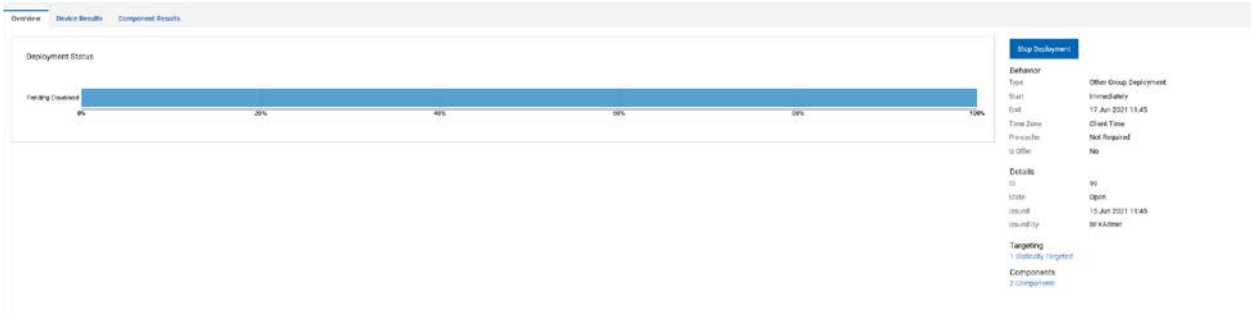


# BigFix Reports: Tracking Deployment Progress

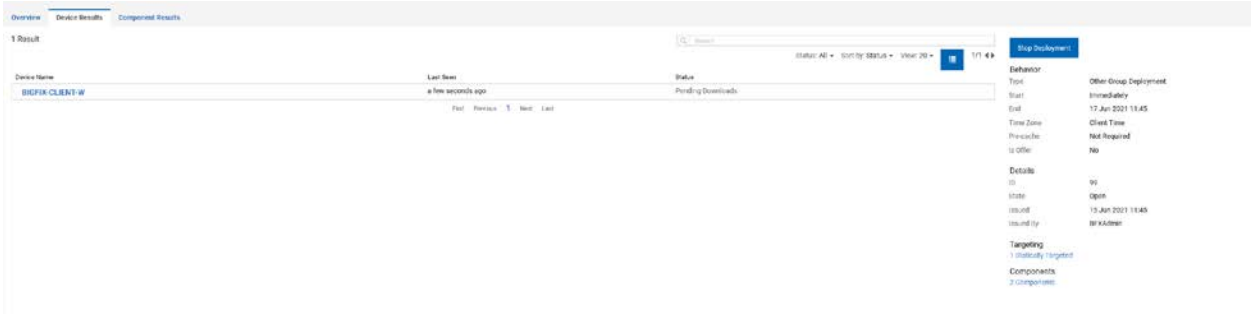
1. We are going to create a report to track the progress of deployments within our environment.

   If you completed the patch exercises, you may remember the Deployment Status window. We can track a deployment by overall deployment status, by deployment per device, and by deployment per component (patch, in this case). See the following three screens for examples.

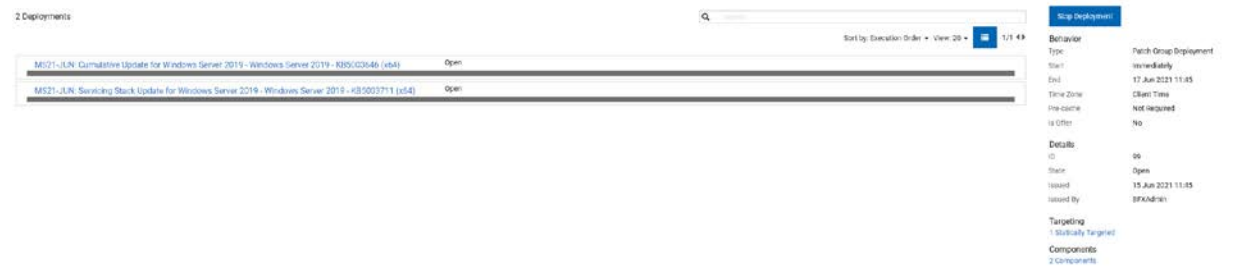
Deployment Status



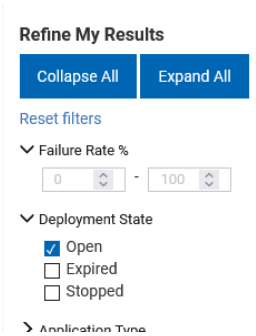
Deployment Status Per Device



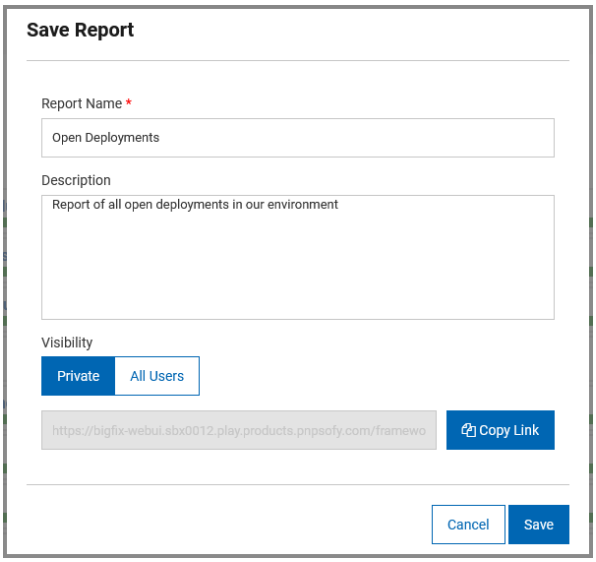
Deployment Startus Per Component



We want to create a report to track all of our open deployments.




28. Click on “Deployments” in the WebUI menu bar
29. The list of filters is on the right, under the “Refine My Results” header.
30. Expand “Deployment State” and check the box next to “Open”
31. Click the “Save Report” button in the Deployments header




a. Provide a meaningful name, to distinguish it from other reports
b. Provide a description for the Report. The description will help others understand the reason for the report
c. You can make the report Private (available only to you) or you can make it available to All Users.
d. You also see the report URL, which you can bookmark for later, or share with others.

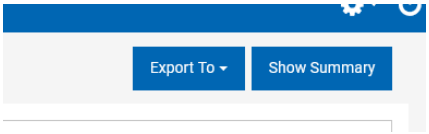
NOTE: the URL is a link to the report in this BigFix environment, and anyone you share the report with must have access to this environment.

32. Remember from the previous example that we can edit the report by modifying the filters. For example, you can modify the filters for this report to track expired deployments, or deployments that require a restart.

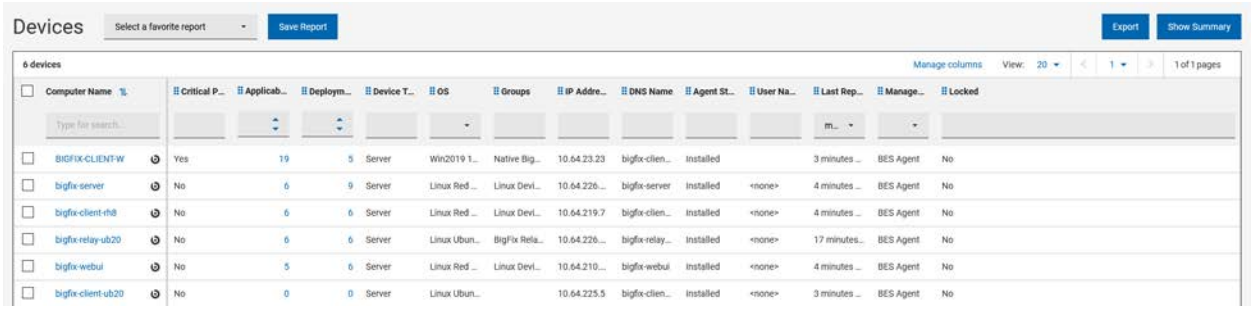
NOTE: You do not have to save the new report to see the report results. The results change as the filter changes.

# BigFix Reports: Viewing Summary Information

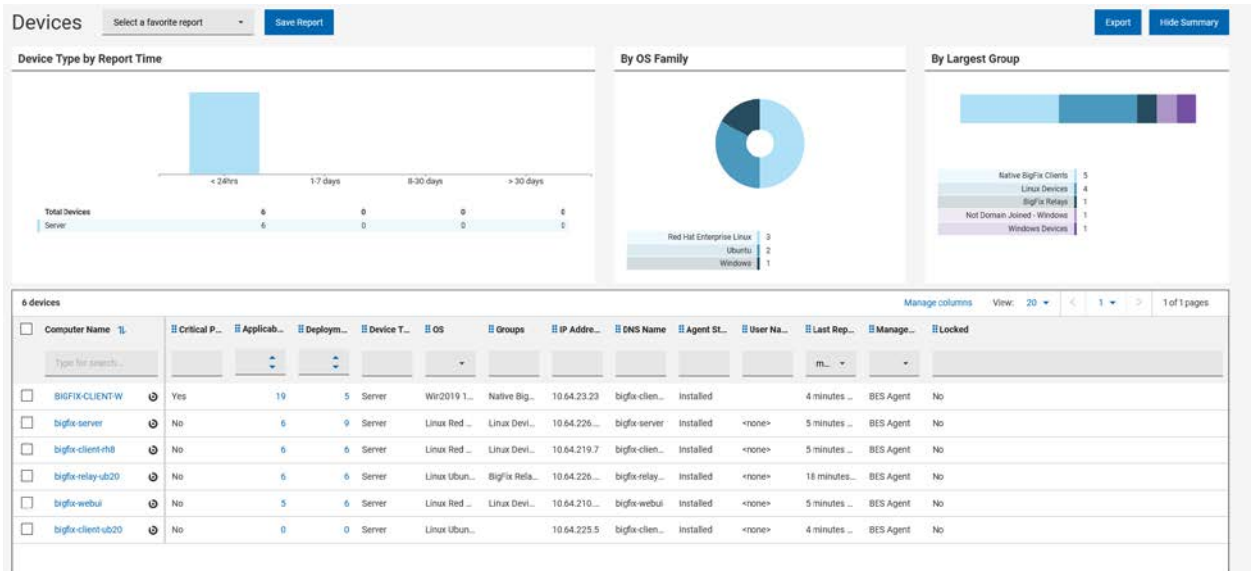
1. We are going to take a look at Summary Reports, previously referred to as In-Line Reporting. Summary Reports are available everywhere in the WebUI where you see the “Show Summary” button in the top right corner of the page.




2. We will start with Devices Summary. Click “Devices” on the blue menu bar at the top of the page.

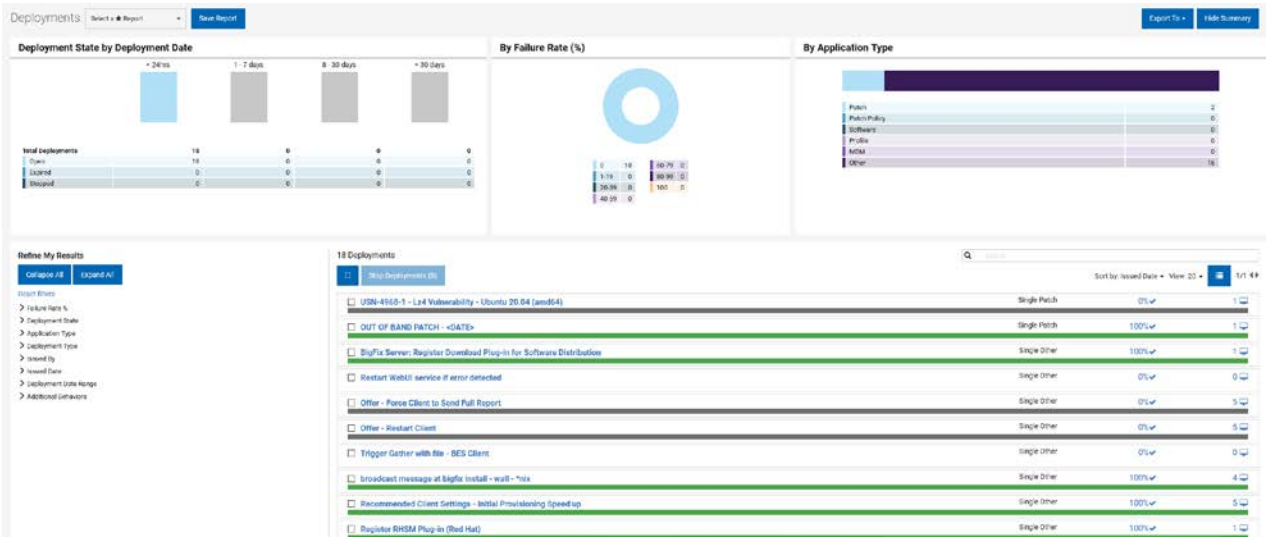



3. Click the “Show Summary” button in the top right of the screen.

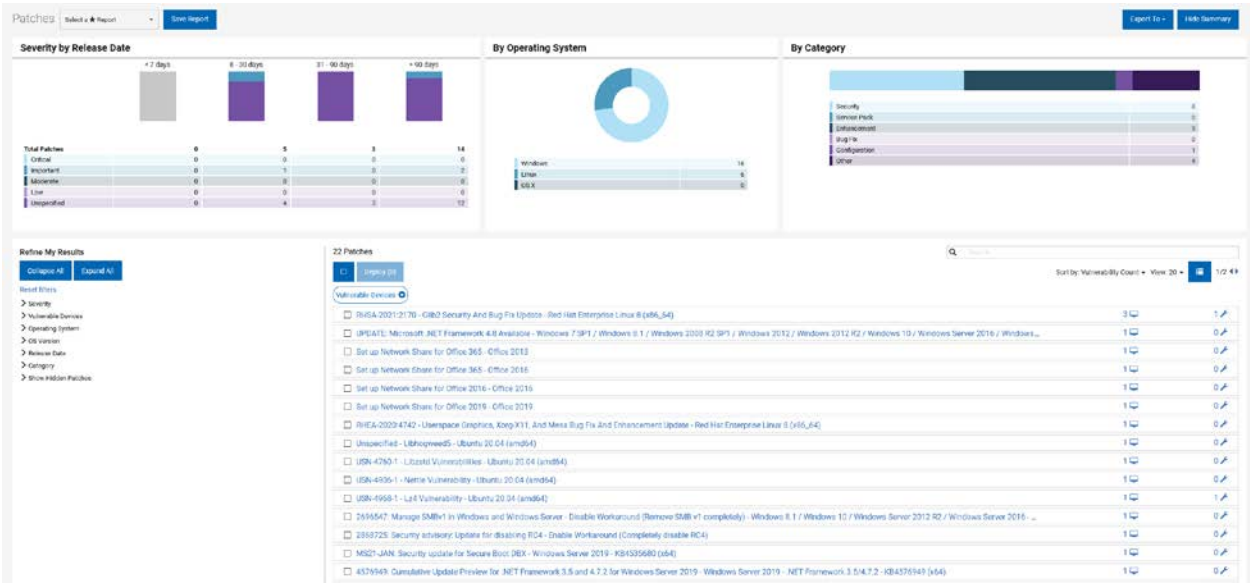



4. This view is a summary view of the devices, or endpoints, in our environment. Take a few minutes to click into the summary charts. You will see that as you click on different items, the device table at the bottom changes, with the appropriate filter applied. You can also clear the filter by clicking on the “x” in the blue oval at the top of the filtered column.
5. This Summary View is also available for Deployments and Patch (screen examples follow)

## Deployments Summary

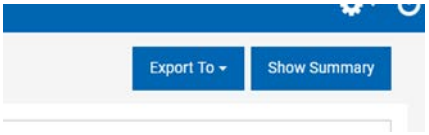



## Patches Summary



# Exporting Reports

6. These Summary Reports can be exported as a comma-separated values file (.csv), a Microsoft Excel file (.xlsx), or a portable document (.pdf).
7. To export the summary report, click on “Export To” in the upper right corner of the page. You can export selected items, all items, or the name column only (with or without headers). Take a few minutes and explore your export options, as well as the resulting exported documents.



# BigFix Reporting: Using Web Reports

## Executive Summary

BigFix Web Reports is a high-level web application that complements and extends the power of BigFix. It connects to one or more BigFix databases to aggregate and analyze your entire network. It allows you to visualize your data in a web browser, with both charts and data listings. Web Reports provides you with a convenient, compact, and timely overview of your BigFix network, no matter how broadly it extends.

Web Reports is organized around domains, which are content groupings with their own set of built-in reports to get you up and running quickly. Domains also act as primary filters that allow you to limit the scope of reports and drill down into your network with finer granularity.

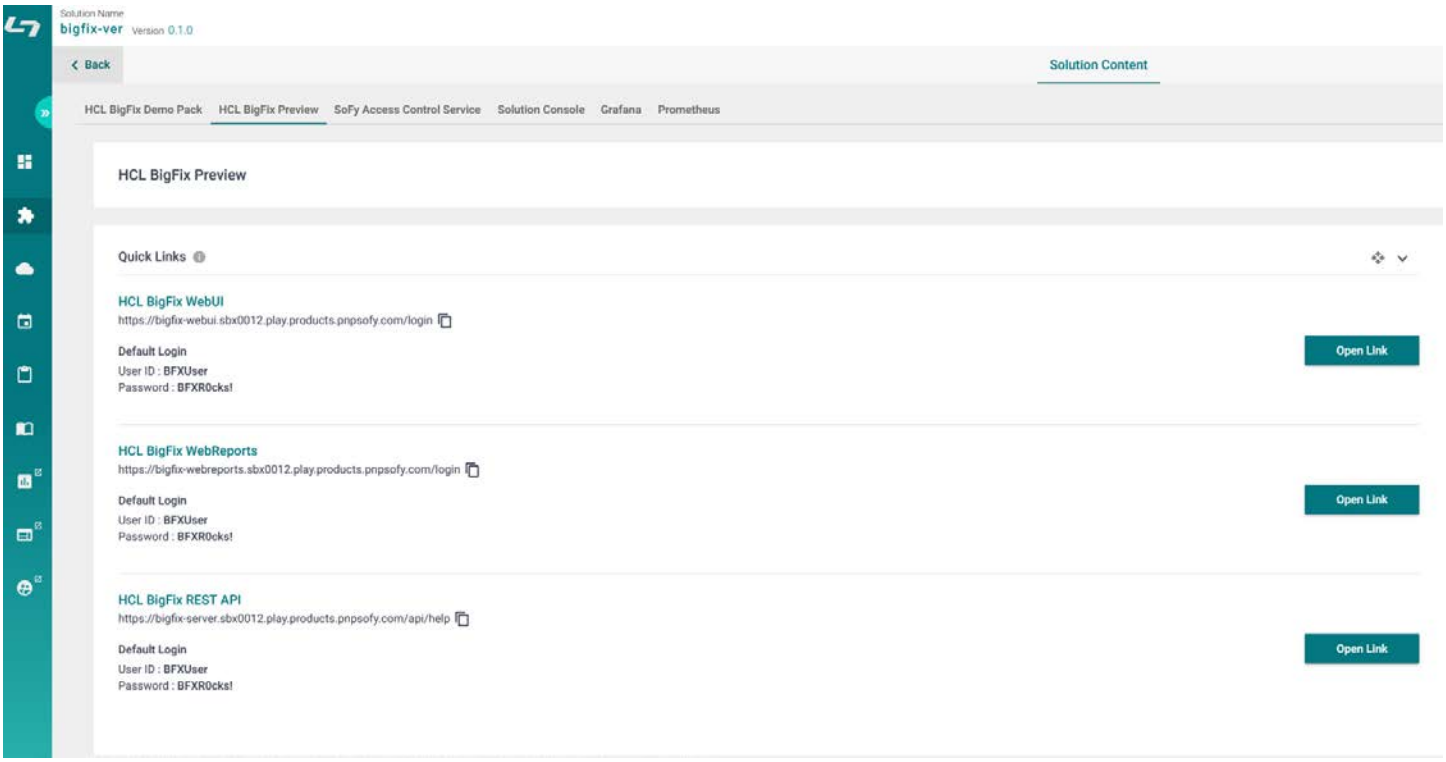
## Scenarios

The BigFix Administrator needs to keep track of data for computer hardware and software, endpoint vulnerabilities, software deployments, compliance remediation, and a host of other information. Here are some of the reports we will explore:

- BigFix Overview Report, which contains graphs and tables that visually represent the general state of your network, as well as the effectiveness of your BigFix deployment.
- Computer Properties List Report provides you with a list of properties of your BigFix Client computers, as well as their values.
- Open Vulnerabilities List Report displays Fixlet messages that are currently relevant.
- Critical Patch Compliance Reports show the administrator information about patches whose source severity is critical. There is a separate report for each operating system.
- Missing Patch Report, which shows the administrator a list of patches that endpoints are missing. There is a separate report for each operating system.
- Other Reports, like Action Lists and Analysis Lists, give the administrator a view into the view of what's going on in the BigFix environment.

# Accessing BigFix Web Reports

1. Web Reports is a web console that we need to log into. You will find the login link and the credentials on the Solution Content page within SoFy.

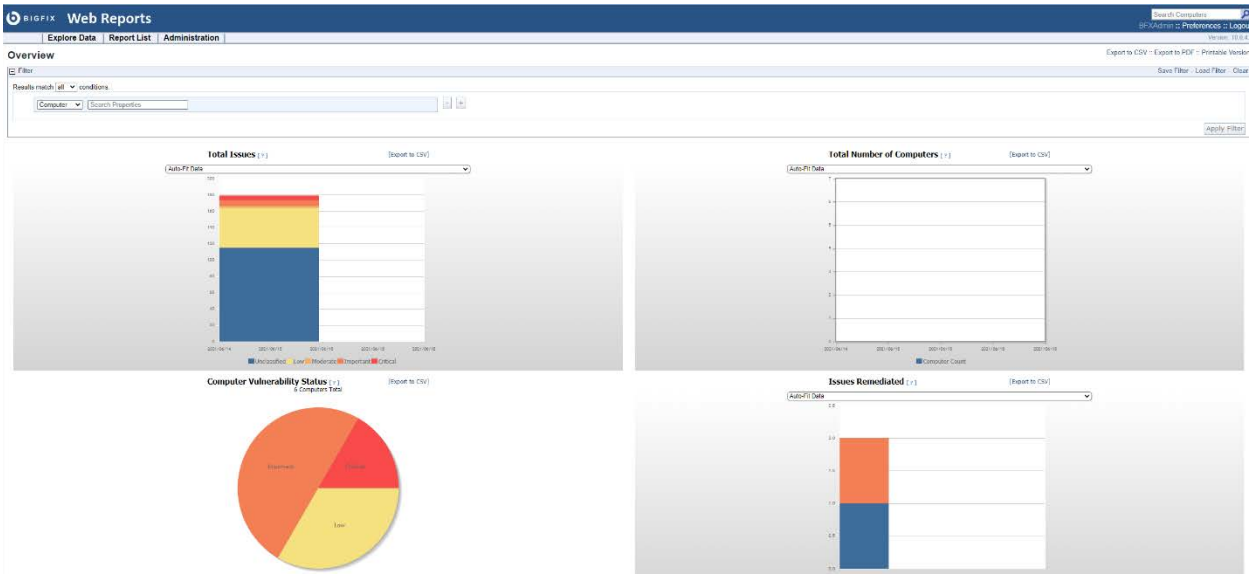



2. Click the "Open Link" button to the right of "HCL BigFix Web Reports" and log in using the credentials provided in the Solution Content.
3. Once you log in, you will see a list of Categories to view reports:
    a. Starred
    b. My Authored
    c. BigFix Management
    d. Patch Management.


NOTE: There may be other categories, depending on what BigFix solutions you have installed.

4. Click on "Report List" in the top center to see a list of reports currently loaded into Web Reports.

5. Select **Overview** from the Report List.
6. The Overview report contains graphs and tables that visually represent the general state of your network, as well as the effectiveness of your BigFix deployment.



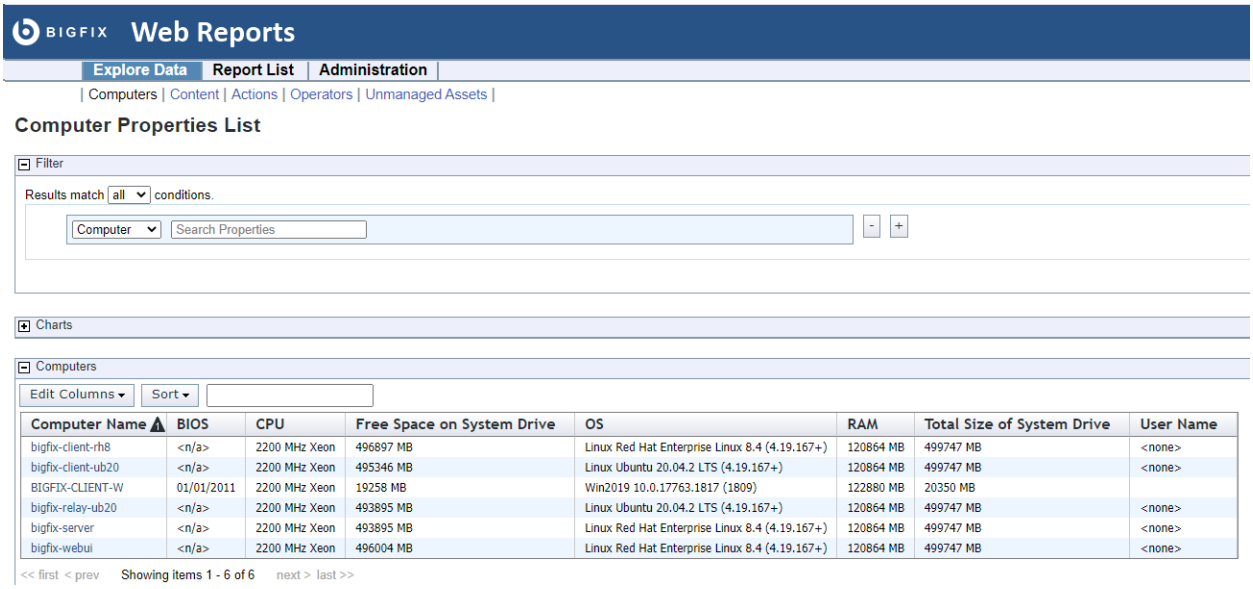

7. Next to the title of each report, there is a bracketed question mark [?], which you can click for additional information.
8. The following sections describe each of the graphs, charts, and tables presented in the Overview.
    a. Total Issues: Reflects the total number of Fixlets (issues) for each computer and then groups them by their severity rating.
    b. Total Number of Computers: Displays the number of computers with the BigFix agent installed on your network over the specified amount of time.
    c. Computer Vulnerability Status: Represents computers grouped according to the severity of their applicable Fixlets.
    d. Issues Remediated: Shows a count of the number of computers that have returned a status of “Fixed” in response to an action over a specified period of time.
    e. Overall Statistics: displays important facts about your network.
    f. Top 10 Critical/Important Issues Detected: Displays Fixlet messages that are currently affecting the largest number of computers in the network.

NOTE: To print the overview report with the graphs and tables, click on “Printable Version” at the top right. **Do not use “Export to PDF” as it is not functional in this demonstration environment**

NOTE: Web Reports users must have sufficient privileges to view reports. Users are considered to have sufficient privileges if they have full rights to all the computers on the server.

# BigFix Web Reports: Computer Properties

9. Select **Computer Properties List** from the Report List.
10. This report provides you with a list of certain properties of your BigFix Client computers. Like many of the listed reports, this is derived from Explore Data, with specific filters and charts. These exist for your convenience, but you can also re-create them yourself with just a few mouse-clicks.

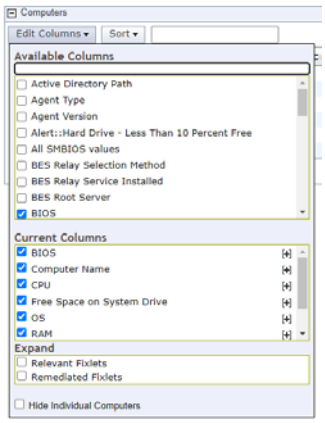



You can select a filter to reduce the size of the list. The column headers refer to important computer properties, such as the BIOS date, the CPU type, free hard disk drive space, the operating system, memory, and username. These properties are standard for out-of-the-box BigFix clients. However, from the console, you can create new computer properties using relevance expressions, and they are also available here.

## Add or Remove Report Columns

You can add or remove columns from Web Reports to add, remove or change the information displayed in the report.

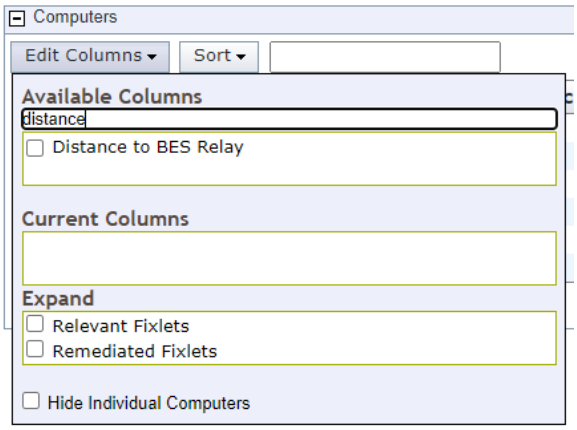
1. Add or remove columns. Click the “Edit Columns” button above the Computer Name column and view the dropdown list.




2. You can add any of the properties listed in the “Available Columns” box

You can also type information into the space below “Available Columns” to find additional property information.

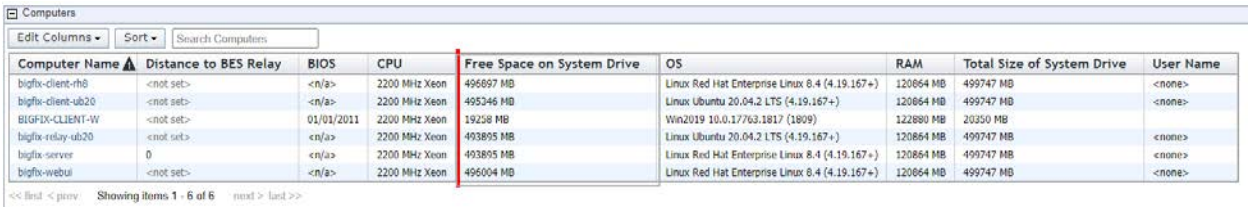
a. We want to add a property that is not listed, like the distance the endpoint is from its Relay.
b. In the box, type “distance”
c. A new property appears in the “Available Columns” box
d. Check the box next to the new property, and you will see the property appear in the “Current Columns” box
e. The column also appears in the report as soon as you check the box.
f. There is no “ok” or “apply” – just click on the page, away from the column editor box. The new column appears to the right of the “Computer Name” column.
g. To remove a column, click the “Edit Columns” button, and uncheck one of the checked boxes. The column is removed immediately.
h.



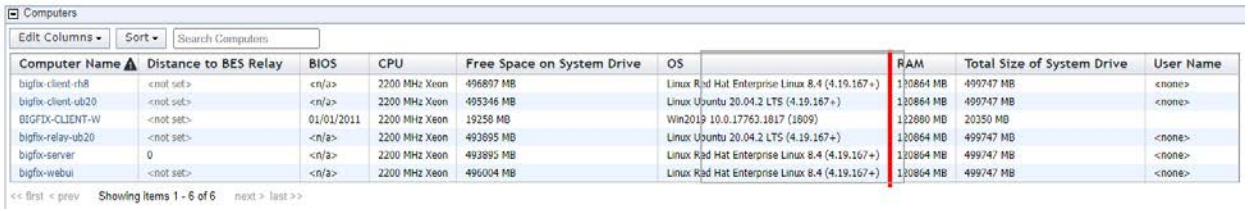

## Move Report Columns

You can move columns around in a report to change the overall display.

3. With the mouse, left click and hold the header of the column you wish to remove.
4. You will see a red vertical bar appear, depicting that column’s location in the report.



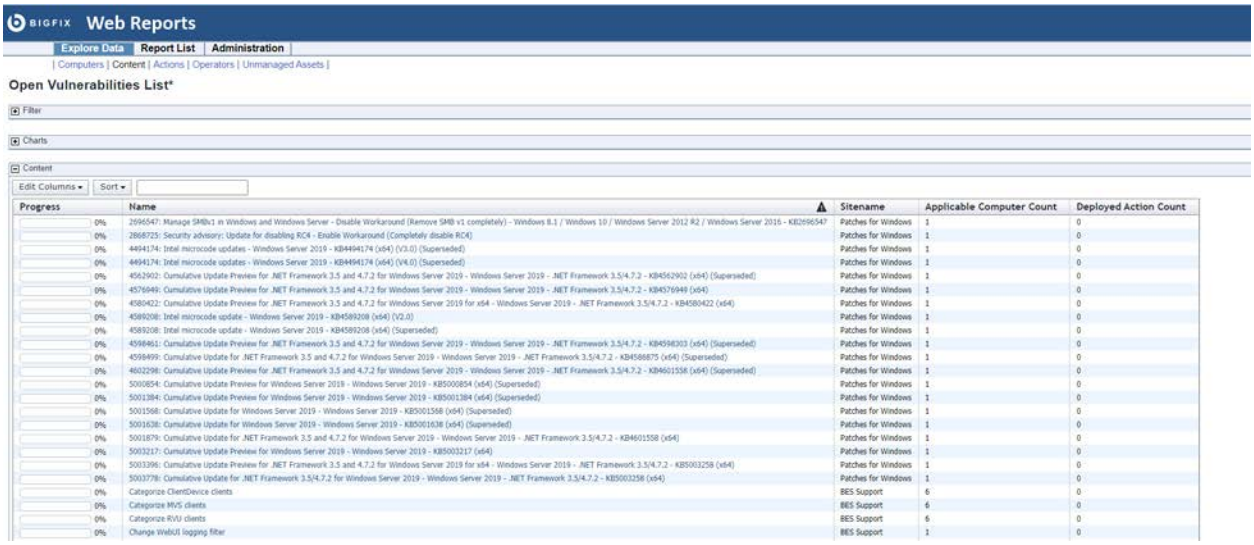

5. Drag the column header to the left or right until the red line appears where you want the column to be.



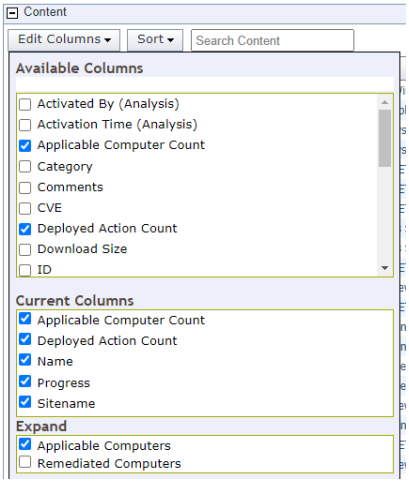

6. Release the mouse button and the column has been moved.


# BigFix Web Reports: Open Vulnerabilities

7. Select **Open Vulnerabilities List** from the Report List.

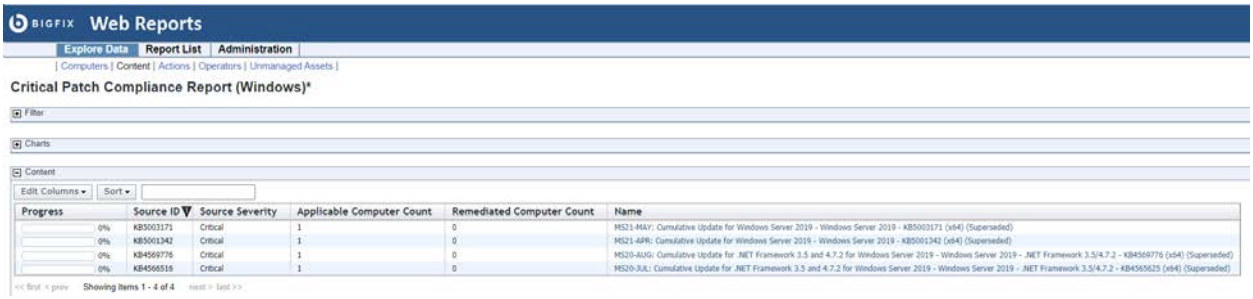



8. This report displays Fixlet messages that are currently relevant. The first column provides a quick visual representation of the progress of each vulnerability. In addition, the report shows the name, site applicable computer count, and deployed action count to complete the report. This report is useful to help you track those issues that can expose your network to potential problems.
9. We want to add some information to this report – we want to see which computers are affected by these vulnerabilities.
    a. Click the “Edit Columns” button
    b. At the bottom of the list in the “Expand” box, select “Applicable Computers”
    c. We can now see the computer names on the right that these vulnerabilities apply to.
    d. Note that when we add the computer, the “Name” column now contains duplicate entries, as more than one endpoint may have the same vulnerability



10. Select Critical Patch Compliance Report (Windows) from the Report List.

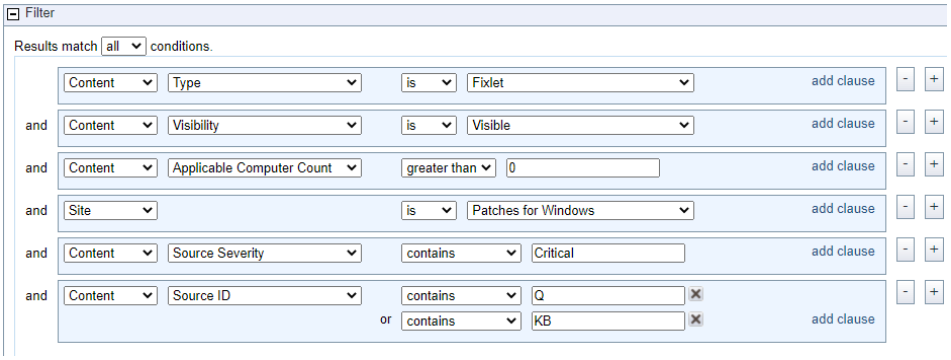



11. This report shows applicable patches to our environment whose source severity is “critical.”

## Working with Filters

1. We want to change this report to include patches of critical and important severity.
2. Click on the “+” next to “Filter below the title of the report

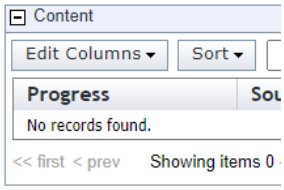

3. You will see the filter contents that produce this report.




4. Next to the fifth line in the report, click “add clause” and type Important in the box.
5. Click the “Apply Filter” button to the bottom right of the filter. When you click the button you will see the report results change.
6. You will also see an asterisk (*) next to the report name. The asterisk means the report has unsaved changes.
7. Click the “Save Report As” button and name the report “Critical & Important Patch Compliance Report (Windows)” The report is saved when the title changes, and you see a blue bar above the title that says, “Report saved”.

# BigFix Web Reports: Missing Patches

1. Select Missing Patch Report 2015 (Windows) from the Report List.
2. There are no records found. Based on the work we did with Filters in the previous scenario, can you guess why there are no records found with this report?
3. Click on the plus (+) sign next to “Filter” – at the bottom of the filter you will see the problem.
4. Change “MS15” in the last Filter entry to “MS” and the current year.



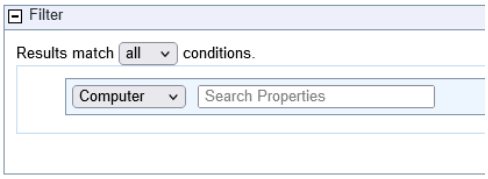


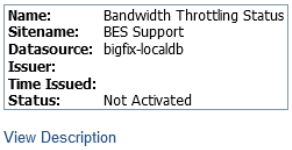
5. For example, if the current year is 2022, you will change the content in the box to “MS22”


6. Click the **Apply Filter** button and watch the results change in the “Content” section of the report.
7. Notice there is now an asterisk (*) next to the report name, which means the report has been changed. Click the **Save Report As** button and save it as “Missing Patch Report (Windows)” – you will know the report has been saved when the asterisk disappears and a bar appears above the report name indicating **Report Saved**.

# BigFix Web Reports: Action and Analysis Lists

1. Select **Action List** from the Report List.
2. The Action List contains information about all the BigFix Actions you see in the WebUI. You can click on the Action Name in the first column to get details about each Action.
3. Click the **Edit Columns** button. Notice that unlike Scenario 4 you do not have the ability to expand the content to see applicable and remediated computers, because this content is about the action that has been issued, not the endpoints it has been issued to. You can however, see the number of endpoints that have been Fixed and Failed, and you can add columns to include property results like Evaluating, Pending Downloads, Waiting, Running, and others. As we have done before, try it out – add and/or remove some columns to see how the report information changes.
4. Select **Analysis List** from the Report List.
5. The Analysis List contains information about all the BigFix Analyses. Analyses are groups of properties that return information about your BigFix environment, like application information, BigFix agent information, hardware information, and much more.
6. Click the name of one of the Analyses, like **Bandwidth Throttling Status**
7. Click on the **View Description** link
8. Another window opens giving a detailed description of what the analysis is, as well as the properties included in it.




NOTE: The content displayed in the Description view is a rendering of content from the BigFix Console, and while there are references to clicking links, there are no links or actionable data within the description page

# BigFix Web Reports: Exploring Data

1. Select **Explore Data** from the menu bar at the top. The resulting report shows Computer information, which corresponds to the list under the "Explore Data" button.


2. Click through the options.
    a. Computers – the current view. Lists computer name, IP Address, Operating System, CPU, and last report time
    b. Content – **CURRENTLY NOT AVAILABLE DUE TO A DATABASE ERROR IN KUBERNETES.** The default is all visible content, which includes Fixlets, Tasks, Analyses and Baselines. You can click on the Name of the content in the first column to get details about each.
    c. Actions – as in scenario 7, this report contains information about all the BigFix Actions you see in the WebUI. You can click on the Action Name in the first column to get details about each Action.
    d. Operators – this report contains information about the BigFix WebUI operators (Note: This is not a list of the Web Reports operators). You can see the type of user, the last time they logged in, if they can view custom content, how many endpoints they can administer, and how many actions they have been deployed.
    e. Unmanaged Assets – you will not have any results in this report view, but this view shows the endpoints that have been discovered by BigFix via an NMAP scan, but do not have the agent currently installed.
3. Return to the Computers report view. We are going to modify this data view by changing the Filter.
    a. Change the filter to "Computer" – "Computer Group" – "is" – "BigFix Relays" and click "Apply Filter"


The number of computers changes because we are filtering the original list.

Feel free to explore the data on this page by adding columns and filters. Remember that if you make a change to the filter, it will not take effect until you click **Apply Filter**

# Software Distribution Using the BigFix WebUI

## Executive Summary

BigFix provides a mechanism to package and deploy software to endpoints across your network from a single location. BigFix gives you the ability to maintain control and visibility into software delivery and installation.

Some of the most significant features of BigFix Software Distribution include:

- Dynamic and policy-based bandwidth throttling to push large files over distributed networks without impacting line-of-business bandwidth.
- Support for roaming endpoints with pre-caching relay infrastructure.
- Features to optimize dynamic and evolving networks.
- Intelligent software distribution based on endpoint characteristics.
- Software distribution wizards and user self-provisioning.
- Continuous software application license usage and metering, including support for existing software repositories.
- Low-cost scalability with minimal infrastructure requirements.

## Scenario

With BigFix Software Distribution you can ensure each software deployment is successful, whether you are distributing one software application to a single computer, or multiple software applications to a larger group of endpoints. BigFix handles prerequisites like Visual C++ components or .net Framework to ensure a successful deployment.

BigFix provides the ability to apply logic to a software distribution, so that endpoints can be targeted based on their properties, and software can be installed, upgraded or skipped based on its properties. For instance, we can setup a package for Google Chrome that contains an install for 32-bit and 64-bit Windows computers, as well as the install for Mac OS. What is more, the software distribution package can include the latest vendor updates, so rather than creating a new application update each time one is released, the latest update is distributed as part of the base package. This can reduce the requirement for deep knowledge of the requirements for every operating system, as the endpoints install the software that is applicable to them and skip the software that is not.

Another example is the “Click-to-Run” version of Microsoft Office. This can be packaged so the payloads are distributed to the endpoints while on the corporate network but downloaded directly from Microsoft if the endpoint is in a home office.

# BigFix Software Distribution: Create a Software Package

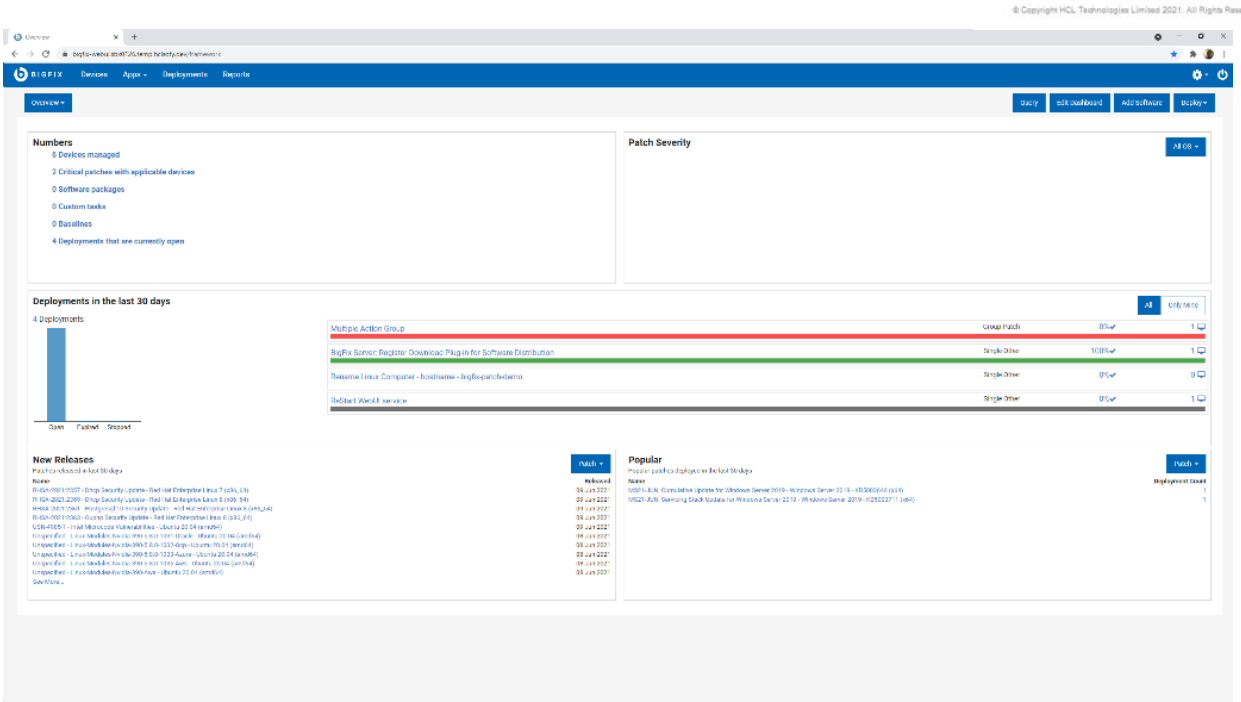
1. To perform the demo, navigate to https://hclsofy.com to create an environment, or to the WebUI URL you bookmarked previously.

NOTE: SoFy Solutions do not last forever; they have a maximum life of 24 hours at any given time. If you wait more than 24 hours without extending, the solution will expire, and you will have to create another one (see Extending Deployment Time for more information).

2. In this scenario we are going to create a software distribution package using BigFix.
3. We will first log into the WebUI.
    a. This URL is located on the Solution Content -> HCL BigFix Preview -> General Information -> Open Link Button to the right of "HCL BigFix WebUI
    b. Use the User ID and Password located on this page to log into the WebUI.

IMPORTANT: The username and the password are both case sensitive!


4. The first page you will see in the BigFix WebUI is the Overview Dashboard.




Take a minute to look around and see what information is available on this page. This is your "at-a-glance" information center for managing your infrastructure. This is data available to you without having to initiate an endpoint scan or run a report against a database. These tiles are customizable as well – you can re-arrange them or gather different data than what is currently visible.

## Obtain Software for Package

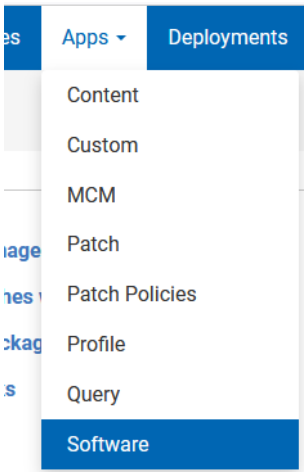
We will use Google Chrome for our software package. Note that you can use the standard executable, but we will download the Windows Installer (MSI) file for use in our application.

1. Navigate to https://chromeenterprise.google/browser/download/
2. Choose the top option, **Chrome bundle for Windows 64-bit**
3. Once downloaded, extract the installers from the zip file
4. The name of the file we will use is **GoogleChromeStandaloneEnterprise64.msi**. Depending on your version, the name of you file *may* be slightly different

## Add Software

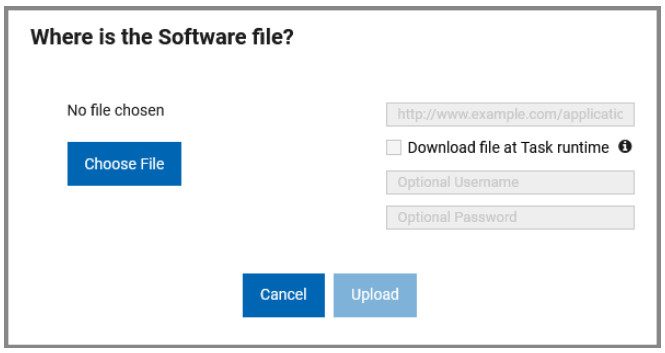
1. From the WebUI Overview Dashboard, Click Apps -> Software.

   Notice that there are no software packages in our environment.



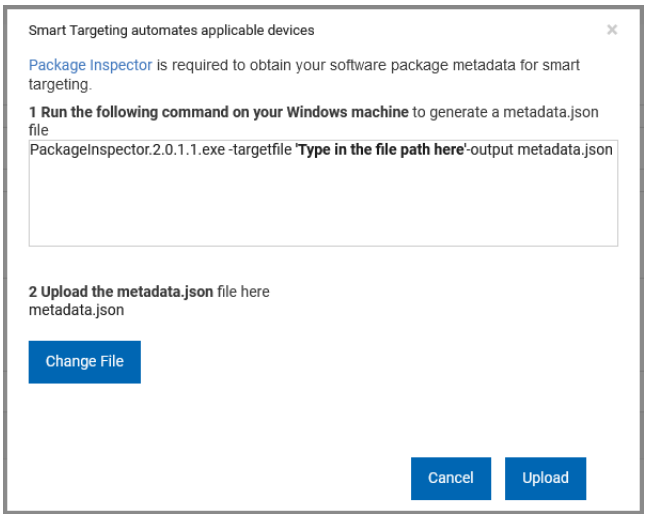

2. Click **Add Software** in the top right corner to create a software package

3. In the resulting box (**Where is the Software file?**), click the **Choose File** button and navigate to the location where you saved **GoogleChromeStandaloneEnterprise64.msi**, and click **Open**
4. Click **Upload**



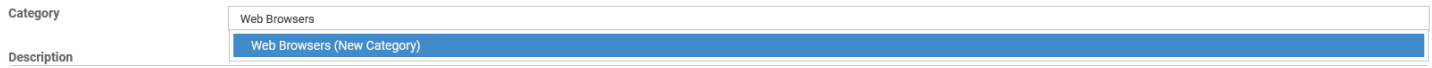
NOTE: If your BigFix Server is running on the Windows platform you will not see the Smart Targeting option. This is because BigFix handles this process natively within Windows. However, our BigFix Server is running on Linux, which is why we see this option. We will go through the Smart Targeting exercise so that you can see the process, and so that our software application information is accurate.

5. **Smart Targeting**. BigFix can automate gathering of application properties and targeting software to applicable devices.
    a. Click the **Smart Targeting** link.
    b. Package Inspector is required to obtain your software package metadata for smart targeting. Click the **Package Inspector** link to download the Package Inspector and save it in the same location as the setup file, to avoid having to specify a file path in the next step.
    c. Open a command prompt and run the following command on your Windows workstation to get the smart targeting information: *PackageInspector.2.0.1.1.exe -targetfile chromesetup.exe -output metadata.json*
    d. Click the **Upload File** box and select the **metadata.json** file you just created.
    e. Click the **Upload** button in the bottom right corner.



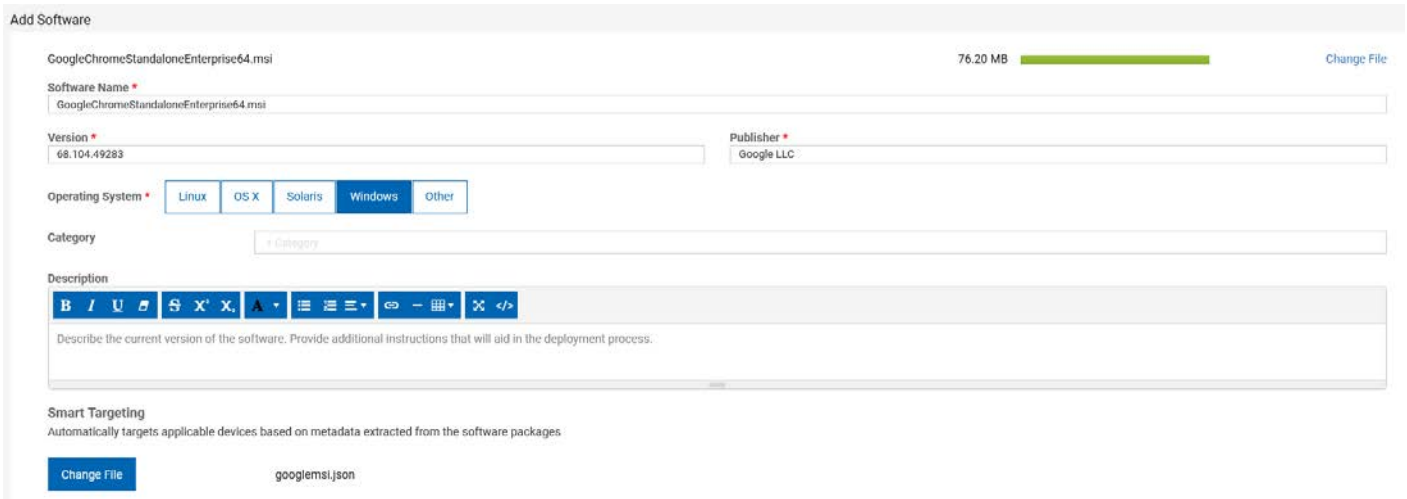

6. Notice that the **Version** and the **Publisher** have been automatically populated, based on the contents of the json file

7. The **Software Name** field is also automatically populated, based on the name of the executable. We will change the name to **Chrome Install for Windows**.
8. Notice that **Windows** is already selected for the operating system
9. Enter **Web Browsers** in the **Category** box. Notice that this is listed as a **New Category**. Make sure you click on the blue box underneath what you typed to add the category to the software package.




10. **Description**. Enter a meaningful description for your software package.

See the screen capture below to confirm your settings Note that our json file has a different name, because we named it to correspond with the file it represents:

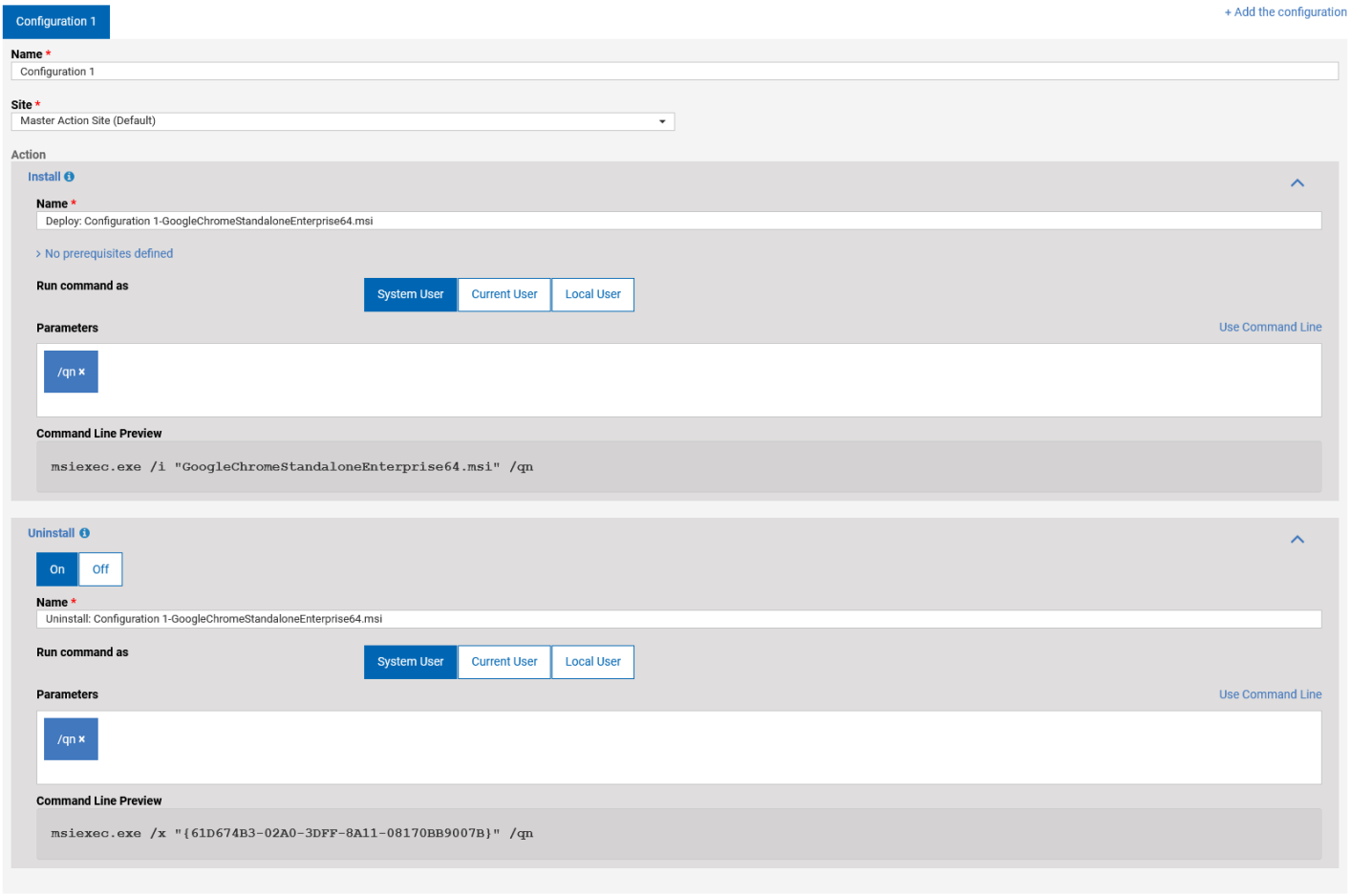


11. Accept the default **Configuration 1** as the **Name**
12. Accept **Master Action Site** as the default **Site**
13. **Expand the** Install **action**
    a. Notice that the **Action** information is already populated because we chose the MSI for our install. The **Parameters** are already populated, as is the command line.
14. Notice the software package automatically includes an **Install**, with an optional **Uninstall**.
    a. Expand the **Uninstall** option and toggle the **On/Off** to **On** (On is in the blue square when it is enabled)

15. Click **Save** to save the software package

See the screen capture below to confirm your settings:




We have just created a simple software distribution package for installing Google Chrome on Windows. There are more settings we will add to this software package, but for now, this package is ready to deploy to our Windows endpoints

# BigFix Software Distribution: Deploy a Software Package, Method 1

In this exercise we are going to deploy a software package based on the Software Packages available in our environment

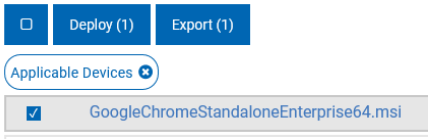
The BigFix WebUI returns us to the application page after saving the new application:


1. Click on **Apps** -> **Software**.

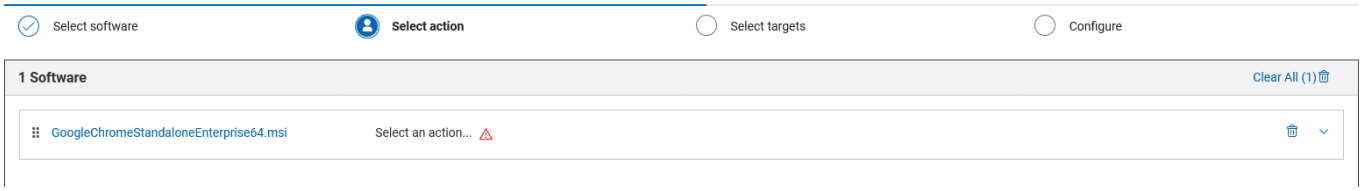
NOTE: We could deploy the software from the previous page, and in production we might do this, but for our exercise, and in order to see a particular feature, we will return to the Software Package list

NOTE: When we created the software package, you created new content in BigFix. The endpoints in the environment automatically evaluate new content added to or created in BigFix to determine if it is applicable to them. For this reason, the Software Package list may be blank. You can either wait for the endpoints to finish evaluating the content, you can refresh the web page, or you can click on the **Applicable Devices** filter to remove the filter. The BigFix WebUI automatically applies this filter so you can see at a glance, what software is applicable to the devices in your environment

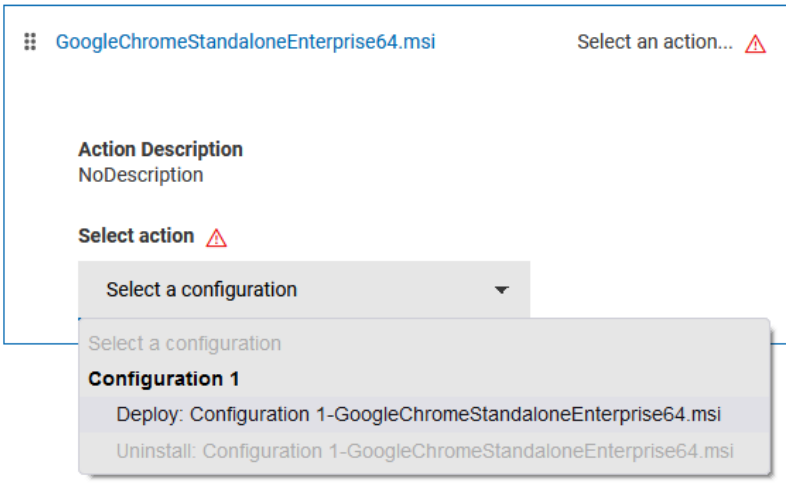
2. Check the box next to the software package you created, and click the blue **Deploy** button



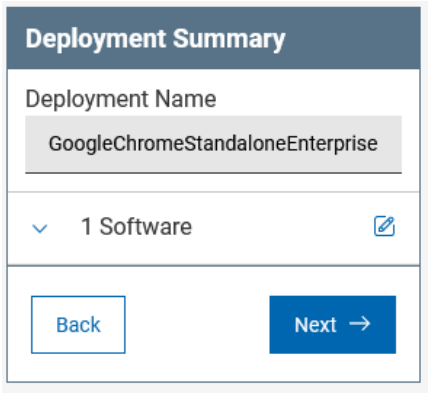

3. The **Deploy Software** wizard appears, with the software package selected.
4. **Select action**. Click the **Select an action…** link



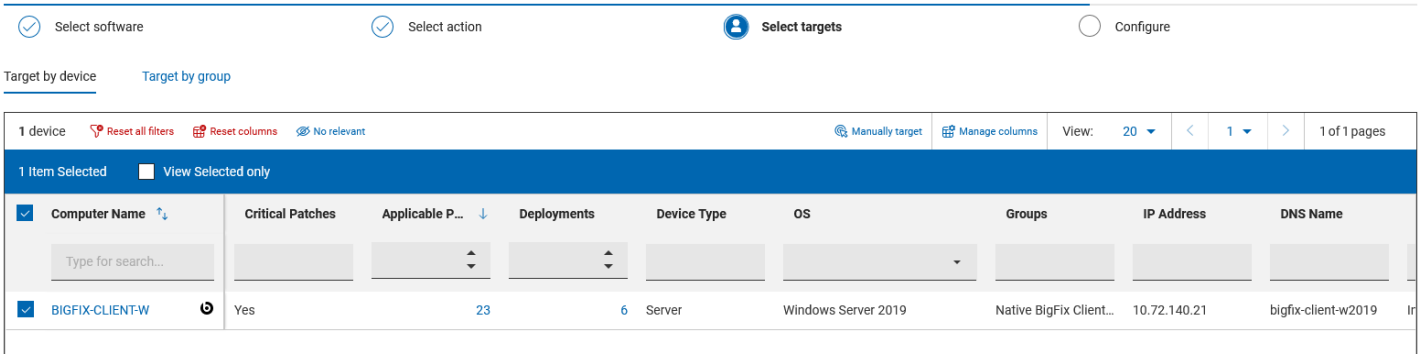
1. Click on the grey **Select a configuration** box
2. Click on the Configuration choice. In our exercise we will choose the **Deploy: Configuration 1…** option.




5. Click the blue **Next** button on the right



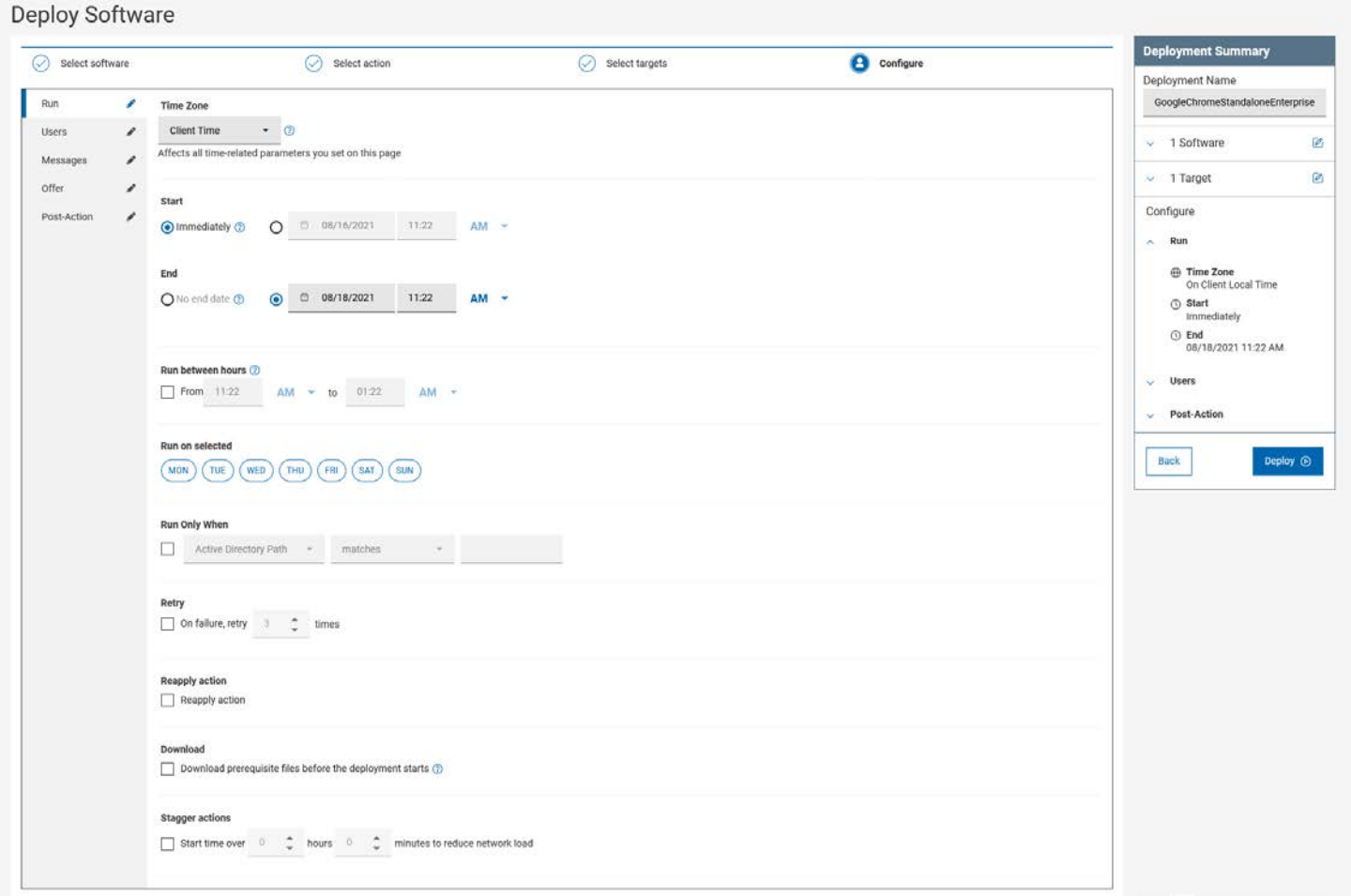

6. **Select Targets**. Select the box next to the endpoint(s) you wish to deploy software to
7. Click the blue **Next** button on the right



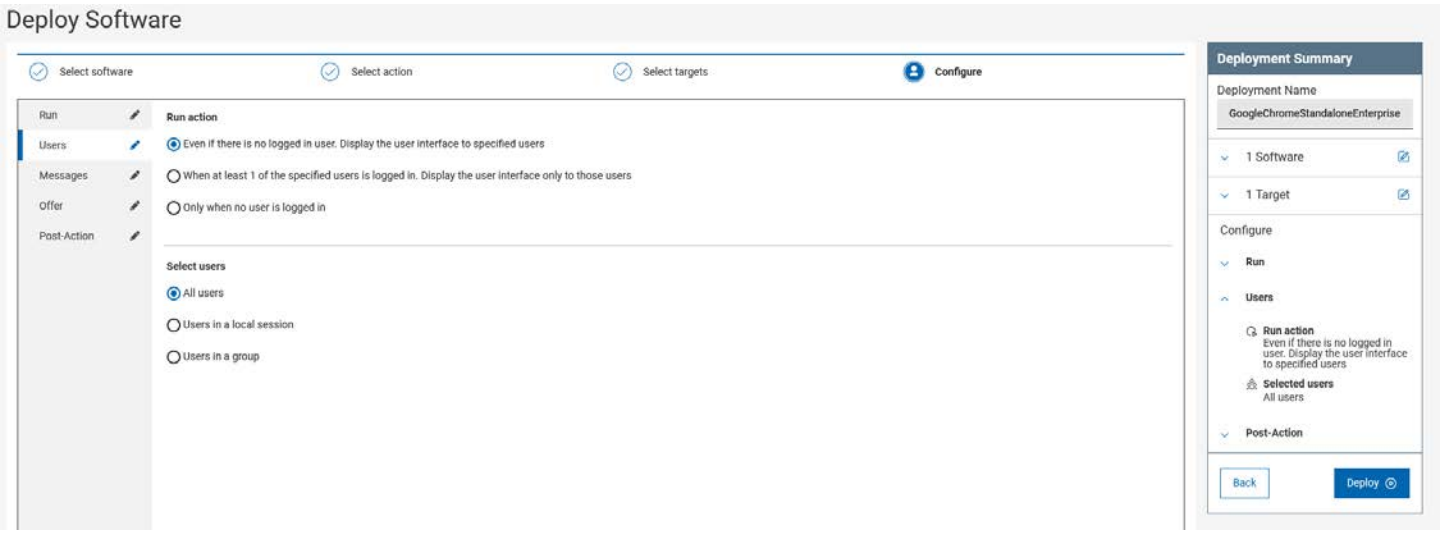

8. **Configure**. In this step we will specify how and when this software package is to be deployed, if and how the end user will interact, and actions to take after the software package has been deployed. There are five screens, and we will go through each one, setting behavior and constraints that correspond to our scenario.

   Instructions for each page in the **Configure** step follow, along with settings for each.

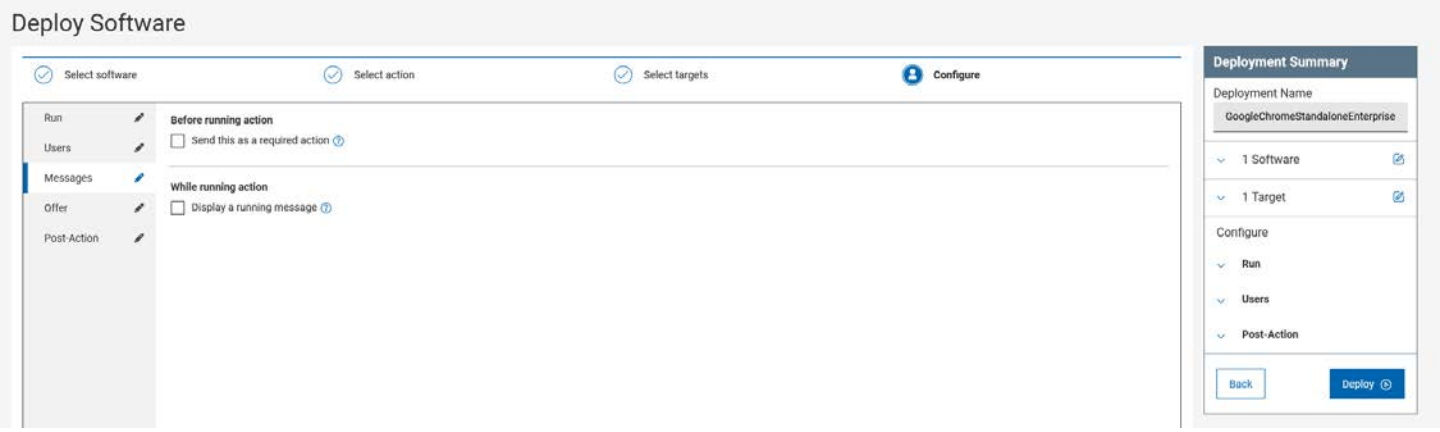
9. **Configure Options: Run**. This page specifies schedule information for deploying our software package. We will accept the defaults on this page.



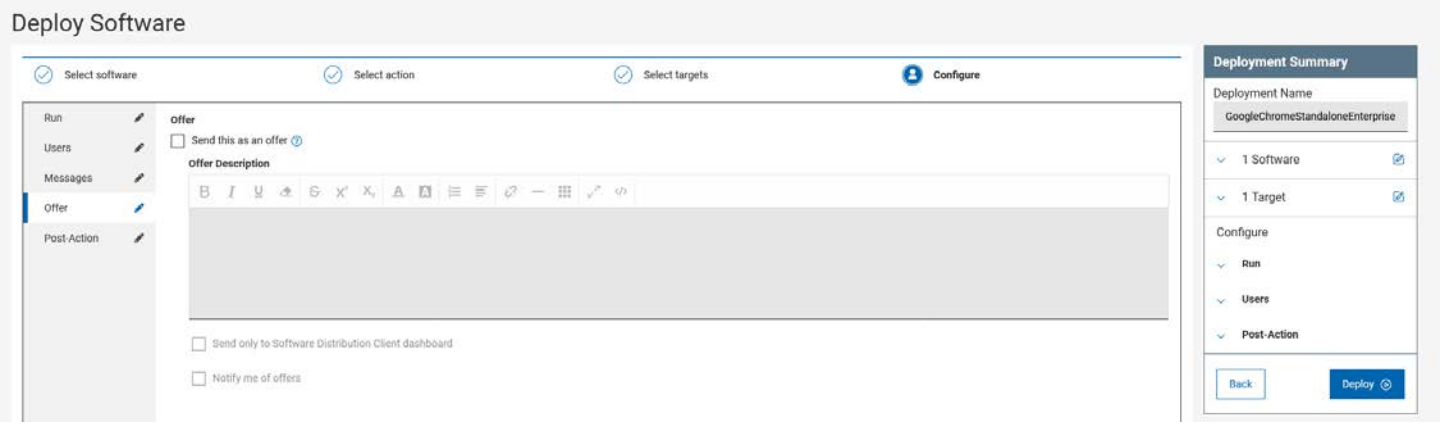

10. **Configure Options: Users**. This page specifies how the application deployment behaves according to logged-in users. We will not make any settings changes on this page.



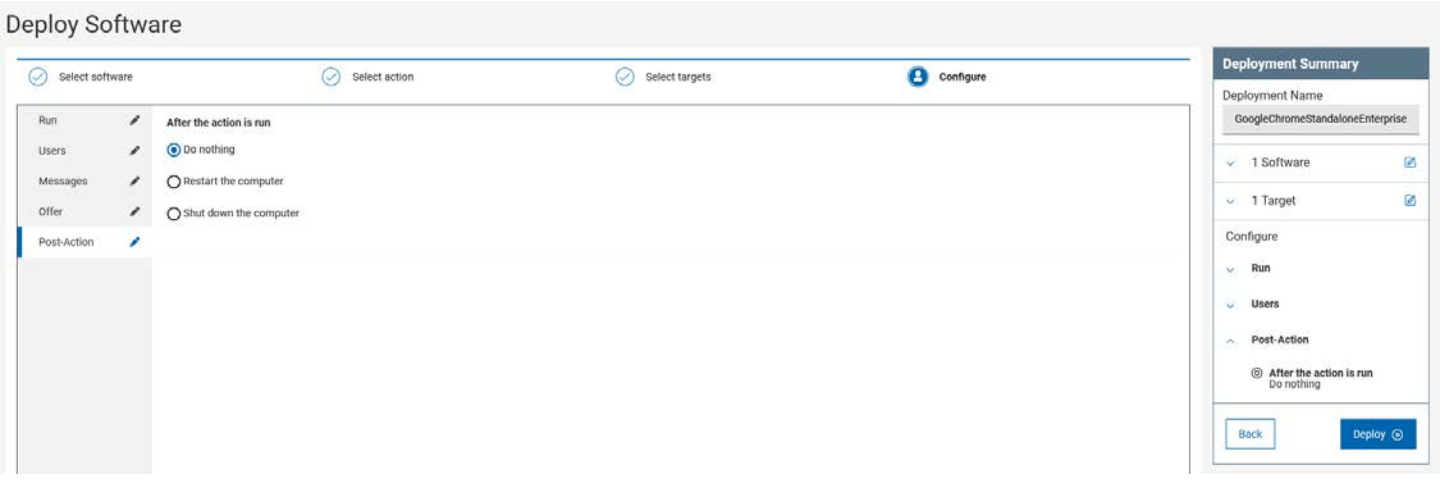
11. **Configure Options: Messages**. This page allows us to display information about a pending and/or running action for end-users. We will not be using messages, as our install is quiet and requires no end-user interaction.




12. **Configure Options: Offers.** This page allows logged-on users to run the patch deployments outside of the "Run" window. We will not be using Offers.




13. **Configure Options: Post Action**. This page allows us to restart or shut down endpoints after distributing software.
    a. There is no need to reboot our endpoint after installing the software, so we will accept the **Do nothing** default selection.




14. Verify your selections as necessary. When you are satisfied with the selections, click the blue **Deploy** button in the right sidebar.

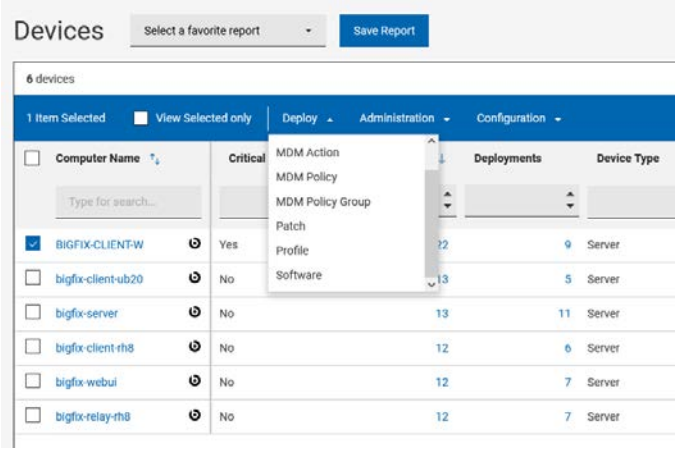
15. You may now watch the application deployment progress in the Deployment window

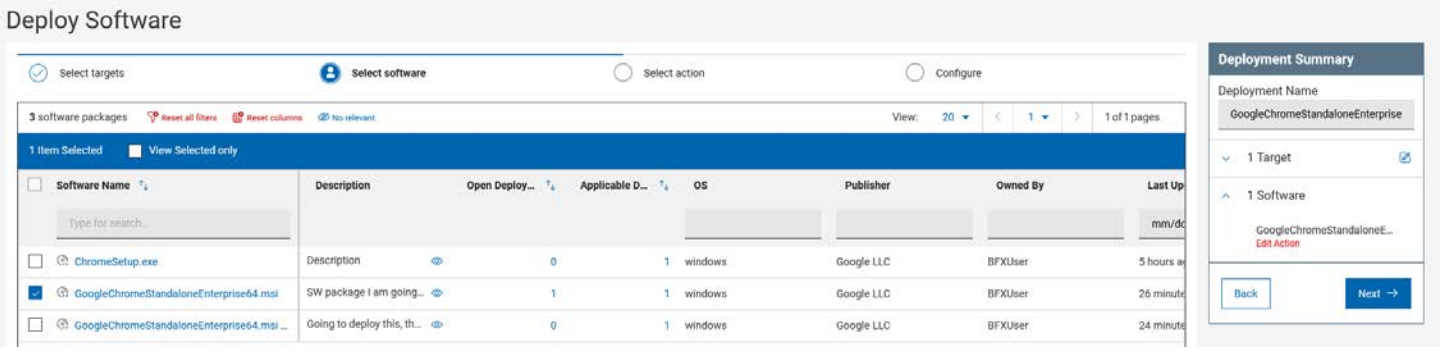
# BigFix Software Distribution: Deploy a Software Package, Method 2

In this exercise we are going to deploy a software package based on Software Packages applicable to a particular device

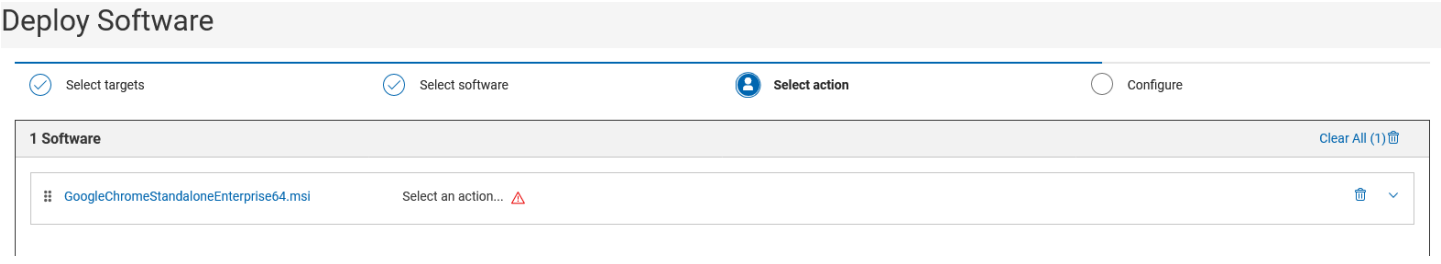
1. Click on **Devices**.
2. Check the box next to the device you deployed the software to in the previous exercise
3. Click **Deploy**
4. Scroll down and select **Software** at the bottom of the drop-down list



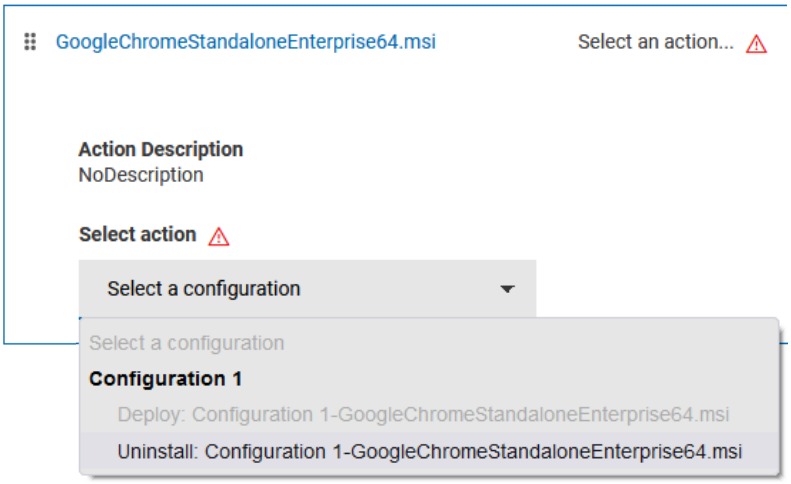

5. The **Deploy Software** wizard appears.
6. Check the box next to the software package we just deployed
7. Click the blue **Next** button



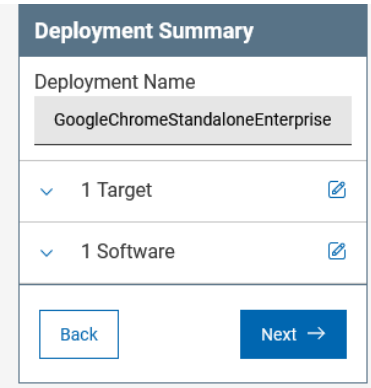

8. Because we started on the Device page, the target device is already selected.
9. Click the **Select an action…** link



10. Click on the grey **Select a configuration** box
11. Click on the Configuration choice. In our exercise we will choose the **Uninstall: Configuration 1…** option.



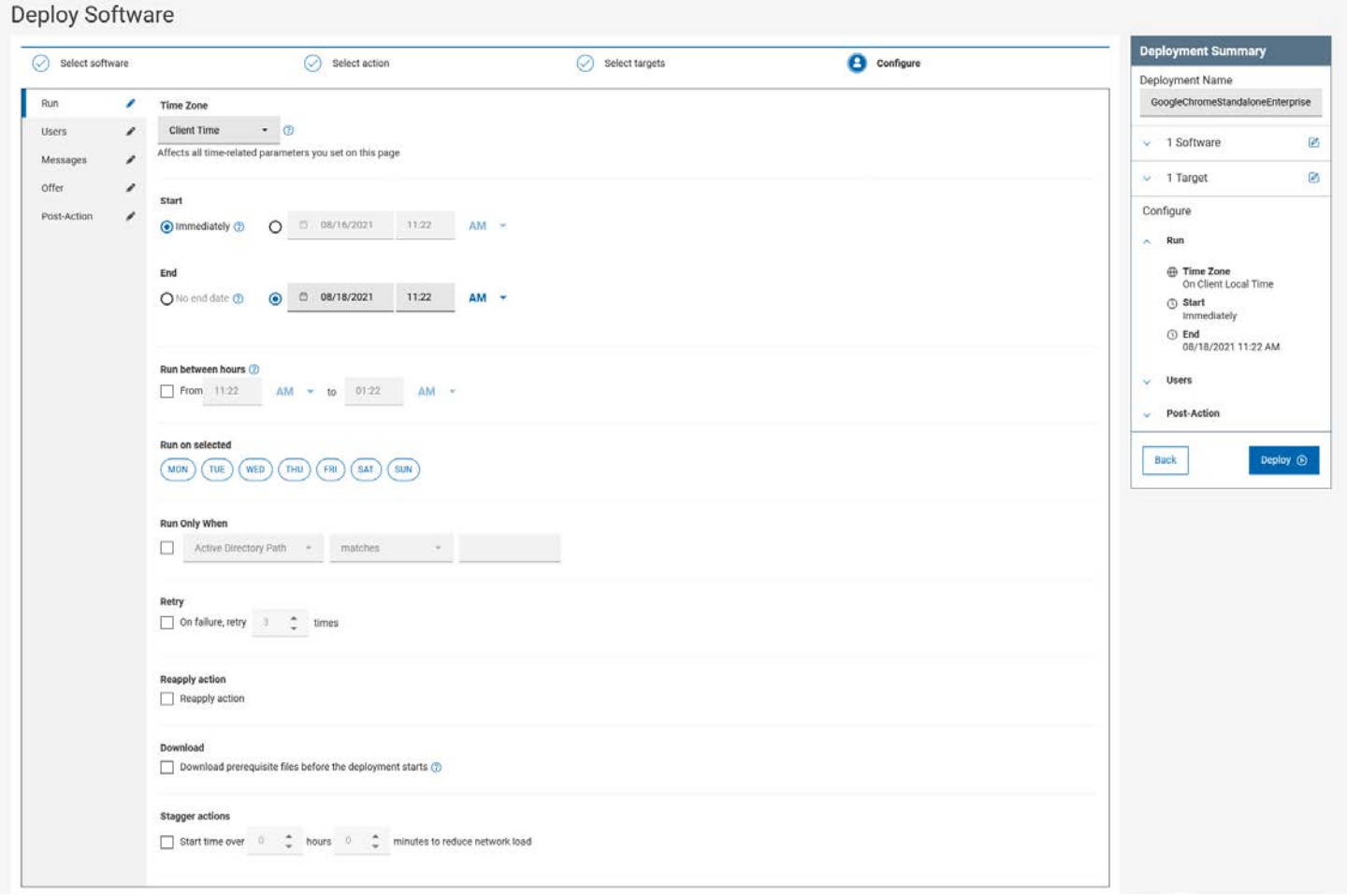

12. Click the blue **Next** button on the right



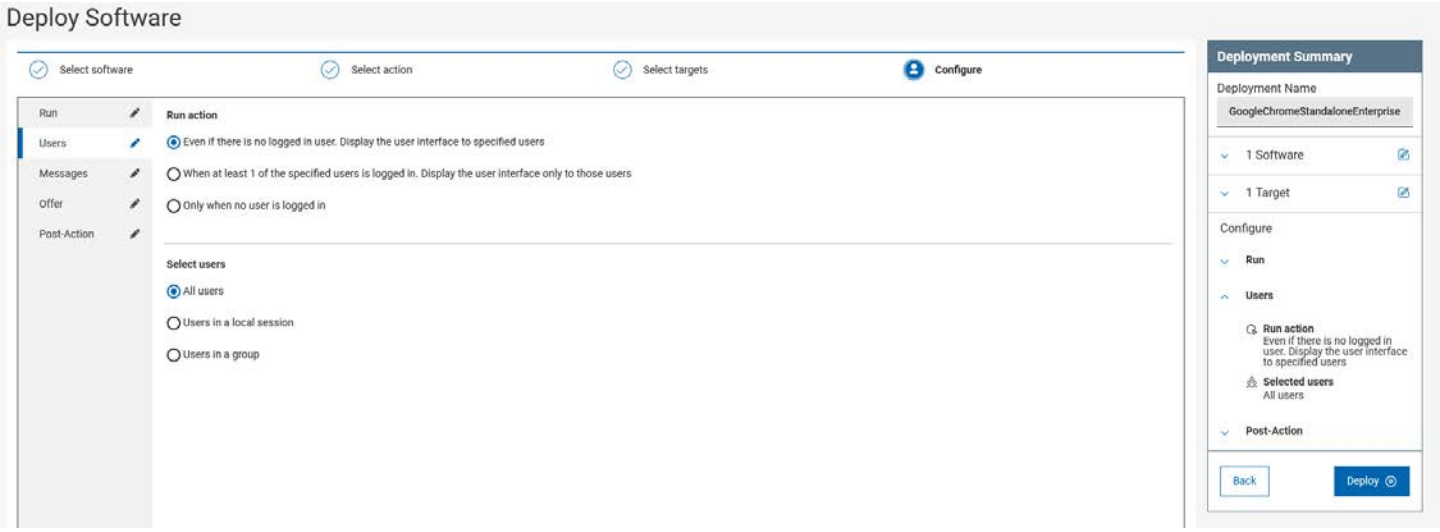

13. **Configure**. In this step we will specify how and when this software package is to be deployed, if and how the end user will interact, and actions to take after the software package has been deployed. There are five screens, and we will go through each one, setting behavior and constraints that correspond to our scenario.

    NOTE: We will not be making any changes to the **Configure** section of the **Deploy Software** wizard. Instructions for each page in the **Configure** step follow for your information, along with settings for each. You may, however, click the blue **Deploy** button if you are already familiar with the **Configure** options.

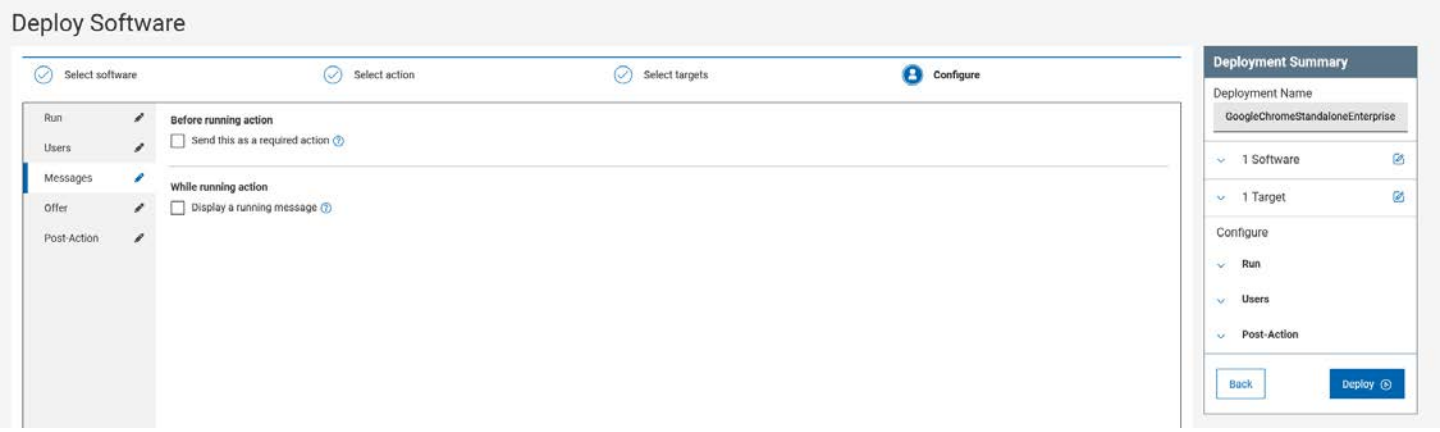
14. **Configure Options: Run**. This page specifies schedule information for deploying our software package. We will accept the defaults on this page.



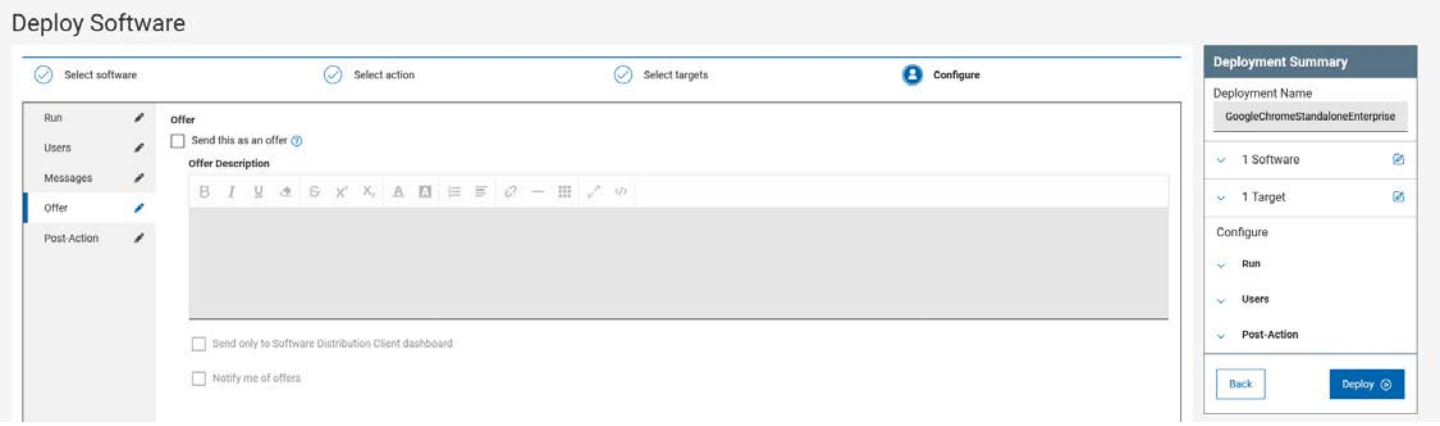

15. **Configure Options: Users**. This page specifies how the application deployment behaves according to logged-in users. We will not make any settings changes on this page.



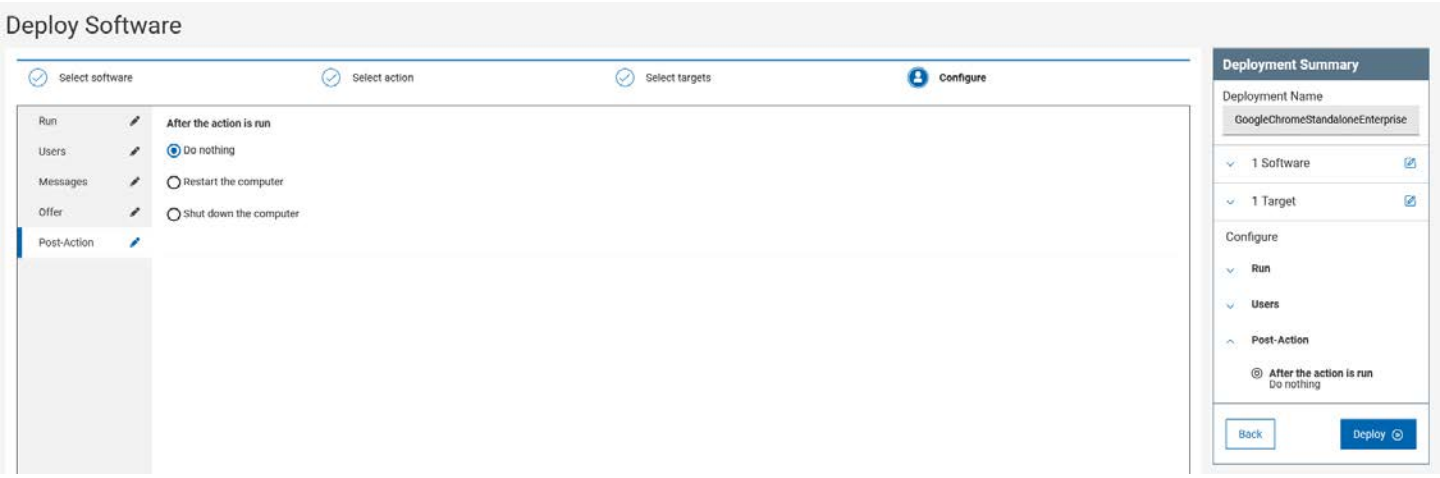
16. **Configure Options: Messages**. This page allows us to display information about a pending and/or running action for end-users. We will not be using messages, as our install is quiet and requires no end-user interaction.



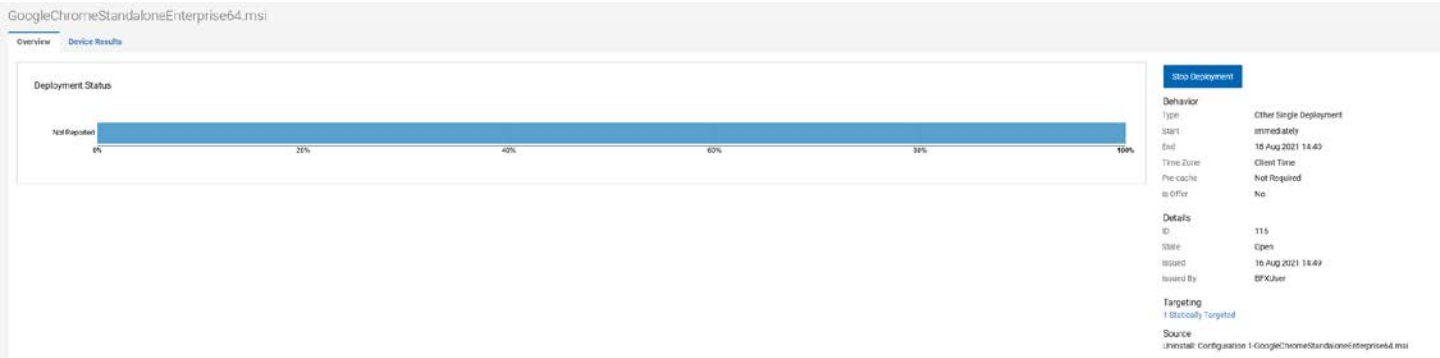

17. **Configure Options: Offers.** This page allows logged-on users to run the patch deployments outside of the "Run" window. We will not be using Offers.



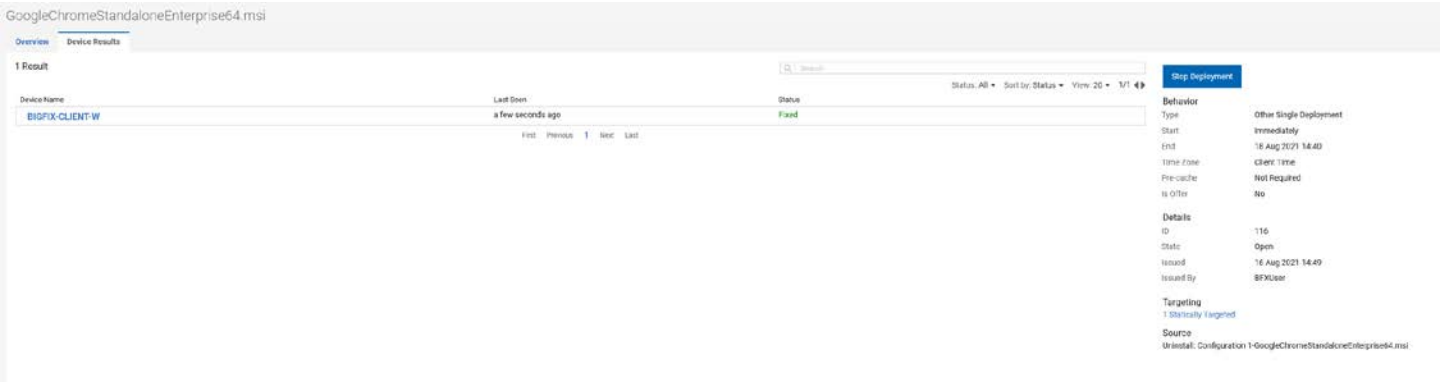

18. **Configure Options: Post Action**. This page allows us to restart or shut down endpoints after distributing software.
    a. There is no need to reboot our endpoint after installing the software, so we will accept the **Do nothing** default selection.



19. Verify your selections as necessary. When you are satisfied with the selections, click the blue **Deploy** button in the right sidebar.
20. You may now watch the application deployment progress in the Deployment window




21. The **Device Results** tab will display the progress for the device. When the status reads **Fixed** the deployment is complete.



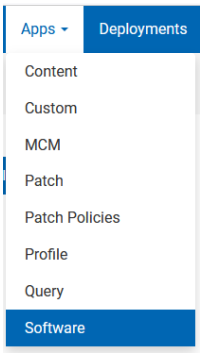
# BigFix Software Distribution: Edit a Software Package

We may need to edit a software package after creating it. In this exercise we will explore this capability.

**WARNING:** Do not edit a software package if it has an associated open deployment, or unexpected consequences may occur, including the inability to use the software package in the future. To edit a software package, stop all deployments the package is currently involved in.

1. You may be logged into the WebUI already. If not, log into the WebUI using the URL and credentials from the SoFy BigFix Solution Console

2. Click on **Apps** -> **Software**.

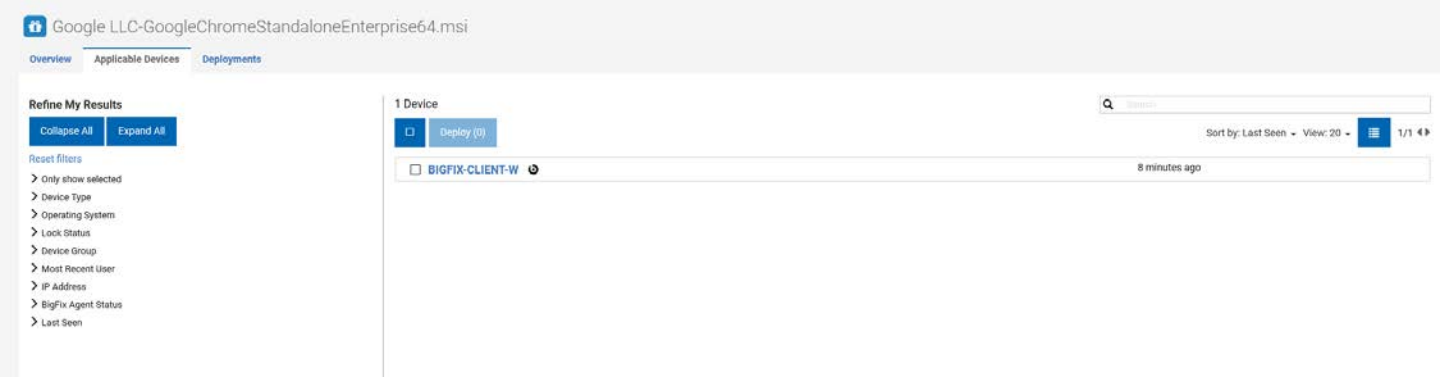



3. Click on the name of the package to edit from the list of packages. We will choose the one we just created in the previous exercise: **GoogleChromeStandaloneEnterprise64.msi**

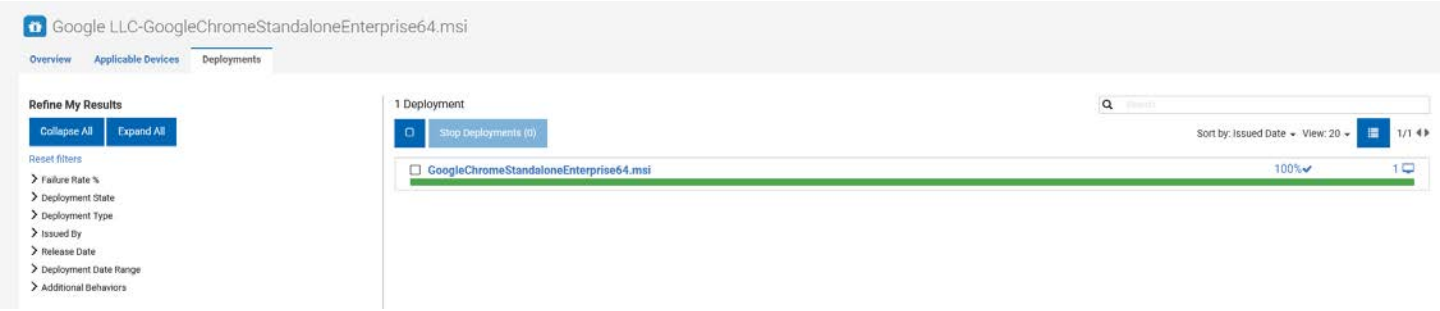

4. We have several options available from this page.
5. On the left side of the page, under the **Overview** tab:
    a. What devices report that this software is applicable to them
    b. What deployments are currently underway for this software package
    **DO NOT EDIT THIS SOFTWARE PACKAGE IF THERE ARE ANY OPEN DEPLOYMENTS. STOP THE DEPLOYMENT(S) FIRST BEFORE EDITING THE PACKAGE**
    c. Results of previous deployments
    d. Number of deployments in the past 24 hours

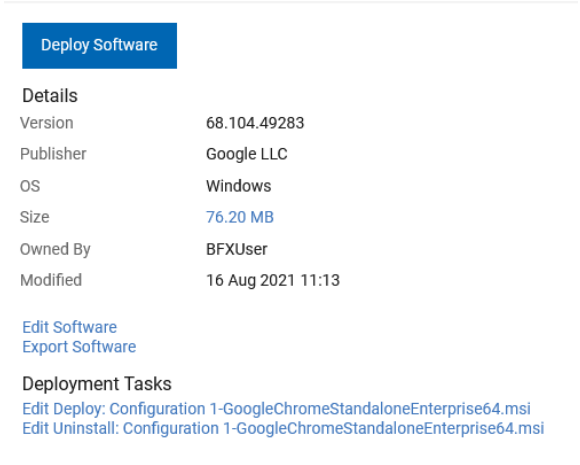
6. On the left side of the page, under the **Applicable Devices** tab:
    a. Devices that have reported that this application is applicable to them
    b. Other filters, under **Refine My Results**, that we can apply




7. On the left side of the page, under the **Deployments** tab:
    a. Deployments of this application package
    b. Other filters, under **Refine My Results**, that we can apply



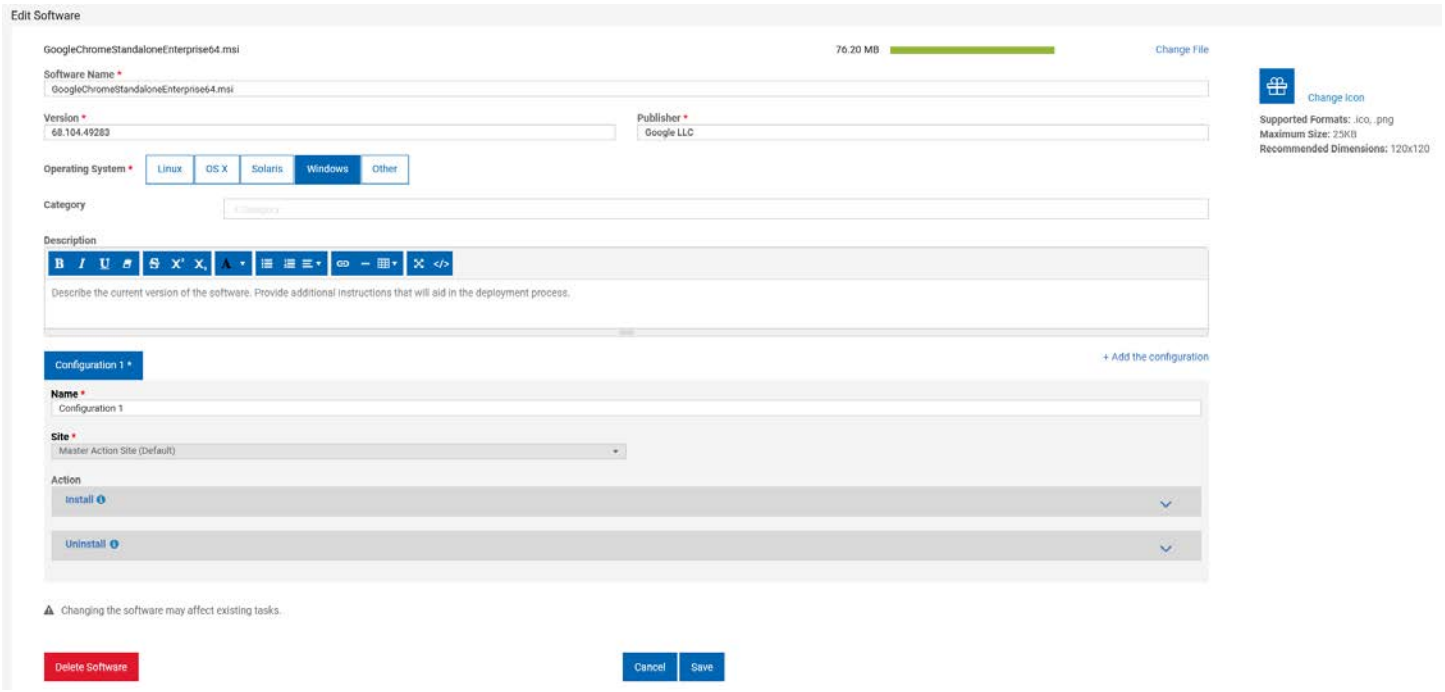

Notice that regardless of the tab we explore, the right side of the screen remains the same:




8. From the panel on the right of the page, we have several options:
    a. We can deploy this software package by clicking on the blue **Deploy Software** button
    b. We can edit the software package by clicking the **Edit Software** link
    c. Export the software package by clicking on the **Export Software** link
    d. Edit the Deployment Tasks by clicking on one of the links under the **Deployment Tasks** link

## Edit Software Deployment Tasks

1. Click the **Edit Software** link. Notice that this is the same window we saw when creating the software package, with a few exceptions:
    a. The header (*Edit Software)*
    b. The warning message that *Changing the software may affect existing tasks*
    c. The red **Delete Software** button, which allows us to delete this software package



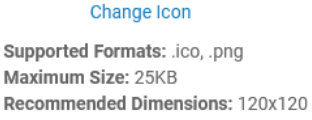

In our exercise, we are going to remove the **Uninstall** option from the package.

NOTE: We could also have clicked on the specific Deployment Task to accomplish this step.

2. Click the down carat to the right of **Uninstall** and toggle the **On/Off** selector to **Off**

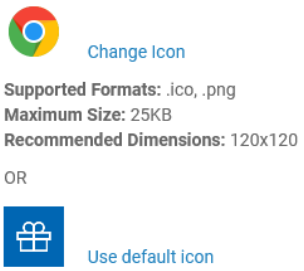
## Add an Icon to a Software Package

3. Before Changing the default icon, we must have an icon file. You can create an icon, obtain an icon from the software vendor, or download an icon file.
    a. Navigate to https://icons8.com/icons/set/chrome
    b. Choose any of the Chrome icons available, as long as it is an **.ico** or **.png** file, less than **120x120**. For this example, we selected the color logo on the top row.
    c. Click **Download**
    d. Select the file type (**PNG**)
    e. Select the size (**96px**)
    f. Click **Download**
4. Click the **Change Icon** link
    a. Browse to the location of the file you just saved
    b. Select the file and click **Open**



5. Notice that the icon appears where the default icon used to be




6. We have completed our editing tasks. Click the blue **Save** button to save the application package

# BigFix Application Programming Interface: Introduction

## Executive Summary

The **Representational S**tate **T**ransfer **A**pplication **P**rogramming **I**nterface (REST API) is the primary programming interface to the BigFix Server. It allows you to perform the majority of the tasks available in the BigFix console by using a set of standardized and operating system independent methods. This API is also key if you want to automate activities, implement your custom BigFix user interface, or integrate with other applications. The REST-API can run the majority of tasks present in the console via a standardized and operating system independent method!

BigFix provides you with:

- The REST API server part, available on the BigFix server, that manipulates the objects stored in the BigFix database.
- A lightweight command-line tool named IEM Command-Line Interface (CLI), that you can use as a REST client to initiate requests towards the REST API server.

You can choose to use your preferred REST Client, in place of the IEM CLI, to issue methods and interact with the BigFix REST server through HTML calls.

## Scenario

Using the REST API to issue an action to a computer without using the BigFix Console of the Web User Interface. The process we will follow utilizes the API for all of our functions:

- Get a list of all computers in the environment
- Get a detailed list of computers that have a specific name
- Get information about Fixlets in the BigFix Environment
- Deploy a fixlet to a computer in the BigFix Environment.
- Gather status of the Action after deployment

This sample scenario and instructions will get you started with using the BigFix REST API. In the scenario that you are going to run you'll see how to query resources (like a list of computers).

The scenario requires that you have:

- Access to the BigFix Server's REST API.
- Administration rights for at least one computer.
- Chrome browser with REST-API client add-on (https://chrome.google.com/webstore/detail/advanced-rest-client/hgmloofddffdnphfgcellkdfbfbjeloo?hl=en-US)

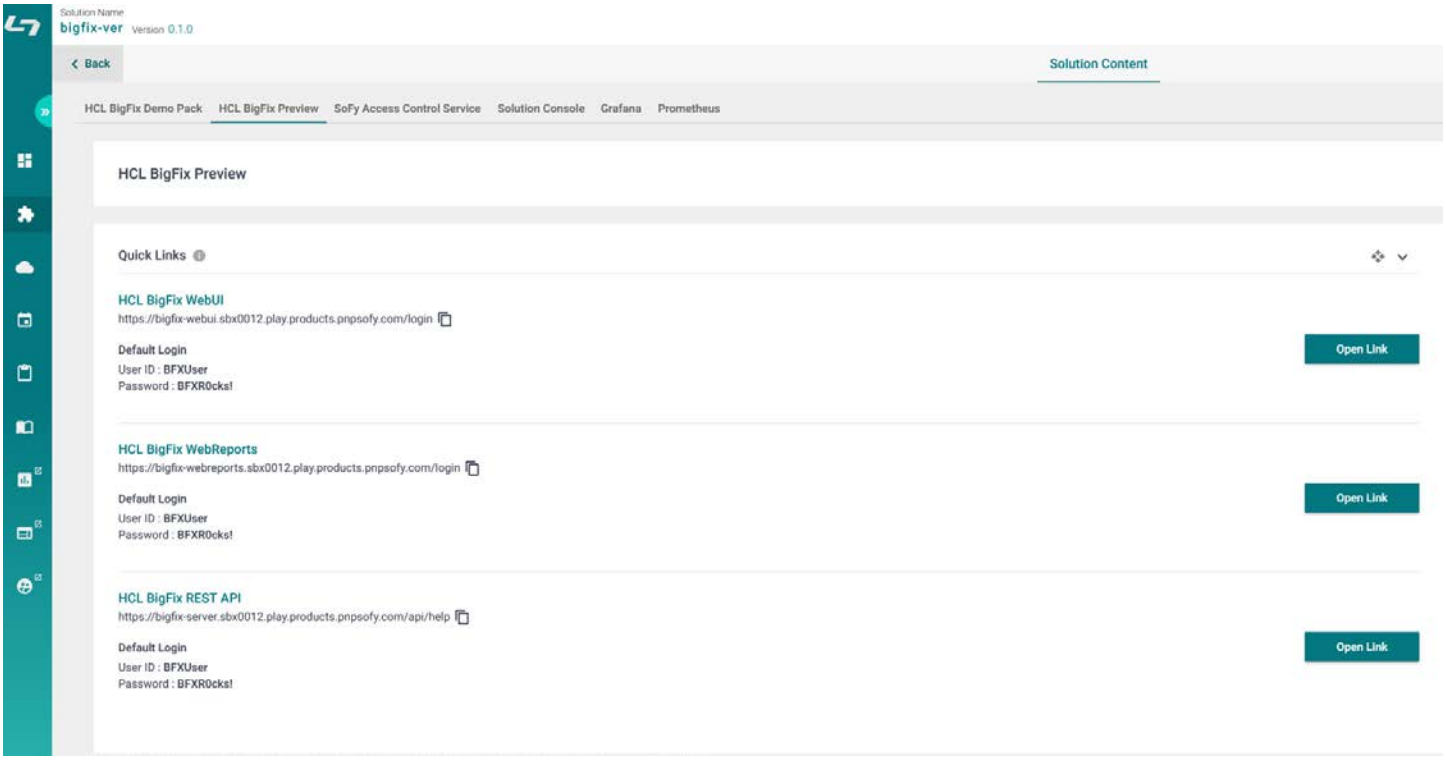
  - OR -
- Firefox browser with the client add-on (https://addons.mozilla.org/en-US/firefox/addon/restclient/).

Now – let's give it a try:

# Accessing BigFix REST API

1. The BigFix REST API is a web interface that we need to log into. You will find the login link and the credentials on the Solution Content page within SoFy.

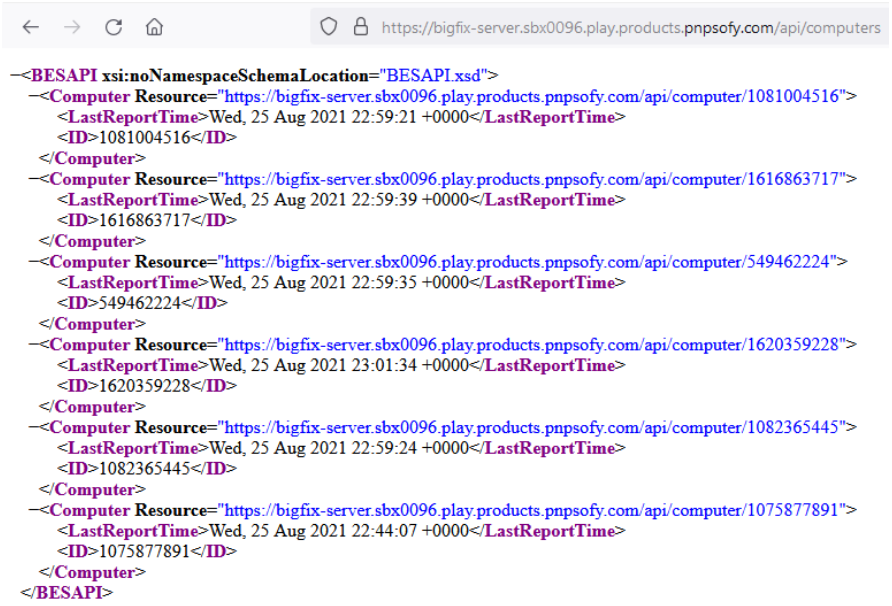



## Access the REST API from a web browser

2. Click the "Open Link" button to the right of **HCL BigFix REST API** and log in using the credentials provided in the Solution Content.
3. Your browser link takes you to <server-fqdn>/api/help
4. We are going to start with a simple command, to get a list of the computers in our environment. Replace **help** with **computers** in the address bar, like this:

   *https://<server-fqdn>/api/**computers***

   This command returns a list of the computer IDs in the environment, and the last time they reported.



5. Let's use some Relevance to find computers with a specific string in the name. We are going to look for computers that have "bigfix" in the name. Copy and paste into the address bar, replacing **computers** with this:

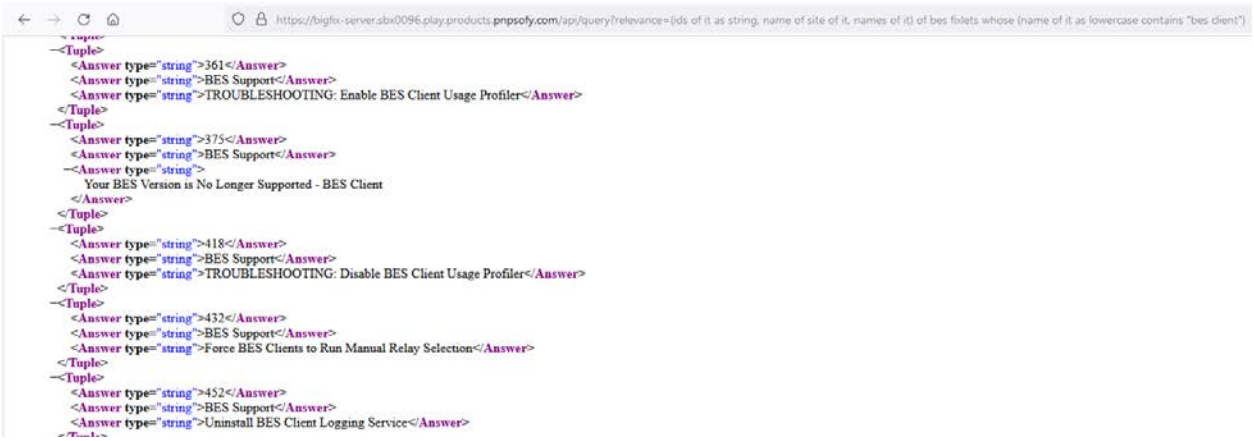
   *query?relevance=(names%20of%20it,%20ids%20of%20it)%20of%20bes%20computers%20whose%20((name%20of%20it%20as%20lowercase%20contains%20%22bigfix%22%20)%20and%20(%20agent%20type%20of%20it%20as%20lowercase%20contains%20%22native%22%20))*

   The information returned from this API query returns the names of the endpoints, as well as the computer ID.


6. Write down one of these computer IDs, that corresponds to one of our ***client*** endpoints. You can use any computer for this exercise except the BigFix Server itself.
7. Now we will use some Relevance to find some information about a fixlet and retrieve the ID, Site, and Title. In our example, we are going to search for some configuration settings Fixlets, but you could also search for a patch (Windows KB or Red Hat Security Advisory) or other fixlet. Copy and paste into the address bar, replacing **everything following "api/"** with this:

   query?relevance=(ids%20of%20it%20as%20string,%20name%20of%20site%20of%20it,%20names%20of%20it)%20of%20bes%20fixlets%20whose%20(name%20of%20it%20as%20lowercase%20contains%20%22bes client%22)

   We should see the list of Fixlets whose title contains "BES Clients"



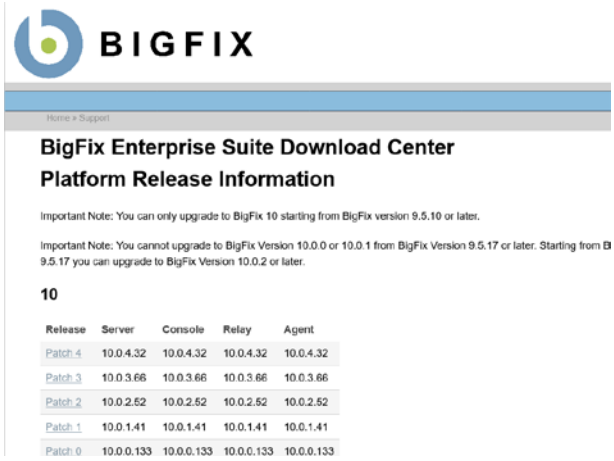
## Using the RESTAPI Command Line Interface (CLI)

Every BigFix Server has a program called **IEM.exe**. This utility is found in the IEM CLI directory of the BES Server directory (by default this is C:\Program Files (x86)\BigFix Enterprise\BES Server\IEM CLI\). This utility allows us to interact with the BigFix Server and run commands using the REST API.

1. In the browser window, scroll down the list of Fixlets we returned in #7 above until you see Fixlet with the ID of **432** and the name of **Force BES Clients to Run Manual Relay Selection** (The screen capture above is scrolled to see this fixlet). We will use this Fixlet and create an action to target one of our endpoints using the API.

   NOTE: This is not something we can do in the browser as this requires us to POST to the API on the BigFix server. We will use the utility mentioned above, called the **RESTAPI Command-line interface (CLI)** to perform this task. By default, this utility resides on the BigFix Server, but we will download it from the BigFix Utilities for this exercise.

2. Navigate to https://support.bigfix.com/bes/release



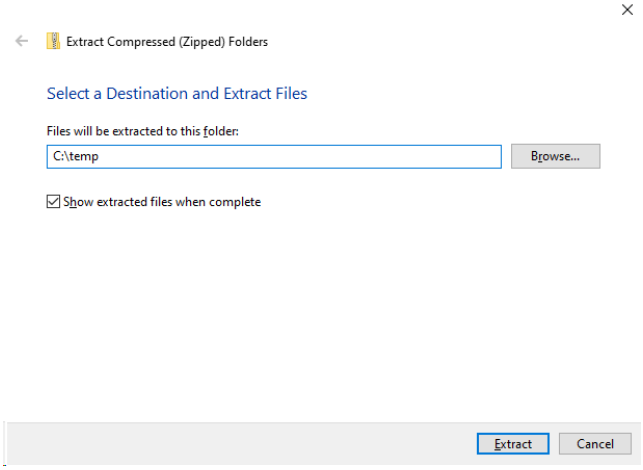

3. Select the most recent BigFix 10 version release (it will be the topmost "Patch #" link under the "10" header

4. Scroll down to the **Utilities** section
5. Click the download link next to **RESTAPI Command-line interface (CLI)**, which is a link to **CLI10.#.#.##.zip**
6. Save the file to your computer

**Utilities**

| Name | Operating System | Download |
|---|---|---|
| QnA/Fixlet Debugger | Windows | Download |
| RESTAPI Command-line interface (CLI) | Windows | Download |
| Airgap Tool | Windows | Download |
| BESRemove | Windows | Download |
| BES Client Compliance SDK | Windows | Download |

7. Extract the zip file to a folder on your computer. For our example, we will use C:\temp



## Creating an XML file to run the BigFix Action

1. Actions run using the RESTAPI Command Line Interface, or CLI tool require an XML file. We will create an XML file that the API will use to create the action on the BigFix Server.
2. Copy and paste the following into a text editor, replacing the text highlighted in yellow with the computer ID we wrote down previously.

```
<BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="BES.xsd">
<SourcedFixletAction>
   <SourceFixlet>
     <Sitename>BES Support</Sitename>
     <FixletID>432</FixletID>
     <Action>Action1</Action>
   </SourceFixlet>
   <Target>
     <ComputerID>1234567890</ComputerID>
   </Target>
</SourcedFixletAction>
</BES>
```

3. Save the file as 'action.xml' to the same folder that you extracted/copied IEM.exe

   NOTE: If you did not write down the computer ID, go back and re-do steps 5-6. We will use a computer ID that corresponds to one of our ***client*** endpoints. You can use any computer for this exercise except the BigFix Server itself.

## Using the RESTAPI Command Line Interface

1. Open a CMD window and change directory to the directory of the IEM tool (the zip file you downloaded and extracted previously). The first thing we need to do is to login with the following command:

   **iem.exe login**
   - Enter the server name. This is the fully-qualified server name in the URL we used previously, **and ":443"**. For example, **bigfix-server.sbx0012.play.products.pnpsofy.com:443** (your server name will be different). You can also get the server name from the SoFy BigFix Solution Console.
   - Enter the user name. This information is in the SoFy BigFix Solution Console
   - Enter the password. This information is in the SoFy BigFix Solution Console

```
c:\temp\CLI10.0.4.32>iem.exe login
Server   : bigfix-server.sbx0096.play.products.pnpsofy.com:443
User     : BFXUser
Password:
Successfully logged in to server!
```

   If you entered the information correctly, you will see **Successfully logged in to server!**

2. Once we have logged in we can submit an action. Actions require an xml file, so we will use the one we created just now – action.xml. We can then use the IEM command to POST the action to the BigFix server via the Restful API:

**iem.exe POST <path to xml> actions**

```
c:\temp\CLI10.0.4.32>iem.exe POST action.xml actions
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BESAPI.xsd">
        <Action Resource="https://bigfix-server.sbx0096.play.products.pnpsofy.com/api/action/122" LastModified="Wed, 25
Aug 2021 22:54:38 +0000">
                <Name>Force BES Clients to Run Manual Relay Selection</Name>
                <ID>122</ID>
        </Action>
</BESAPI>
```

We are provided an XML response with the ID of the action. **Take note of the action ID (in the screen capture above, on the "<Action Resource=…" line. The action ID is 122, but yours will be different**

We can now check on the status of the action as follows:

3. Get a list of actions. Now we will return to the browser and get a list of actions. Enter **actions** after **api/** in the address bar, like this:

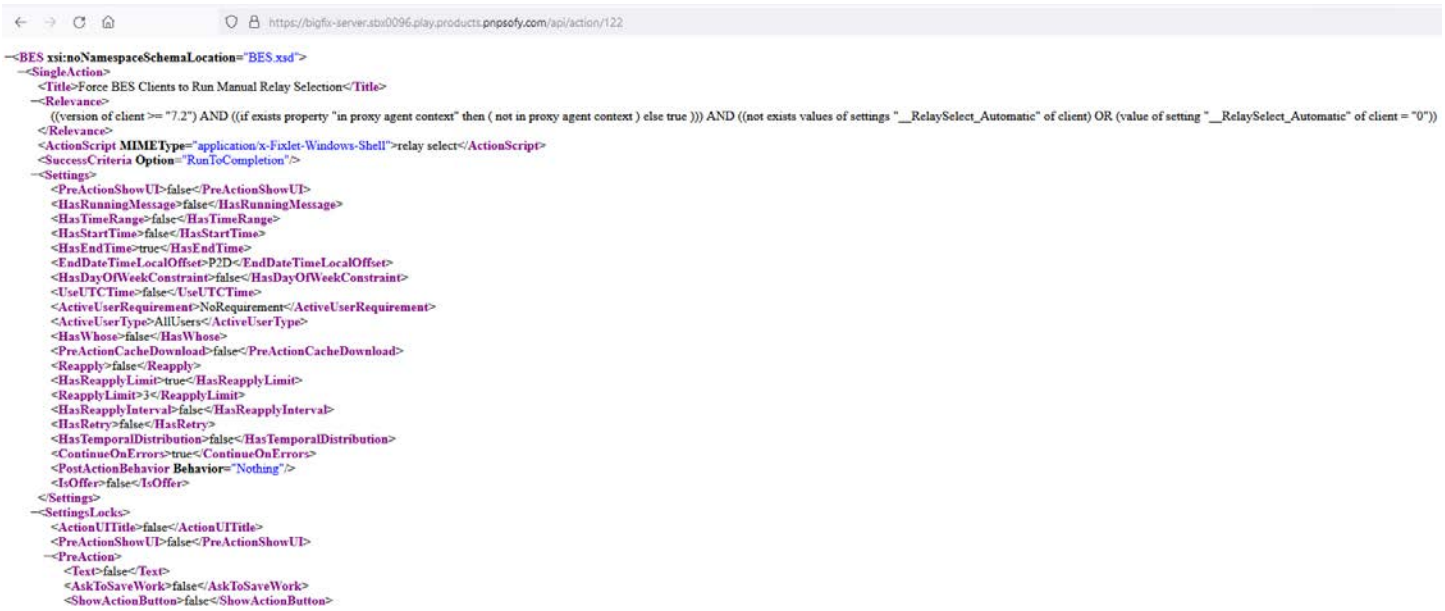
   https://<server-fqdn>/api/actions

```
−<Action Resource="https://bigfix-server.sbx0096.play.products.pnpsofy.com/api/action/122" LastModified="Wed, 25 Aug 2021 22:54:38 +0000">
    <Name>Force BES Clients to Run Manual Relay Selection</Name>
    <ID>122</ID>
  </Action>
```

NOTE: if you did not capture the action ID that was displayed at the command prompt using IEM.exe, you can search for it in the list of actions returned. It will most likely be the last one in the list, at the bottom.

4. Now we can pull back the details of the specific action that we just submitted. Type the following, replacing the yellow highlighted text with your action ID:

   https://<server-fqdn>/api/action/122



```
https://bigfix-server.sbx0096.play.products.pnpsofy.com/api/action/122

−<BES xsi:noNamespaceSchemaLocation="BES.xsd">
  −<SingleAction>
    <Title>Force BES Clients to Run Manual Relay Selection</Title>
  −<Relevance>
     ((version of client >= "7.2") AND ((if exists property "in proxy agent context" then ( not in proxy agent context ) else true ))) AND ((not exists values of settings "__RelaySelect_Automatic" of client) OR (value of setting "__RelaySelect_Automatic" of client = "0"))
   </Relevance>
   <ActionScript MIMEType="application/x-Fixlet-Windows-Shell">relay select</ActionScript>
   <SuccessCriteria Option="RunToCompletion"/>
  −<Settings>
     <PreActionShowUI>false</PreActionShowUI>
     <HasRunningMessage>false</HasRunningMessage>
     <HasTimeRange>false</HasTimeRange>
     <HasStartTime>false</HasStartTime>
     <HasEndTime>true</HasEndTime>
     <EndDateTimeLocalOffset>P2D</EndDateTimeLocalOffset>
     <HasDayOfWeekConstraint>false</HasDayOfWeekConstraint>
     <UseUTCTime>false</UseUTCTime>
     <ActiveUserRequirement>NoRequirement</ActiveUserRequirement>
     <ActiveUserType>AllUsers</ActiveUserType>
     <HasWhose>false</HasWhose>
     <PreActionCacheDownload>false</PreActionCacheDownload>
     <Reapply>false</Reapply>
     <HasReapplyLimit>true</HasReapplyLimit>
     <ReapplyLimit>3</ReapplyLimit>
     <HasReapplyInterval>false</HasReapplyInterval>
     <HasRetry>false</HasRetry>
     <HasTemporalDistribution>false</HasTemporalDistribution>
     <ContinueOnErrors>true</ContinueOnErrors>
     <PostActionBehavior Behavior="Nothing"/>
     <IsOffer>false</IsOffer>
   </Settings>
  −<SettingsLocks>
     <ActionUITitle>false</ActionUITitle>
     <PreActionShowUI>false</PreActionShowUI>
    −<PreAction>
       <Text>false</Text>
       <AskToSaveWork>false</AskToSaveWork>
       <ShowActionButton>false</ShowActionButton>
```

5. Finally, to see the actual status of the action we can enter the following, replacing the yellow highlighted text with your action ID:

   *https://<server-fqdn>/api/action/122/status*

```
https://bigfix-server.sbx0096.play.products.pnpsofy.com/api/action/122/status

−<BESAPI xsi:noNamespaceSchemaLocation="BESAPI.xsd">
  −<ActionResults Resource="https://bigfix-server.sbx0096.play.products.pnpsofy.com/api/action/122/status">
     <ActionID>122</ActionID>
     <Status>Open</Status>
     <DateIssued>Wed, 25 Aug 2021 22:54:38 +0000</DateIssued>
    −<Computer ID="1620359228" Name="BIGFIX-CLIENT-W">
       <Status>The action executed successfully.</Status>
       <State IsError="0">3</State>
       <ApplyCount>1</ApplyCount>
       <RetryCount>1</RetryCount>
       <LineNumber>2</LineNumber>
       <StartTime>Wed, 25 Aug 2021 22:55:33 +0000</StartTime>
       <EndTime>Wed, 25 Aug 2021 22:55:33 +0000</EndTime>
     </Computer>
   </ActionResults>
 </BESAPI>
```

This scenario is an introduction to using the BigFix REST API. You can learn more by visiting https://developer.bigfix.com/rest-api/

# Document Version Information

| Date | Version | Author | Notes |
|---|---|---|---|
| 6/16/2021 | 1.0 | Ben Dixon | Initial document |
| 8/5/2021 | 1.1 | Ben Dixon | Updates for BigFix 10.0.4 |
| 8/10/2021 | 1.5 | Ben Dixon | Consolidated workbooks for various exercises |
| 8/16/2021 | 1.6 | Ben Dixon | Finalized SWD exercises, removed API exercise b/c of typos API will be included in next version |
| 8/25/2021 | 1.7 | Ben Dixon, Michael Thompson | Added AIP exercises |